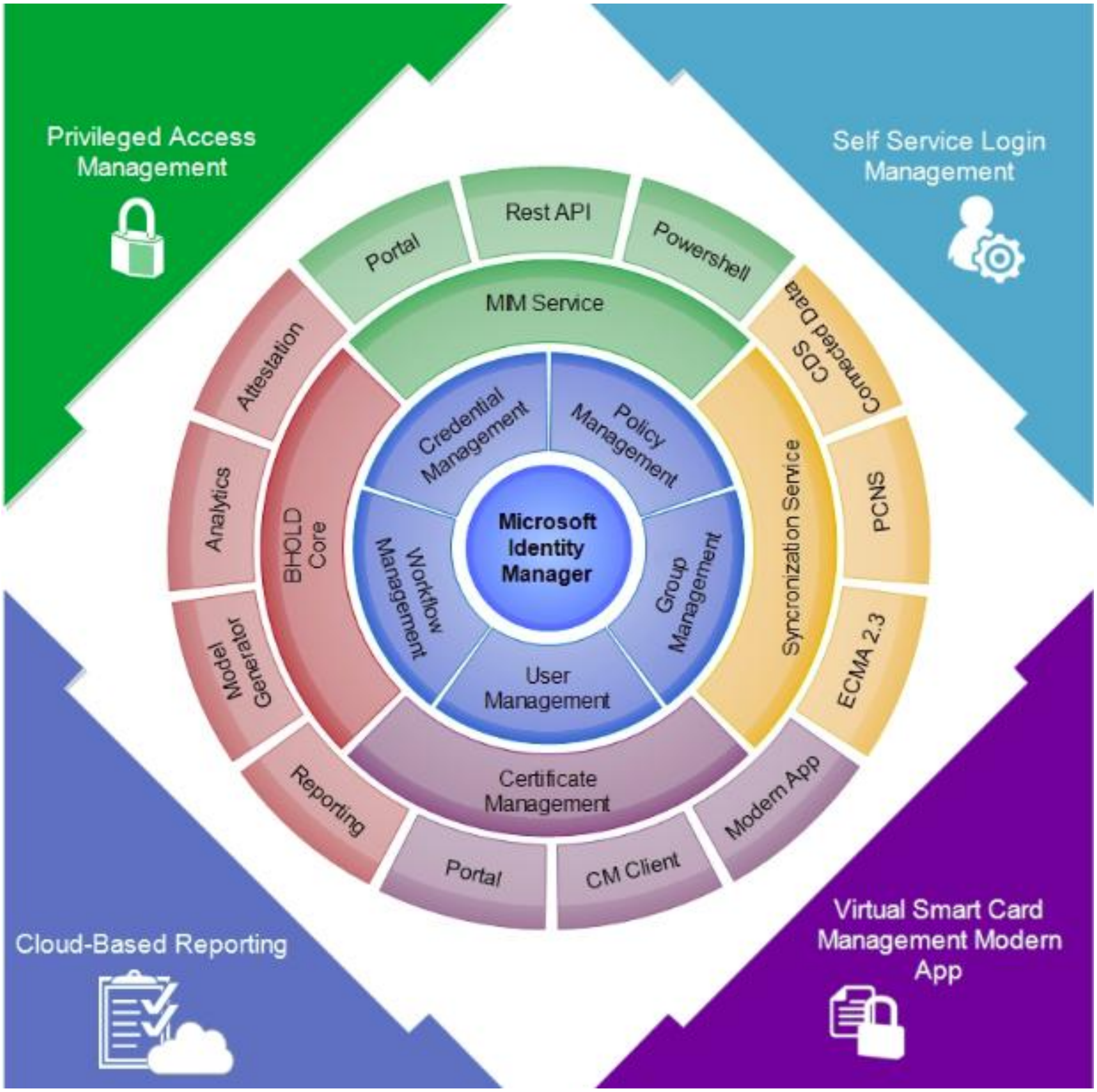
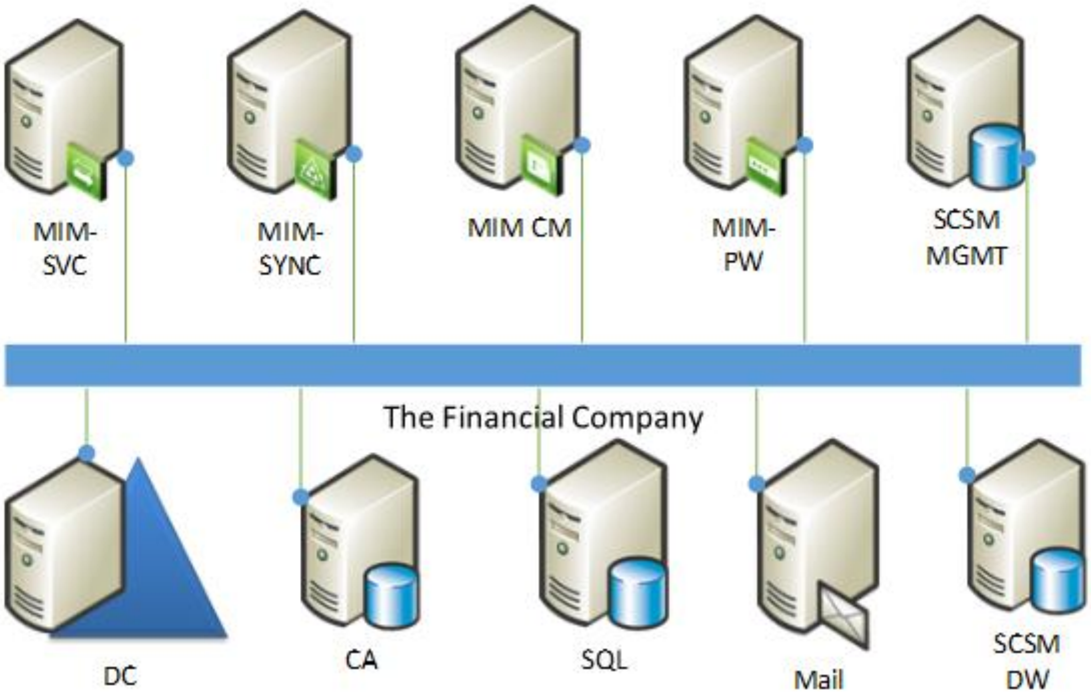
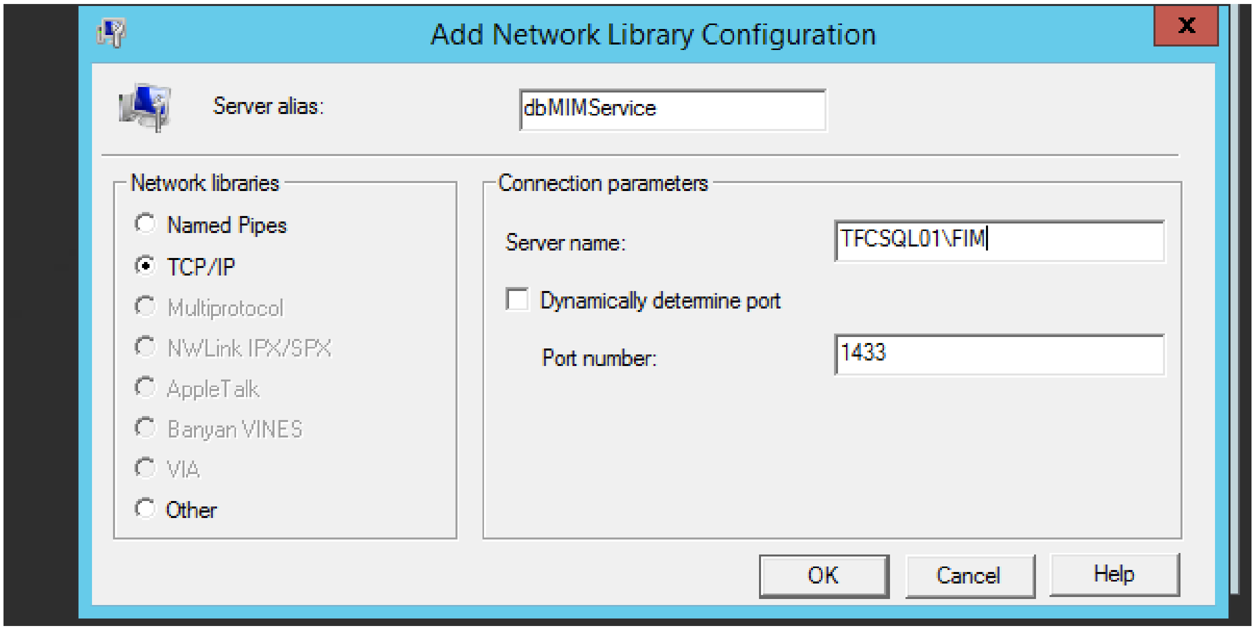
Chapter 1: Overview of Microsoft Identity Manager 2016




MIM-
SVC
MIM-
SYNC
MIM CM
MIM-
PW
SCSM
MGMT
The Financial Company
DC
CA
SQL
Mail
SCSM
DW



Server alias: dbMIMService

Network libraries

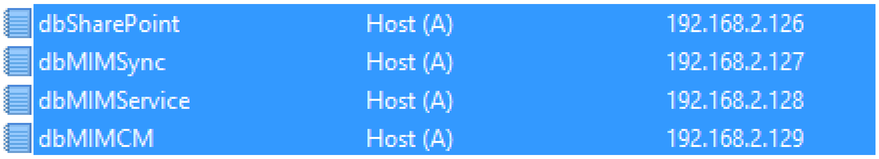
○ Named Pipes
● TCP/IP
○ Multiprotocol
○ NWLink IPX/SPX
○ AppleTalk
○ Banyan VINES
○ VIA
○ Other

Connection parameters

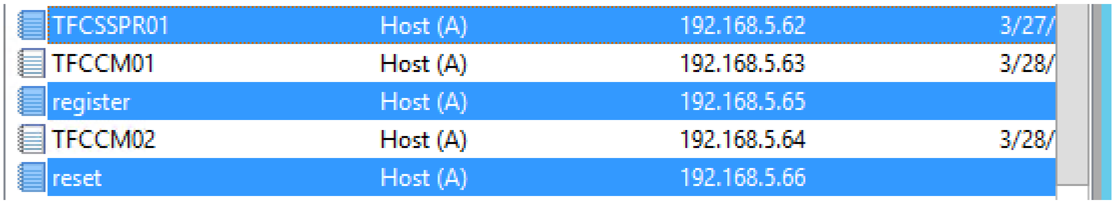
Server name: TFCSQL01\FIM

□ Dynamically determine port

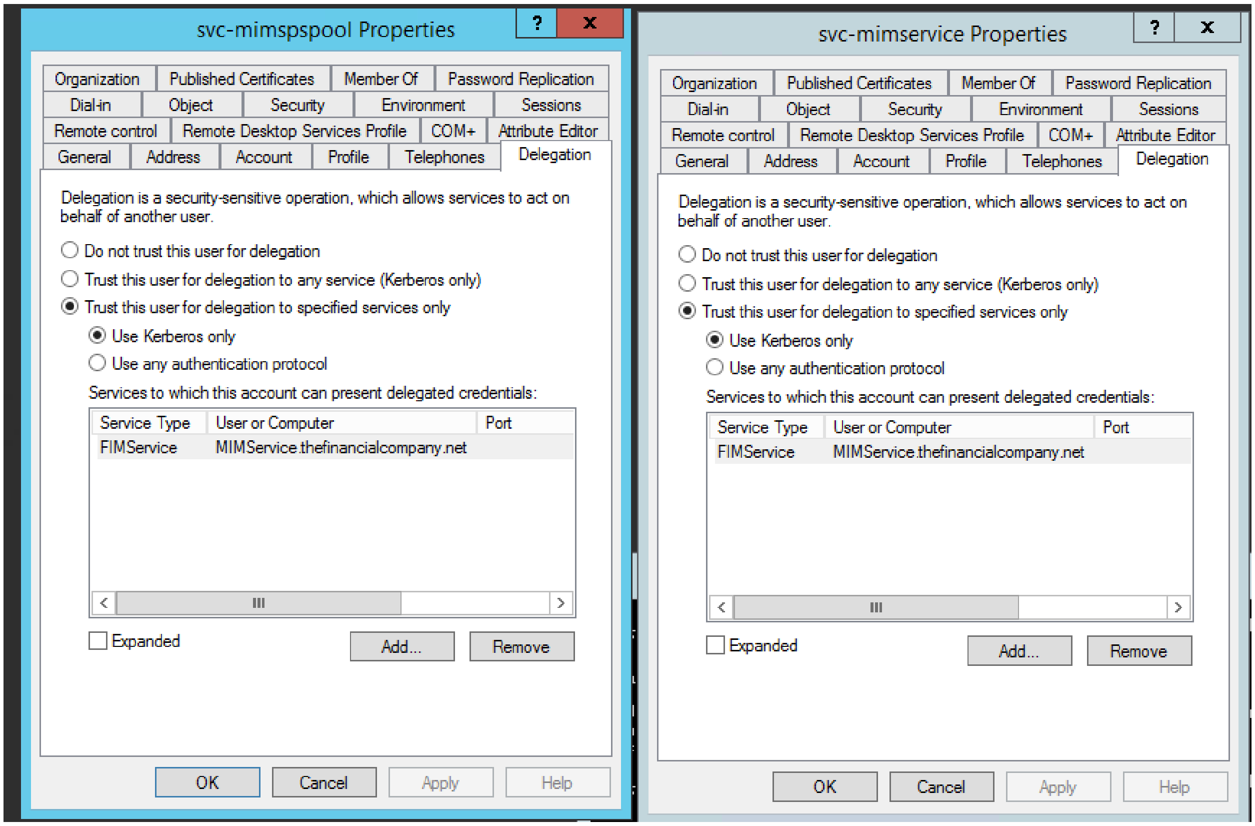
Port number: 1433



dbSharePoint	Host (A)	192.168.2.126
dbMIMSync	Host (A)	192.168.2.127
dbMIMService	Host (A)	192.168.2.128
dbMIMCM	Host (A)	192.168.2.129



TFCSSPR01	Host (A)	192.168.5.62	3/27/
TFCCM01	Host (A)	192.168.5.63	3/28/
register	Host (A)	192.168.5.65	
TFCCM02	Host (A)	192.168.5.64	3/28/
reset	Host (A)	192.168.5.66	



svc-mimspspool Properties

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

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port
FIMService	MIMService.thefinancialcompany.net	

□ Expanded

svc-mimservice Properties

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

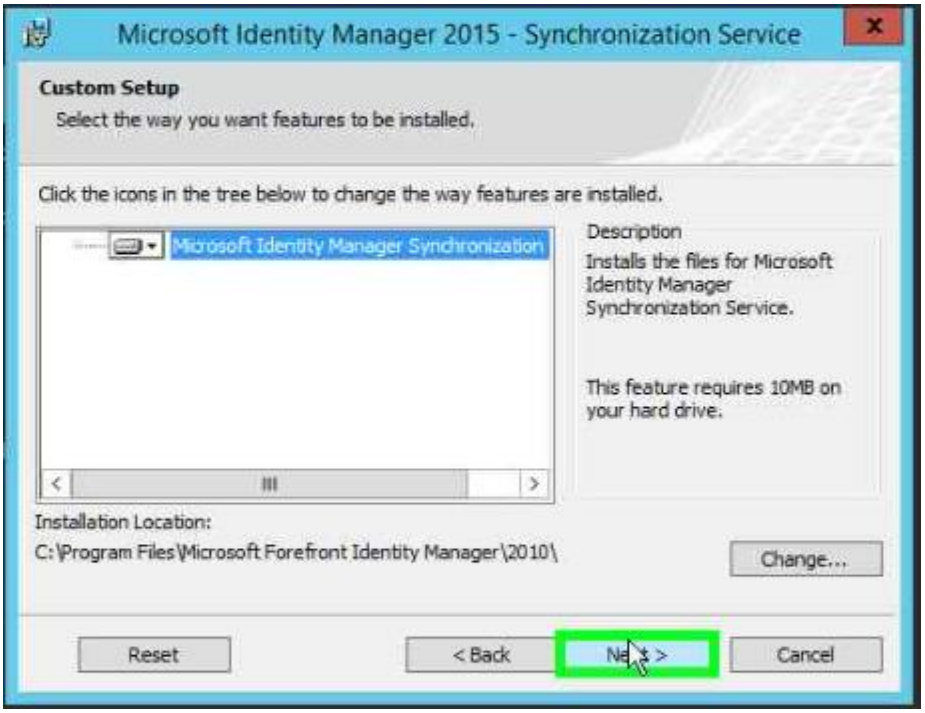
● Use Kerberos only

○ Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port
FIMService	MIMService.thefinancialcompany.net	

□ Expanded



Microsoft Identity Manager 2015 - Synchronization Service

Custom Setup

Select the way you want features to be installed.

Click the icons in the tree below to change the way features are installed.

Microsoft Identity Manager Synchronization

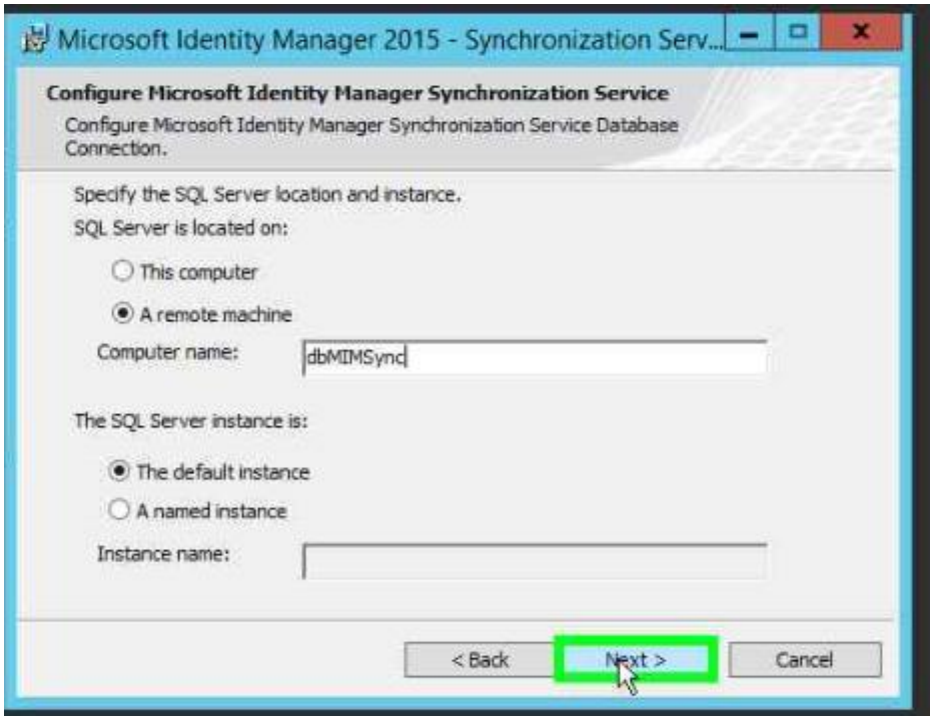
Description

Installs the files for Microsoft Identity Manager Synchronization Service.

This feature requires 10MB on your hard drive.

Installation Location:

C:\Program Files\Microsoft Forefront Identity Manager\2010\



Configure Microsoft Identity Manager Synchronization Service

Configure Microsoft Identity Manager Synchronization Service Database Connection.

Specify the SQL Server location and instance.

SQL Server is located on:

○ This computer

● A remote machine

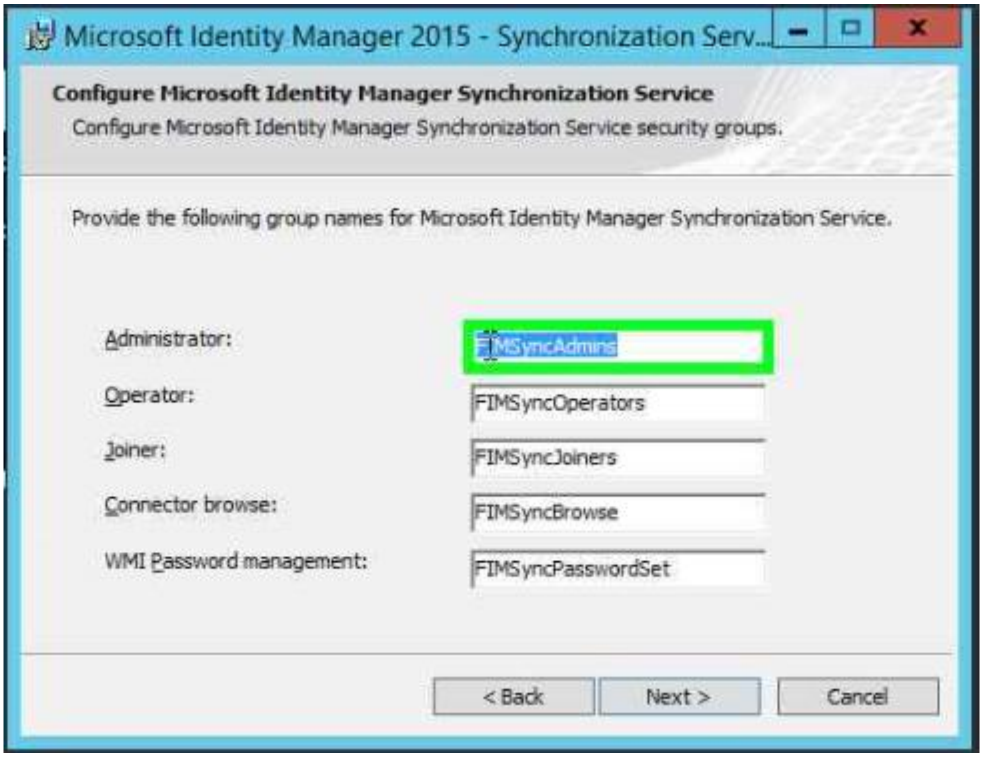
Computer name: dbMIMSync

The SQL Server instance is:

● The default instance

○ A named instance

Instance name:



Configure Microsoft Identity Manager Synchronization Service

Configure Microsoft Identity Manager Synchronization Service security groups.

Provide the following group names for Microsoft Identity Manager Synchronization Service.

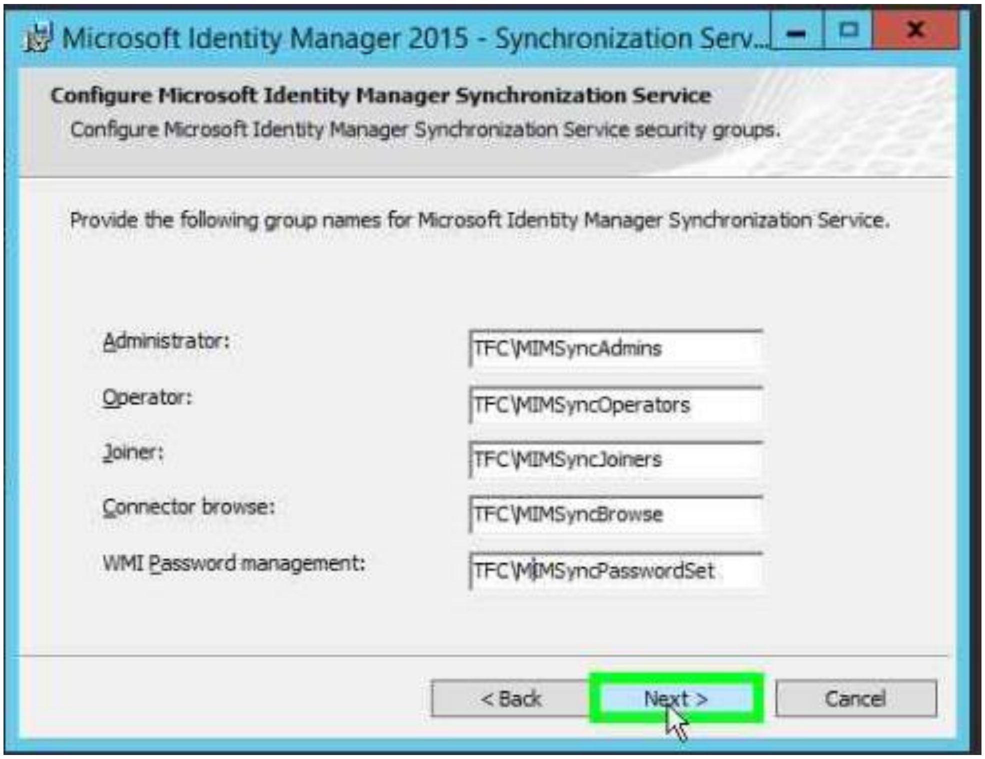
Administrator: FIMSyncAdmins

Operator: FIMSyncOperators

Joiner: FIMSyncJoiners

Connector browse: FIMSyncBrowse

WMI Password management: FIMSyncPasswordSet



Microsoft Identity Manager 2015 - Synchronization Serv...

Configure Microsoft Identity Manager Synchronization Service

Configure Microsoft Identity Manager Synchronization Service security groups.

Provide the following group names for Microsoft Identity Manager Synchronization Service.

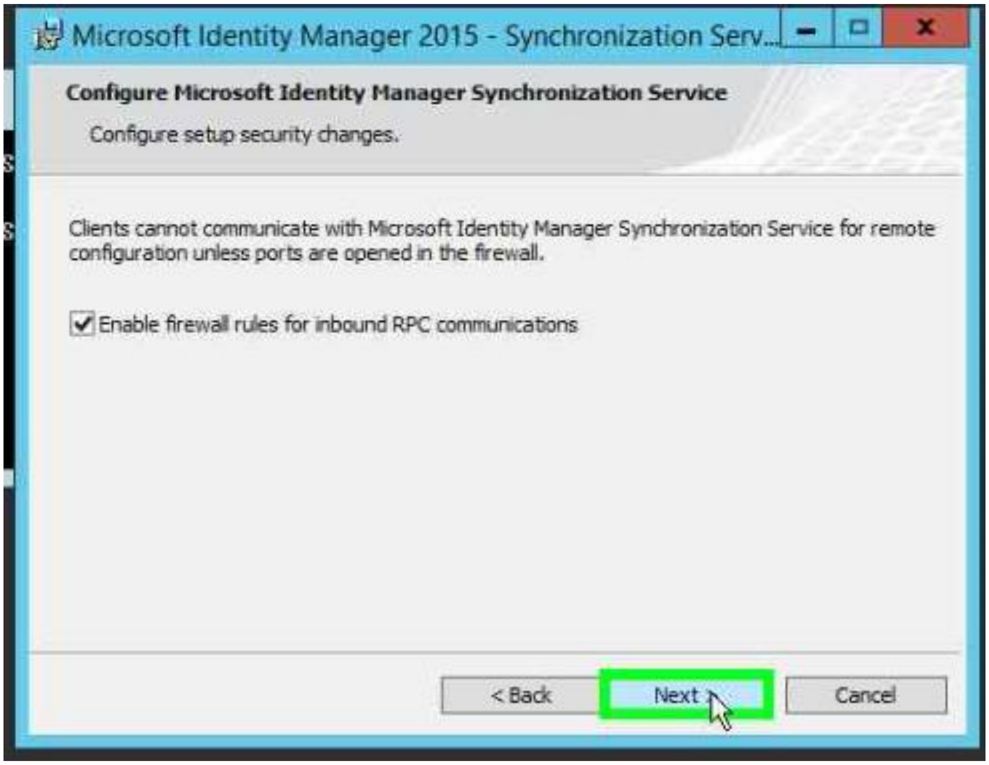
Administrator: TFC\MIMSyncAdmins

Operator: TFC\MIMSyncOperators

Joiner: TFC\MIMSyncJoiners

Connector browse: TFC\MIMSyncBrowse

WMI Password management: TFC\MIMSyncPasswordSet



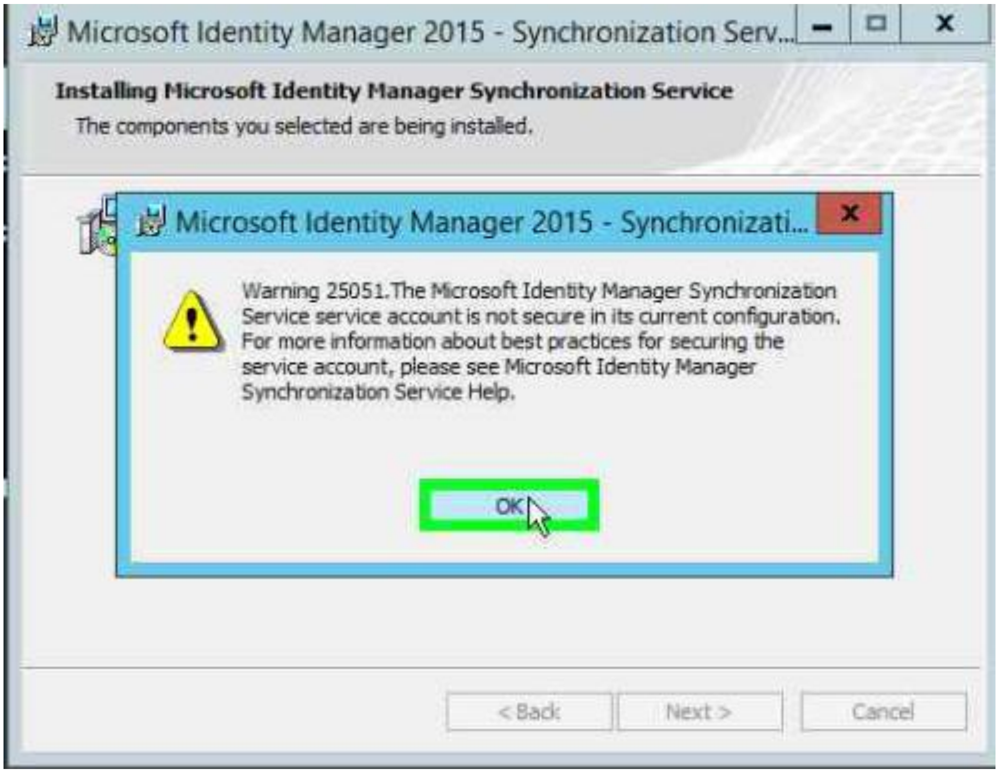
Microsoft Identity Manager 2015 - Synchronization Serv...

Configure Microsoft Identity Manager Synchronization Service

Configure setup security changes.

Clients cannot communicate with Microsoft Identity Manager Synchronization Service for remote configuration unless ports are opened in the firewall.

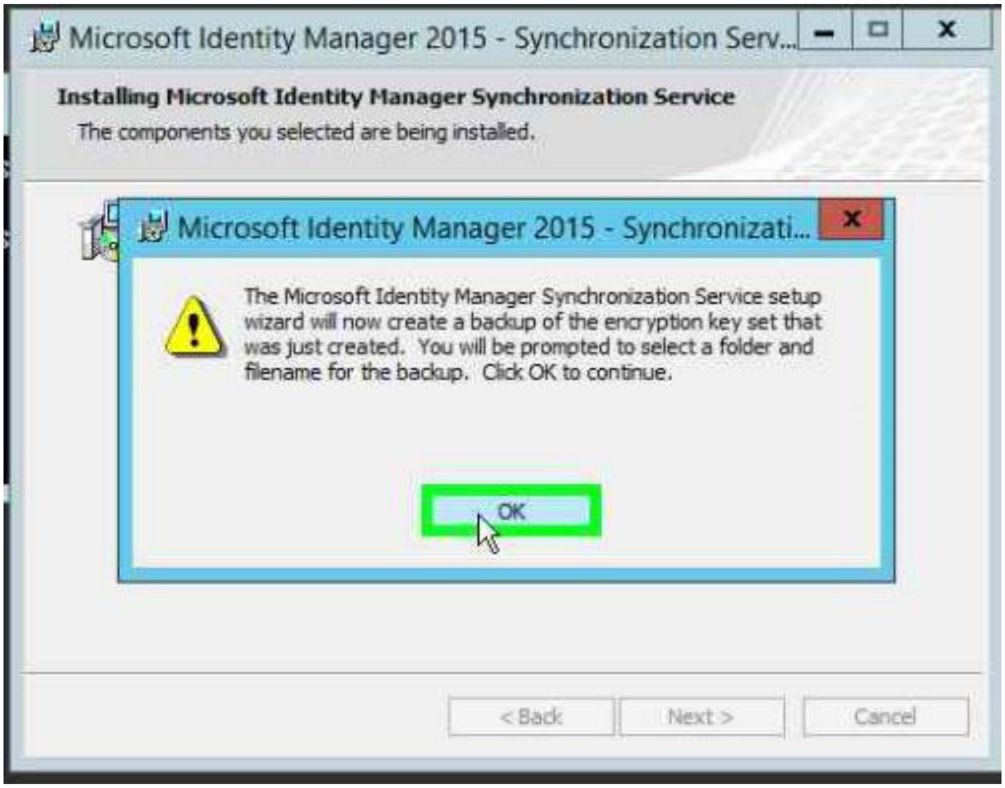
☑ Enable firewall rules for inbound RPC communications


Microsoft Identity Manager 2015 - Synchronization Serv...
Microsoft Identity Manager 2015 - Synchronizati...
OK
< Back
Next >
Cancel

Installing Microsoft Identity Manager Synchronization Service

The components you selected are being installed.

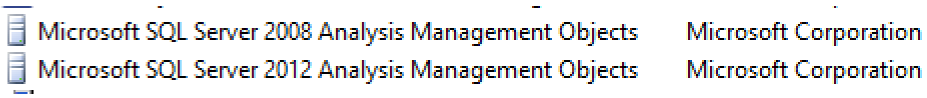
Warning 25051.The Microsoft Identity Manager Synchronization Service service account is not secure in its current configuration. For more information about best practices for securing the service account, please see Microsoft Identity Manager Synchronization Service Help.


Microsoft Identity Manager 2015 - Synchronization Serv...
Microsoft Identity Manager 2015 - Synchronizati...
OK
< Back
Next >
Cancel

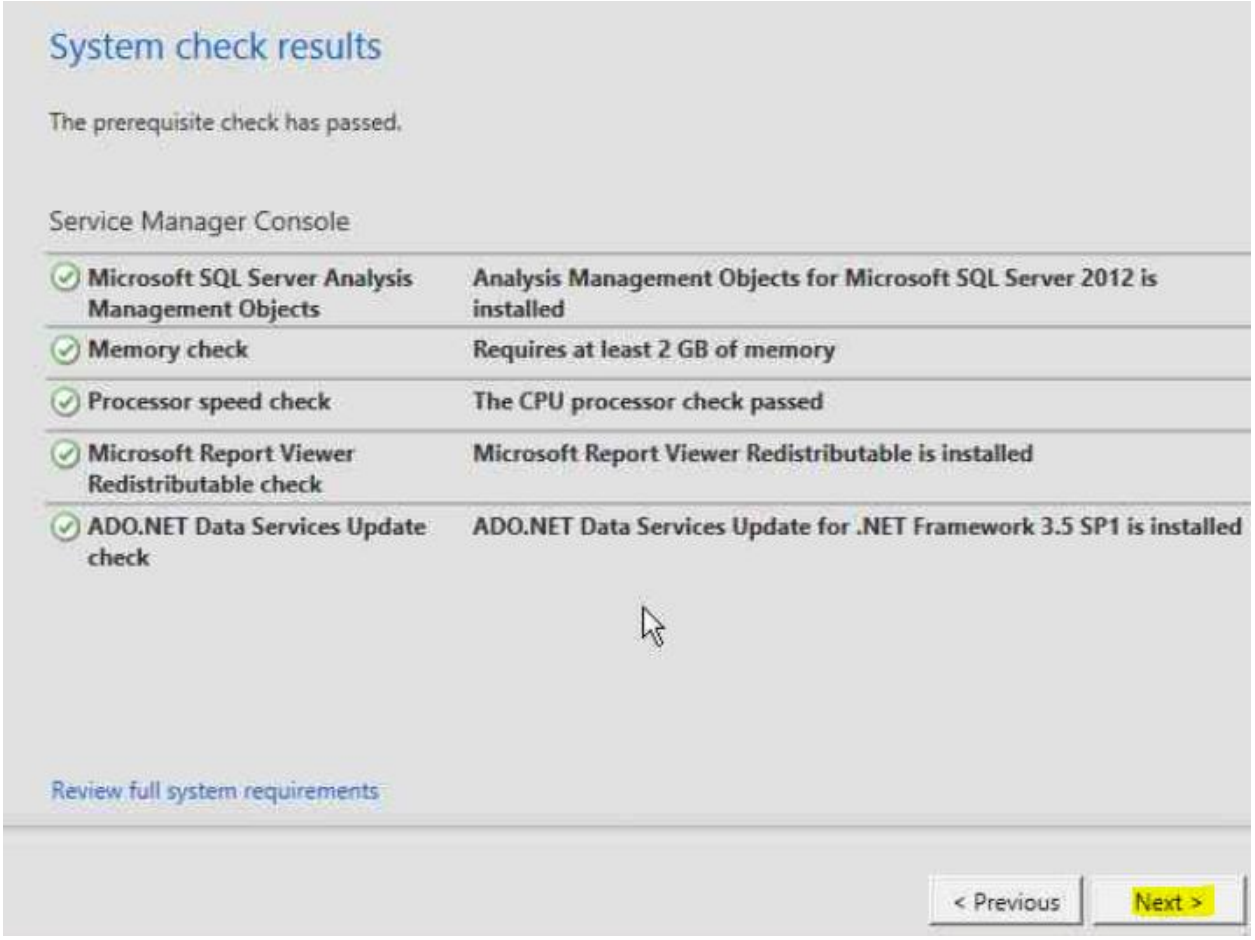
Installing Microsoft Identity Manager Synchronization Service

The components you selected are being installed.

The Microsoft Identity Manager Synchronization Service setup wizard will now create a backup of the encryption key set that was just created. You will be prompted to select a folder and filename for the backup. Click OK to continue.



Microsoft SQL Server 2008 Analysis Management Objects	Microsoft Corporation
Microsoft SQL Server 2012 Analysis Management Objects	Microsoft Corporation

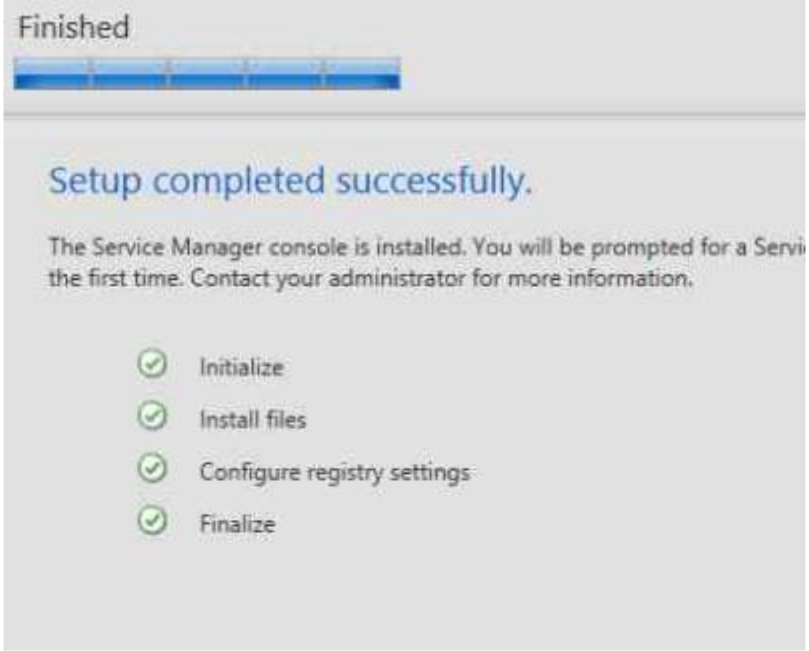


System check results

The prerequisite check has passed.

Service Manager Console

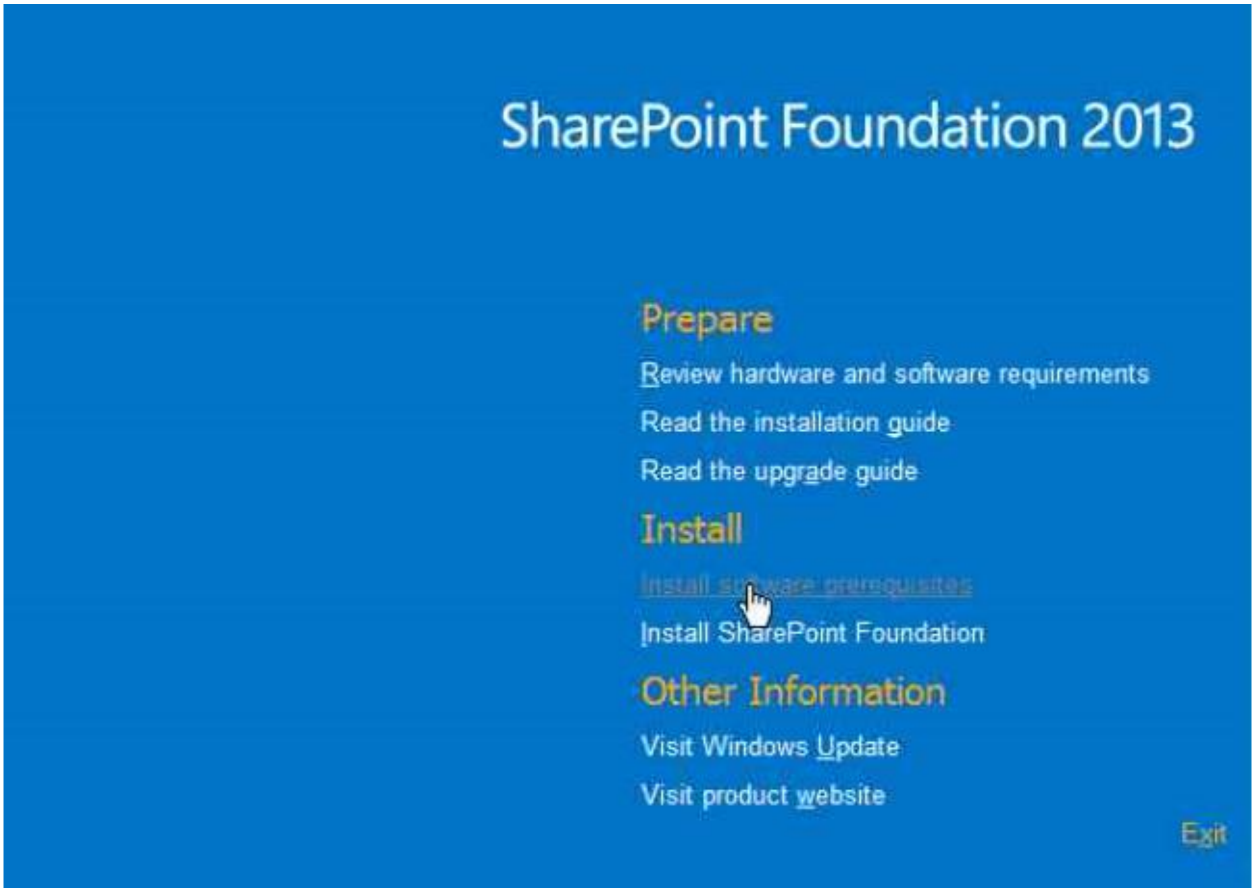
✓ Microsoft SQL Server Analysis Management Objects	Analysis Management Objects for Microsoft SQL Server 2012 is installed
✓ Memory check	Requires at least 2 GB of memory
✓ Processor speed check	The CPU processor check passed
✓ Microsoft Report Viewer Redistributable check	Microsoft Report Viewer Redistributable is installed
✓ ADO.NET Data Services Update check	ADO.NET Data Services Update for .NET Framework 3.5 SP1 is installed

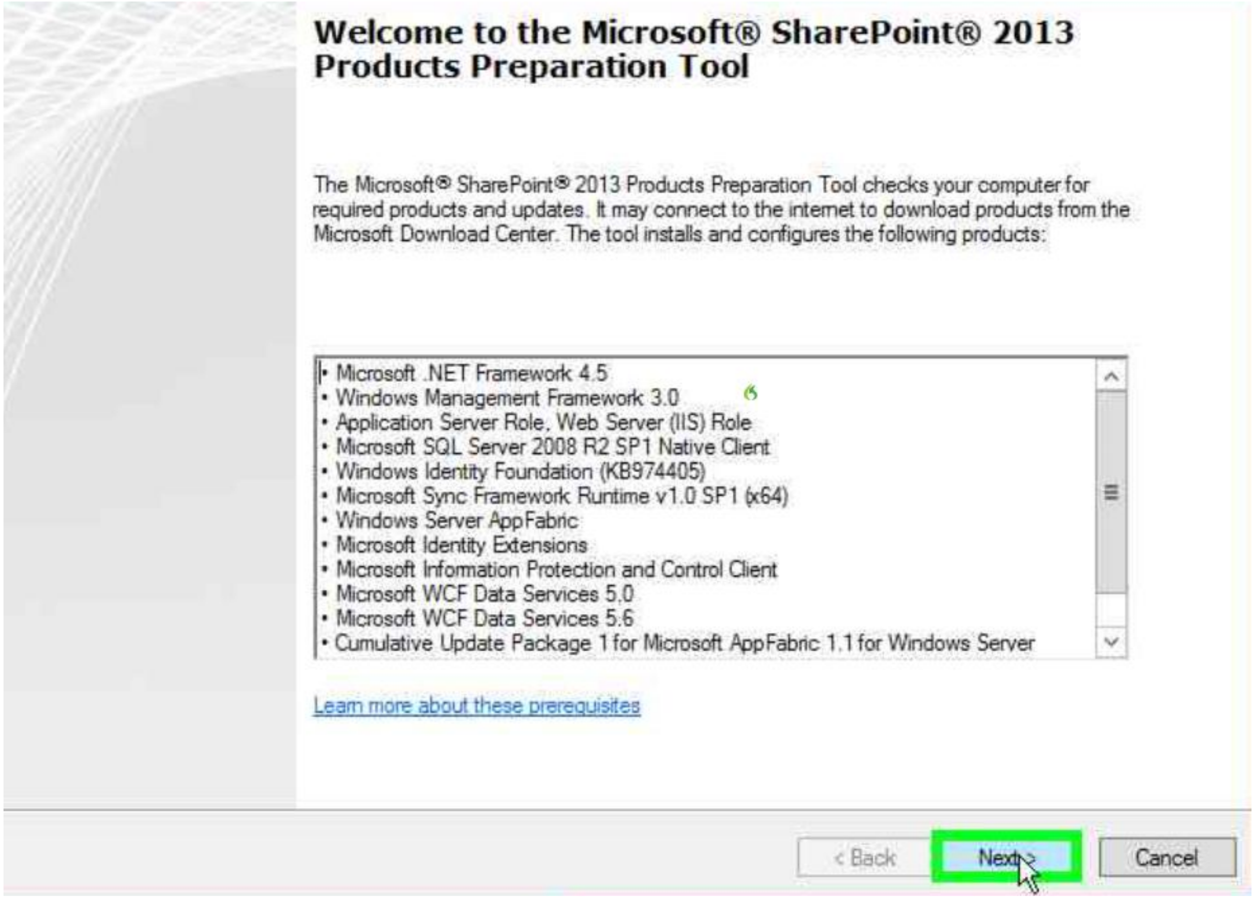


Setup completed successfully.

The Service Manager console is installed. You will be prompted for a Servi
the first time. Contact your administrator for more information.

- ✓ Initialize
- ✓ Install files
- ✓ Configure registry settings
- ✓ Finalize


SharePoint Foundation 2013
Prepare
Review hardware and software requirements
Read the installation guide
Read the upgrade guide
Install
Install software prerequisites
Install SharePoint Foundation
Other Information
Visit Windows Update
Visit product website
Exit

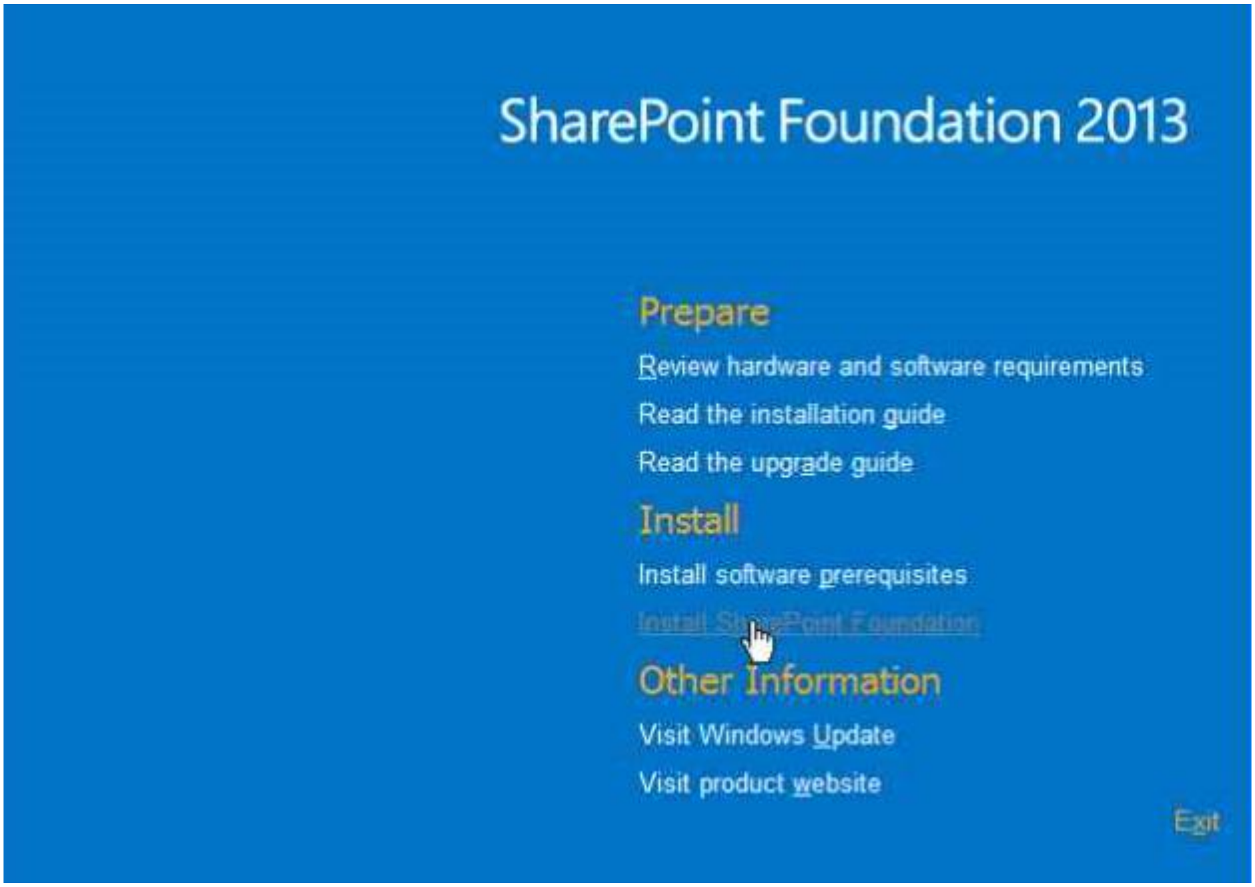


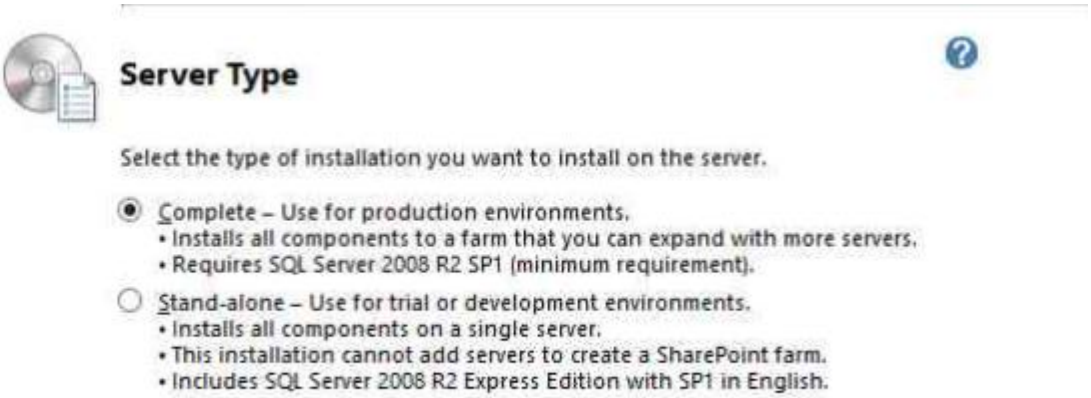
Welcome to the Microsoft® SharePoint® 2013 Products Preparation Tool

The Microsoft® SharePoint® 2013 Products Preparation Tool checks your computer for required products and updates. It may connect to the internet to download products from the Microsoft Download Center. The tool installs and configures the following products:

- Microsoft .NET Framework 4.5
- Windows Management Framework 3.0
- Application Server Role, Web Server (IIS) Role
- Microsoft SQL Server 2008 R2 SP1 Native Client
- Windows Identity Foundation (KB974405)
- Microsoft Sync Framework Runtime v1.0 SP1 (x64)
- Windows Server AppFabric
- Microsoft Identity Extensions
- Microsoft Information Protection and Control Client
- Microsoft WCF Data Services 5.0
- Microsoft WCF Data Services 5.6
- Cumulative Update Package 1 for Microsoft AppFabric 1.1 for Windows Server

Learn more about these prerequisites


SharePoint Foundation 2013
Prepare
Review hardware and software requirements
Read the installation guide
Read the upgrade guide
Install
Install software prerequisites
Install SharePoint Foundation
Other Information
Visit Windows Update
Visit product website
Exit

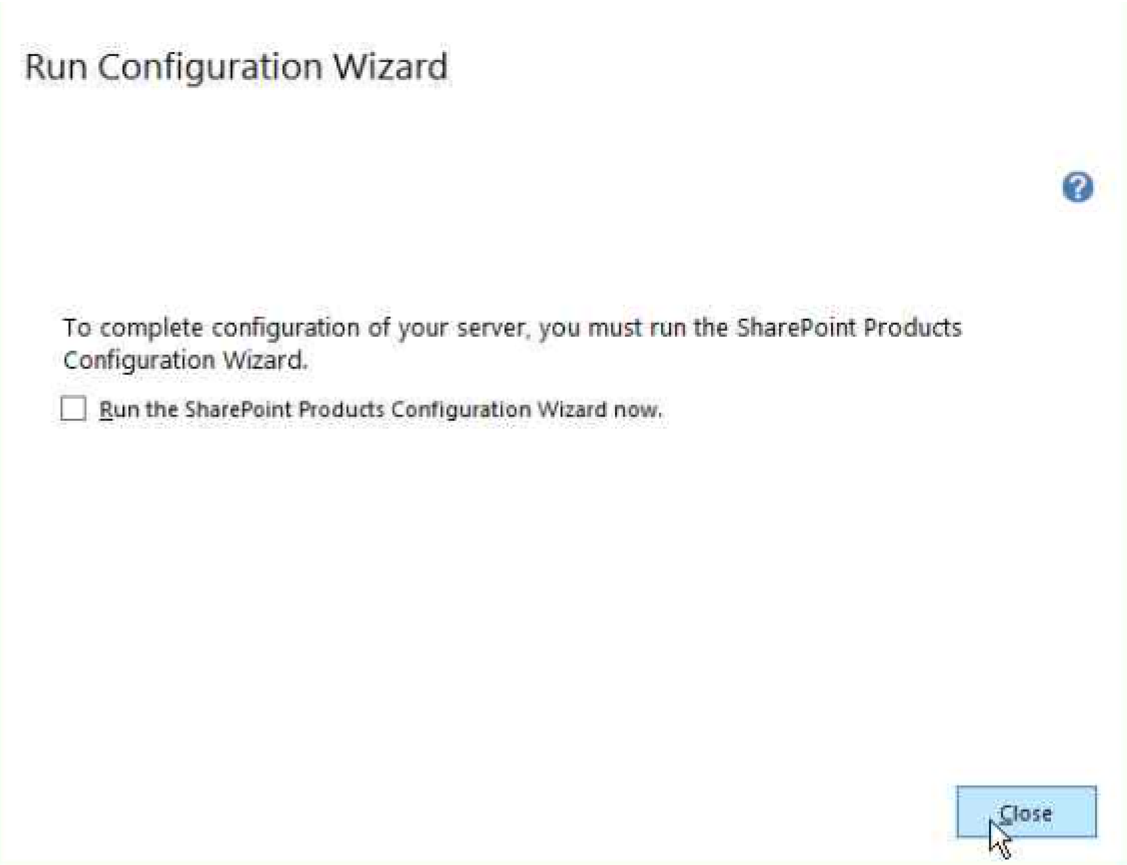


Server Type

Select the type of installation you want to install on the server.

● Complete – Use for production environments.
- Installs all components to a farm that you can expand with more servers.
- Requires SQL Server 2008 R2 SP1 (minimum requirement).

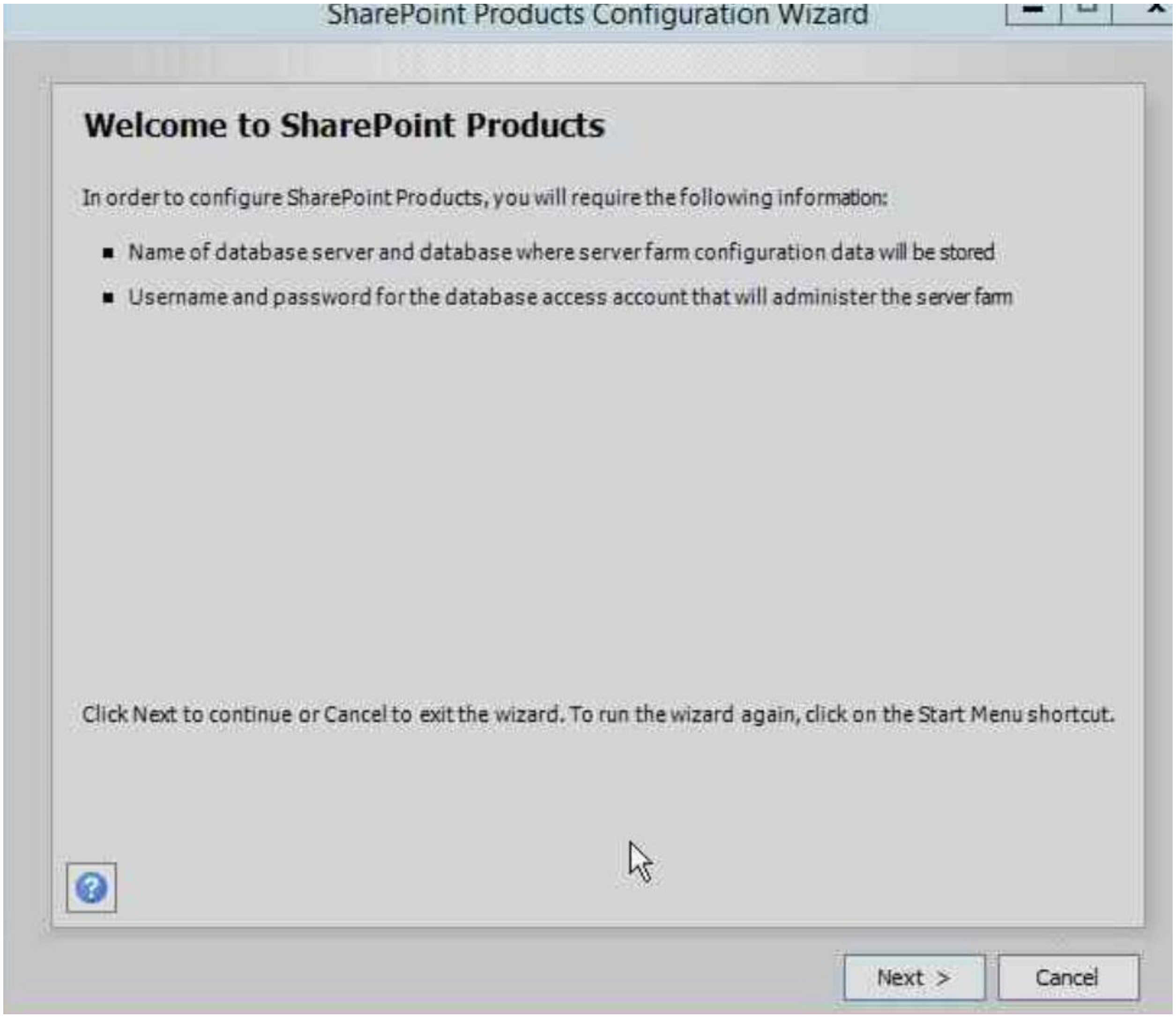
○ Stand-alone – Use for trial or development environments.
- Installs all components on a single server.
- This installation cannot add servers to create a SharePoint farm.
- Includes SQL Server 2008 R2 Express Edition with SP1 in English.



Run Configuration Wizard

To complete configuration of your server, you must run the SharePoint Products Configuration Wizard.

☐ Run the SharePoint Products Configuration Wizard now.

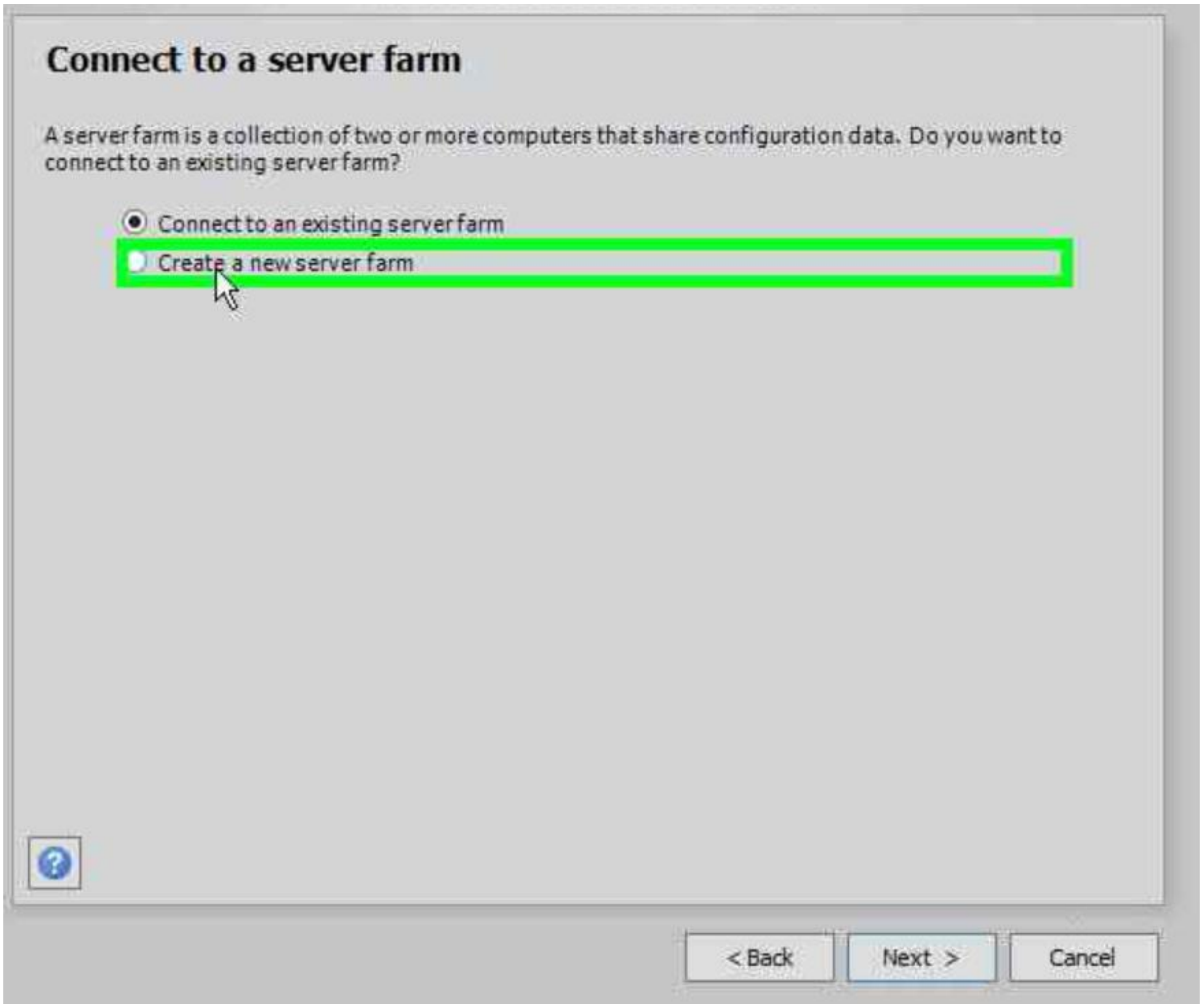


Welcome to SharePoint Products

In order to configure SharePoint Products, you will require the following information:

- Name of database server and database where server farm configuration data will be stored
- Username and password for the database access account that will administer the server farm

Click Next to continue or Cancel to exit the wizard. To run the wizard again, click on the Start Menu shortcut.

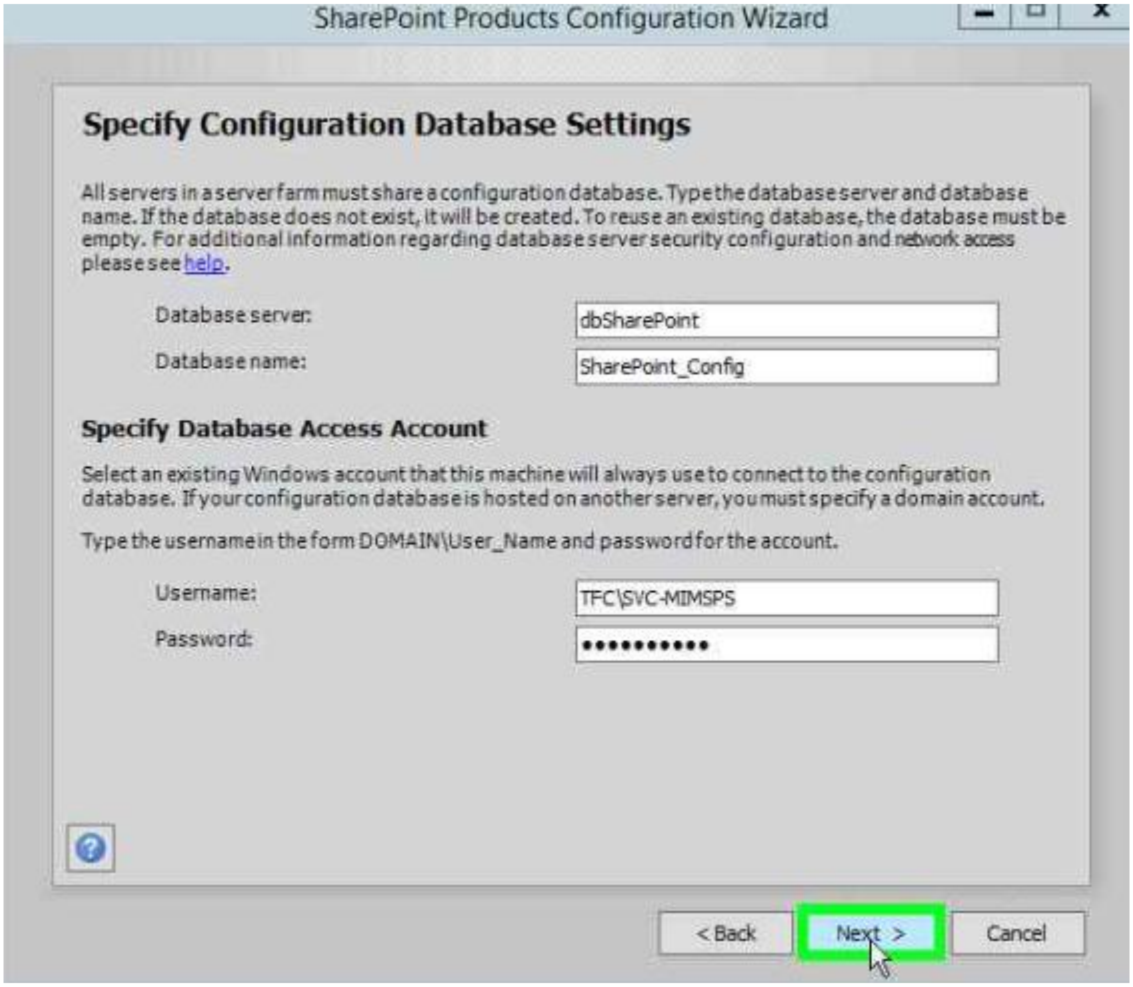


Connect to a server farm

A server farm is a collection of two or more computers that share configuration data. Do you want to connect to an existing server farm?

● Connect to an existing server farm

○ Create a new server farm



SharePoint Products Configuration Wizard

Specify Configuration Database Settings

All servers in a server farm must share a configuration database. Type the database server and database name. If the database does not exist, it will be created. To reuse an existing database, the database must be empty. For additional information regarding database server security configuration and network access please see help.

Database server: dbSharePoint

Database name: SharePoint_Config

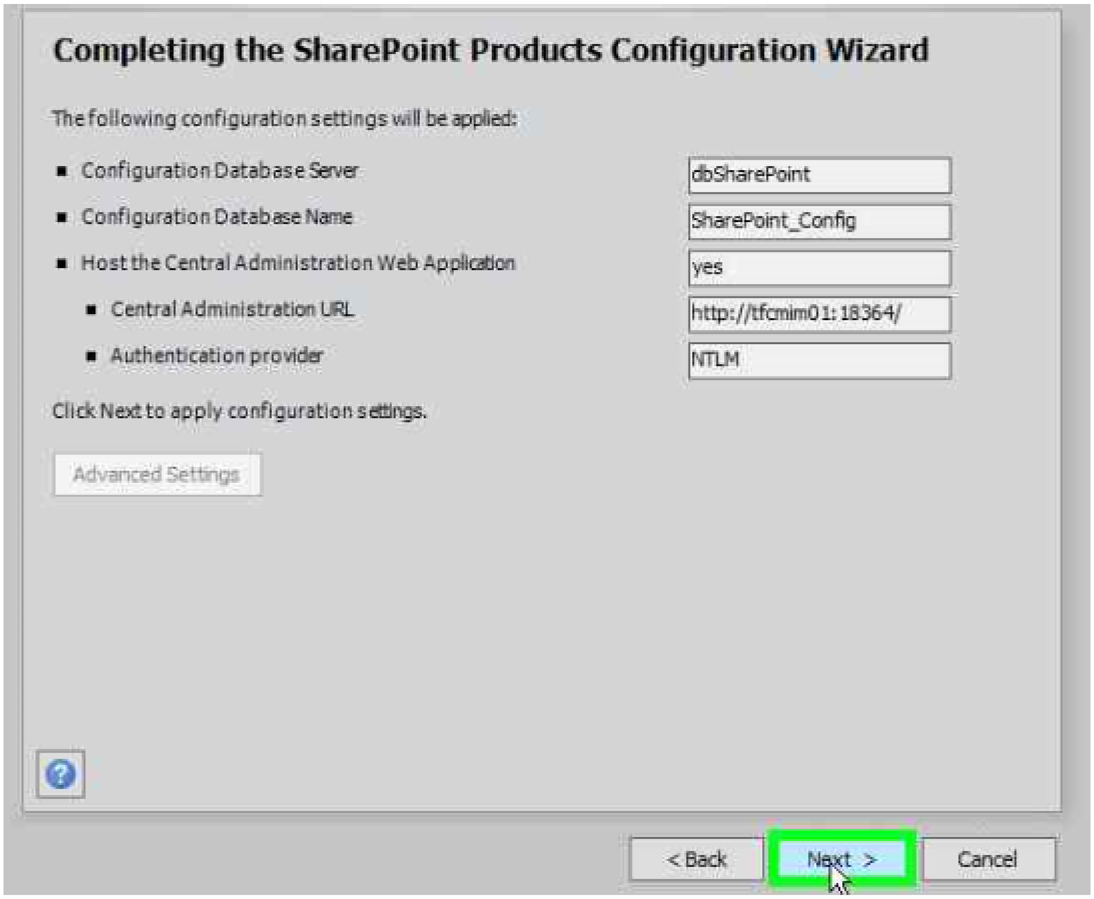
Specify Database Access Account

Select an existing Windows account that this machine will always use to connect to the configuration database. If your configuration database is hosted on another server, you must specify a domain account.

Type the username in the form DOMAIN\User_Name and password for the account.

Username: TFC\SVC-MIMSPS

Password: •••••••••••

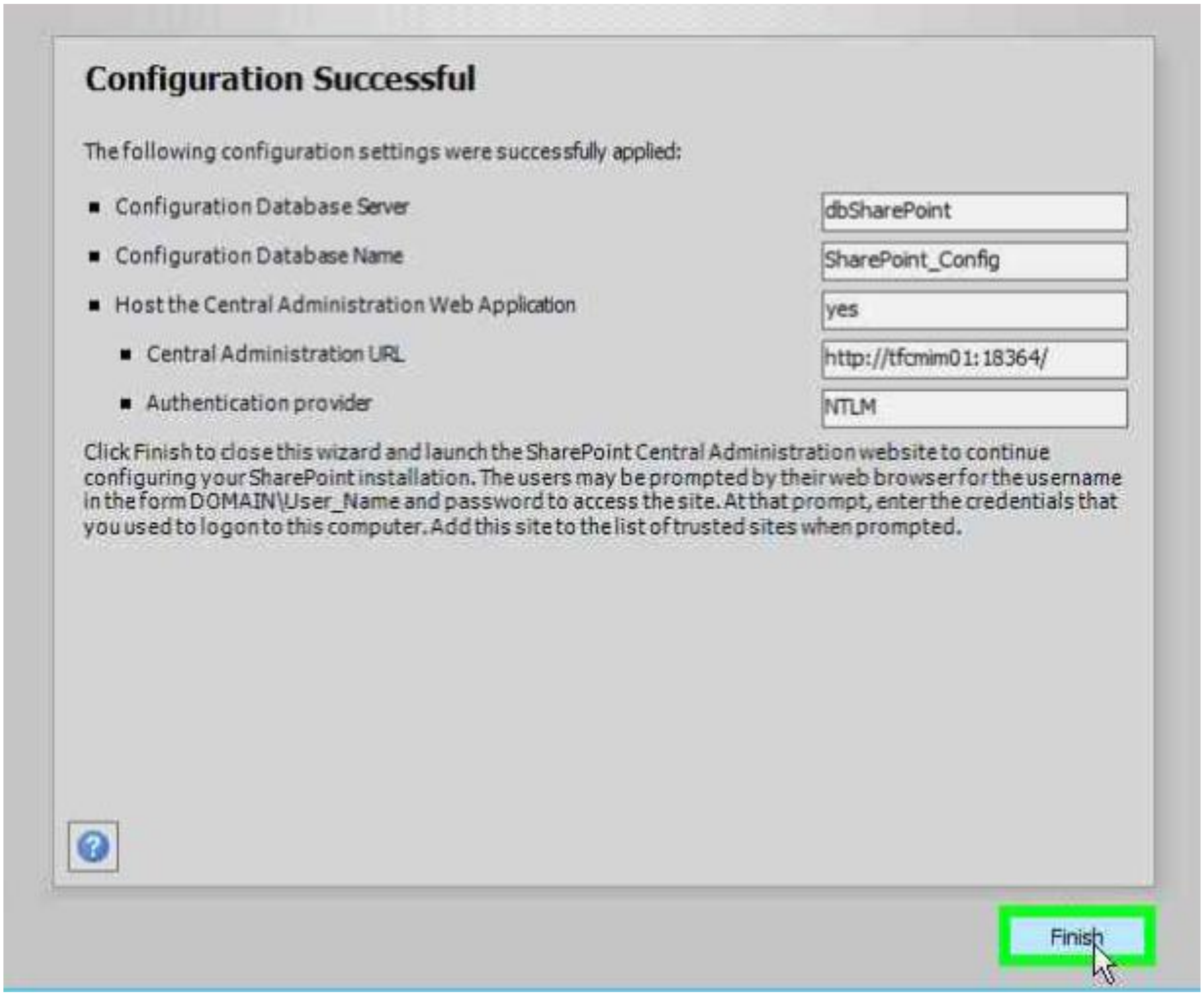


Completing the SharePoint Products Configuration Wizard

The following configuration settings will be applied:

- Configuration Database Server: dbSharePoint
- Configuration Database Name: SharePoint_Config
- Host the Central Administration Web Application: yes
  - Central Administration URL: http://tfcmim01:18364/
  - Authentication provider: NTLM

Click Next to apply configuration settings.

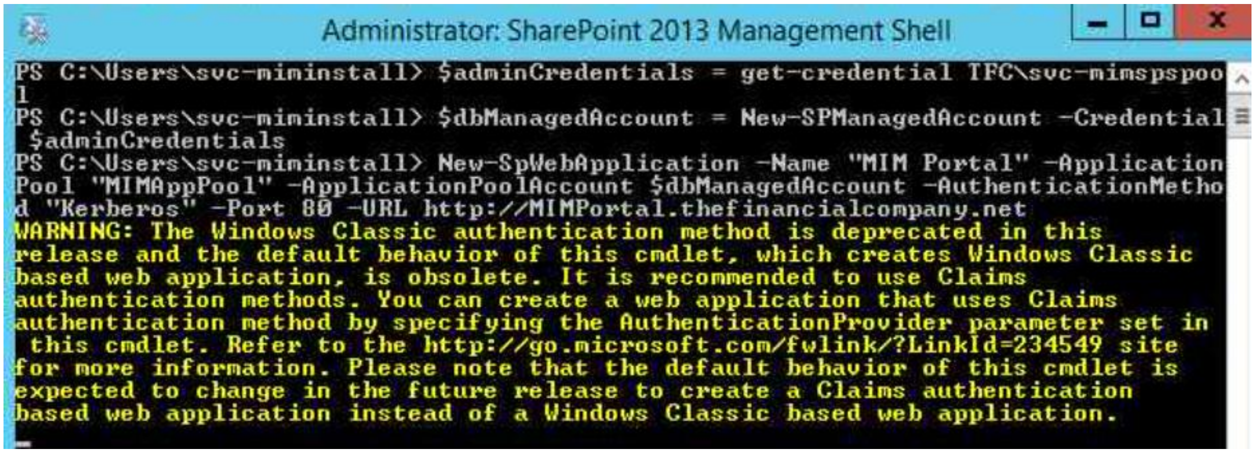


Configuration Successful

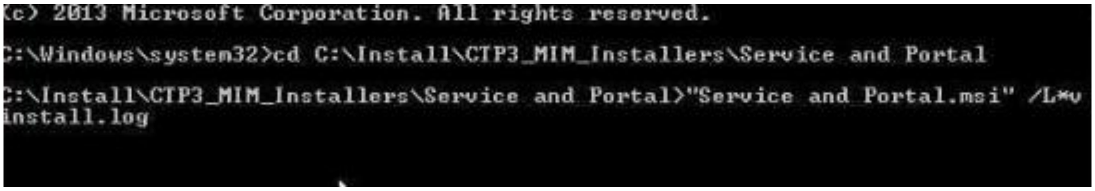
The following configuration settings were successfully applied:

- Configuration Database Server: dbSharePoint
- Configuration Database Name: SharePoint_Config
- Host the Central Administration Web Application: yes
  - Central Administration URL: http://tfcmim01:18364/
  - Authentication provider: NTLM

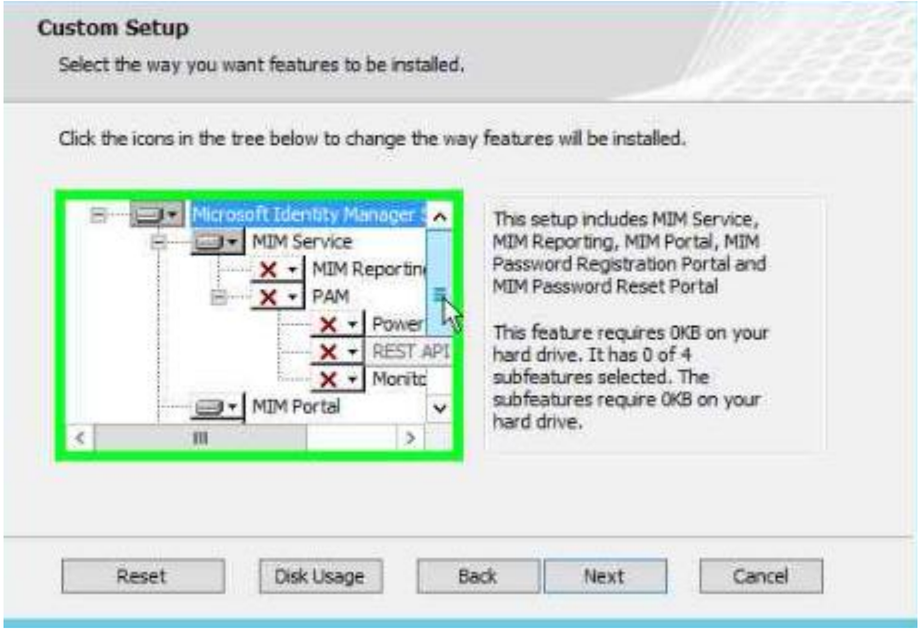
Click Finish to close this wizard and launch the SharePoint Central Administration website to continue configuring your SharePoint installation. The users may be prompted by their web browser for the username in the form DOMAIN\User_Name and password to access the site. At that prompt, enter the credentials that you used to logon to this computer. Add this site to the list of trusted sites when prompted.



```
PS C:\Users\svc-miminstall> $adminCredentials = get-credential TFC\svc-mimspspoo
l
PS C:\Users\svc-miminstall> $dbManagedAccount = New-SPManagedAccount -Credential
 $adminCredentials
PS C:\Users\svc-miminstall> New-SpWebApplication -Name "MIM Portal" -Application
Pool "MIMAppPool" -ApplicationPoolAccount $dbManagedAccount -AuthenticationMetho
d "Kerberos" -Port 80 -URL http://MIMPortal.thefinancialcompany.net
WARNING: The Windows Classic authentication method is deprecated in this
release and the default behavior of this cmdlet, which creates Windows Classic
based web application, is obsolete. It is recommended to use 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.
_
```



```
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Install\CTP3_MIM_Installers\Service and Portal

C:\Install\CTP3_MIM_Installers\Service and Portal>"Service and Portal.msi" /L*v
install.log
```



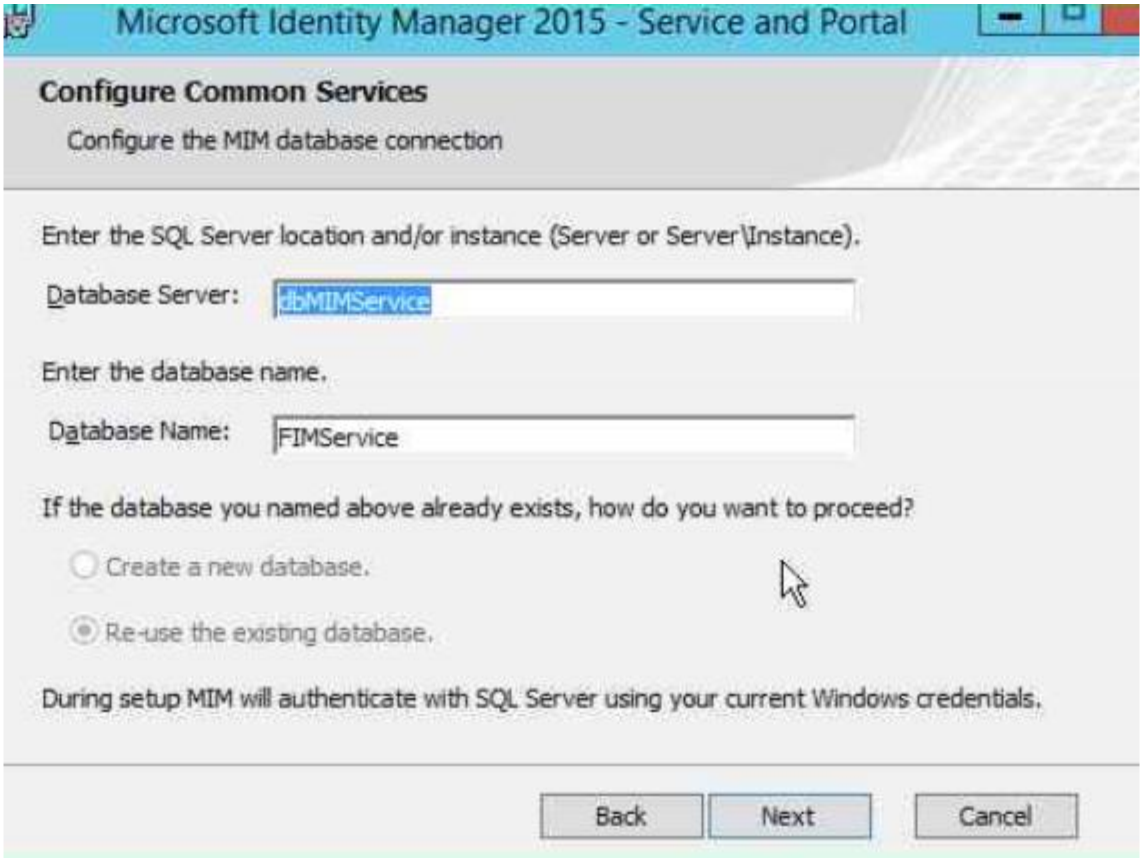
Custom Setup

Select the way you want features to be installed.

Click the icons in the tree below to change the way features will be installed.

This setup includes MIM Service, MIM Reporting, MIM Portal, MIM Password Registration Portal and MIM Password Reset Portal

This feature requires 0KB on your hard drive. It has 0 of 4 subfeatures selected. The subfeatures require 0KB on your hard drive.



Microsoft Identity Manager 2015 - Service and Portal

Configure Common Services

Configure the MIM database connection

Enter the SQL Server location and/or instance (Server or Server\Instance).

Database Server: dbMIMService

Enter the database name.

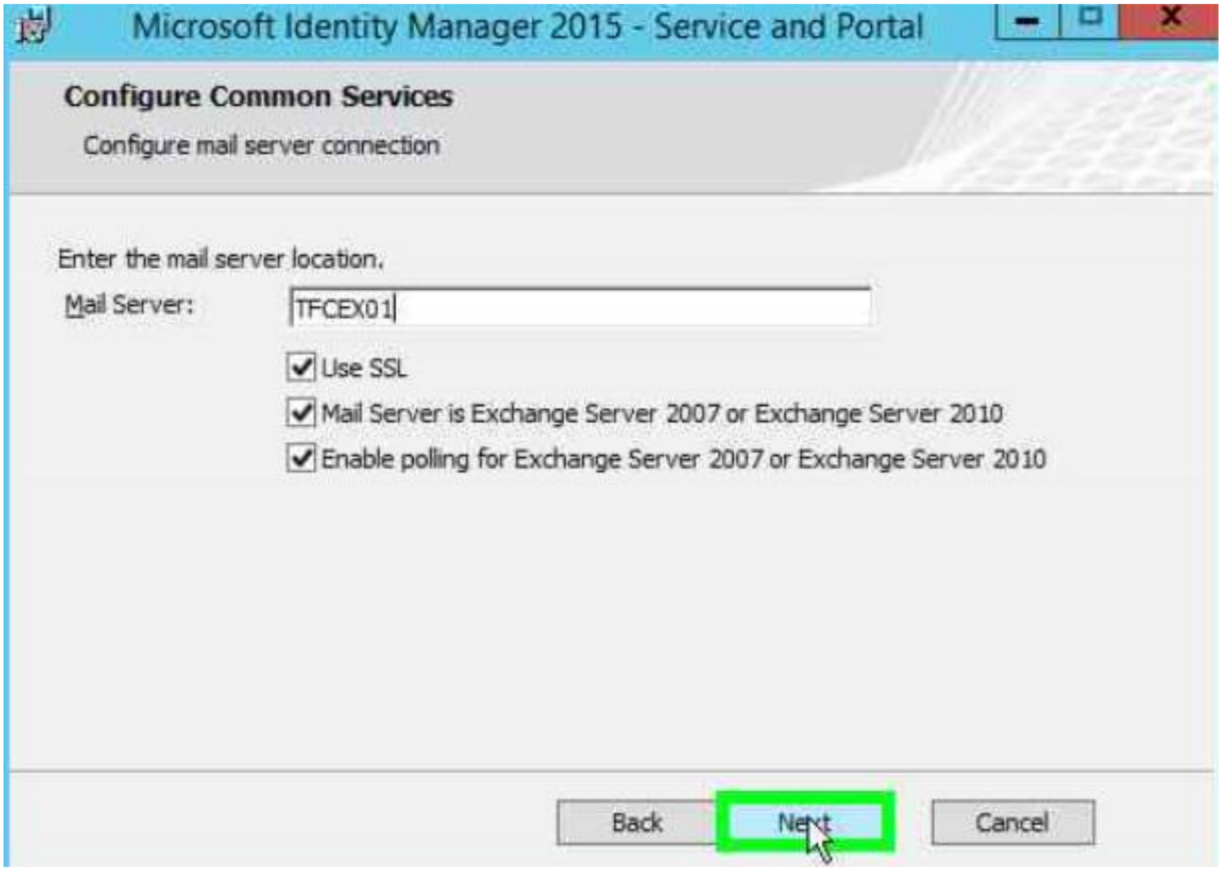
Database Name: FIMService

If the database you named above already exists, how do you want to proceed?

○ Create a new database.

● Re-use the existing database.

During setup MIM will authenticate with SQL Server using your current Windows credentials.



Microsoft Identity Manager 2015 - Service and Portal

Configure Common Services

Configure mail server connection

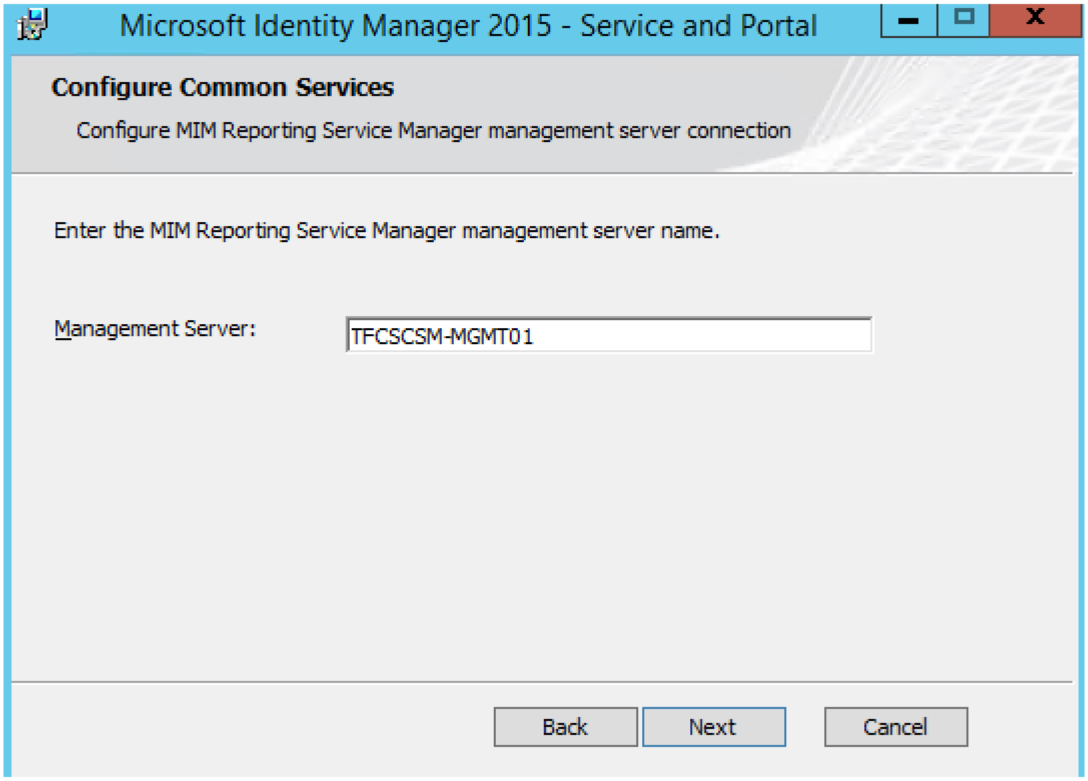
Enter the mail server location.

Mail Server: TFCEX01

☑ Use SSL

☑ Mail Server is Exchange Server 2007 or Exchange Server 2010

☑ Enable polling for Exchange Server 2007 or Exchange Server 2010



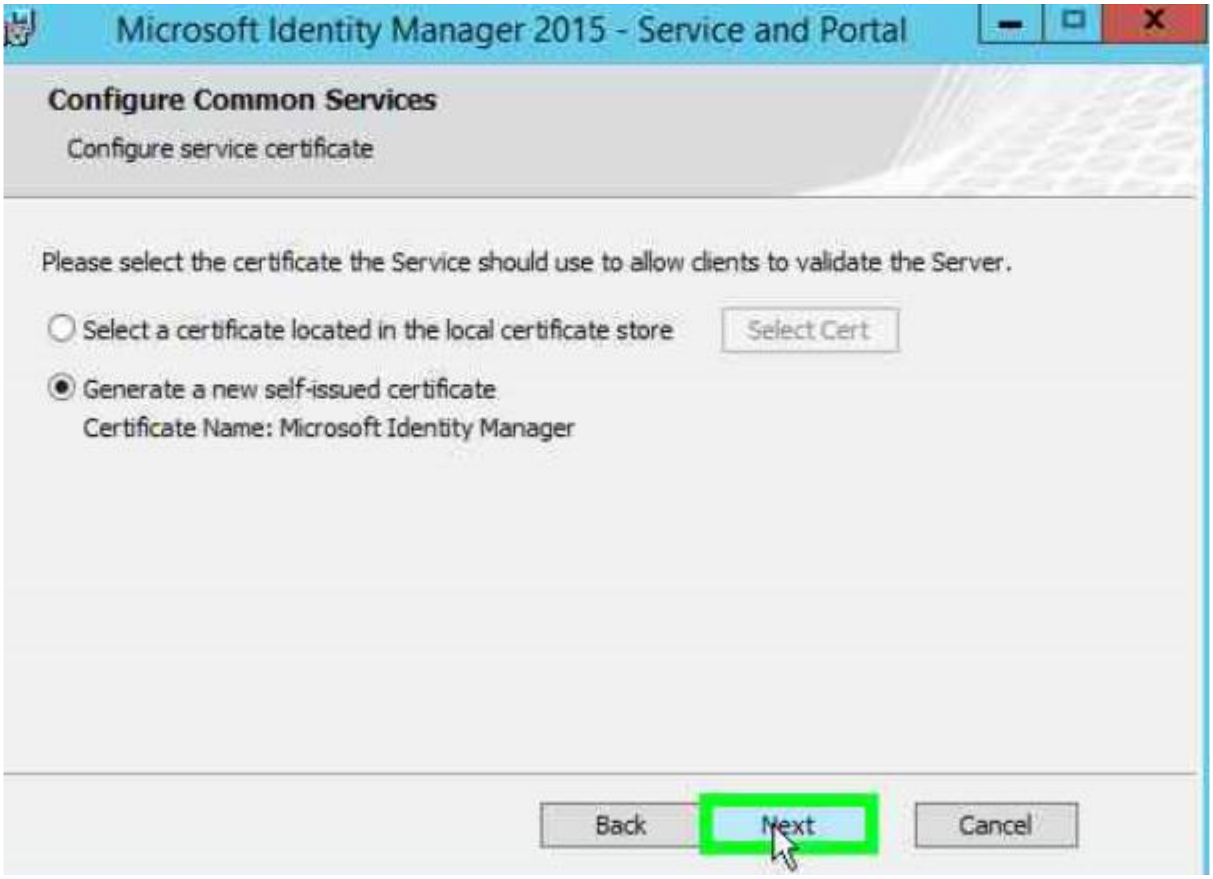
Microsoft Identity Manager 2015 - Service and Portal

Configure Common Services

Configure MIM Reporting Service Manager management server connection

Enter the MIM Reporting Service Manager management server name.

Management Server: TFCSCSM-MGMT01



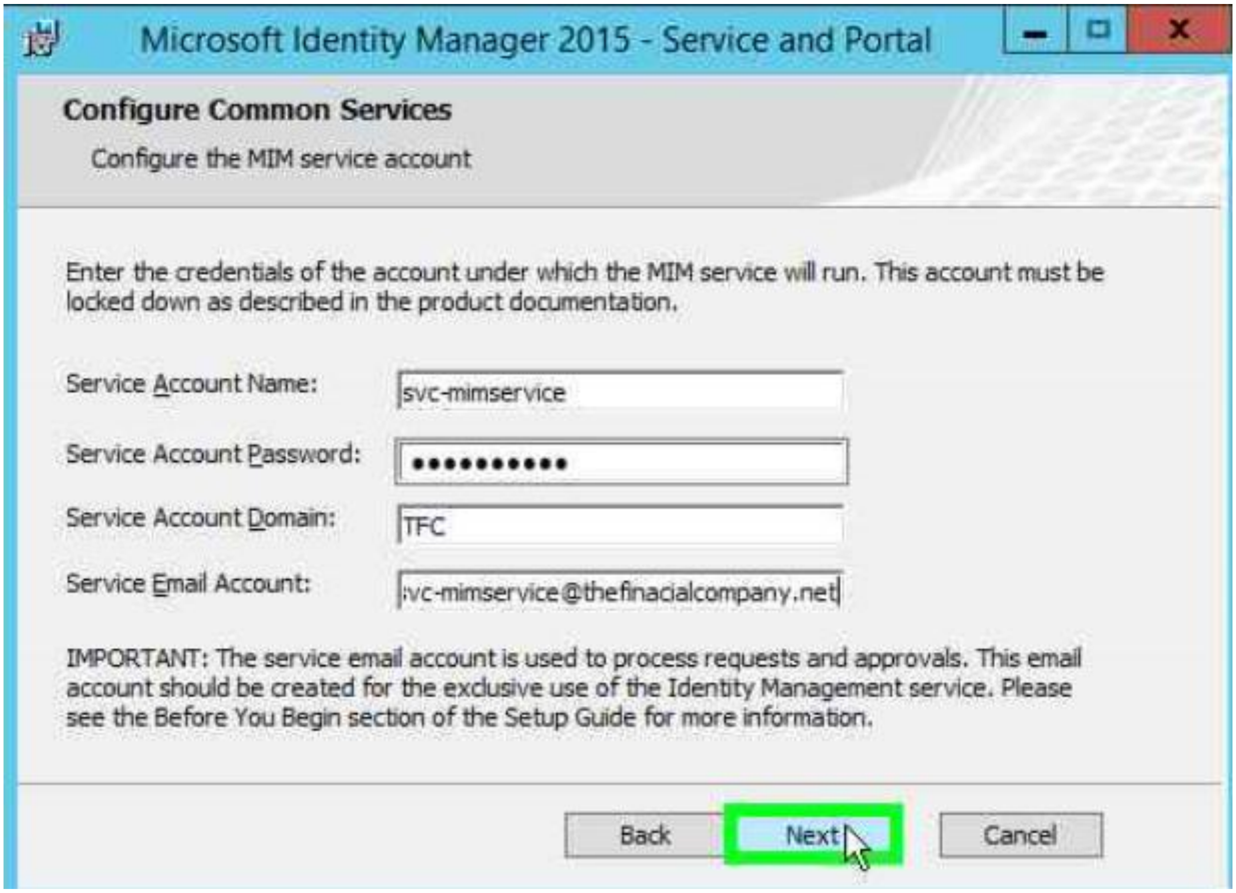
Configure Common Services

Configure service certificate

Please select the certificate the Service should use to allow clients to validate the Server.

○ Select a certificate located in the local certificate store

● Generate a new self-issued certificate
Certificate Name: Microsoft Identity Manager



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.

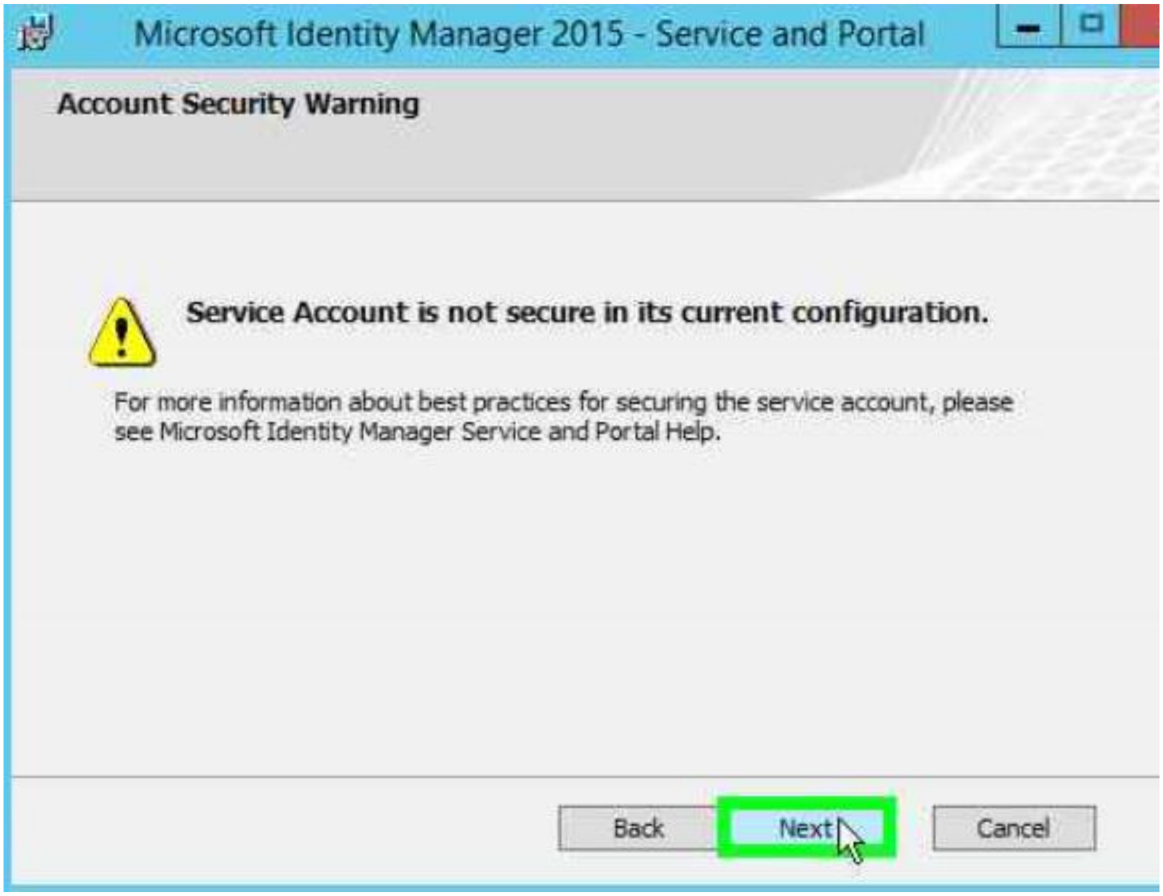
Service Account Name: svc-mimservice

Service Account Password: ●●●●●●●●●●●

Service Account Domain: TFC

Service Email Account: svc-mimservice@thefinacialcompany.net

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.

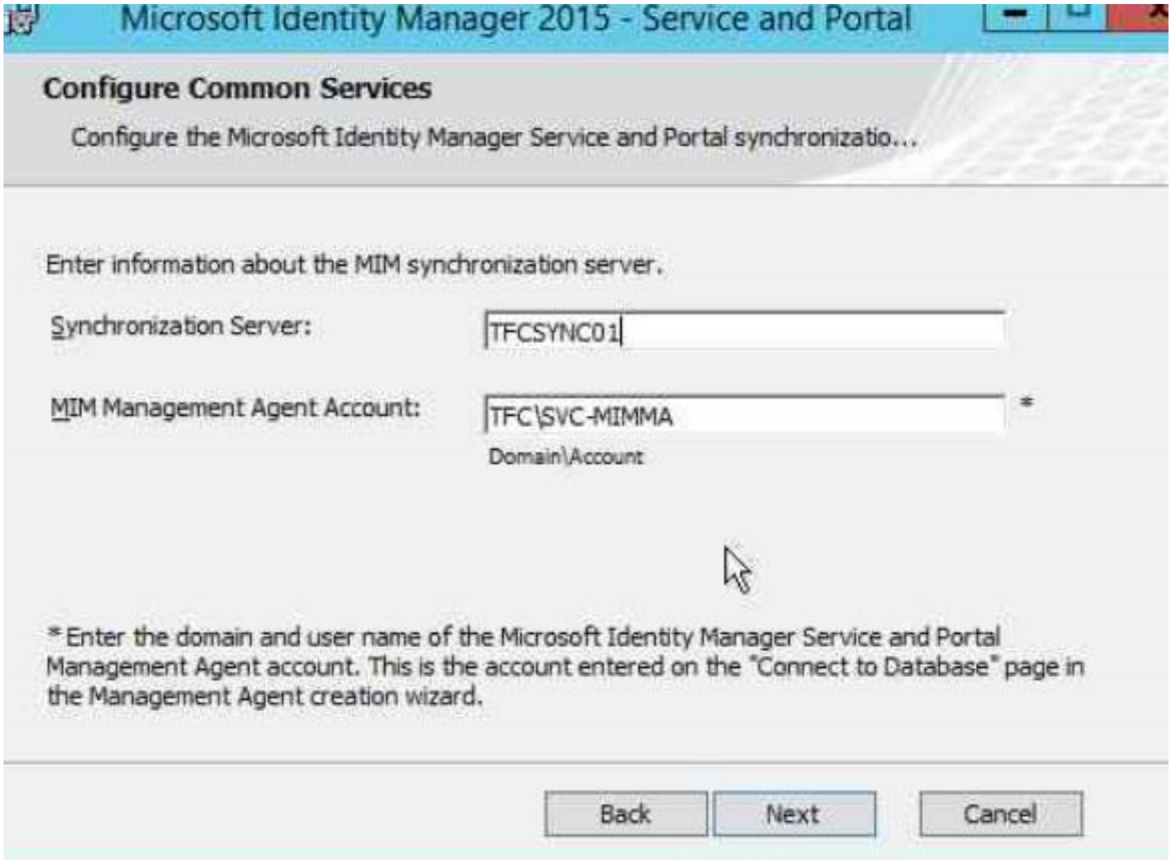


Microsoft Identity Manager 2015 - Service and Portal

Account Security Warning

Service Account is not secure in its current configuration.

For more information about best practices for securing the service account, please see Microsoft Identity Manager Service and Portal Help.



Microsoft Identity Manager 2015 - Service and Portal

Configure Common Services

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

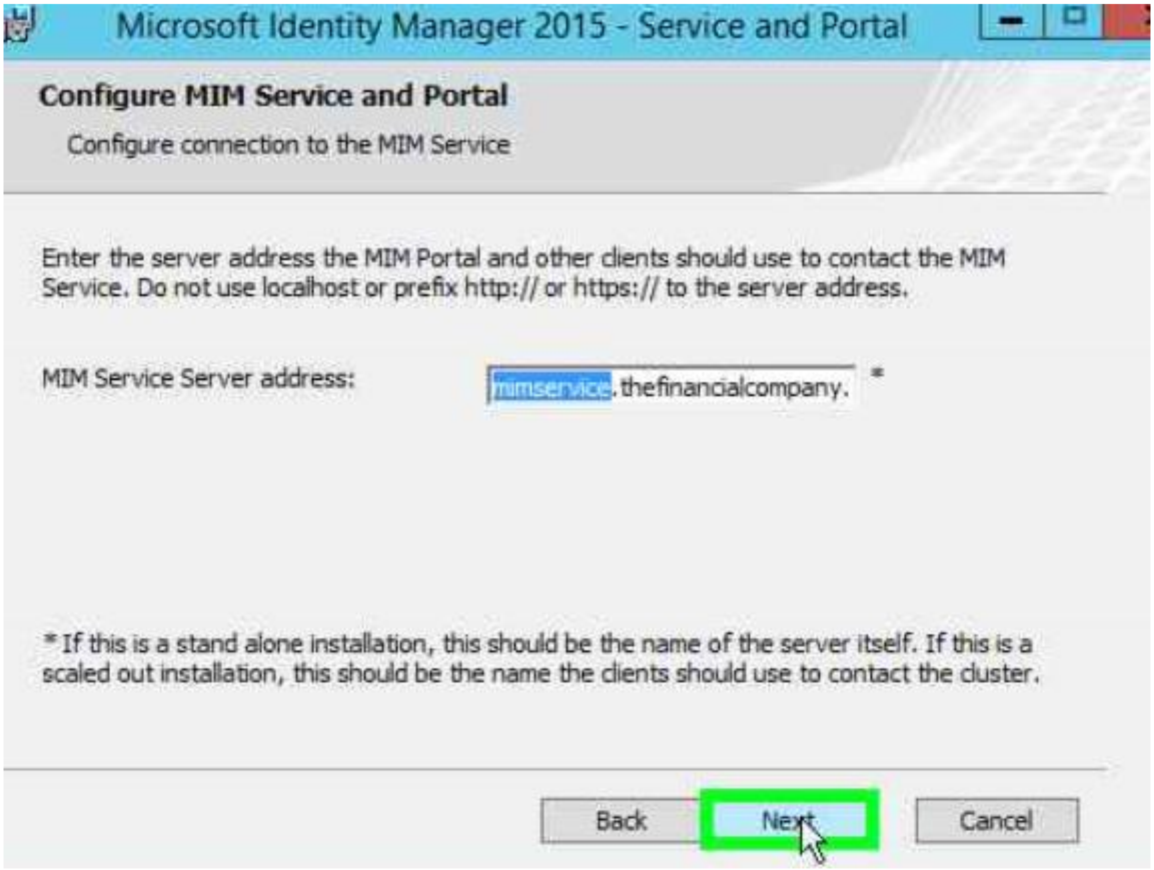
Enter information about the MIM synchronization server.

Synchronization Server: TFCSYNC01

MIM Management Agent Account: TFC\SVC-MIMMA *

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.



Microsoft Identity Manager 2015 - Service and Portal

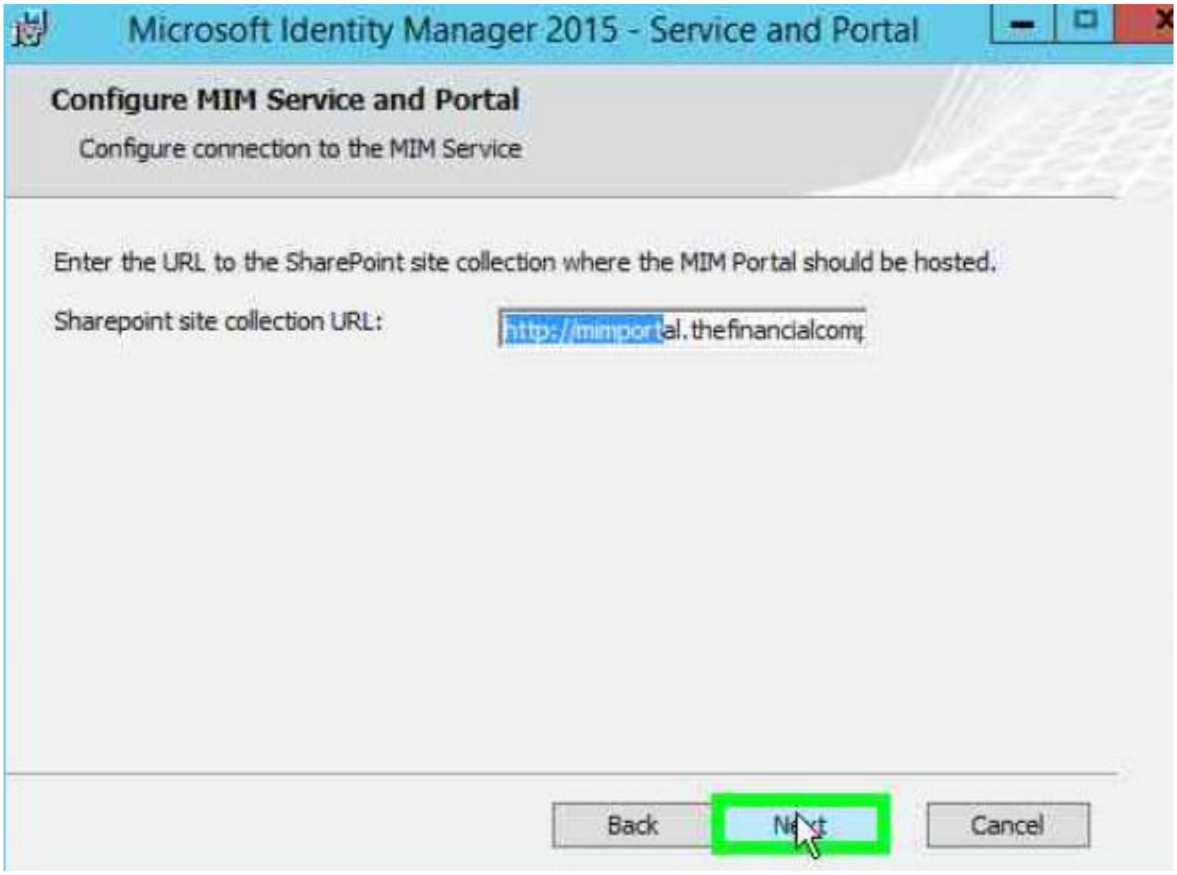
Configure MIM Service and Portal

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: mimservice.thefinancialcompany. *

* 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.

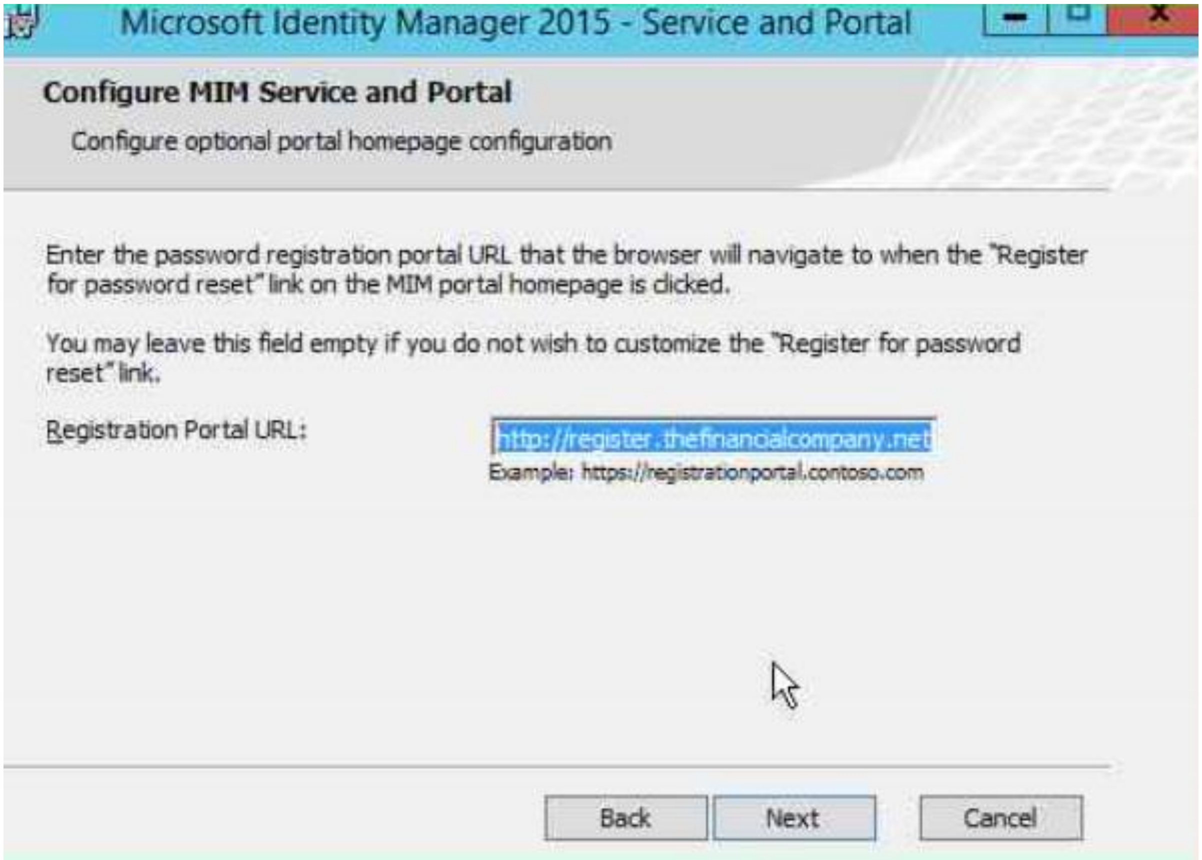


Configure MIM Service and Portal

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: http://mimportal.thefinancialcomp



Configure MIM Service and Portal

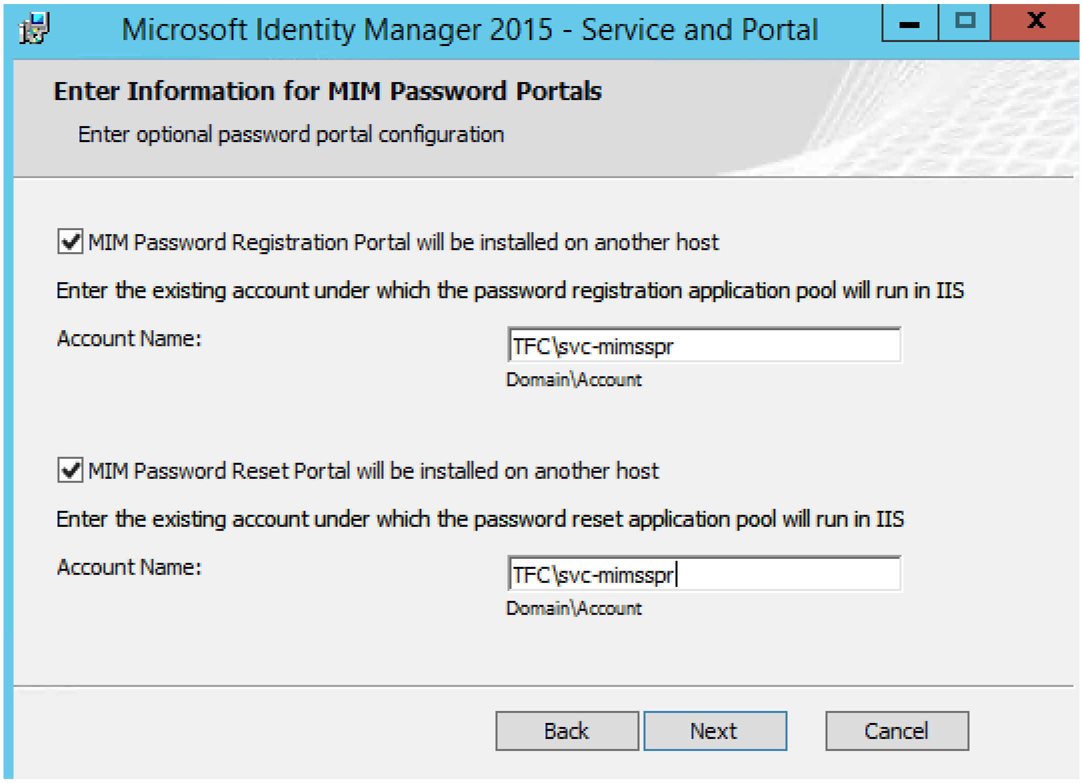
Configure optional portal homepage configuration

Enter the password registration portal URL that the browser will navigate to when the "Register for password reset" link on the MIM portal homepage is clicked.

You may leave this field empty if you do not wish to customize the "Register for password reset" link.

Registration Portal URL: http://register.thefinancialcompany.net

Example: https://registrationportal.contoso.com



Enter Information for MIM Password Portals

Enter optional password portal configuration

☑ MIM Password Registration Portal will be installed on another host

Enter the existing account under which the password registration application pool will run in IIS

Account Name: TFC\svc-mimsspr

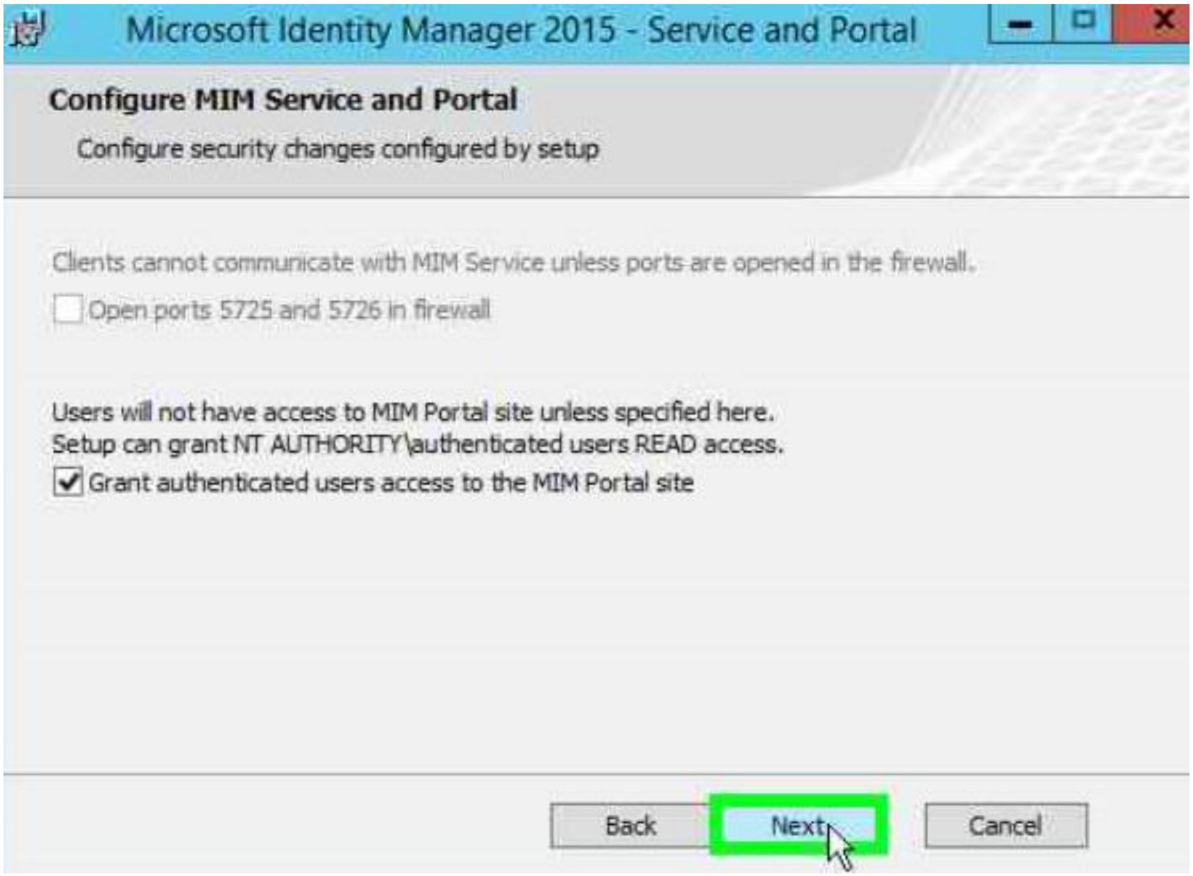
Domain\Account

☑ MIM Password Reset Portal will be installed on another host

Enter the existing account under which the password reset application pool will run in IIS

Account Name: TFC\svc-mimsspr

Domain\Account



Microsoft Identity Manager 2015 - Service and Portal

Configure MIM Service and Portal

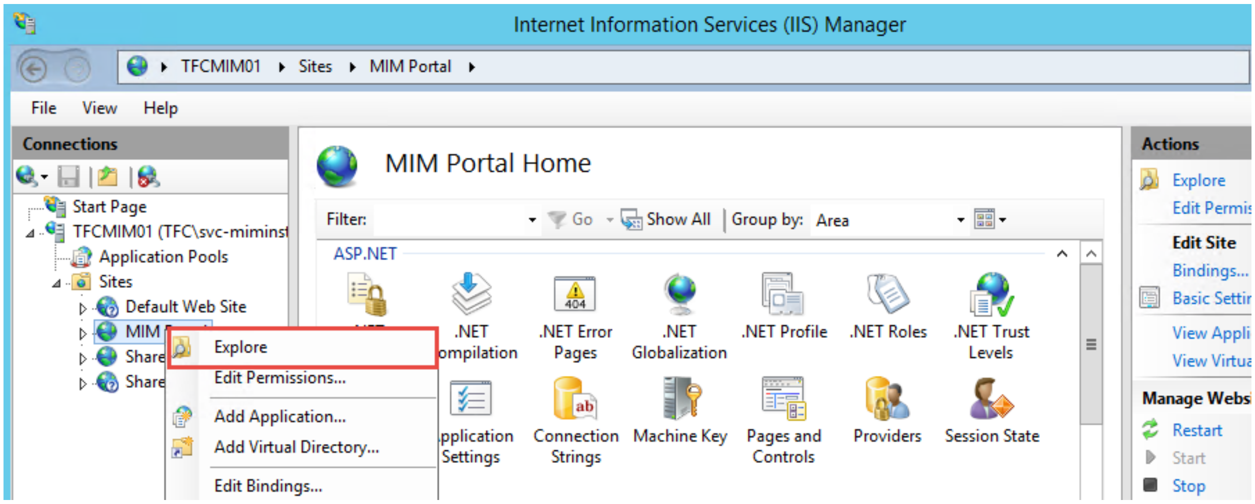
Configure security changes configured by setup

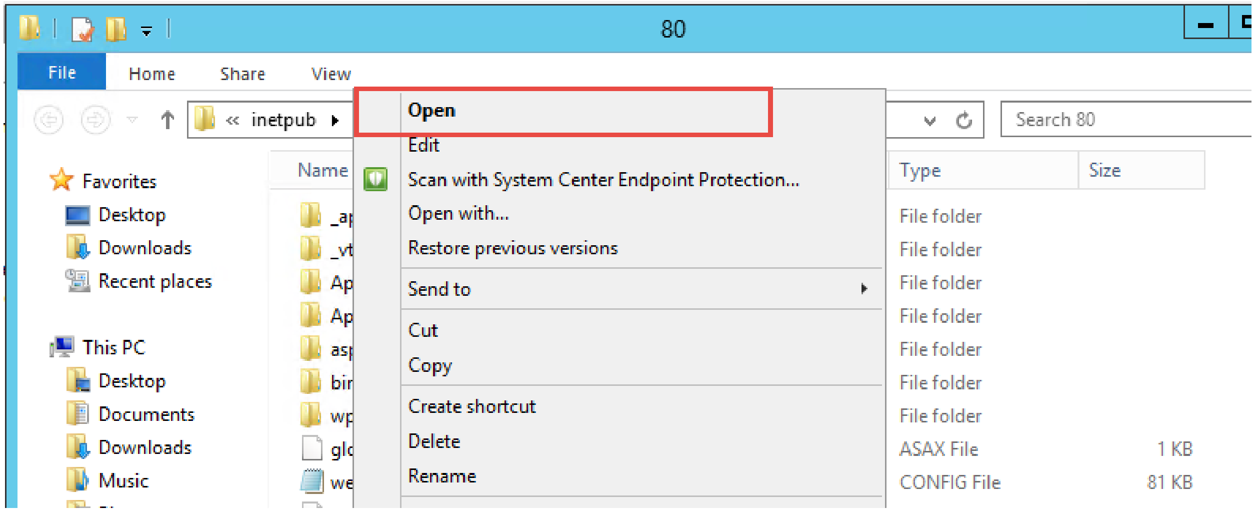
Clients cannot communicate with MIM Service unless ports are opened in the firewall.

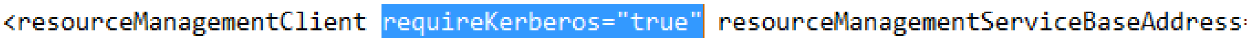
□ Open ports 5725 and 5726 in firewall

Users will not have access to MIM Portal site unless specified here.
Setup can grant NT AUTHORITY\authenticated users READ access.

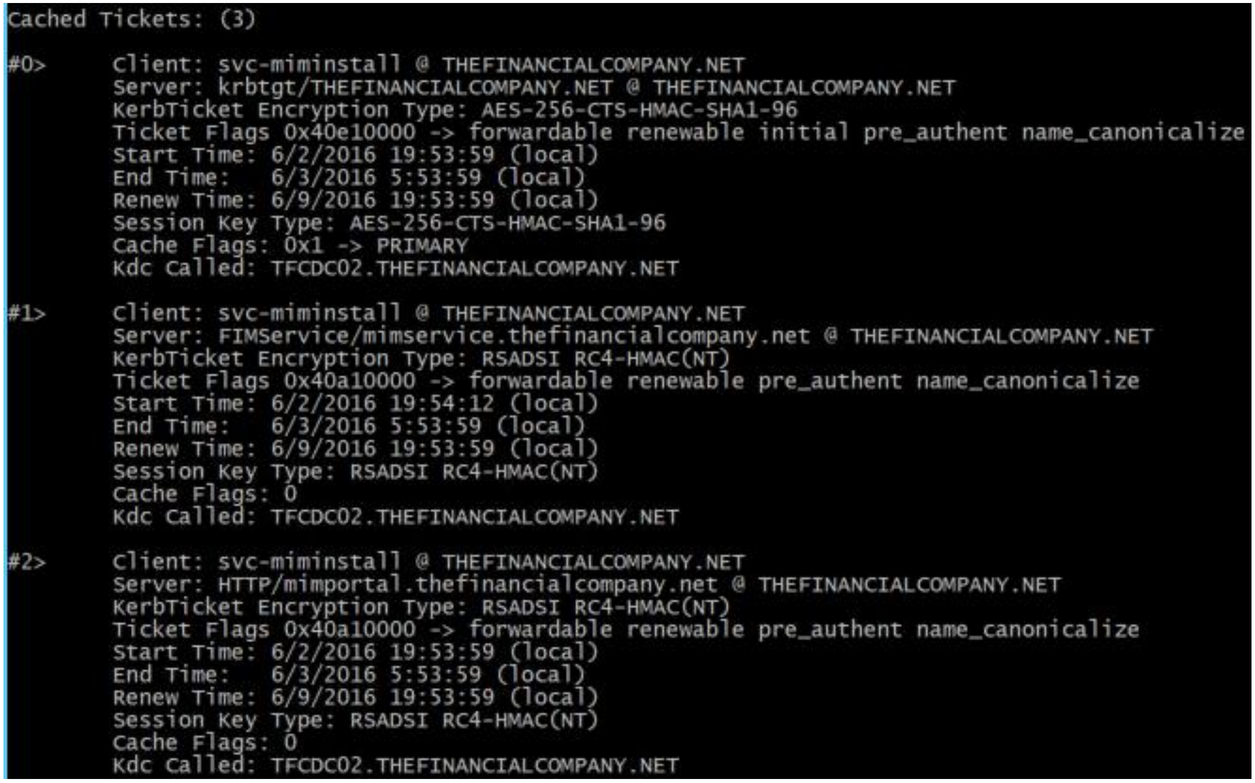
☑ Grant authenticated users access to the MIM Portal site



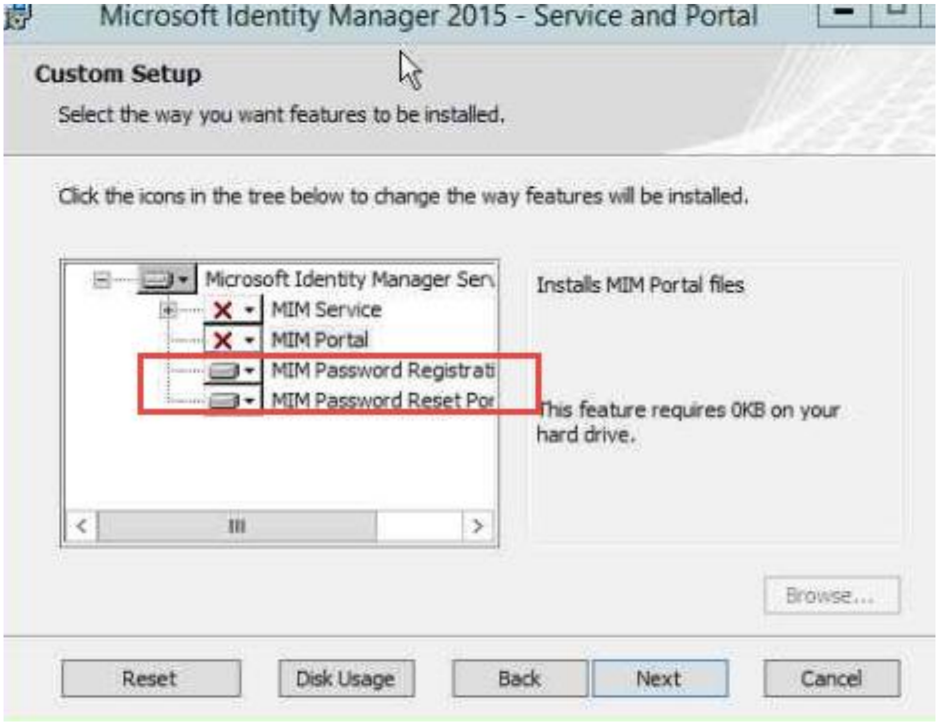




```
<resourceManagementClient requireKerberos="true" resourceManagementServiceBaseAddress=
```



```
Cached Tickets: (3)

#0>     Client: svc-miminstall @ THEFINANCIALCOMPANY.NET
        Server: krbtgt/THEFINANCIALCOMPANY.NET @ THEFINANCIALCOMPANY.NET
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
        Start Time: 6/2/2016 19:53:59 (local)
        End Time:   6/3/2016 5:53:59 (local)
        Renew Time: 6/9/2016 19:53:59 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called: TFCDC02.THEFINANCIALCOMPANY.NET

#1>     Client: svc-miminstall @ THEFINANCIALCOMPANY.NET
        Server: FIMService/mimservice.thefinancialcompany.net @ THEFINANCIALCOMPANY.NET
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
        Start Time: 6/2/2016 19:54:12 (local)
        End Time:   6/3/2016 5:53:59 (local)
        Renew Time: 6/9/2016 19:53:59 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0
        Kdc Called: TFCDC02.THEFINANCIALCOMPANY.NET

#2>     Client: svc-miminstall @ THEFINANCIALCOMPANY.NET
        Server: HTTP/mimportal.thefinancialcompany.net @ THEFINANCIALCOMPANY.NET
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
        Start Time: 6/2/2016 19:53:59 (local)
        End Time:   6/3/2016 5:53:59 (local)
        Renew Time: 6/9/2016 19:53:59 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0
        Kdc Called: TFCDC02.THEFINANCIALCOMPANY.NET
```


Microsoft Identity Manager 2015 - Service and Portal

Custom Setup

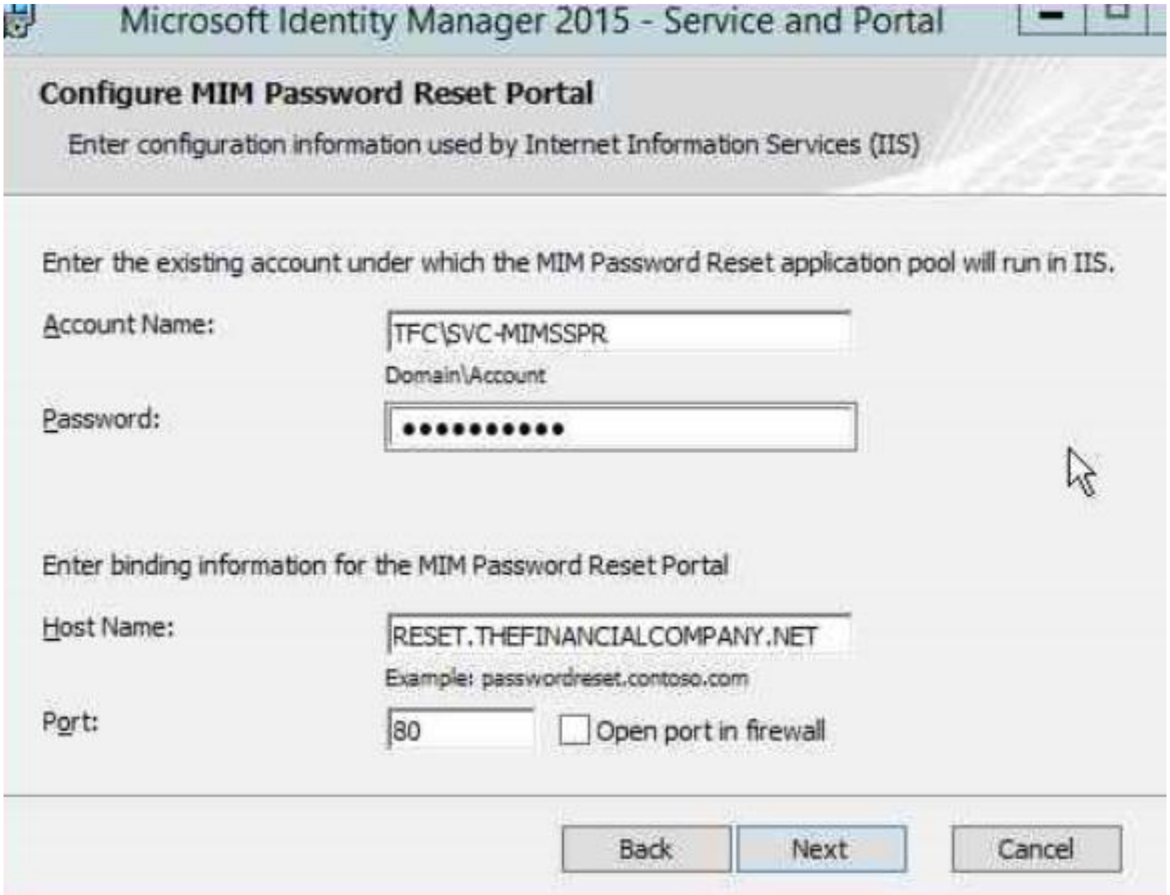
Select the way you want features to be installed.

Click the icons in the tree below to change the way features will be installed.

- Microsoft Identity Manager Serv
  - ☒ MIM Service
  - ☒ MIM Portal
  - MIM Password Registrati
  - MIM Password Reset Por

Installs MIM Portal files

This feature requires 0KB on your hard drive.


Microsoft Identity Manager 2015 - Service and Portal

Configure MIM Password Reset Portal

Enter configuration information used by Internet Information Services (IIS)

Enter the existing account under which the MIM Password Reset application pool will run in IIS.

Account Name: TFC\SVC-MIMSSPR

Domain\Account

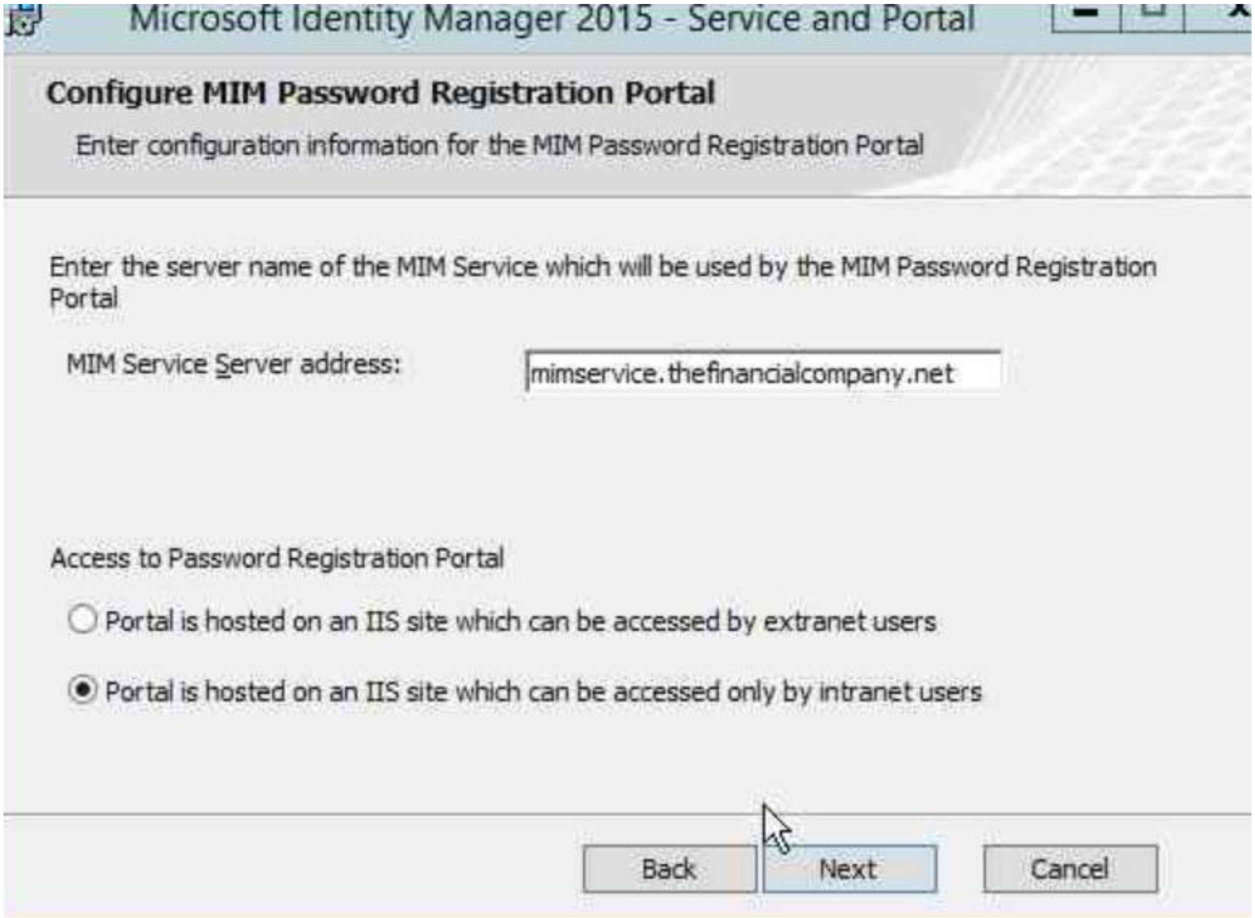
Password: ●●●●●●●●●●●

Enter binding information for the MIM Password Reset Portal

Host Name: RESET.THEFINANCIALCOMPANY.NET

Example: passwordreset.contoso.com

Port: 80 □ Open port in firewall



Configure MIM Password Registration Portal

Enter configuration information for the MIM Password Registration Portal

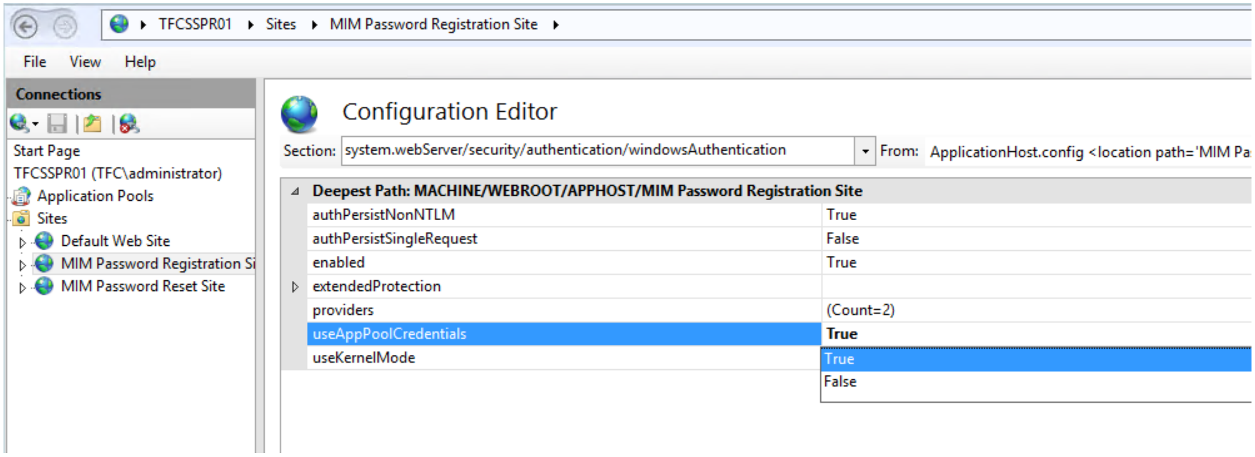
Enter the server name of the MIM Service which will be used by the MIM Password Registration Portal

MIM Service Server address: mimservice.thefinancialcompany.net

Access to Password Registration Portal

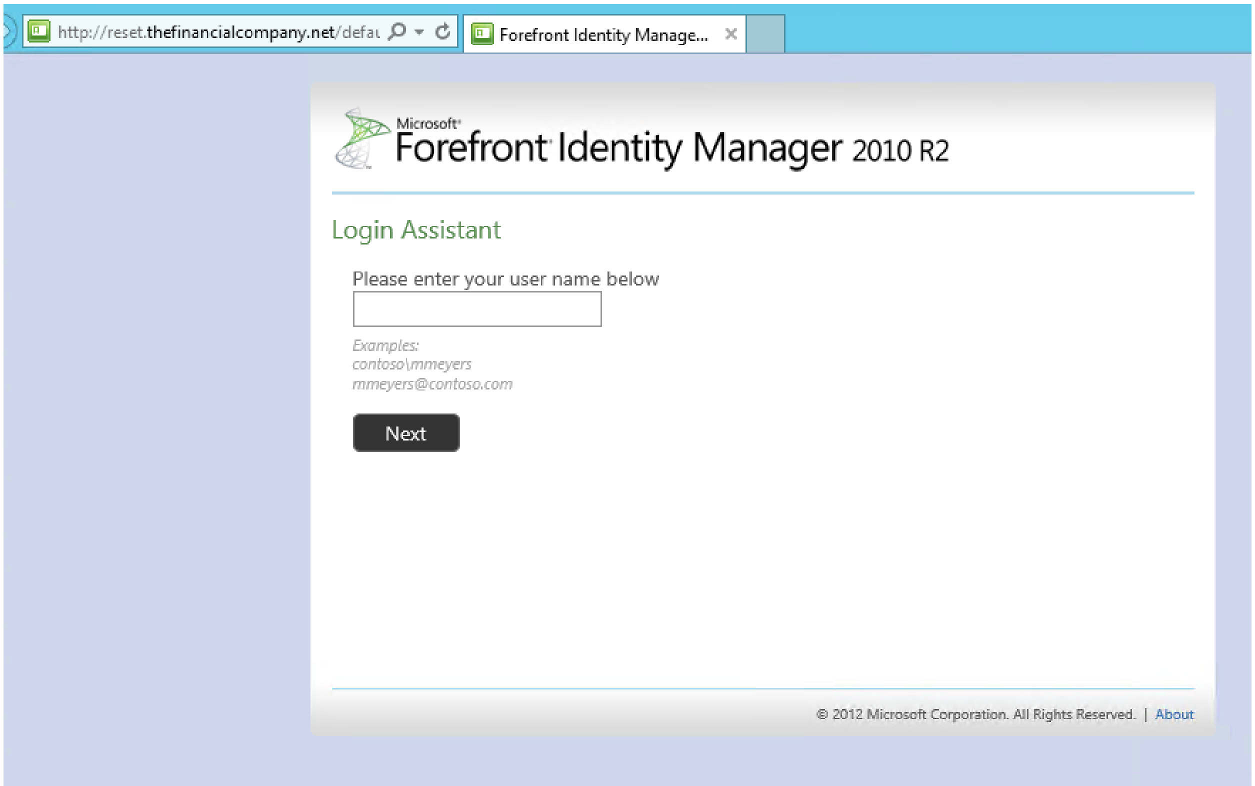
○ Portal is hosted on an IIS site which can be accessed by extranet users

● Portal is hosted on an IIS site which can be accessed only by intranet users



Section: system.webServer/security/authentication/windowsAuthentication From: ApplicationHost.config <location path='MIM Pa

Deepest Path: MACHINE/WEBROOT/APPHOST/MIM Password Registration Site	
authPersistNonNTLM	True
authPersistSingleRequest	False
enabled	True
extendedProtection	
providers	(Count=2)
useAppPoolCredentials	**True**
useKernelMode	True False


http://reset.thefinancialcompany.net/defau
Forefront Identity Manage...

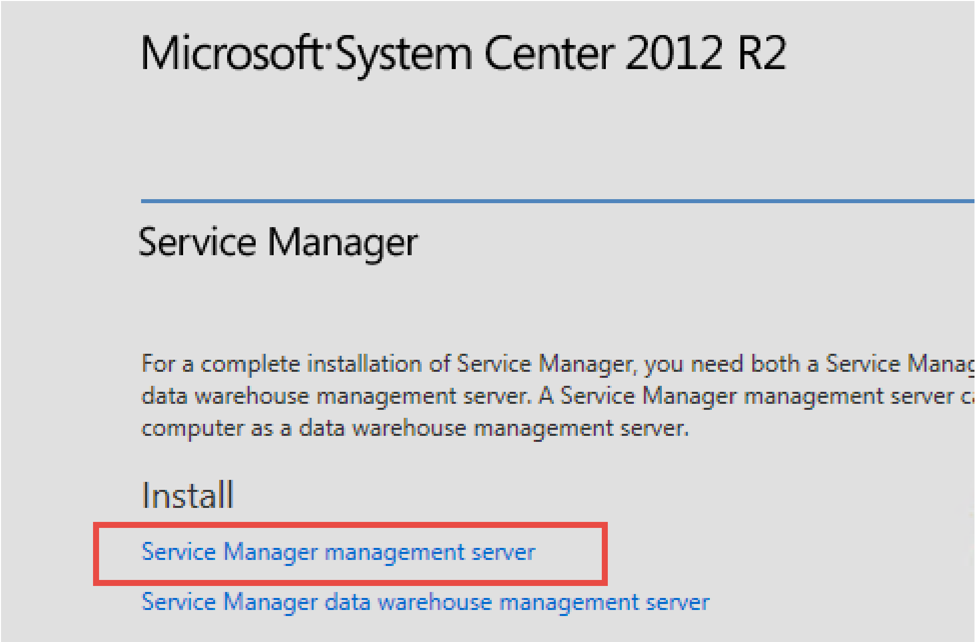
Microsoft® Forefront® Identity Manager 2010 R2

Login Assistant

Please enter your user name below

Examples:
contoso\mmeyers
mmeyers@contoso.com

© 2012 Microsoft Corporation. All Rights Reserved. | About



Microsoft® System Center 2012 R2

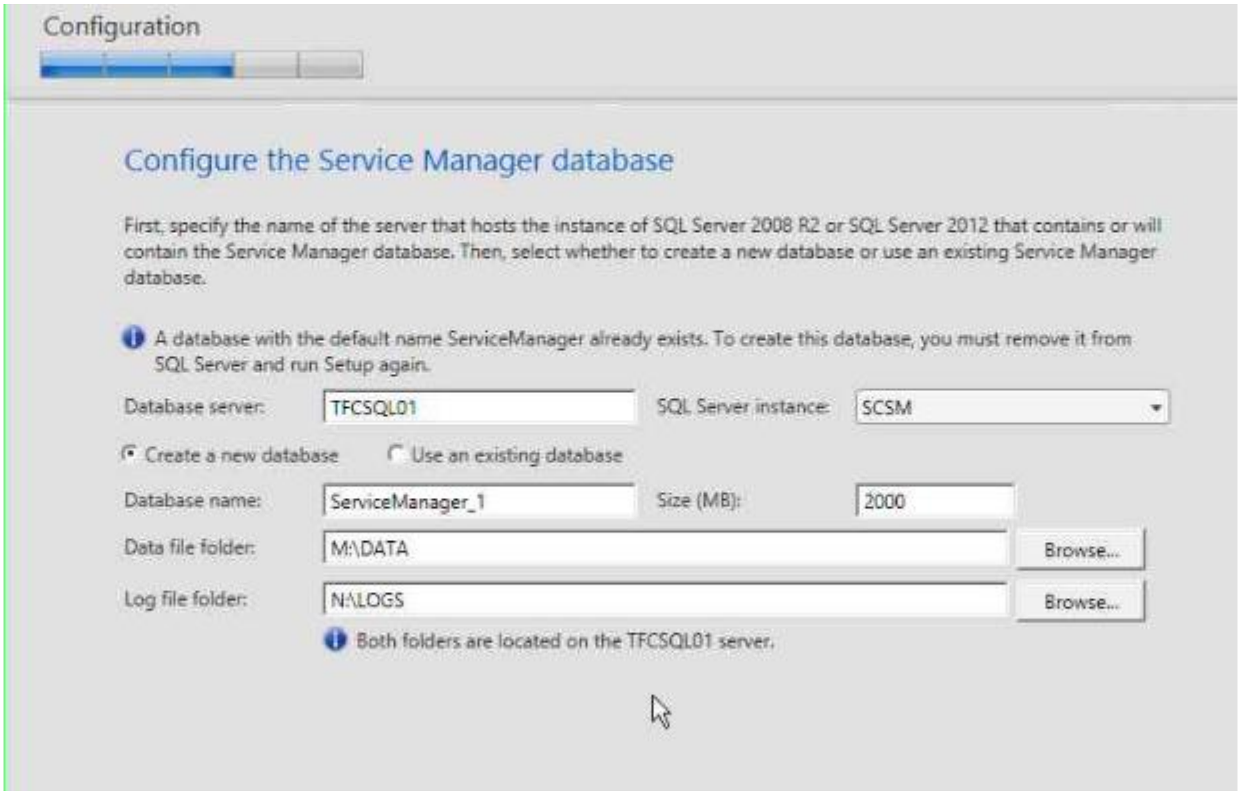
Service Manager

For a complete installation of Service Manager, you need both a Service Manag
data warehouse management server. A Service Manager management server c
computer as a data warehouse management server.

Install

Service Manager management server

Service Manager data warehouse management server



Configuration

Configure the Service Manager database

First, specify the name of the server that hosts the instance of SQL Server 2008 R2 or SQL Server 2012 that contains or will contain the Service Manager database. Then, select whether to create a new database or use an existing Service Manager database.

A database with the default name ServiceManager already exists. To create this database, you must remove it from SQL Server and run Setup again.

Database server: TFCSQL01 SQL Server instance: SCSM

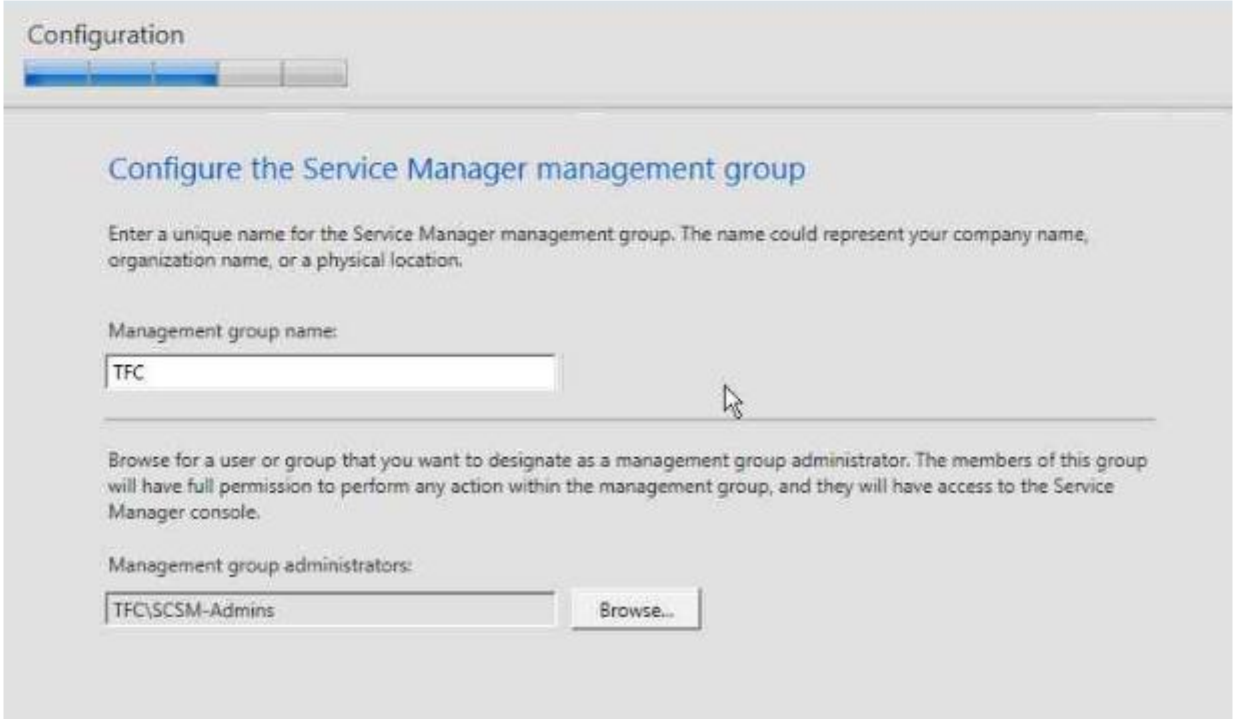
● Create a new database ○ Use an existing database

Database name: ServiceManager_1 Size (MB): 2000

Data file folder: M:\DATA

Log file folder: N:\LOGS

Both folders are located on the TFCSQL01 server.



Configuration

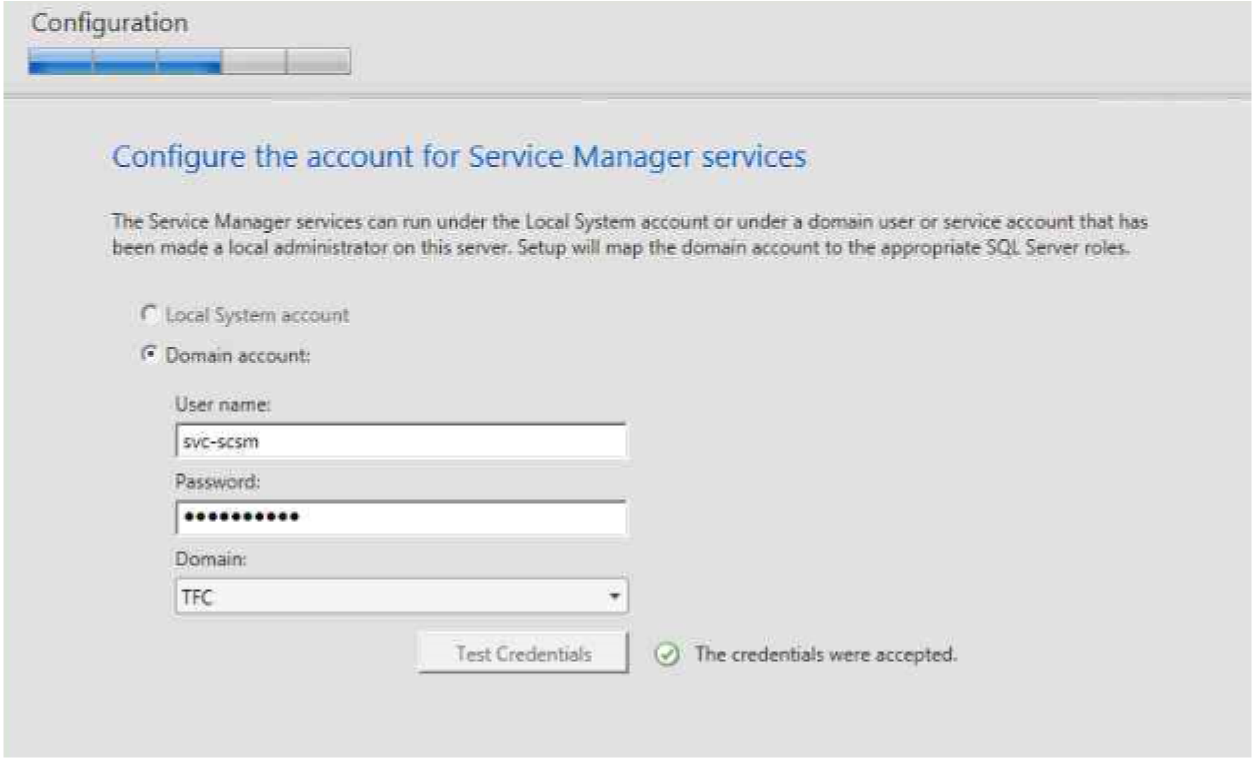
Configure the Service Manager management group

Enter a unique name for the Service Manager management group. The name could represent your company name, organization name, or a physical location.

Management group name: TFC

Browse for a user or group that you want to designate as a management group administrator. The members of this group will have full permission to perform any action within the management group, and they will have access to the Service Manager console.

Management group administrators: TFC\SCSM-Admins



Configure the account for Service Manager services

The Service Manager services can run under the Local System account or under a domain user or service account that has been made a local administrator on this server. Setup will map the domain account to the appropriate SQL Server roles.

○ Local System account

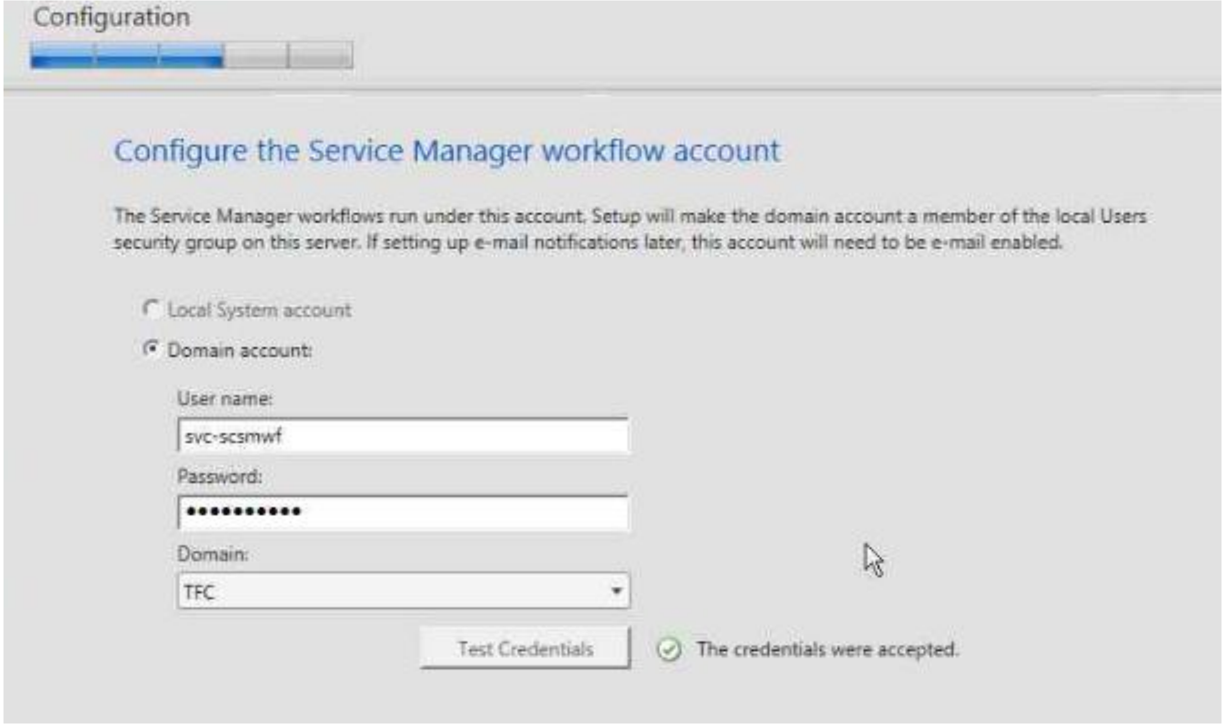
● Domain account:

User name: svc-scsm

Password: ●●●●●●●●●●●

Domain: TFC

✓ The credentials were accepted.



Configure the Service Manager workflow account

The Service Manager workflows run under this account. Setup will make the domain account a member of the local Users security group on this server. If setting up e-mail notifications later, this account will need to be e-mail enabled.

○ Local System account

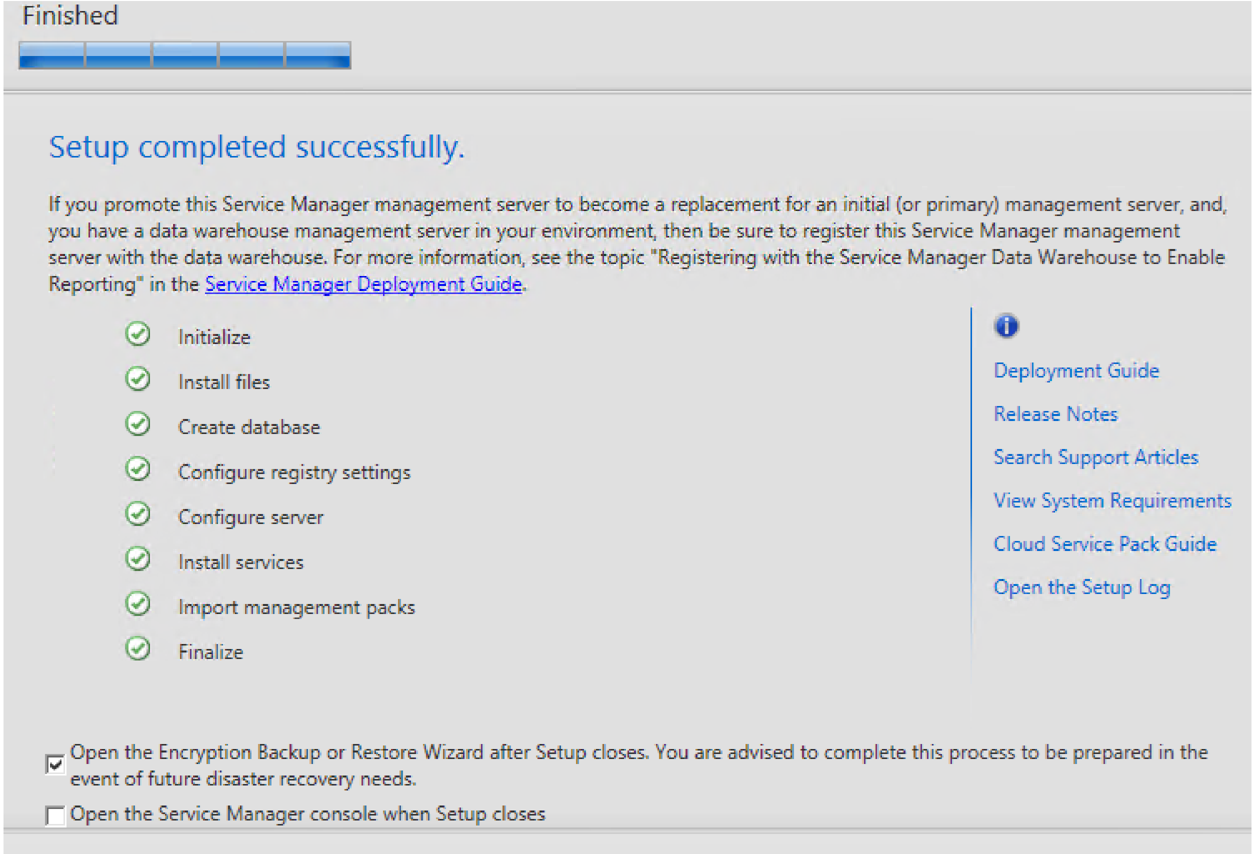
● Domain account:

User name: svc-scsmwf

Password: ●●●●●●●●●●●

Domain: TFC

✓ The credentials were accepted.



Finished

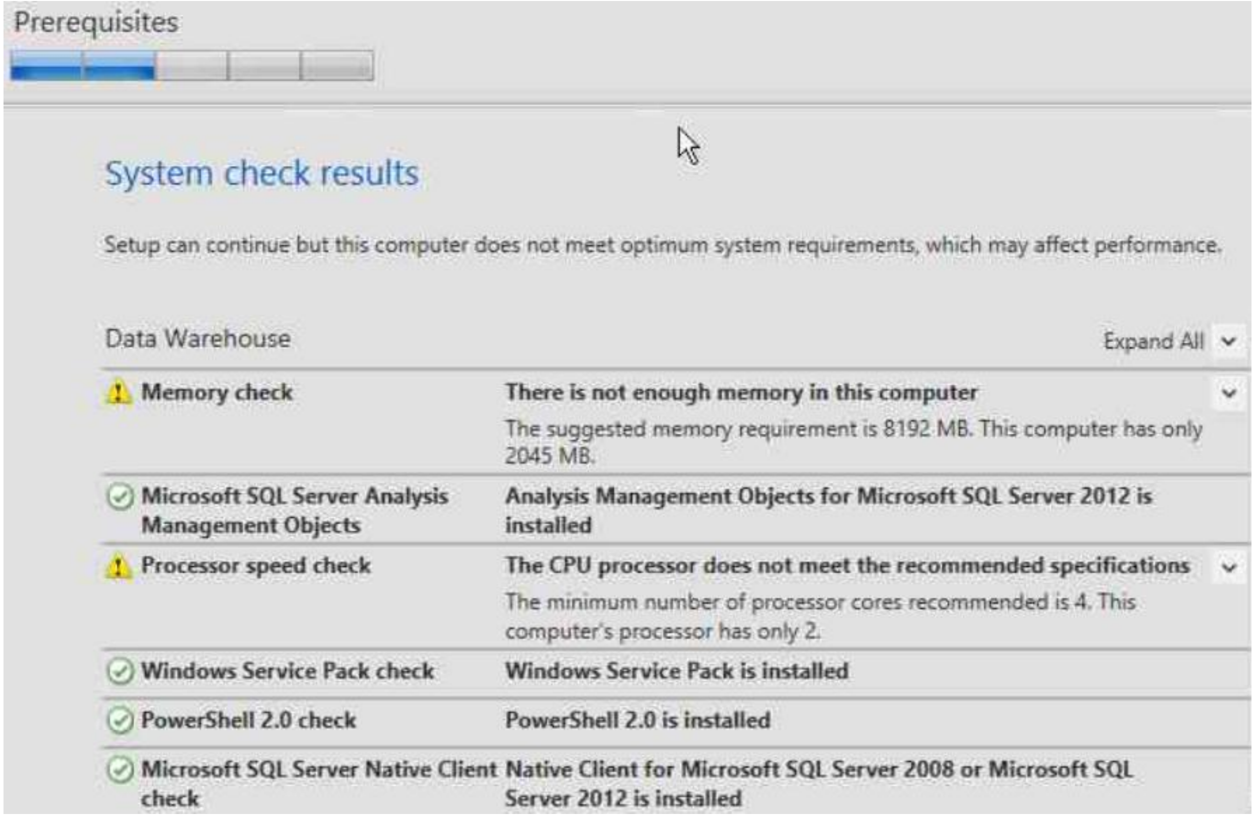
Setup completed successfully.

If you promote this Service Manager management server to become a replacement for an initial (or primary) management server, and, you have a data warehouse management server in your environment, then be sure to register this Service Manager management server with the data warehouse. For more information, see the topic "Registering with the Service Manager Data Warehouse to Enable Reporting" in the Service Manager Deployment Guide.

- ✓ Initialize
- ✓ Install files
- ✓ Create database
- ✓ Configure registry settings
- ✓ Configure server
- ✓ Install services
- ✓ Import management packs
- ✓ Finalize

☑ Open the Encryption Backup or Restore Wizard after Setup closes. You are advised to complete this process to be prepared in the event of future disaster recovery needs.

□ Open the Service Manager console when Setup closes



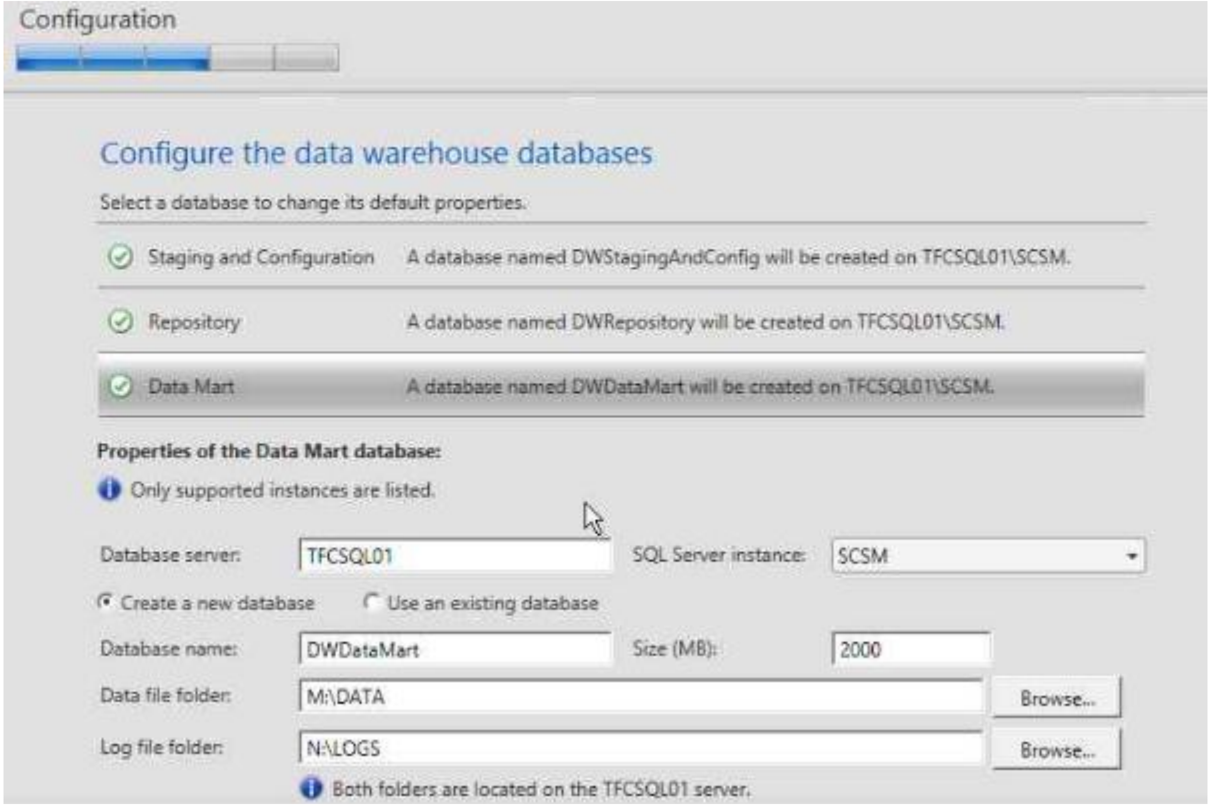
Prerequisites

System check results

Setup can continue but this computer does not meet optimum system requirements, which may affect performance.

Data Warehouse Expand All

⚠ **Memory check**	**There is not enough memory in this computer** The suggested memory requirement is 8192 MB. This computer has only 2045 MB.
✓ **Microsoft SQL Server Analysis Management Objects**	**Analysis Management Objects for Microsoft SQL Server 2012 is installed**
⚠ **Processor speed check**	**The CPU processor does not meet the recommended specifications** The minimum number of processor cores recommended is 4. This computer's processor has only 2.
✓ **Windows Service Pack check**	**Windows Service Pack is installed**
✓ **PowerShell 2.0 check**	**PowerShell 2.0 is installed**
✓ **Microsoft SQL Server Native Client check**	**Native Client for Microsoft SQL Server 2008 or Microsoft SQL Server 2012 is installed**



Configuration

Configure the data warehouse databases

Select a database to change its default properties.

✓ Staging and Configuration	A database named DWStagingAndConfig will be created on TFCSQL01\SCSM.
✓ Repository	A database named DWRepository will be created on TFCSQL01\SCSM.
✓ Data Mart	A database named DWDataMart will be created on TFCSQL01\SCSM.

Properties of the Data Mart database:

Only supported instances are listed.

Database server: TFCSQL01   SQL Server instance: SCSM

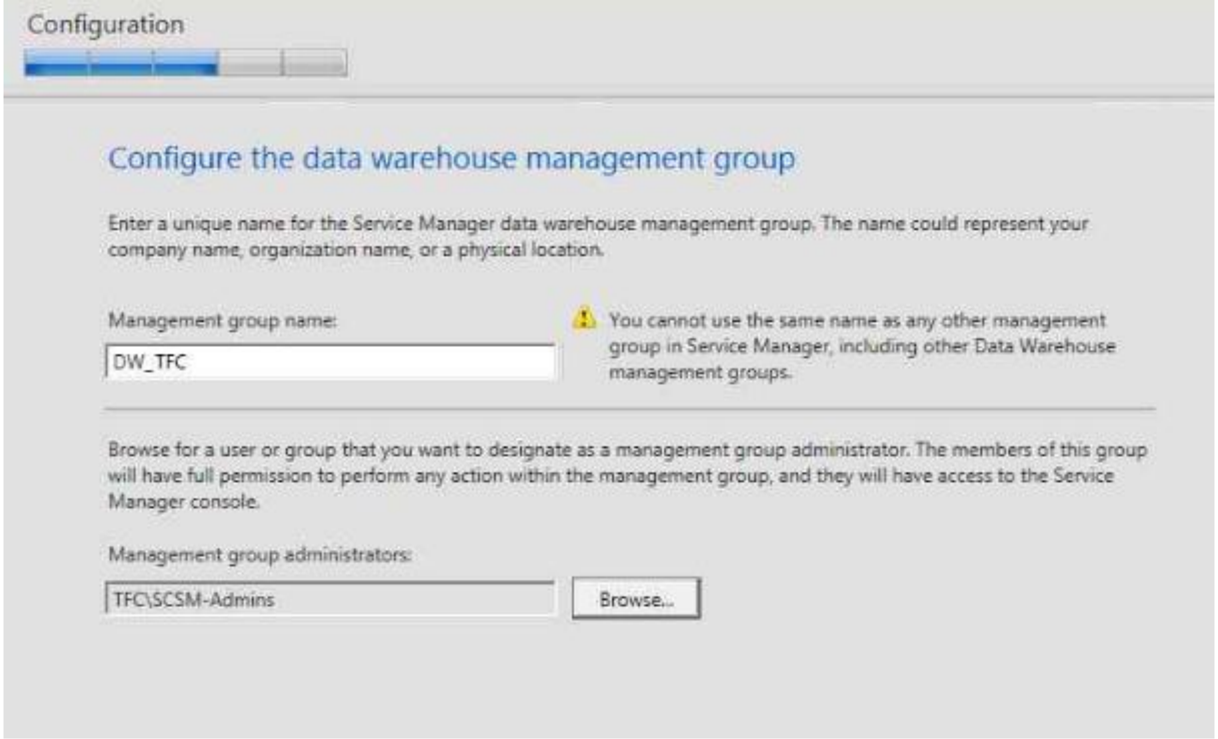
● Create a new database   ○ Use an existing database

Database name: DWDataMart   Size (MB): 2000

Data file folder: M:\DATA

Log file folder: N:\LOGS

Both folders are located on the TFCSQL01 server.



Configuration

Configure the data warehouse management group

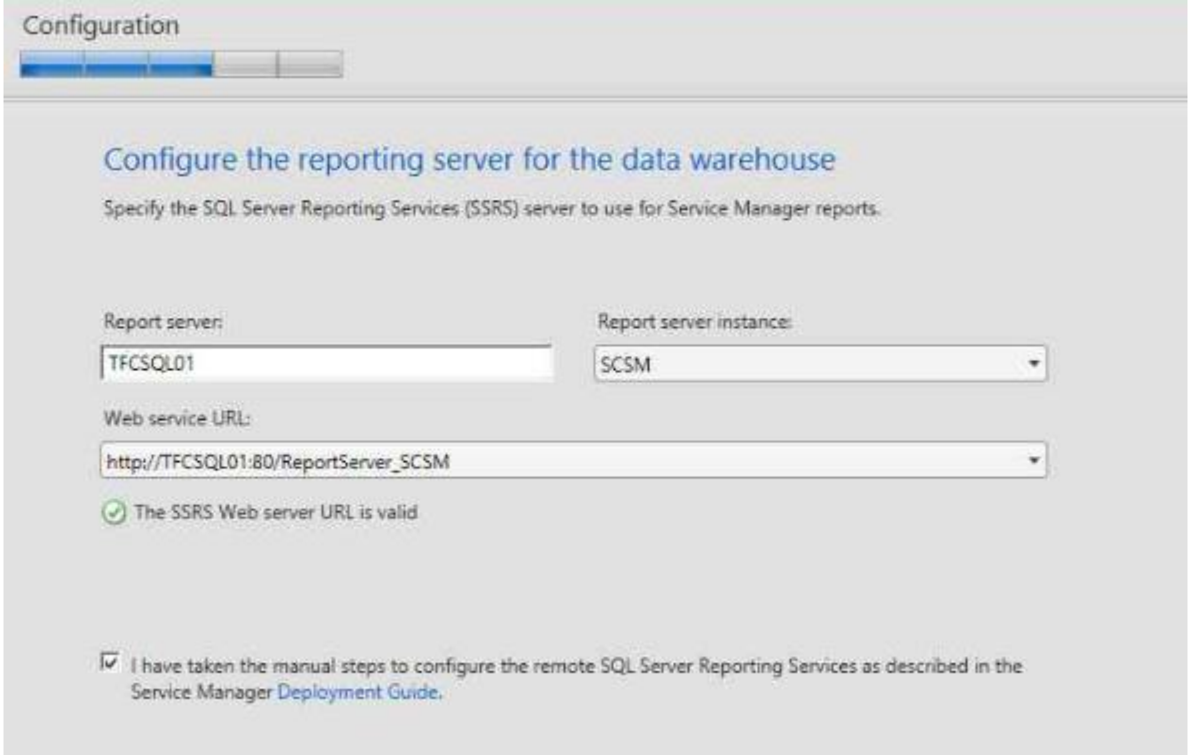
Enter a unique name for the Service Manager data warehouse management group. The name could represent your company name, organization name, or a physical location.

Management group name: DW_TFC

You cannot use the same name as any other management group in Service Manager, including other Data Warehouse management groups.

Browse for a user or group that you want to designate as a management group administrator. The members of this group will have full permission to perform any action within the management group, and they will have access to the Service Manager console.

Management group administrators: TFC\SCSM-Admins



Configuration

Configure the reporting server for the data warehouse

Specify the SQL Server Reporting Services (SSRS) server to use for Service Manager reports.

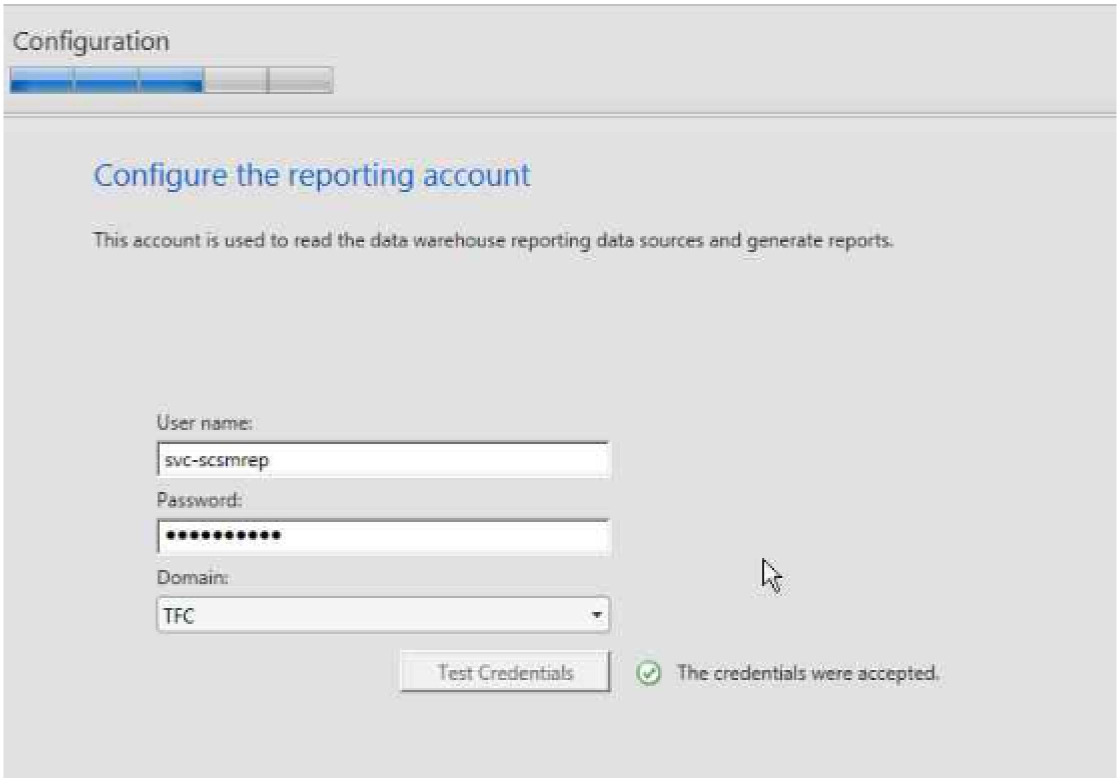
Report server: TFCSQL01

Report server instance: SCSM

Web service URL: http://TFCSQL01:80/ReportServer_SCSM

✓ The SSRS Web server URL is valid

☑ I have taken the manual steps to configure the remote SQL Server Reporting Services as described in the Service Manager Deployment Guide.



Configuration

Configure the reporting account

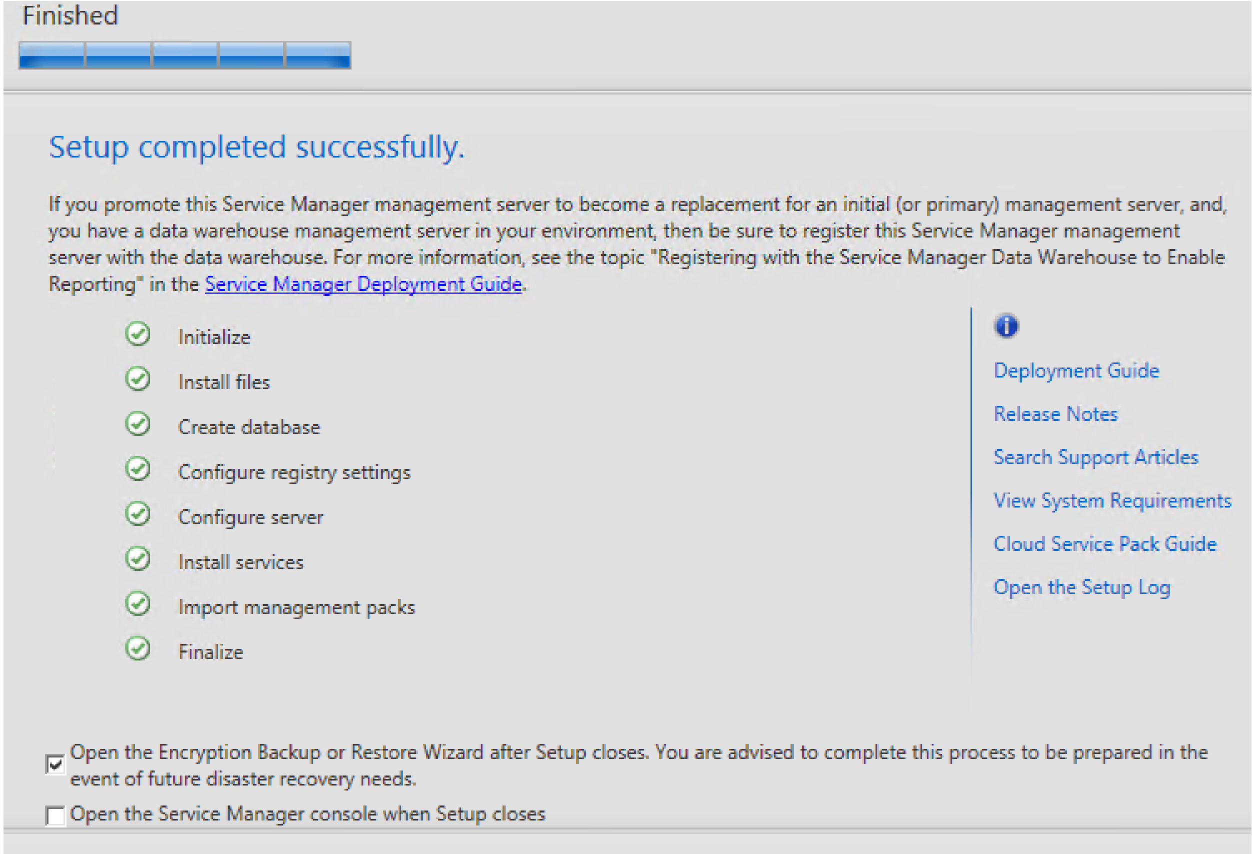
This account is used to read the data warehouse reporting data sources and generate reports.

User name: svc-scsmrep

Password: ●●●●●●●●●●●

Domain: TFC

✓ The credentials were accepted.



Finished

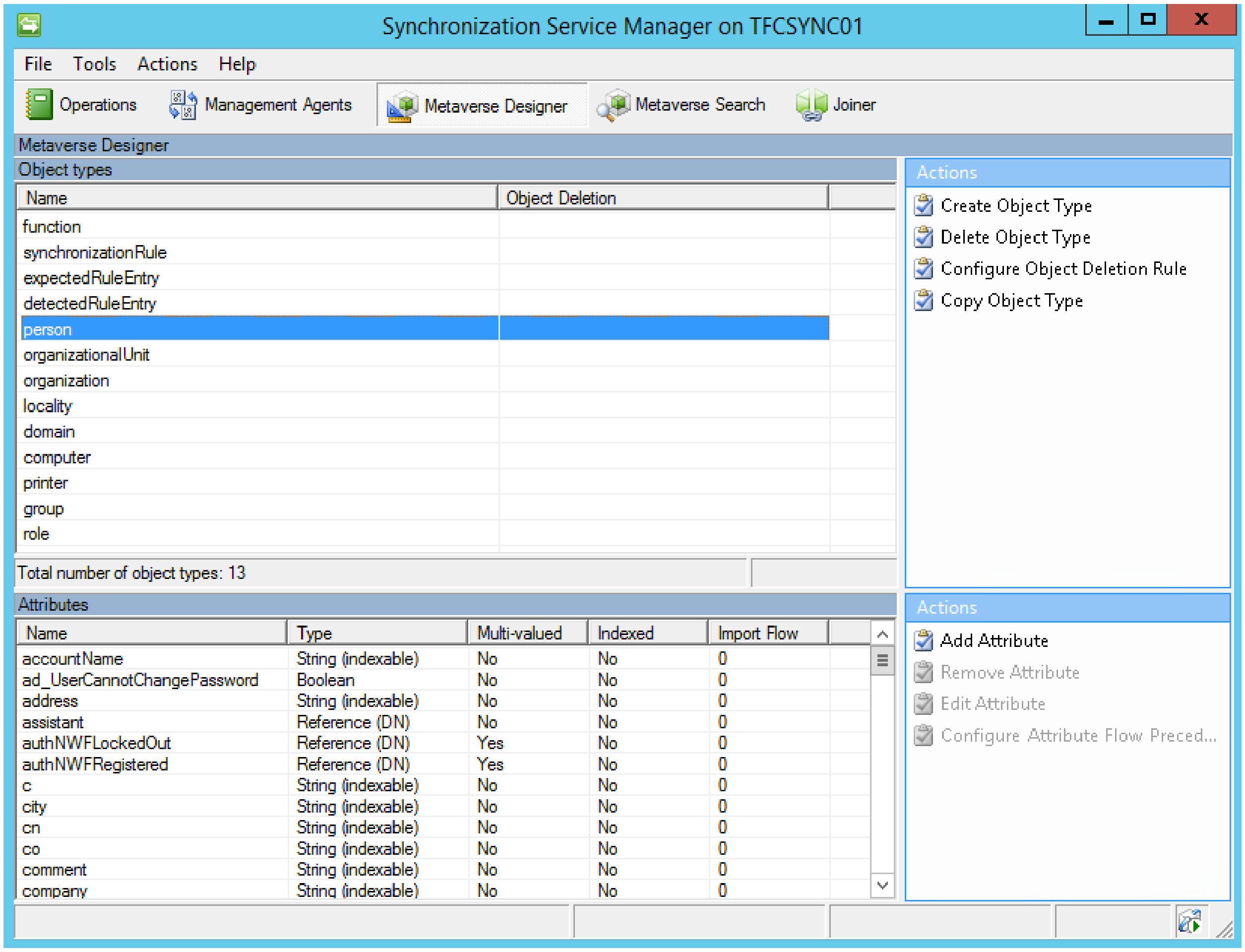
Setup completed successfully.

If you promote this Service Manager management server to become a replacement for an initial (or primary) management server, and, you have a data warehouse management server in your environment, then be sure to register this Service Manager management server with the data warehouse. For more information, see the topic "Registering with the Service Manager Data Warehouse to Enable Reporting" in the Service Manager Deployment Guide.

- ✓ Initialize
- ✓ Install files
- ✓ Create database
- ✓ Configure registry settings
- ✓ Configure server
- ✓ Install services
- ✓ Import management packs
- ✓ Finalize

☑ Open the Encryption Backup or Restore Wizard after Setup closes. You are advised to complete this process to be prepared in the event of future disaster recovery needs.

□ Open the Service Manager console when Setup closes



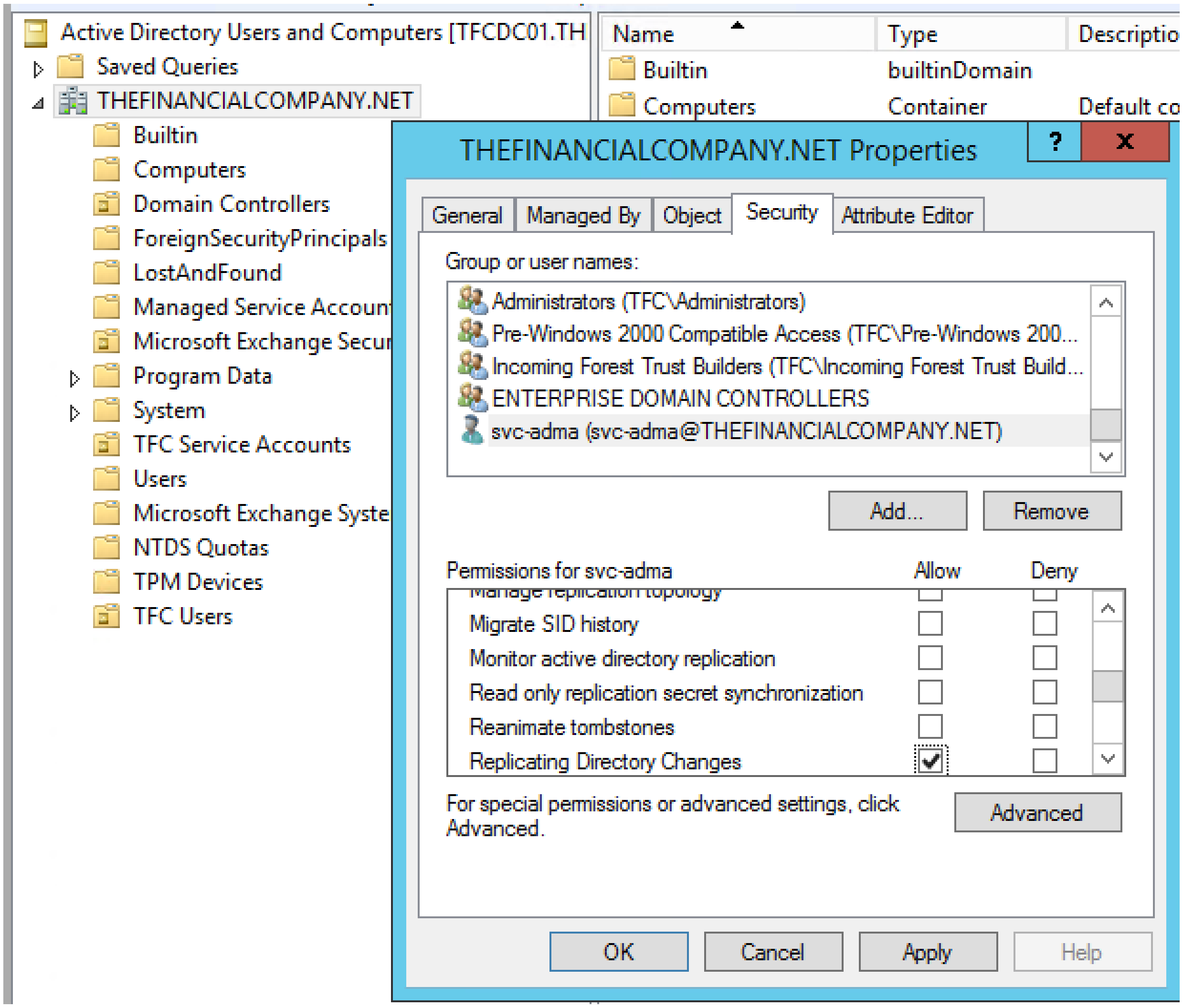
Object types

Name	Object Deletion
function	
synchronizationRule	
expectedRuleEntry	
detectedRuleEntry	
person	
organizationalUnit	
organization	
locality	
domain	
computer	
printer	
group	
role	

Total number of object types: 13

Attributes

Name	Type	Multi-valued	Indexed	Import Flow
accountName	String (indexable)	No	No	0
ad_UserCannotChangePassword	Boolean	No	No	0
address	String (indexable)	No	No	0
assistant	Reference (DN)	No	No	0
authNWFLockedOut	Reference (DN)	Yes	No	0
authNWFRegistered	Reference (DN)	Yes	No	0
c	String (indexable)	No	No	0
city	String (indexable)	No	No	0
cn	String (indexable)	No	No	0
co	String (indexable)	No	No	0
comment	String (indexable)	No	No	0
company	String (indexable)	No	No	0



Active Directory Users and Computers [TFCDC01.TH

- Saved Queries
- THEFINANCIALCOMPANY.NET
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - LostAndFound
  - Managed Service Accoun
  - Microsoft Exchange Secu
  - Program Data
  - System
  - TFC Service Accounts
  - Users
  - Microsoft Exchange Syste
  - NTDS Quotas
  - TPM Devices
  - TFC Users

Name	Type	Descriptio
Builtin	builtinDomain	
Computers	Container	Default co

THEFINANCIALCOMPANY.NET Properties

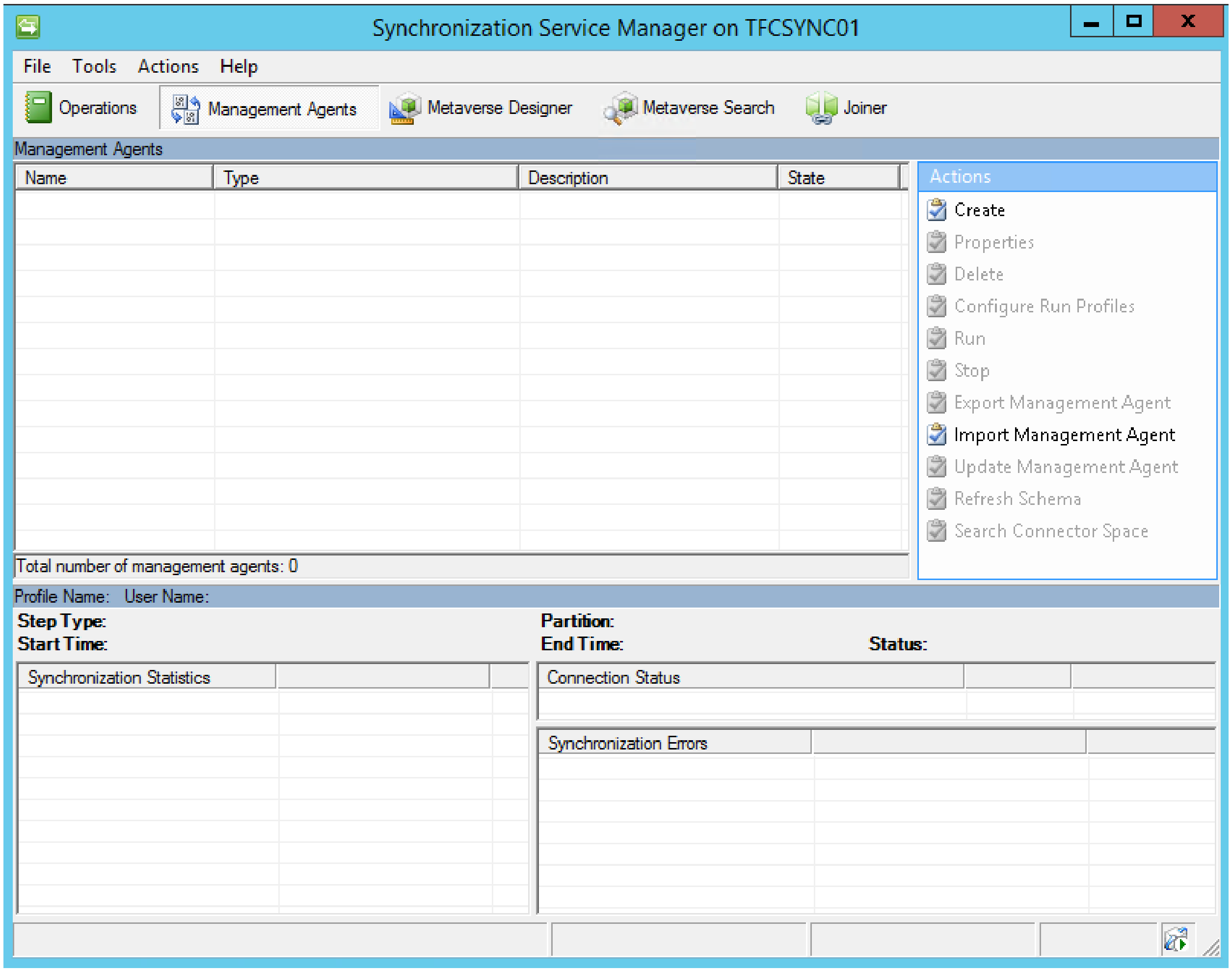
General | Managed By | Object | Security | Attribute Editor

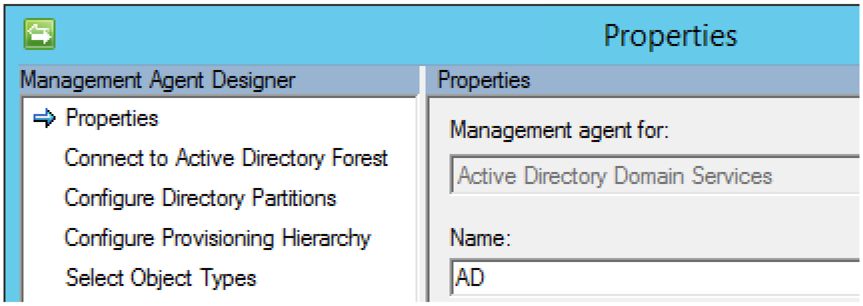
Group or user names:

- Administrators (TFC\Administrators)
- Pre-Windows 2000 Compatible Access (TFC\Pre-Windows 200...
- Incoming Forest Trust Builders (TFC\Incoming Forest Trust Build...
- ENTERPRISE DOMAIN CONTROLLERS
- svc-adma (svc-adma@THEFINANCIALCOMPANY.NET)

Permissions for svc-adma	Allow	Deny
Manage replication topology	□	□
Migrate SID history	□	□
Monitor active directory replication	□	□
Read only replication secret synchronization	□	□
Reanimate tombstones	□	□
Replicating Directory Changes	☑	□

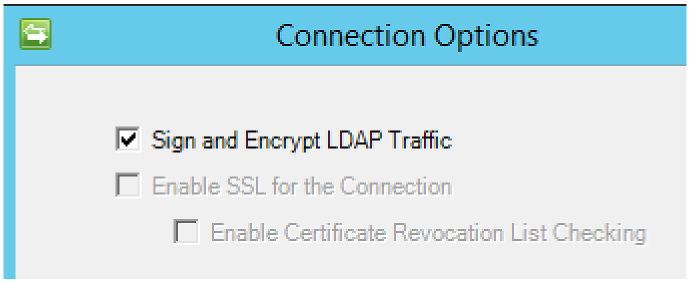
For special permissions or advanced settings, click Advanced.




Properties
Management Agent Designer
Properties
Connect to Active Directory Forest
Configure Directory Partitions
Configure Provisioning Hierarchy
Select Object Types
Properties

Management agent for: Active Directory Domain Services

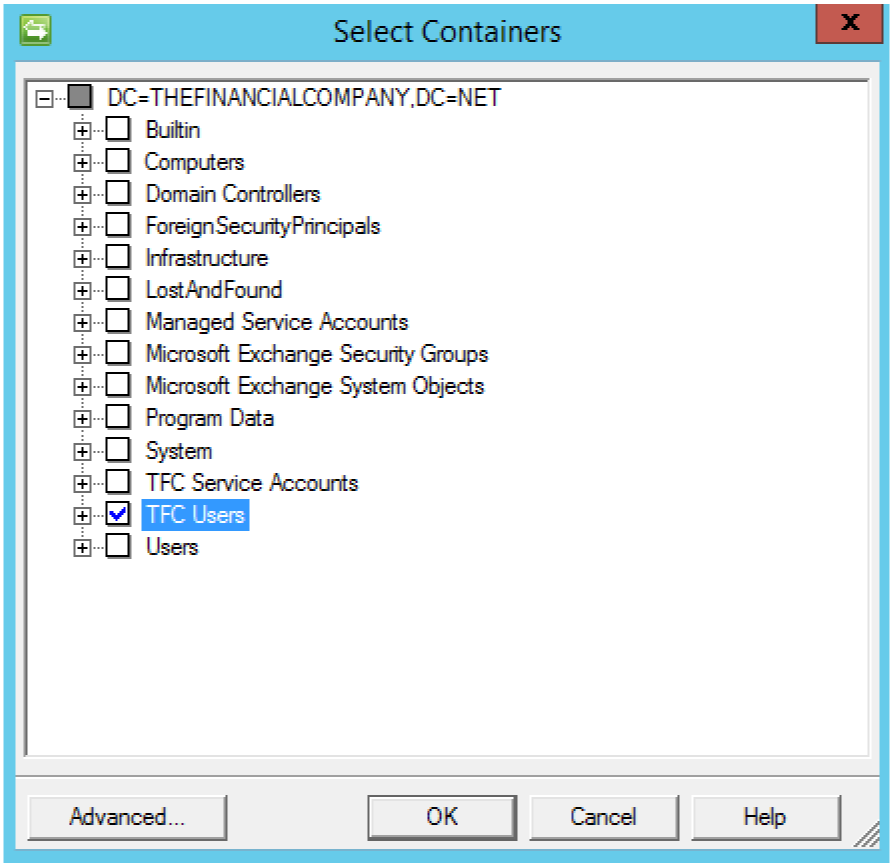
Name: AD



☑ Sign and Encrypt LDAP Traffic

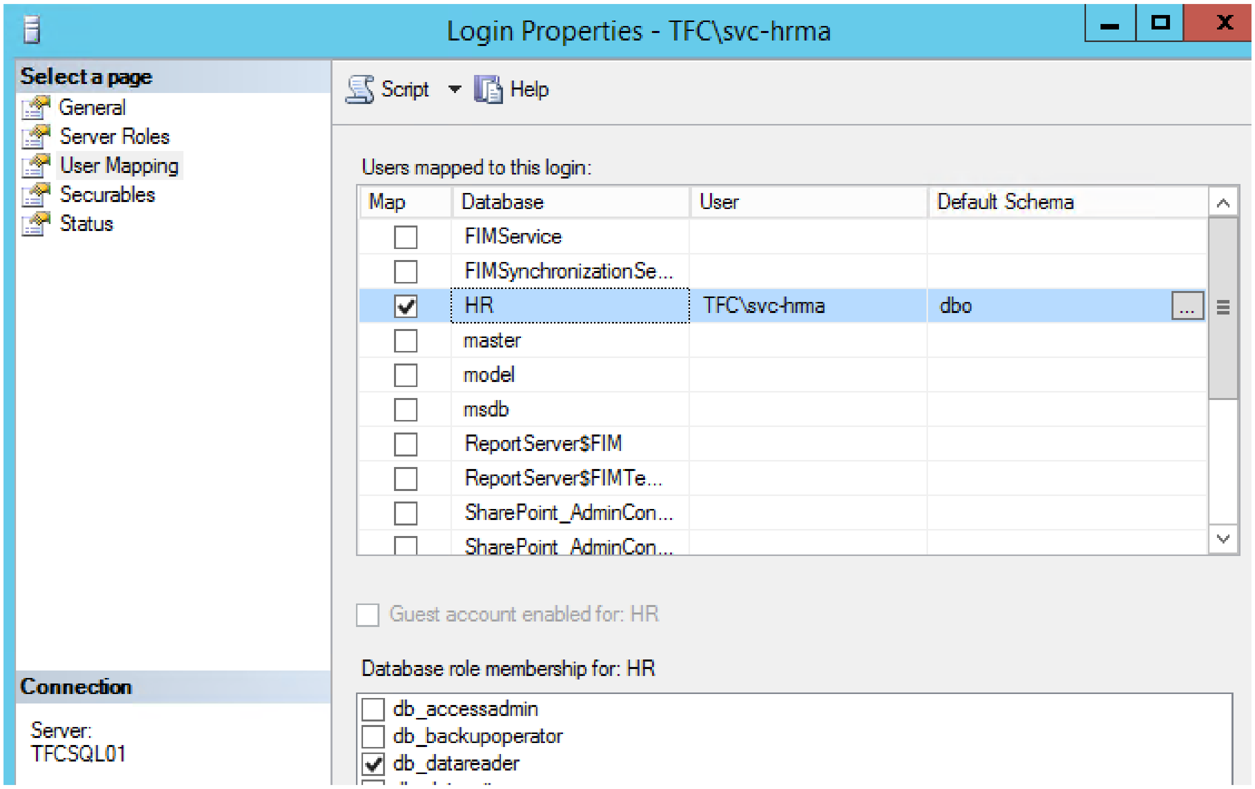
□ Enable SSL for the Connection

□ Enable Certificate Revocation List Checking



Select Containers

- ■ DC=THEFINANCIALCOMPANY,DC=NET
  - □ Builtin
  - □ Computers
  - □ Domain Controllers
  - □ ForeignSecurityPrincipals
  - □ Infrastructure
  - □ LostAndFound
  - □ Managed Service Accounts
  - □ Microsoft Exchange Security Groups
  - □ Microsoft Exchange System Objects
  - □ Program Data
  - □ System
  - □ TFC Service Accounts
  - ☑ TFC Users
  - □ Users



Login Properties - TFC\svc-hrma

Users mapped to this login:

Map	Database	User	Default Schema
□	FIMService		
□	FIMSynchronizationSe...		
☑	HR	TFC\svc-hrma	dbo
□	master		
□	model		
□	msdb		
□	ReportServer$FIM		
□	ReportServer$FIMTe...		
□	SharePoint_AdminCon...		
□	SharePoint_AdminCon...		

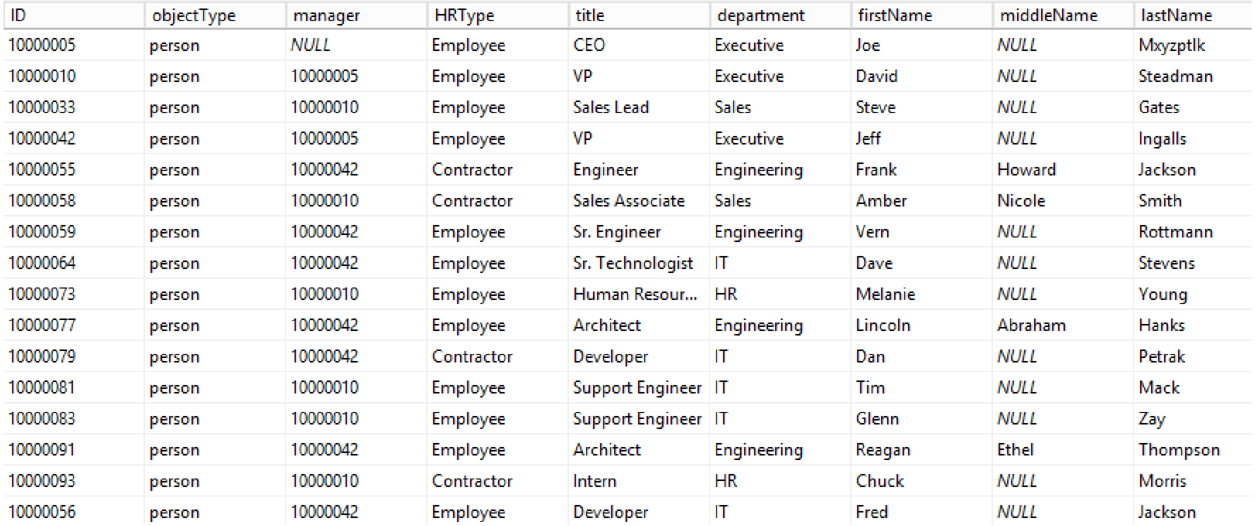
□ Guest account enabled for: HR

Database role membership for: HR

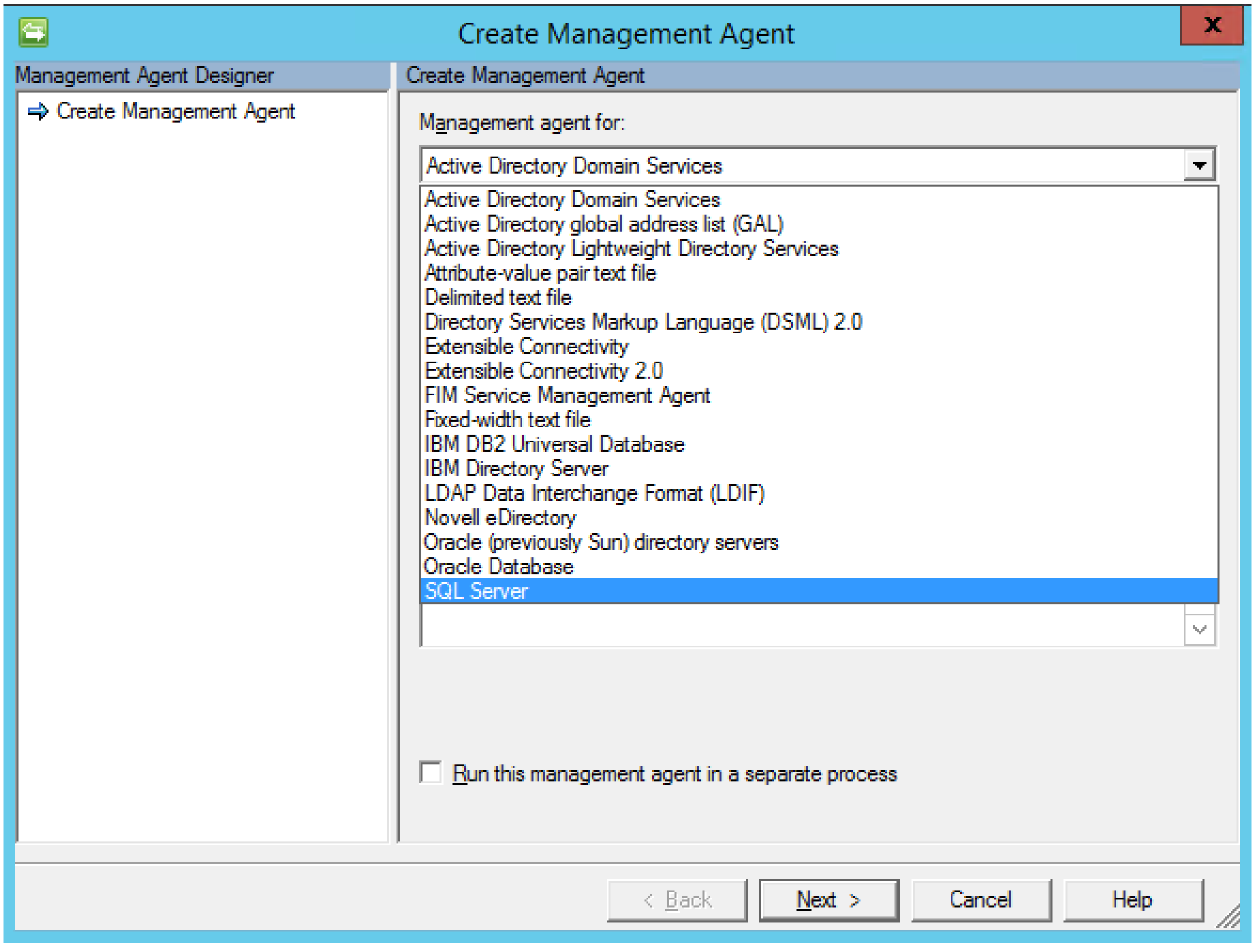
□ db_accessadmin
□ db_backupoperator
☑ db_datareader

Connection

Server:
TFCSQL01



ID	objectType	manager	HRType	title	department	firstName	middleName	lastName
10000005	person	*NULL*	Employee	CEO	Executive	Joe	*NULL*	Mxyzptlk
10000010	person	10000005	Employee	VP	Executive	David	*NULL*	Steadman
10000033	person	10000010	Employee	Sales Lead	Sales	Steve	*NULL*	Gates
10000042	person	10000005	Employee	VP	Executive	Jeff	*NULL*	Ingalls
10000055	person	10000042	Contractor	Engineer	Engineering	Frank	Howard	Jackson
10000058	person	10000010	Contractor	Sales Associate	Sales	Amber	Nicole	Smith
10000059	person	10000042	Employee	Sr. Engineer	Engineering	Vern	*NULL*	Rottmann
10000064	person	10000042	Employee	Sr. Technologist	IT	Dave	*NULL*	Stevens
10000073	person	10000010	Employee	Human Resour...	HR	Melanie	*NULL*	Young
10000077	person	10000042	Employee	Architect	Engineering	Lincoln	Abraham	Hanks
10000079	person	10000042	Contractor	Developer	IT	Dan	*NULL*	Petrak
10000081	person	10000010	Employee	Support Engineer	IT	Tim	*NULL*	Mack
10000083	person	10000010	Employee	Support Engineer	IT	Glenn	*NULL*	Zay
10000091	person	10000042	Employee	Architect	Engineering	Reagan	Ethel	Thompson
10000093	person	10000010	Contractor	Intern	HR	Chuck	*NULL*	Morris
10000056	person	10000042	Employee	Developer	IT	Fred	*NULL*	Jackson



Create Management Agent

Management Agent Designer

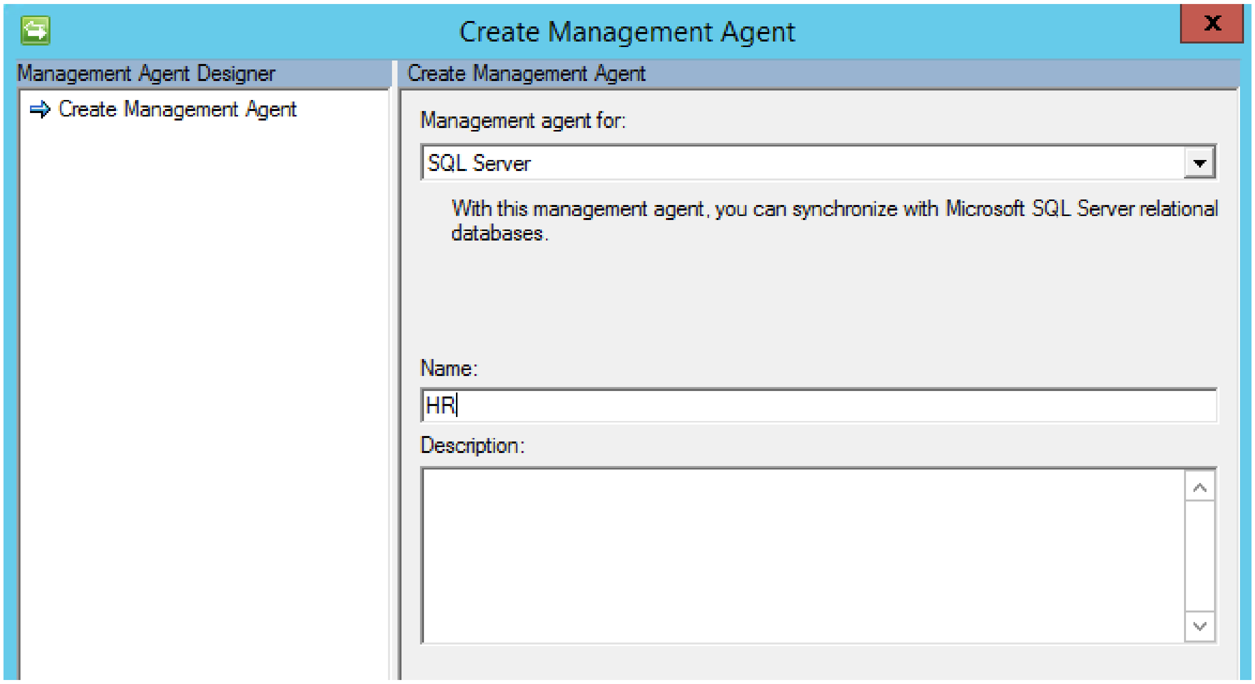
Create Management Agent

Management agent for:

Active Directory Domain Services

Active Directory Domain Services
Active Directory global address list (GAL)
Active Directory Lightweight Directory Services
Attribute-value pair text file
Delimited text file
Directory Services Markup Language (DSML) 2.0
Extensible Connectivity
Extensible Connectivity 2.0
FIM Service Management Agent
Fixed-width text file
IBM DB2 Universal Database
IBM Directory Server
LDAP Data Interchange Format (LDIF)
Novell eDirectory
Oracle (previously Sun) directory servers
Oracle Database
SQL Server

☐ Run this management agent in a separate process

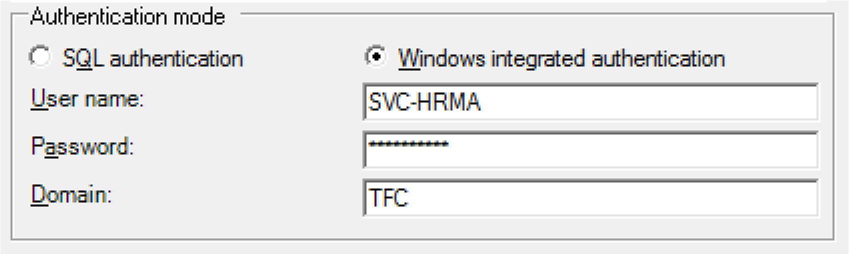


Management agent for: SQL Server

With this management agent, you can synchronize with Microsoft SQL Server relational databases.

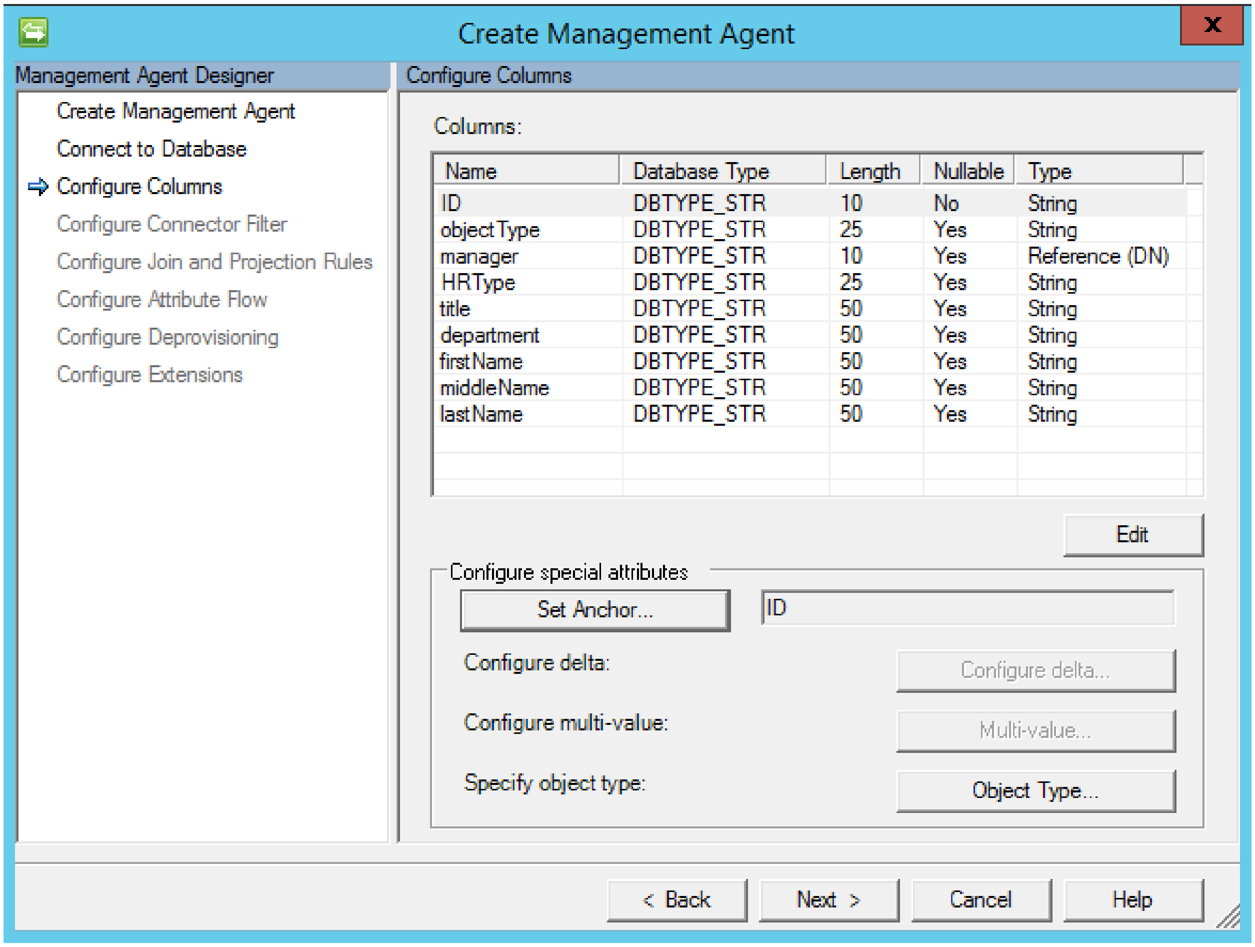
Name: HR

Description:


Authentication mode

○ SQL authentication ● Windows integrated authentication

User name:	SVC-HRMA
Password:	***********
Domain:	TFC



Columns:

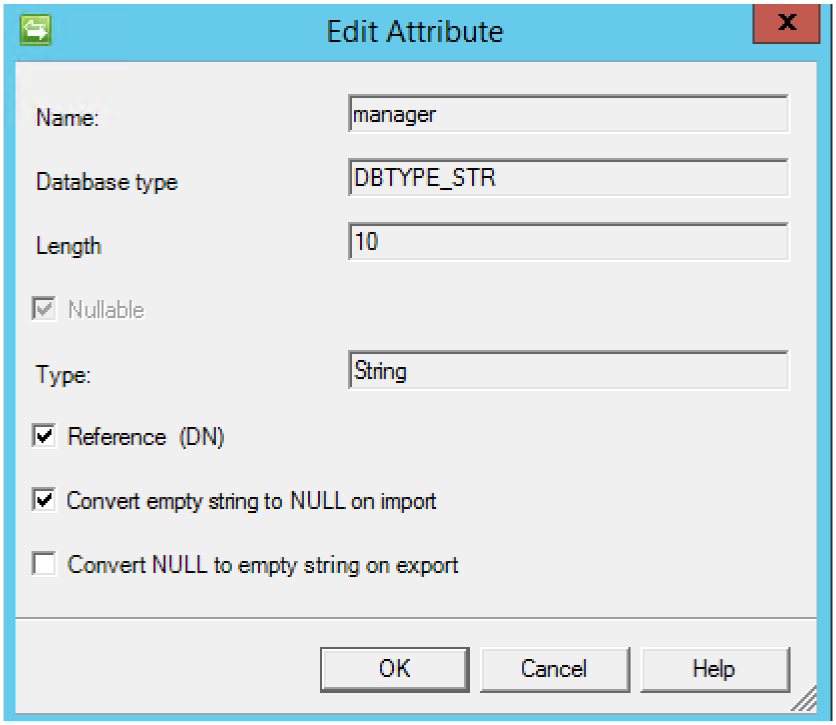
Name	Database Type	Length	Nullable	Type
ID	DBTYPE_STR	10	No	String
objectType	DBTYPE_STR	25	Yes	String
manager	DBTYPE_STR	10	Yes	Reference (DN)
HRType	DBTYPE_STR	25	Yes	String
title	DBTYPE_STR	50	Yes	String
department	DBTYPE_STR	50	Yes	String
firstName	DBTYPE_STR	50	Yes	String
middleName	DBTYPE_STR	50	Yes	String
lastName	DBTYPE_STR	50	Yes	String

Set Anchor...: ID

Configure delta:

Configure multi-value:

Specify object type:



Name: manager

Database type: DBTYPE_STR

Length: 10

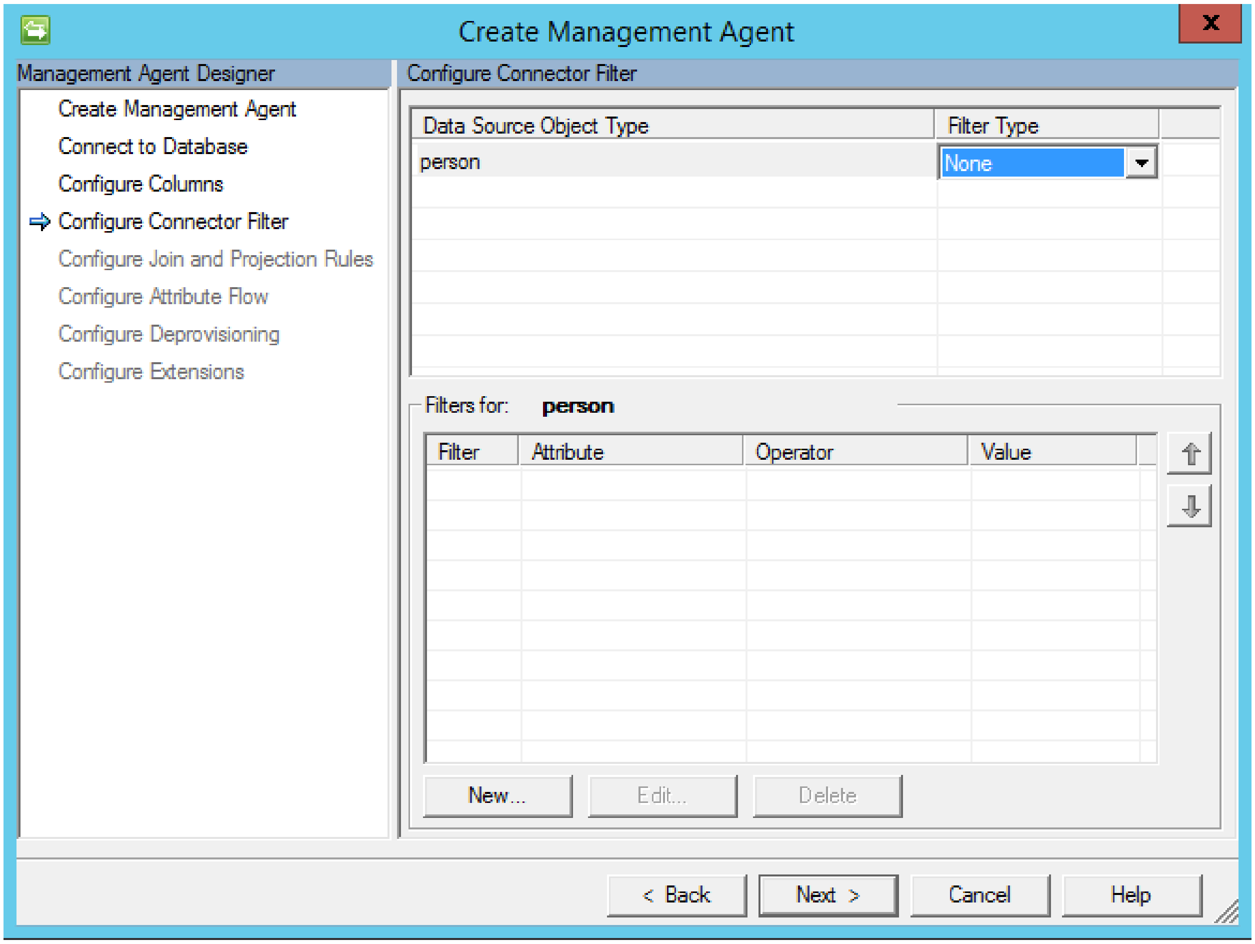
☑ Nullable

Type: String

☑ Reference (DN)

☑ Convert empty string to NULL on import

☐ Convert NULL to empty string on export

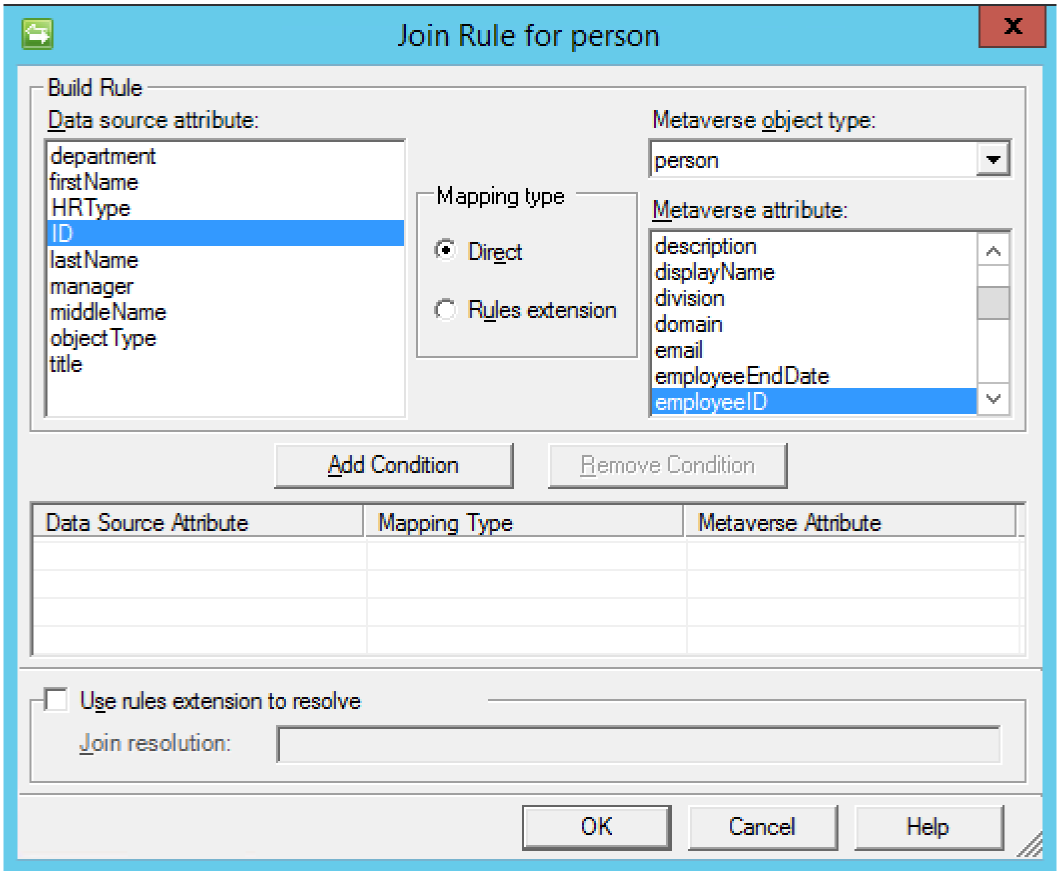


Create Management Agent

Configure Connector Filter

Data Source Object Type	Filter Type
person	None

Filters for: **person**


Join Rule for person

Build Rule

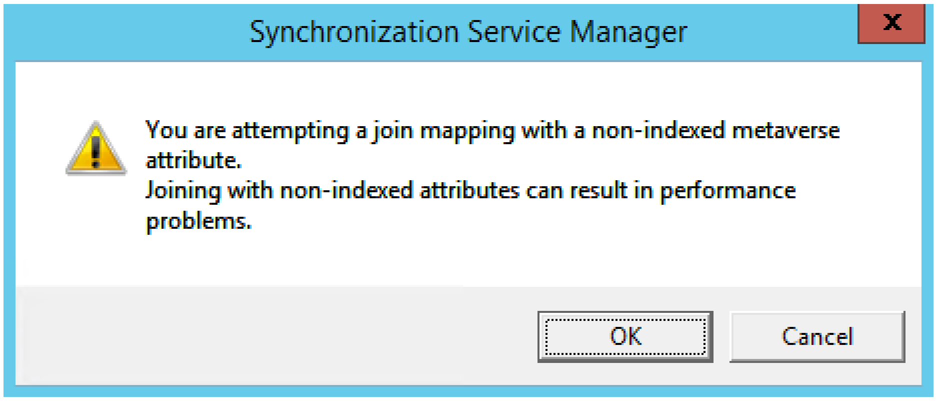
Data source attribute: ID

Mapping type: ● Direct

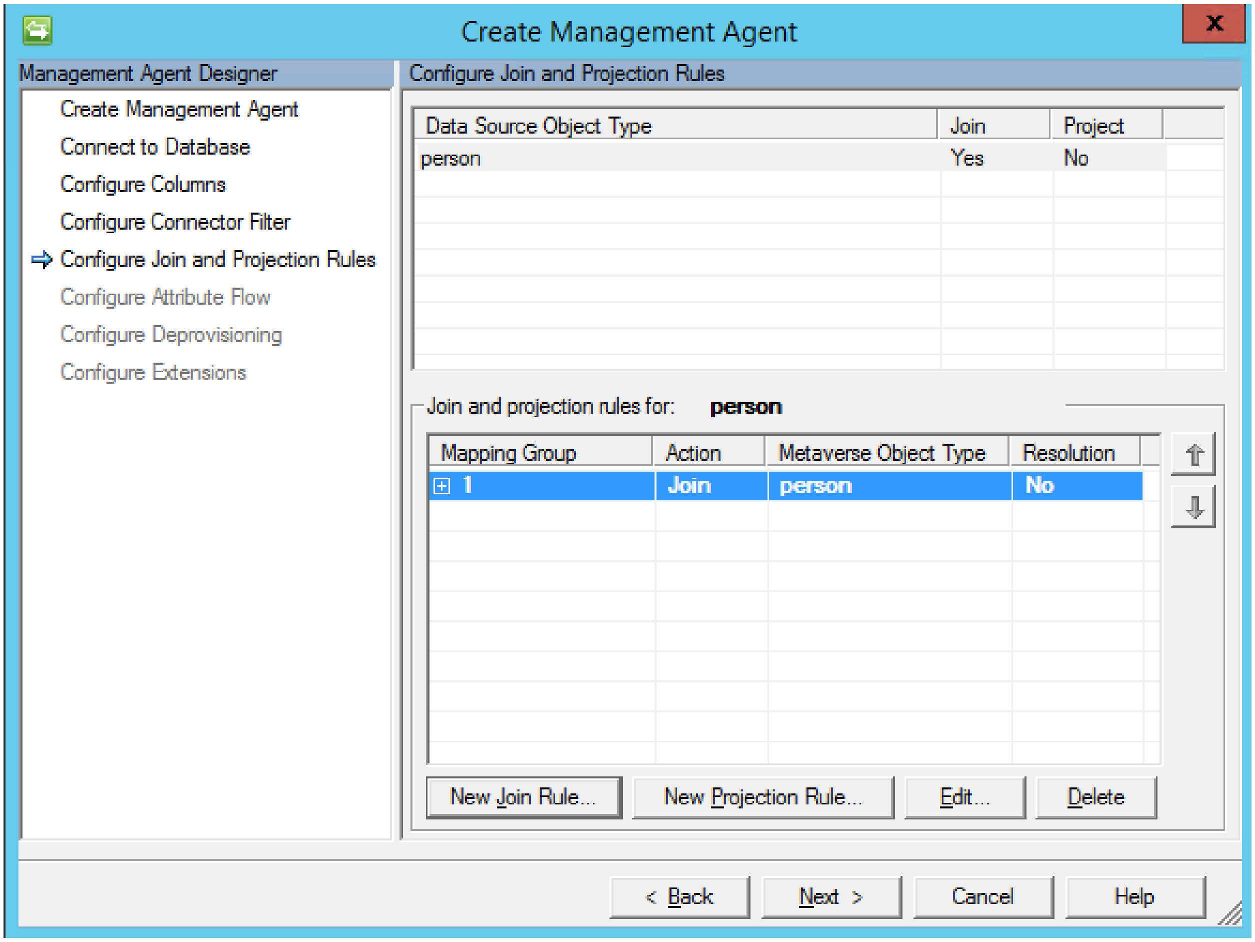
Metaverse object type: person

Metaverse attribute: employeeID

☐ Use rules extension to resolve


Synchronization Service Manager

You are attempting a join mapping with a non-indexed metaverse attribute.
Joining with non-indexed attributes can result in performance problems.

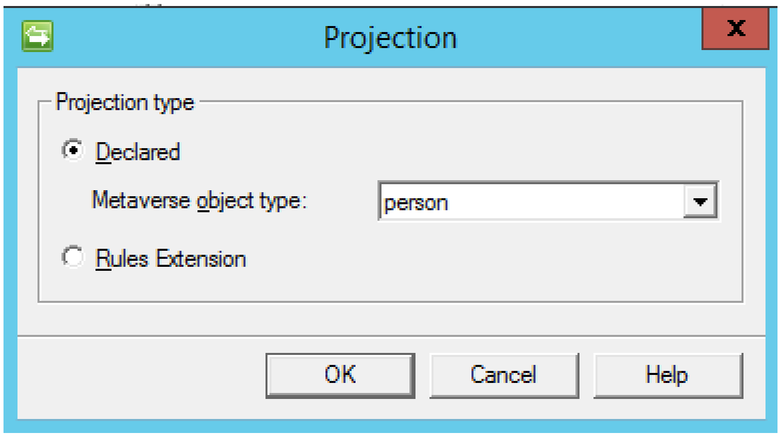


Configure Join and Projection Rules

Data Source Object Type	Join	Project
person	Yes	No

Join and projection rules for: **person**

Mapping Group	Action	Metaverse Object Type	Resolution
⊞ 1	Join	person	No

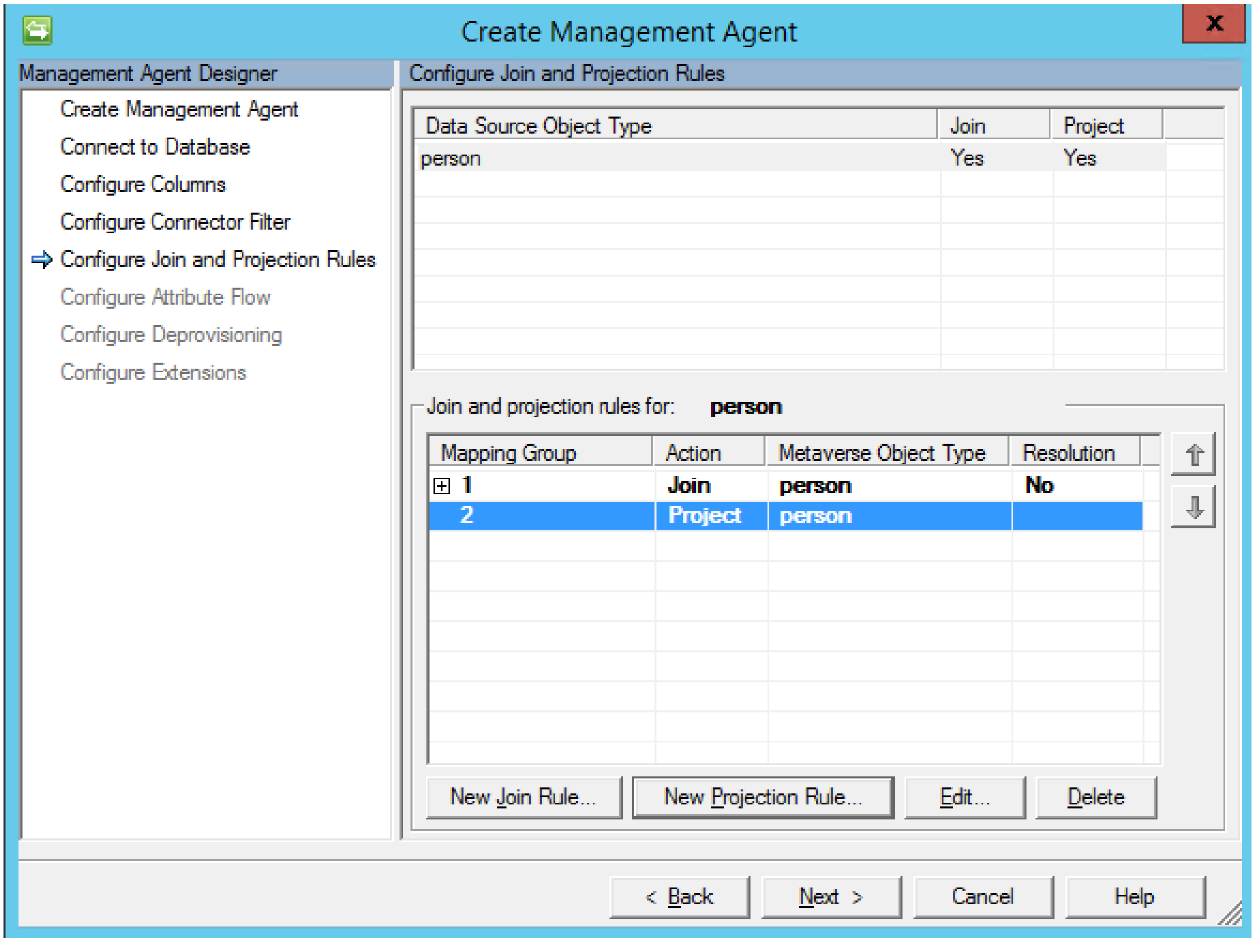


Projection type

● Declared

Metaverse object type: person

○ Rules Extension

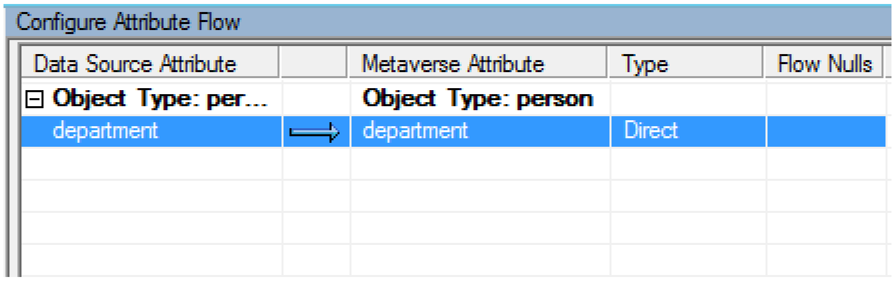


Configure Join and Projection Rules

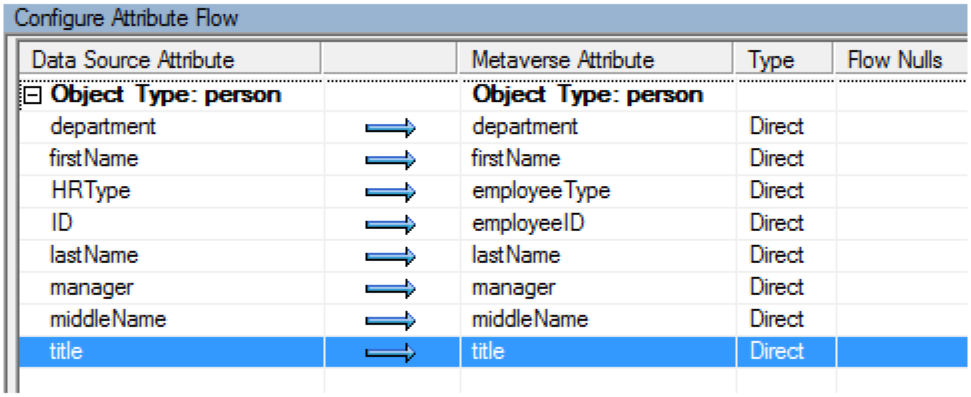
Data Source Object Type	Join	Project
person	Yes	Yes

Join and projection rules for: **person**

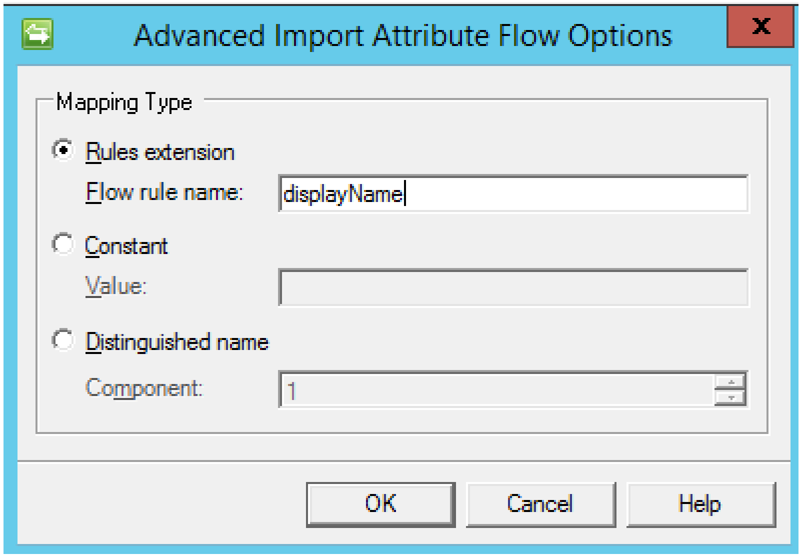
Mapping Group	Action	Metaverse Object Type	Resolution
⊞ **1**	**Join**	**person**	**No**
2	Project	person	


Configure Attribute Flow

Data Source Attribute		Metaverse Attribute	Type	Flow Nulls
⊟ **Object Type: per...**		**Object Type: person**		
department	⟹	department	Direct	


Configure Attribute Flow

Data Source Attribute		Metaverse Attribute	Type	Flow Nulls
⊟ **Object Type: person**		**Object Type: person**		
department	⟹	department	Direct	
firstName	⟹	firstName	Direct	
HRType	⟹	employeeType	Direct	
ID	⟹	employeeID	Direct	
lastName	⟹	lastName	Direct	
manager	⟹	manager	Direct	
middleName	⟹	middleName	Direct	
title	⟹	title	Direct	



Advanced Import Attribute Flow Options

Mapping Type

● Rules extension

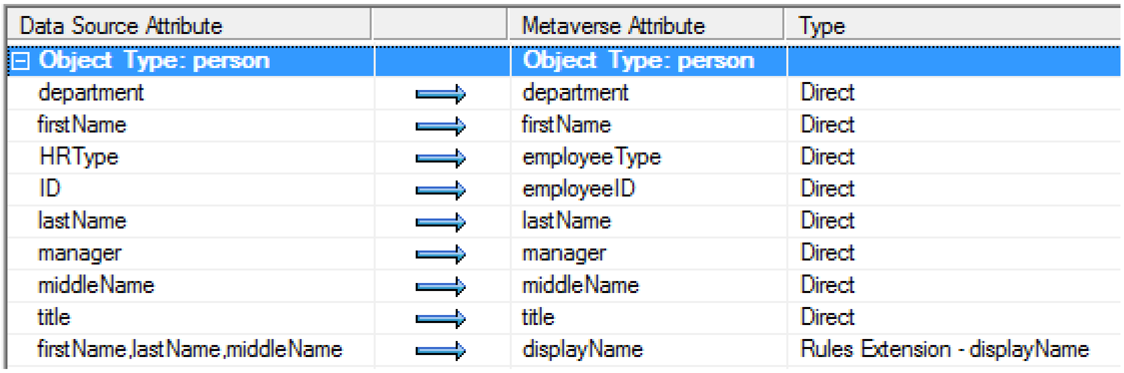
Flow rule name: displayName

○ Constant

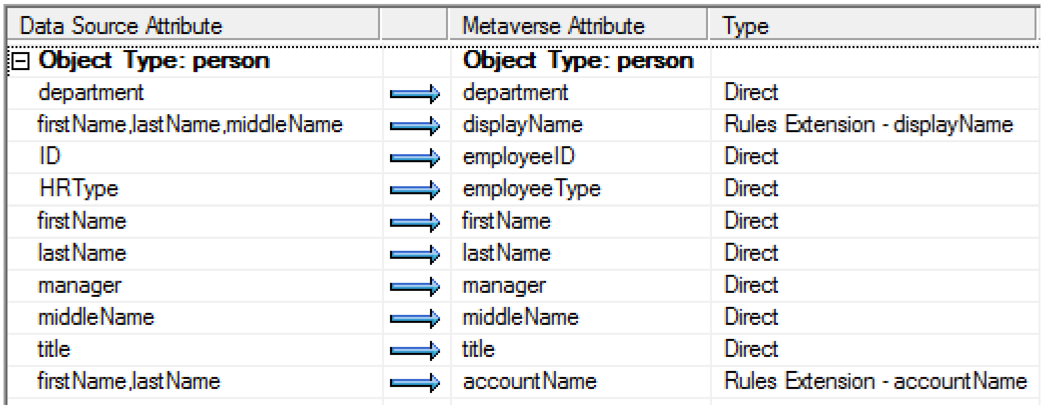
Value:

○ Distinguished name

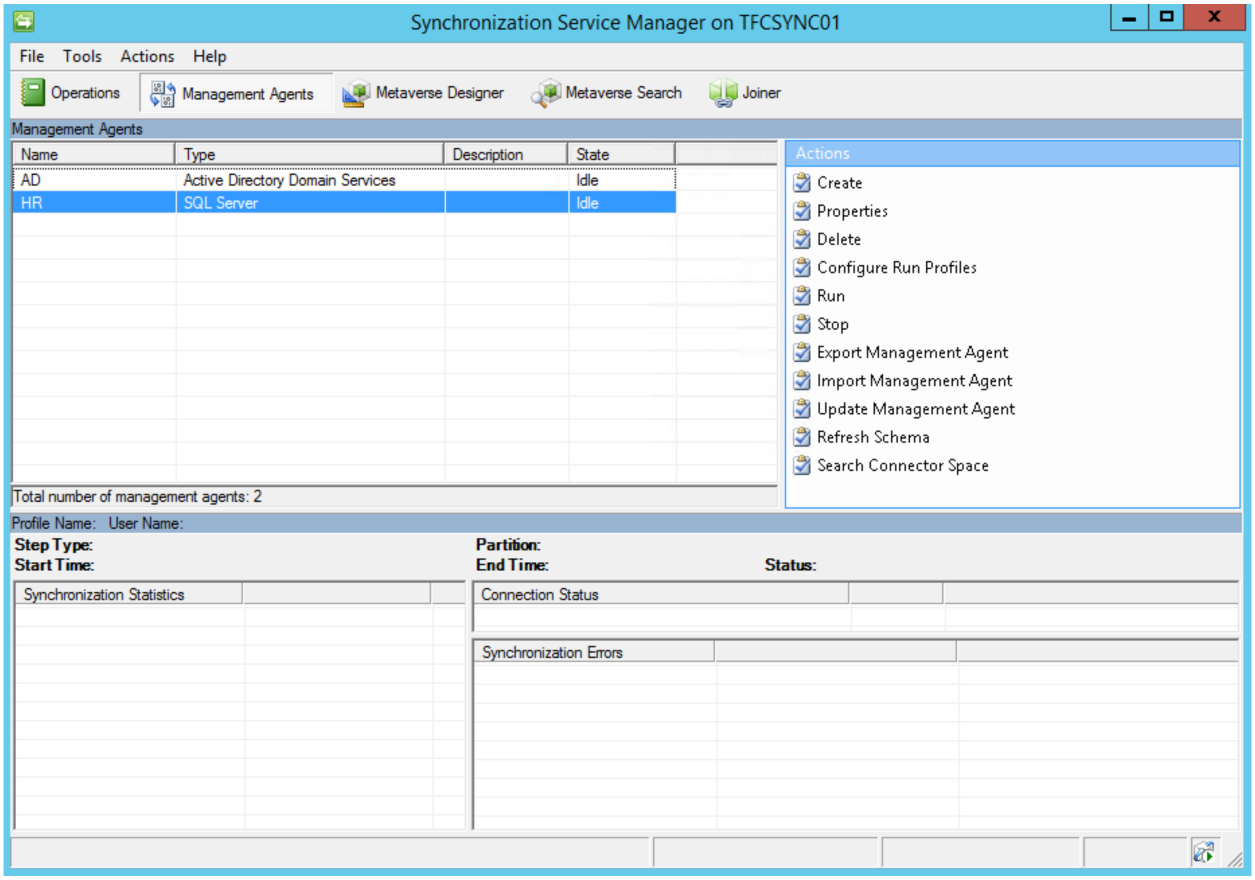
Component: 1



Data Source Attribute		Metaverse Attribute	Type
⊟ Object Type: person		Object Type: person	
department	⟹	department	Direct
firstName	⟹	firstName	Direct
HRType	⟹	employeeType	Direct
ID	⟹	employeeID	Direct
lastName	⟹	lastName	Direct
manager	⟹	manager	Direct
middleName	⟹	middleName	Direct
title	⟹	title	Direct
firstName,lastName,middleName	⟹	displayName	Rules Extension - displayName



Data Source Attribute		Metaverse Attribute	Type
⊟ Object Type: person		Object Type: person	
department	⟹	department	Direct
firstName,lastName,middleName	⟹	displayName	Rules Extension - displayName
ID	⟹	employeeID	Direct
HRType	⟹	employeeType	Direct
firstName	⟹	firstName	Direct
lastName	⟹	lastName	Direct
manager	⟹	manager	Direct
middleName	⟹	middleName	Direct
title	⟹	title	Direct
firstName,lastName	⟹	accountName	Rules Extension - accountName



Name	Type	Description	State
AD	Active Directory Domain Services		Idle
HR	SQL Server		Idle

Total number of management agents: 2

Profile Name: User Name:

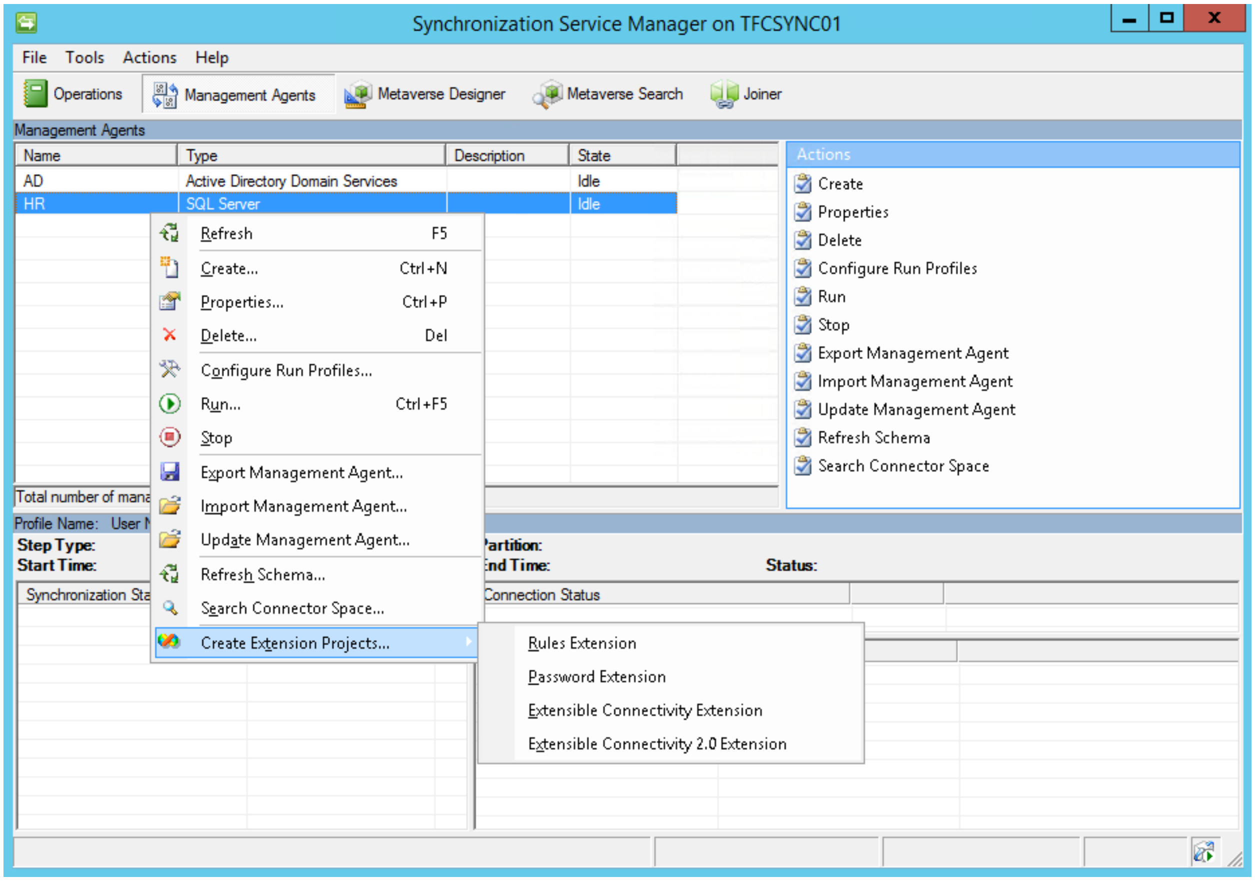
Step Type:

Start Time:

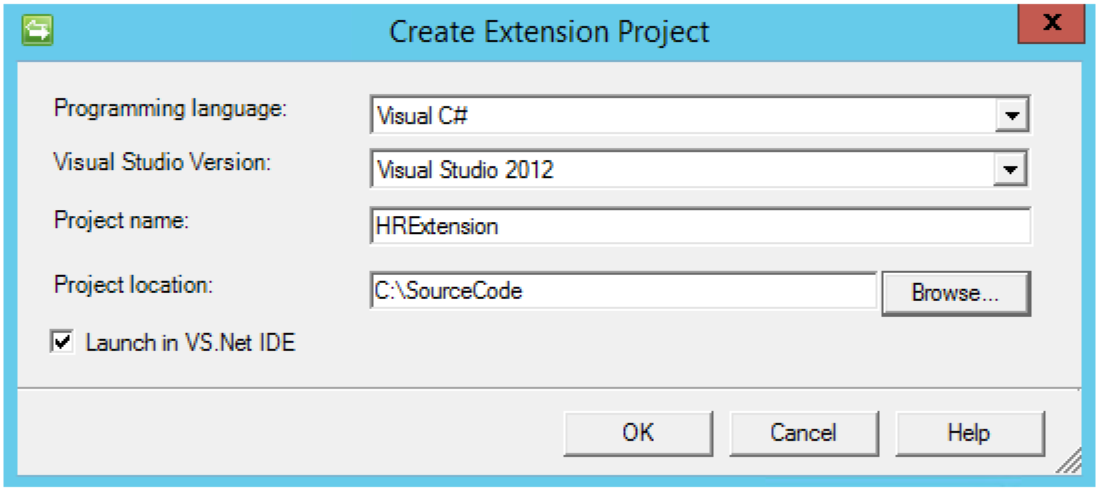
Partition:

End Time:

Status:



Name	Type	Description	State
AD	Active Directory Domain Services		Idle
HR	SQL Server		Idle



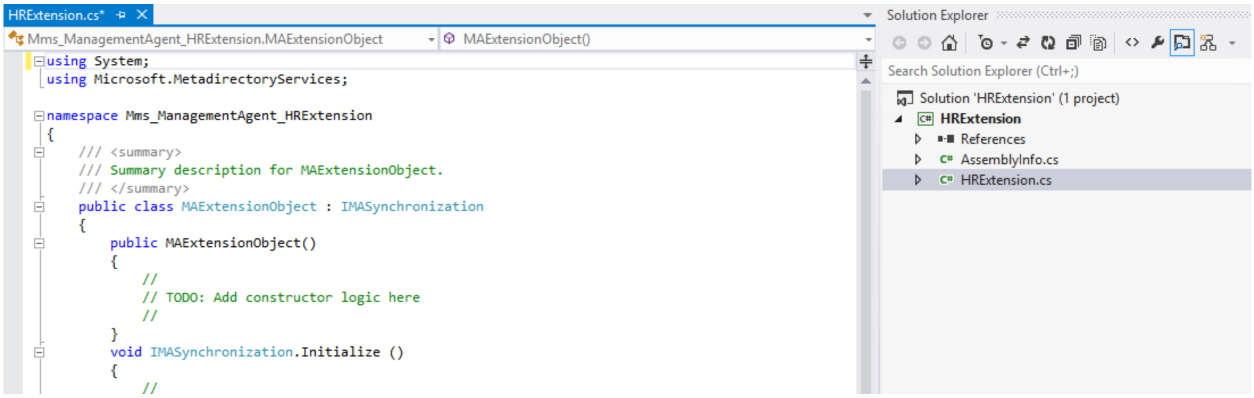
Programming language: Visual C#

Visual Studio Version: Visual Studio 2012

Project name: HRExtension

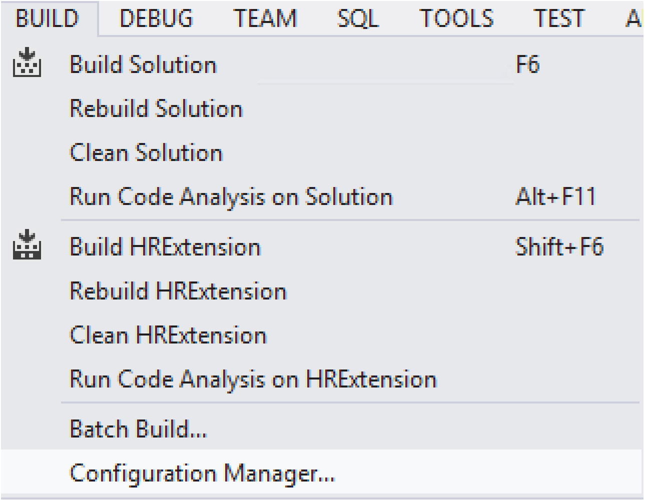
Project location: C:\SourceCode

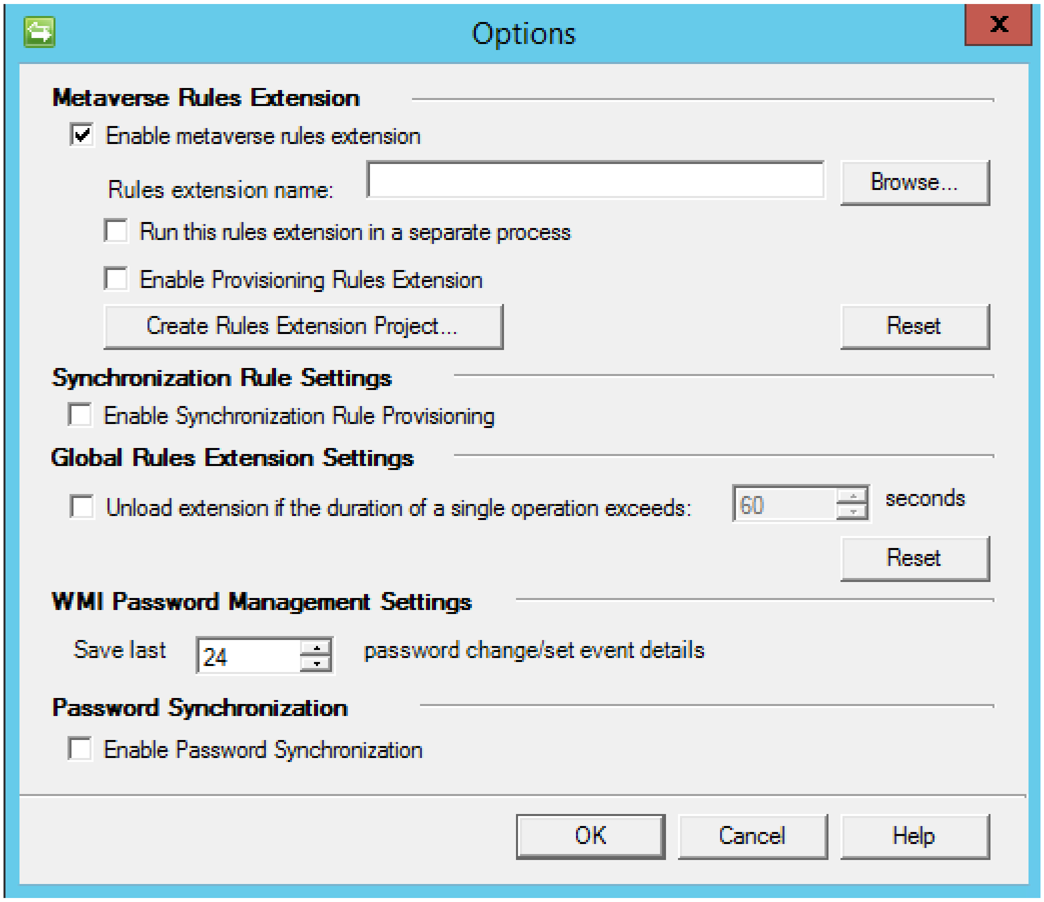
☑ Launch in VS.Net IDE


HRExtension.cs*
Mms_ManagementAgent_HRExtension.MAExtensionObject
MAExtensionObject()
Solution Explorer
Search Solution Explorer (Ctrl+;)
Solution 'HRExtension' (1 project)
HRExtension
References
AssemblyInfo.cs
HRExtension.cs

```
using System;
using Microsoft.MetadirectoryServices;

namespace Mms_ManagementAgent_HRExtension
{
    /// <summary>
    /// Summary description for MAExtensionObject.
    /// </summary>
    public class MAExtensionObject : IMASynchronization
    {
        public MAExtensionObject()
        {
            //
            // TODO: Add constructor logic here
            //
        }
        void IMASynchronization.Initialize ()
        {
            //
```

```
void IMASynchronization.MapAttributesForImport( string FlowRuleName, CSEntry csentry, MVEntry mventry)
{
    switch (FlowRuleName)
    {
        case "displayName":
            string firstName = string.Empty;
            string lastName = string.Empty;
            string middleInitial = string.Empty;

            if (csentry["firstName"].IsPresent)
            {
                firstName = csentry["firstName"].Value;
            }

            if (csentry["middleName"].IsPresent)
            {
                if (csentry["middleName"].Value.Length >= 1)
                {
                    middleInitial = csentry["middleName"].Value.Substring(0,1);
                }
            }

            if (csentry["lastName"].IsPresent)
            {
                lastName = csentry["lastName"].Value;
            }
            mventry["displayName"].Value = firstName + " " + middleInitial + " " + lastName;
            break;
    }
}
```





Metaverse Rules Extension

☑ Enable metaverse rules extension

Rules extension name:

□ Run this rules extension in a separate process

□ Enable Provisioning Rules Extension

Synchronization Rule Settings

□ Enable Synchronization Rule Provisioning

Global Rules Extension Settings

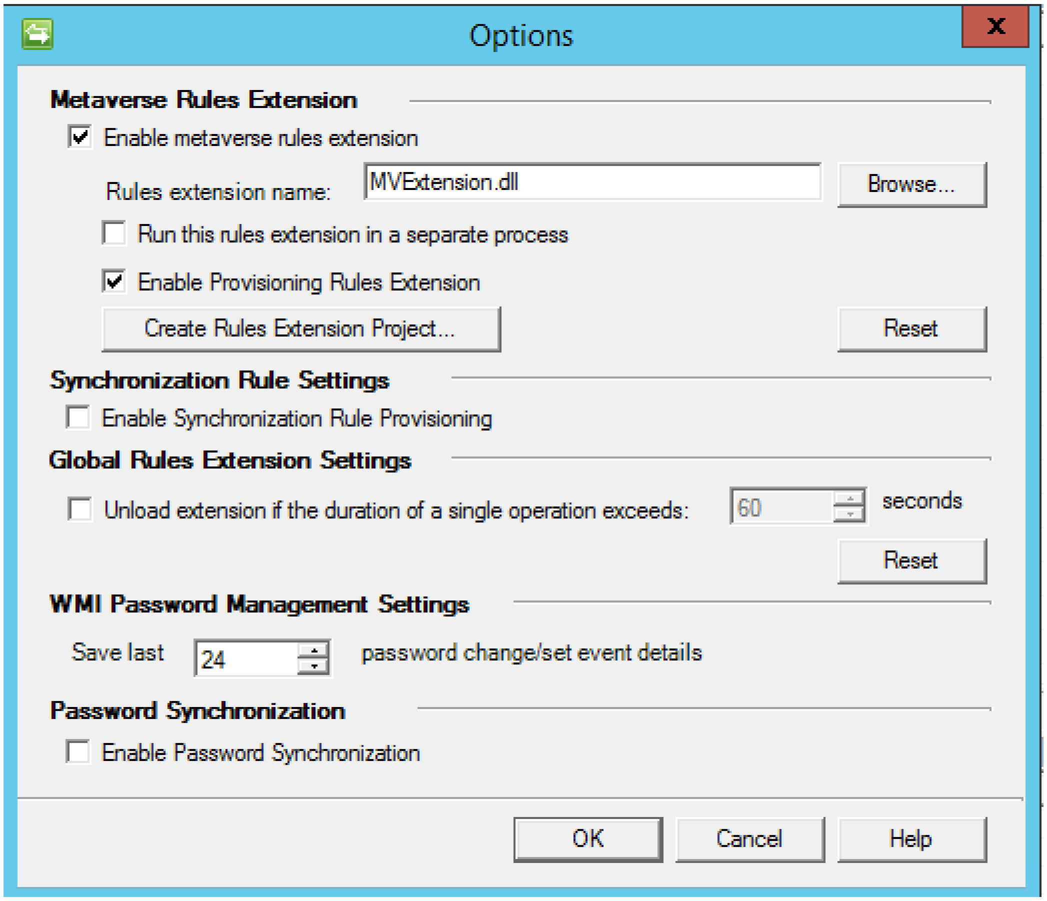
□ Unload extension if the duration of a single operation exceeds: 60 seconds

WMI Password Management Settings

Save last 24 password change/set event details

Password Synchronization

□ Enable Password Synchronization



Metaverse Rules Extension

☑ Enable metaverse rules extension

Rules extension name: MVExtension.dll

□ Run this rules extension in a separate process

☑ Enable Provisioning Rules Extension

Synchronization Rule Settings

□ Enable Synchronization Rule Provisioning

Global Rules Extension Settings

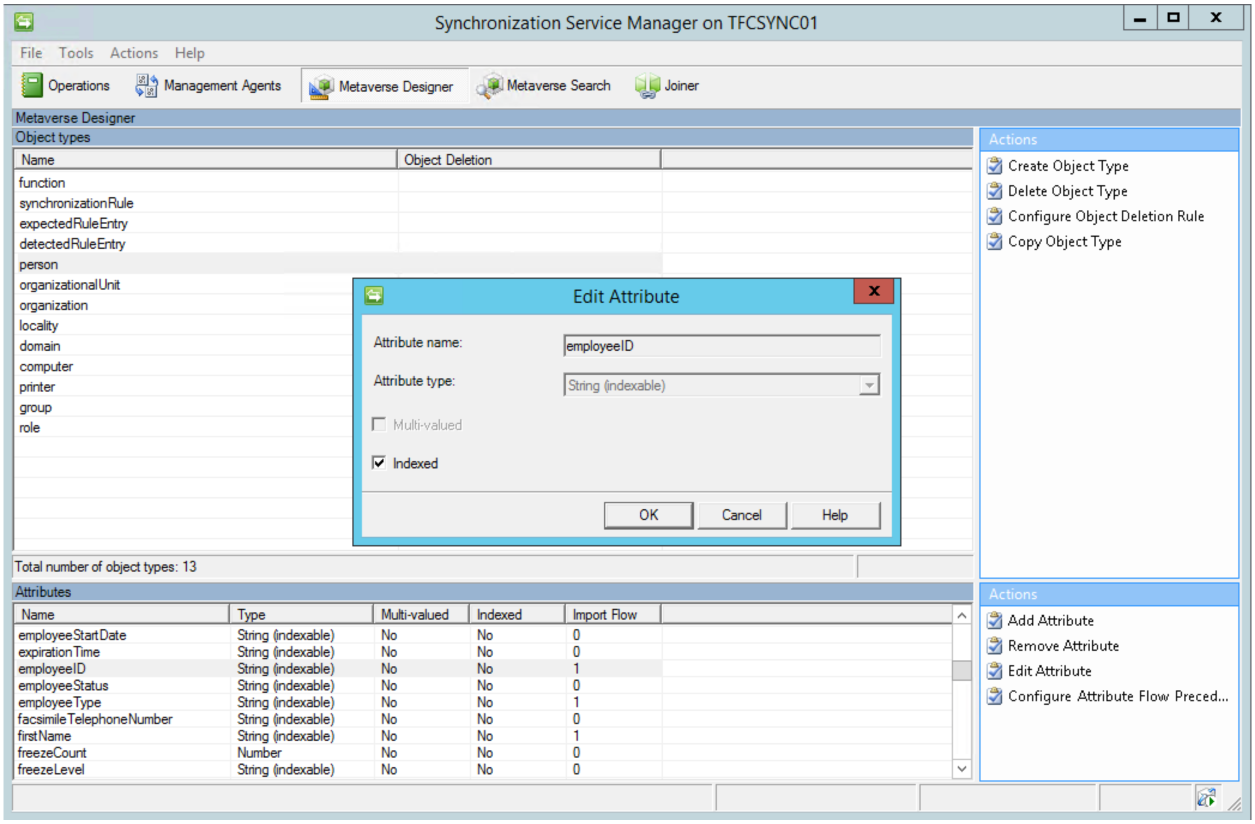
□ Unload extension if the duration of a single operation exceeds: 60 seconds

WMI Password Management Settings

Save last 24 password change/set event details

Password Synchronization

□ Enable Password Synchronization



Name	Object Deletion
function	
synchronizationRule	
expectedRuleEntry	
detectedRuleEntry	
person	
organizationalUnit	
organization	
locality	
domain	
computer	
printer	
group	
role	

Total number of object types: 13

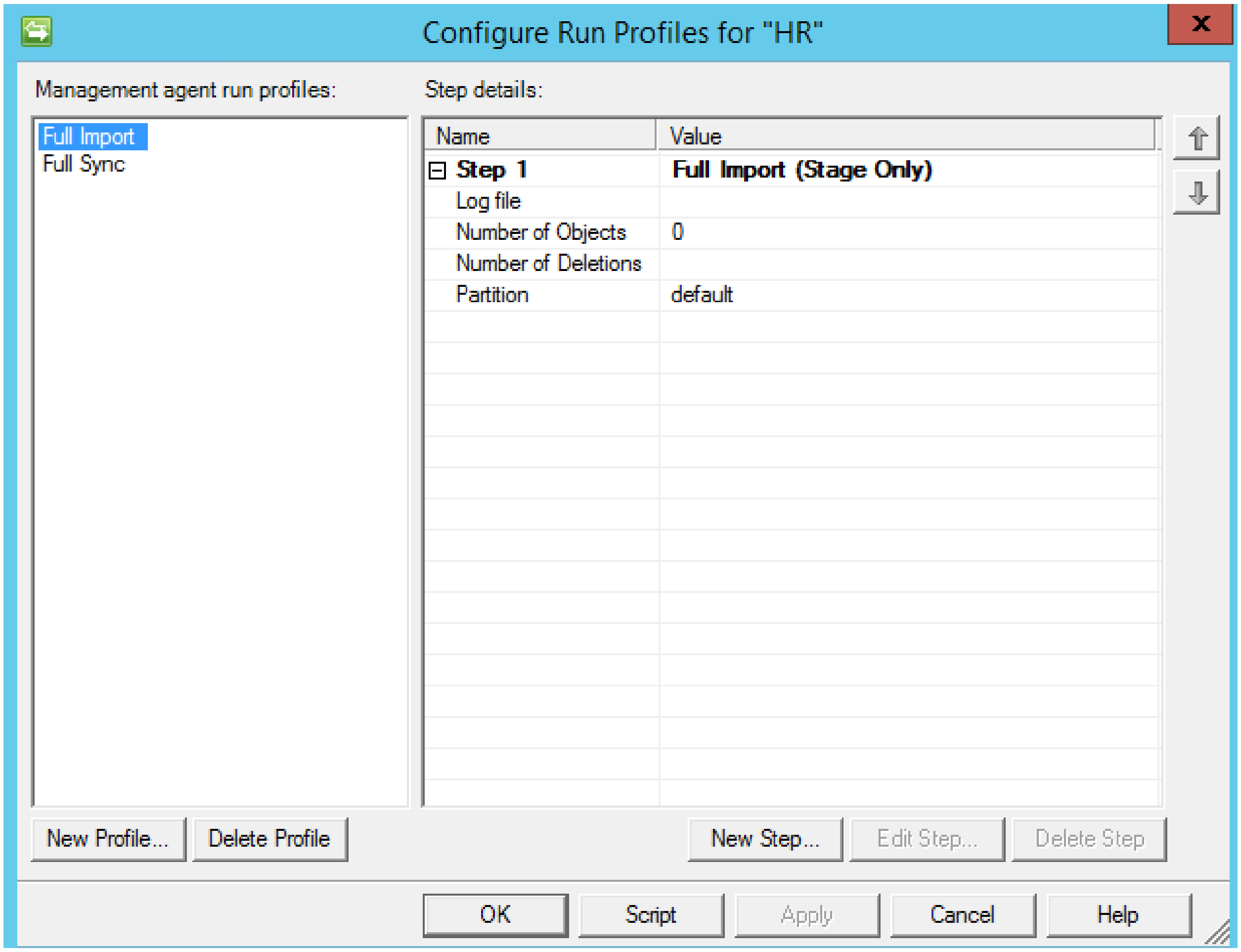
Attribute name: employeeID

Attribute type: String (indexable)

□ Multi-valued

☑ Indexed

Name	Type	Multi-valued	Indexed	Import Flow
employeeStartDate	String (indexable)	No	No	0
expirationTime	String (indexable)	No	No	0
employeeID	String (indexable)	No	No	1
employeeStatus	String (indexable)	No	No	0
employeeType	String (indexable)	No	No	1
facsimileTelephoneNumber	String (indexable)	No	No	0
firstName	String (indexable)	No	No	1
freezeCount	Number	No	No	0
freezeLevel	String (indexable)	No	No	0



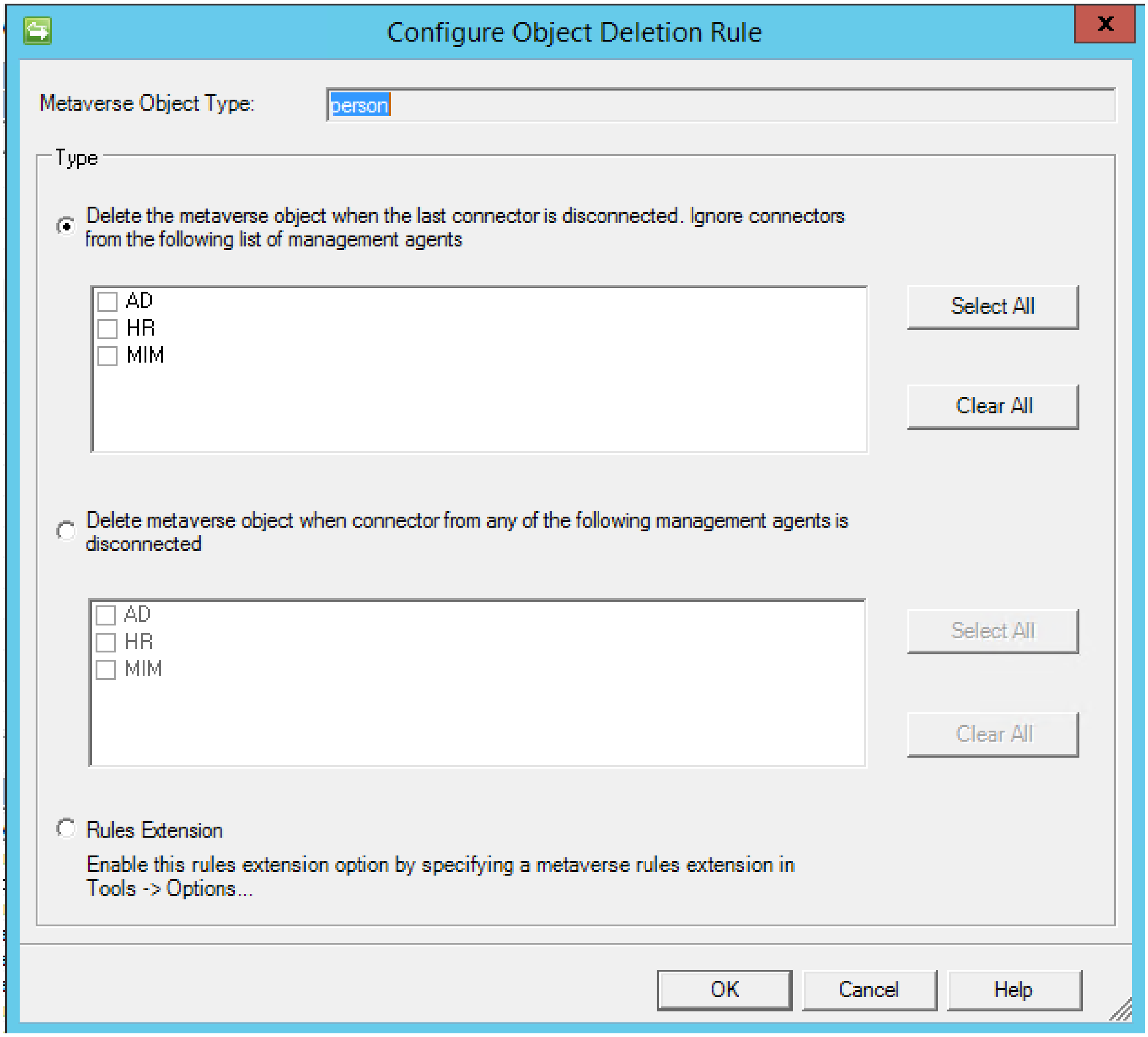
Configure Run Profiles for "HR"

Management agent run profiles:

- Full Import
- Full Sync

Step details:

Name	Value
Step 1	**Full Import (Stage Only)**
Log file	
Number of Objects	0
Number of Deletions	
Partition	default



Configure Object Deletion Rule

Metaverse Object Type: person

Type

● Delete the metaverse object when the last connector is disconnected. Ignore connectors from the following list of management agents

□ AD
□ HR
□ MIM

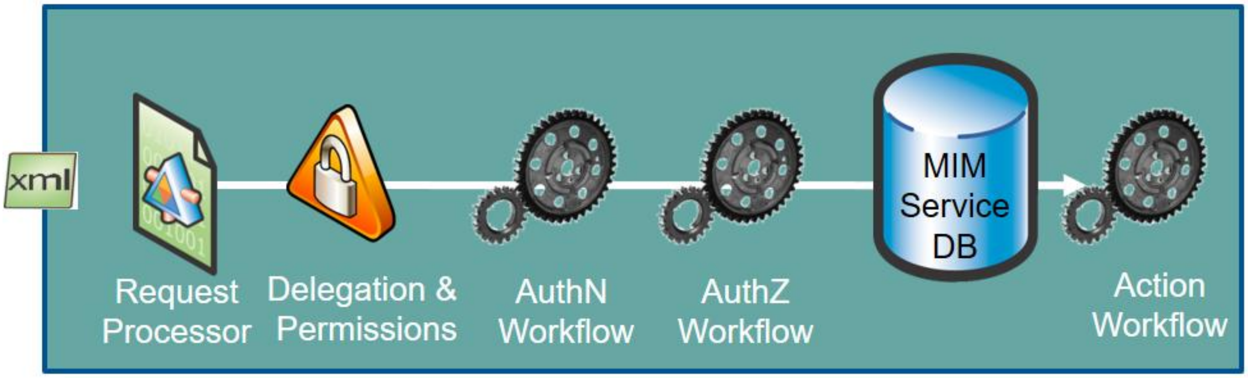
○ Delete metaverse object when connector from any of the following management agents is disconnected

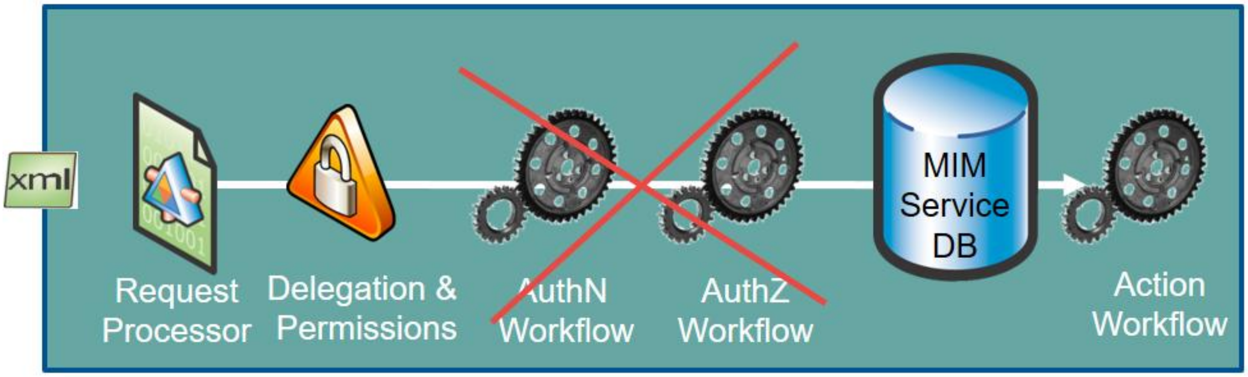
□ AD
□ HR
□ MIM

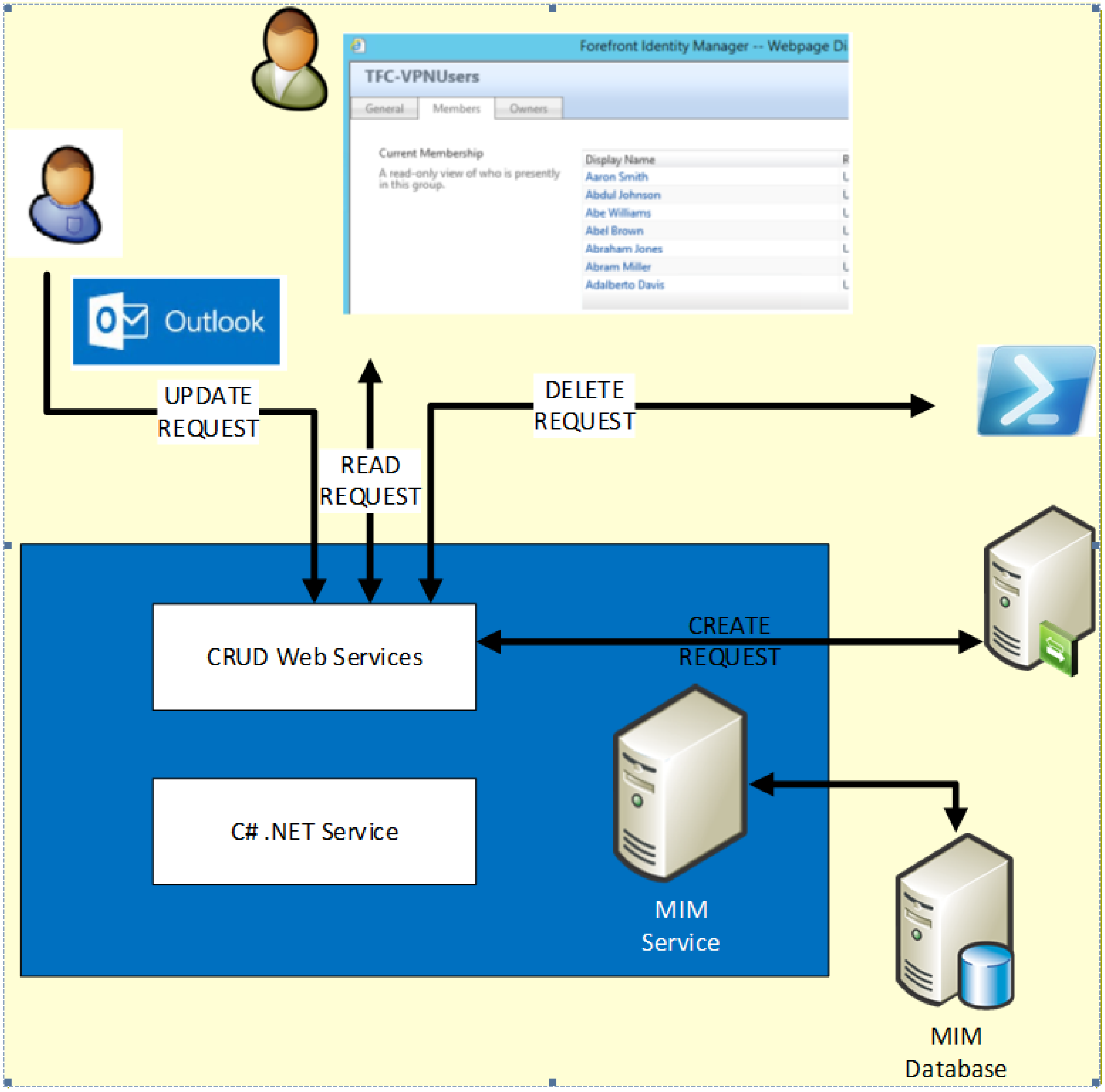
○ Rules Extension

Enable this rules extension option by specifying a metaverse rules extension in Tools -> Options...

Chapter 4: MIM Service Configuration





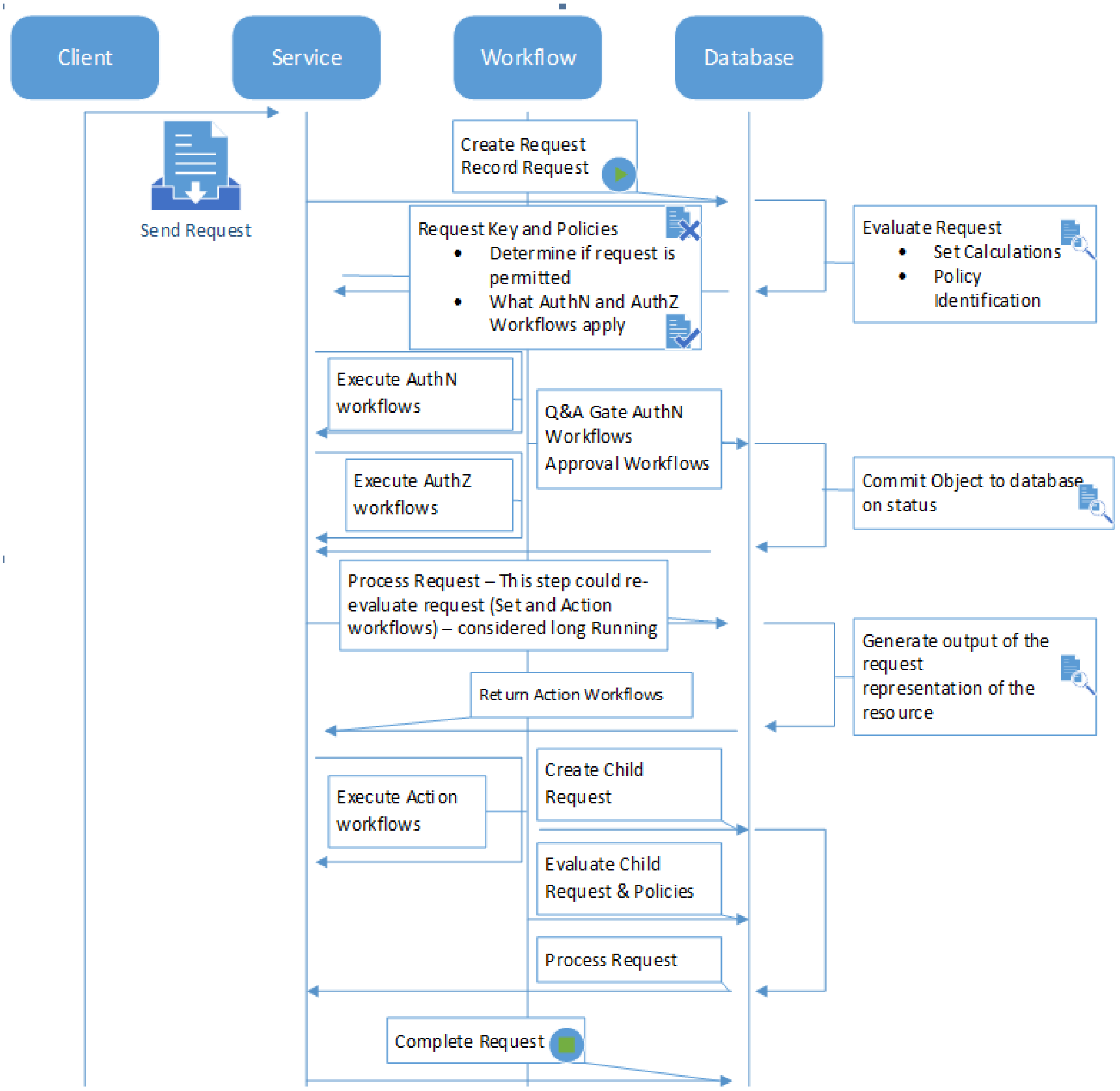


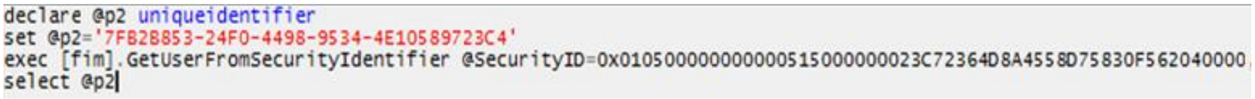
TFC-VPNUsers

Current Membership

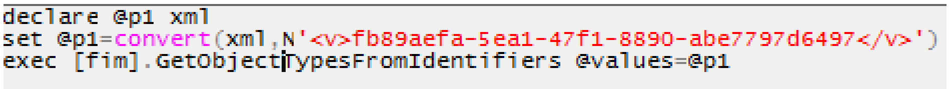
A read-only view of who is presently in this group.

Display Name	R
Aaron Smith	L
Abdul Johnson	L
Abe Williams	L
Abel Brown	L
Abraham Jones	L
Abram Miller	L
Adalberto Davis	L

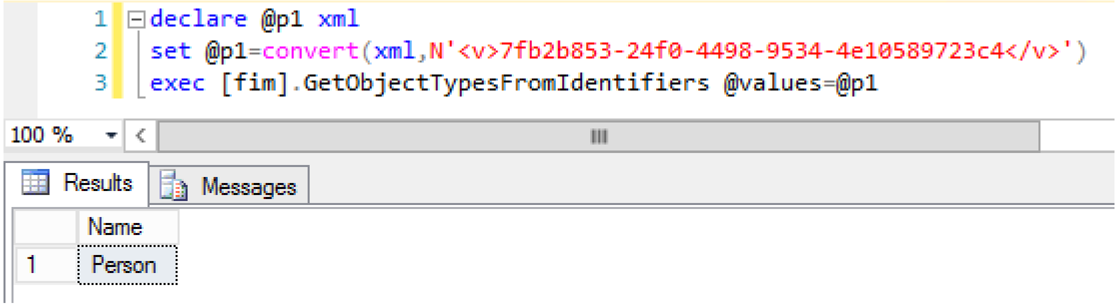




```
declare @p2 uniqueidentifier
set @p2='7FB28853-24F0-4498-9534-4E10589723C4'
exec [fim].GetUserFromSecurityIdentifier @SecurityID=0x01050000000000051500000023C72364D8A4558D75830F562040000,
select @p2
```

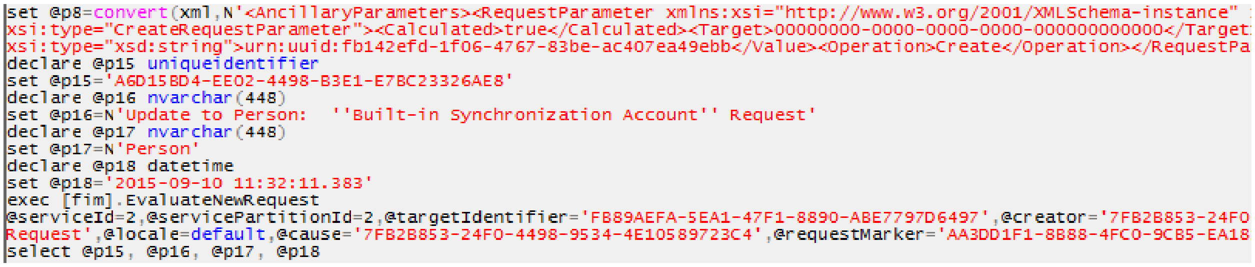


```
declare @p1 xml
set @p1=convert(xml,N'<v>fb89aefa-5ea1-47f1-8890-abe7797d6497</v>')
exec [fim].GetObjectTypesFromIdentifiers @values=@p1
```

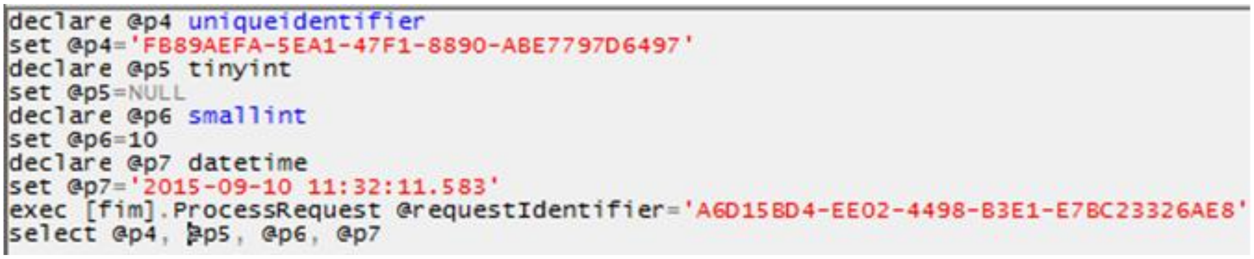


```
declare @p1 xml
set @p1=convert(xml,N'<v>7fb2b853-24f0-4498-9534-4e10589723c4</v>')
exec [fim].GetObjectTypesFromIdentifiers @values=@p1
```

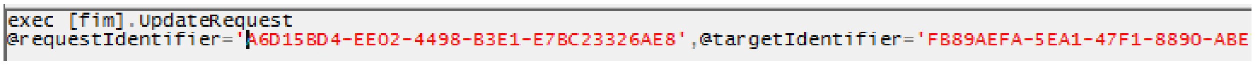
	Name
1	Person



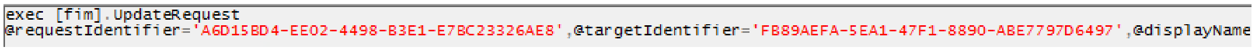
```
set @p8=convert(xml,N'<AncillaryParameters><RequestParameter xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="CreateRequestParameter"><Calculated>true</Calculated><Target>00000000-0000-0000-0000-000000000000</Target
xsi:type="xsd:string">urn:uuid:fb142efd-1f06-4767-83be-ac407ea49ebb</Value><Operation>Create</Operation></RequestPa
declare @p15 uniqueidentifier
set @p15='A6D15BD4-EE02-4498-B3E1-E7BC23326AE8'
declare @p16 nvarchar(448)
set @p16=N'Update to Person:  ''Built-in Synchronization Account'' Request'
declare @p17 nvarchar(448)
set @p17=N'Person'
declare @p18 datetime
set @p18='2015-09-10 11:32:11.383'
exec [fim].EvaluateNewRequest
@serviceId=2,@servicePartitionId=2,@targetIdentifier='FB89AEFA-5EA1-47F1-8890-ABE7797D6497',@creator='7FB2B853-24F0
Request',@locale=default,@cause='7FB2B853-24F0-4498-9534-4E10589723C4',@requestMarker='AA3DD1F1-8B88-4FC0-9CB5-EA18
select @p15, @p16, @p17, @p18
```



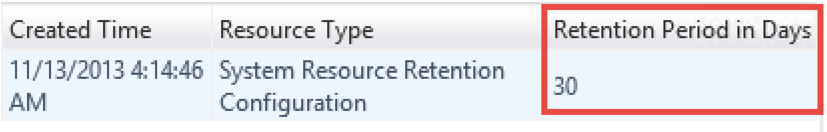
```
declare @p4 uniqueidentifier
set @p4='FB89AEFA-5EA1-47F1-8890-ABE7797D6497'
declare @p5 tinyint
set @p5=NULL
declare @p6 smallint
set @p6=10
declare @p7 datetime
set @p7='2015-09-10 11:32:11.583'
exec [fim].ProcessRequest @requestIdentifier='A6D15BD4-EE02-4498-B3E1-E7BC23326AE8'
select @p4, @p5, @p6, @p7
```



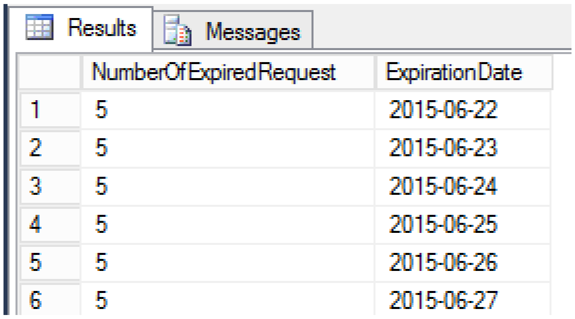
```
exec [fim].UpdateRequest
@requestIdentifier='A6D15BD4-EE02-4498-B3E1-E7BC23326AE8',@targetIdentifier='FB89AEFA-5EA1-47F1-8890-ABE
```



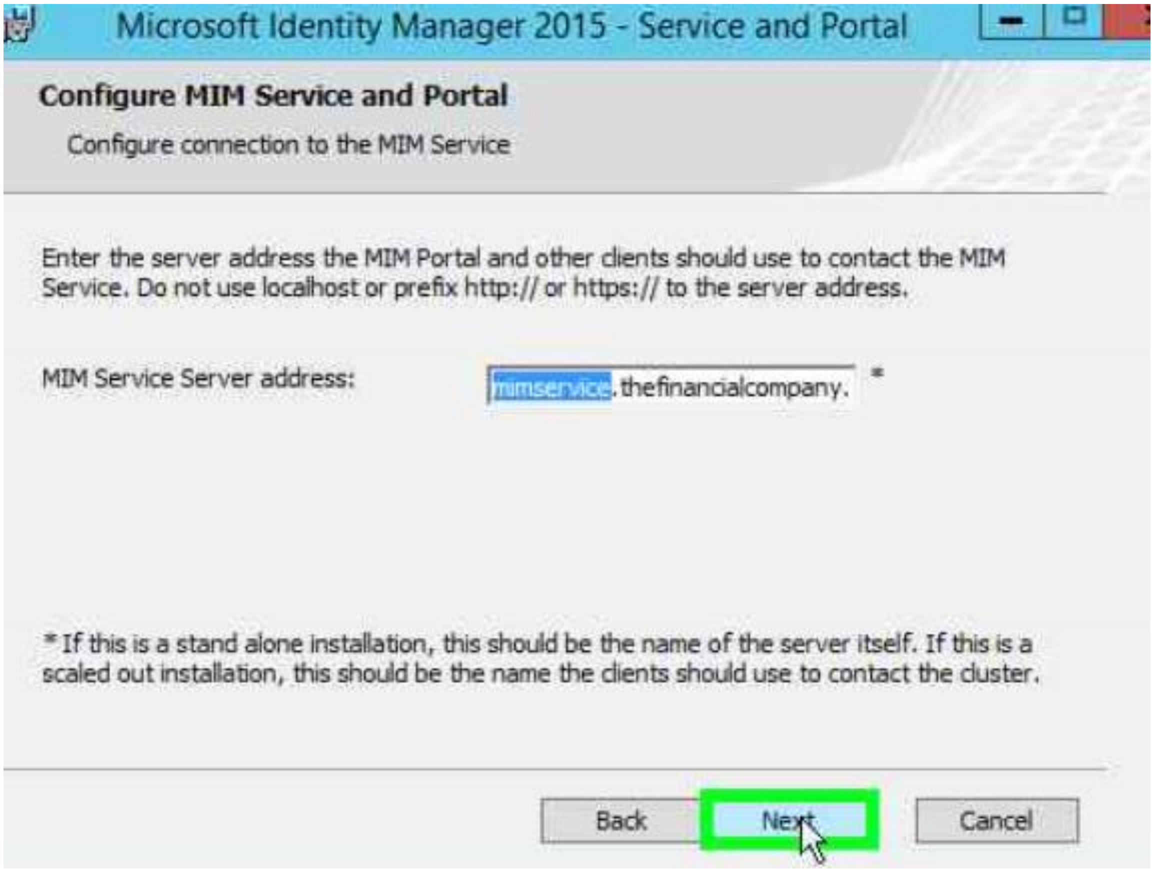
```
exec [fim].UpdateRequest
@requestIdentifier='A6D15BD4-EE02-4498-B3E1-E7BC23326AE8',@targetIdentifier='FB89AEFA-5EA1-47F1-8890-ABE7797D6497',@displayName
```



Created Time	Resource Type	Retention Period in Days
11/13/2013 4:14:46 AM	System Resource Retention Configuration	30



	NumberOfExpiredRequest	ExpirationDate
1	5	2015-06-22
2	5	2015-06-23
3	5	2015-06-24
4	5	2015-06-25
5	5	2015-06-26
6	5	2015-06-27



Microsoft Identity Manager 2015 - Service and Portal

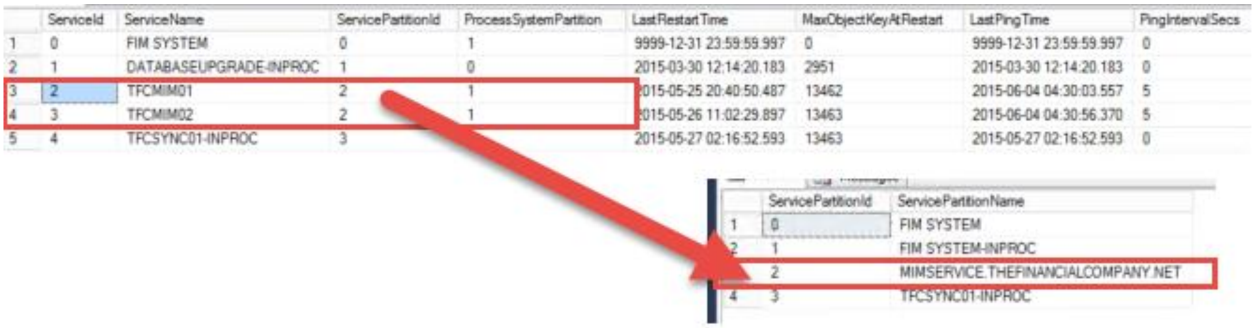
Configure MIM Service and Portal

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: mimservice.thefinancialcompany. *

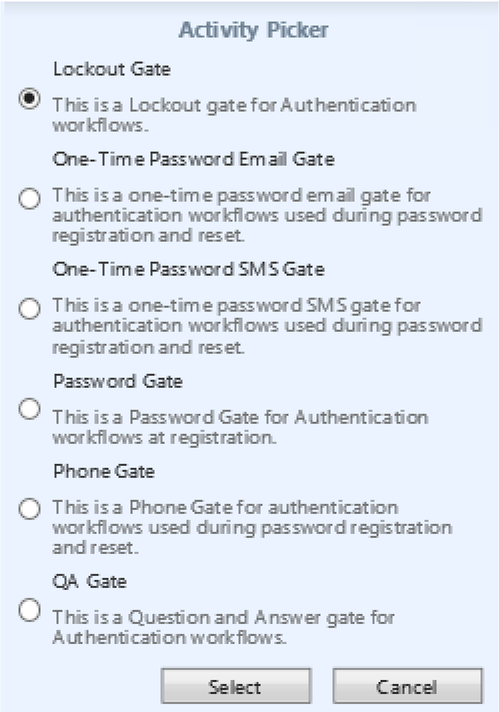
* If this is a stand alone installation, this should be the name of the server itself. If this is a scaled out installation, this should be the name the clients should use to contact the cluster.



	ServiceId	ServiceName	ServicePartitionId	ProcessSystemPartition	LastRestart Time	MaxObjectKeyAtRestart	LastPingTime	PingIntervalSecs
1	0	FIM SYSTEM	0	1	9999-12-31 23:59:59.997	0	9999-12-31 23:59:59.997	0
2	1	DATABASEUPGRADE-INPROC	1	0	2015-03-30 12:14:20.183	2951	2015-03-30 12:14:20.183	0
3	2	TFCMIM01	2	1	2015-05-25 20:40:50.487	13462	2015-06-04 04:30:03.557	5
4	3	TFCMIM02	2	1	2015-05-26 11:02:29.897	13463	2015-06-04 04:30:56.370	5
5	4	TFCSYNC01-INPROC	3		2015-05-27 02:16:52.593	13463	2015-05-27 02:16:52.593	0

	ServicePartitionId	ServicePartitionName
1	0	FIM SYSTEM
2	1	FIM SYSTEM-INPROC
	2	MIMSERVICE.THEFINANCIALCOMPANY.NET
4	3	TFCSYNC01-INPROC

```
<resourceManagementClient resourceManagementServiceBaseAddress="mimservice.thefinancialcompany.net" />
<resourceManagementService externalHostName="mimservice.thefinancialcompany.net" />
```



Activity Picker

● Lockout Gate
This is a Lockout gate for Authentication workflows.

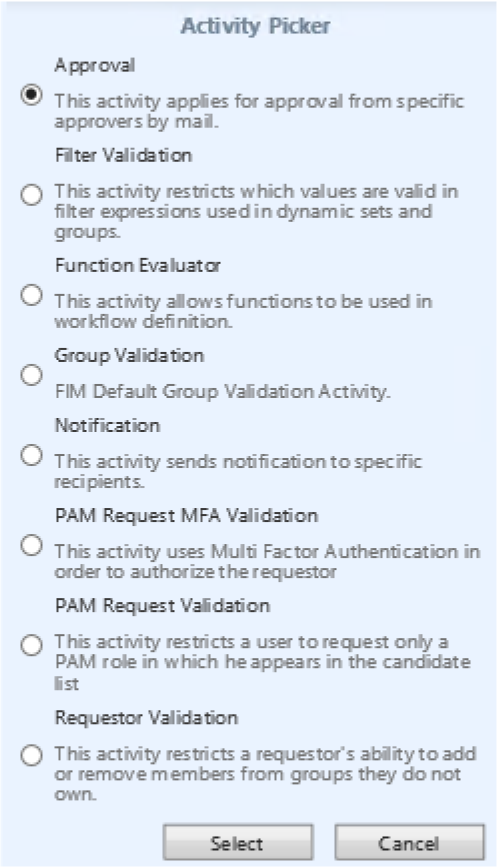
○ One-Time Password Email Gate
This is a one-time password email gate for authentication workflows used during password registration and reset.

○ One-Time Password SMS Gate
This is a one-time password SMS gate for authentication workflows used during password registration and reset.

○ Password Gate
This is a Password Gate for Authentication workflows at registration.

○ Phone Gate
This is a Phone Gate for authentication workflows used during password registration and reset.

○ QA Gate
This is a Question and Answer gate for Authentication workflows.



Activity Picker

● Approval
This activity applies for approval from specific approvers by mail.

○ Filter Validation
This activity restricts which values are valid in filter expressions used in dynamic sets and groups.

○ Function Evaluator
This activity allows functions to be used in workflow definition.

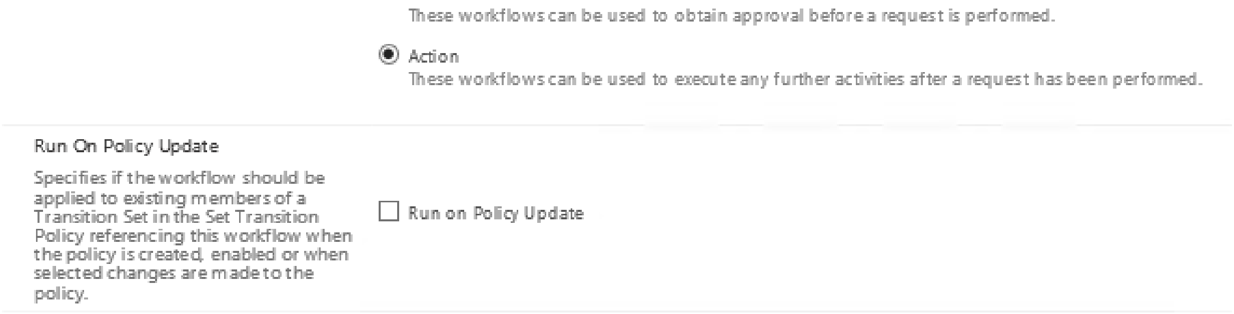
○ Group Validation
FIM Default Group Validation Activity.

○ Notification
This activity sends notification to specific recipients.

○ PAM Request MFA Validation
This activity uses Multi Factor Authentication in order to authorize the requestor

○ PAM Request Validation
This activity restricts a user to request only a PAM role in which he appears in the candidate list

○ Requestor Validation
This activity restricts a requestor's ability to add or remove members from groups they do not own.



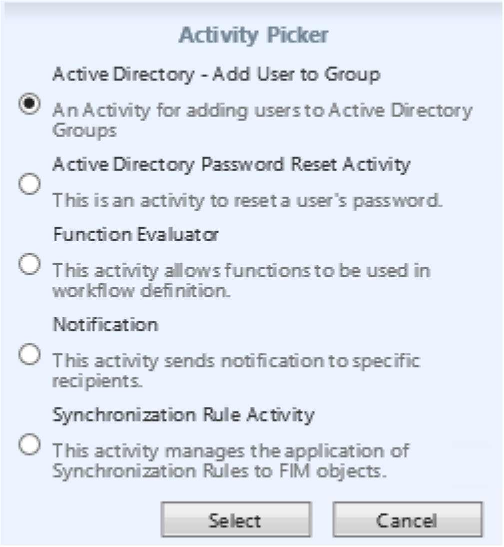
These workflows can be used to obtain approval before a request is performed.

● Action
These workflows can be used to execute any further activities after a request has been performed.

Run On Policy Update

Specifies if the workflow should be applied to existing members of a Transition Set in the Set Transition Policy referencing this workflow when the policy is created, enabled or when selected changes are made to the policy.

□ Run on Policy Update



Activity Picker

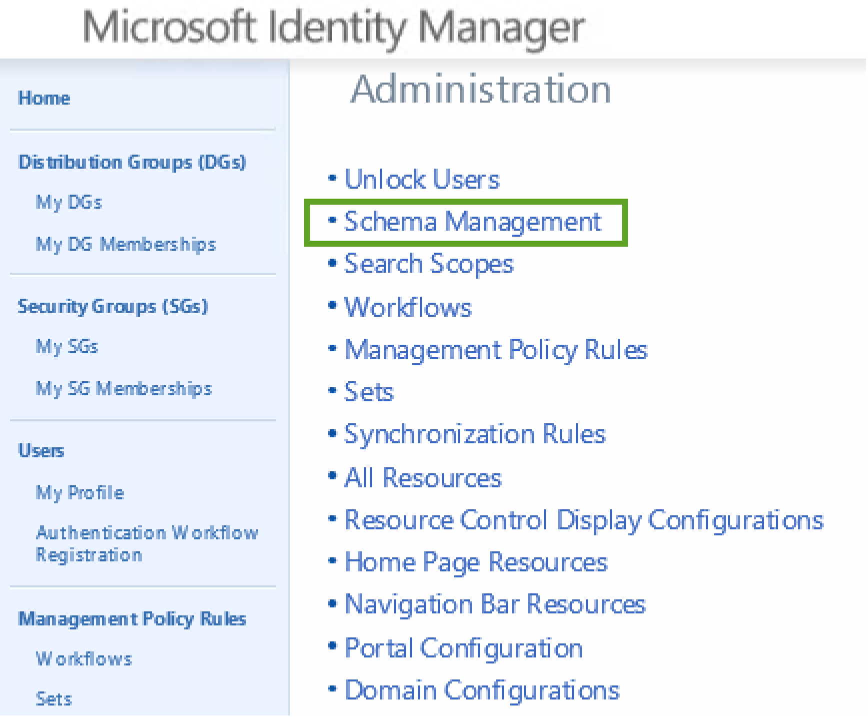
● Active Directory - Add User to Group
An Activity for adding users to Active Directory Groups

○ Active Directory Password Reset Activity
This is an activity to reset a user's password.

○ Function Evaluator
This activity allows functions to be used in workflow definition.

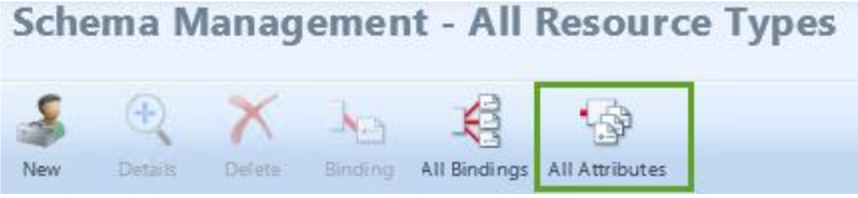
○ Notification
This activity sends notification to specific recipients.

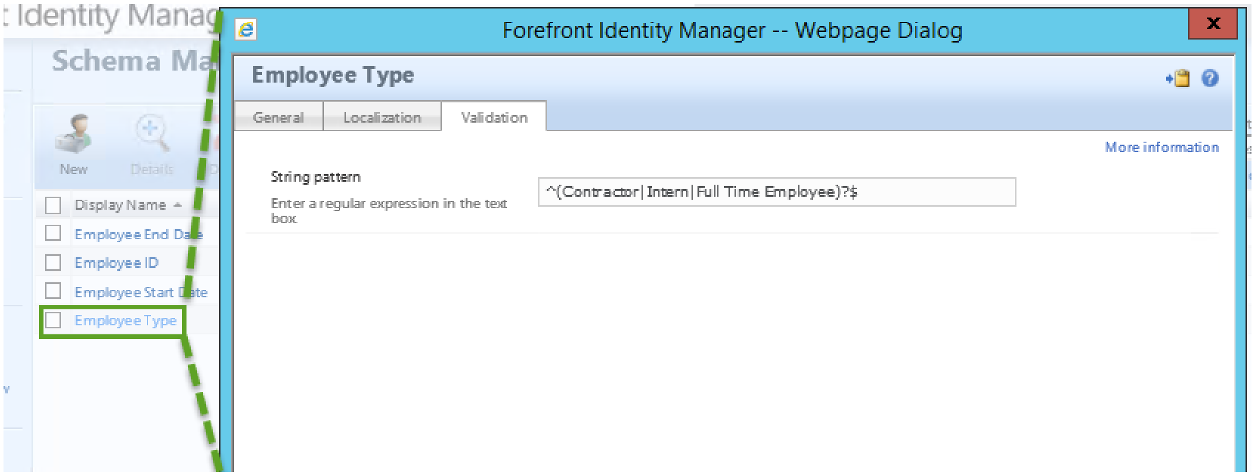
○ Synchronization Rule Activity
This activity manages the application of Synchronization Rules to FIM objects.



Administration

- Unlock Users
- Schema Management
- Search Scopes
- Workflows
- Management Policy Rules
- Sets
- Synchronization Rules
- All Resources
- Resource Control Display Configurations
- Home Page Resources
- Navigation Bar Resources
- Portal Configuration
- Domain Configurations



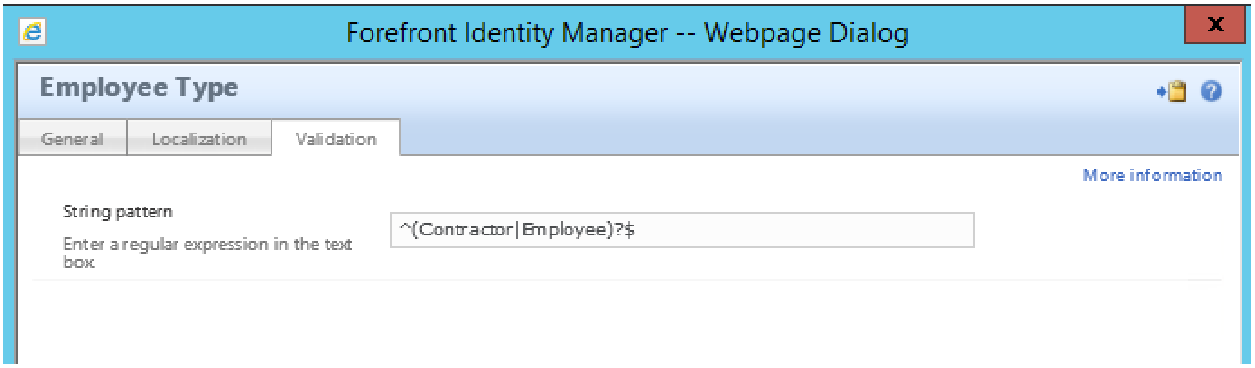


□ Display Name
□ Employee End Date
□ Employee ID
□ Employee Start Date
□ Employee Type

String pattern

Enter a regular expression in the text box

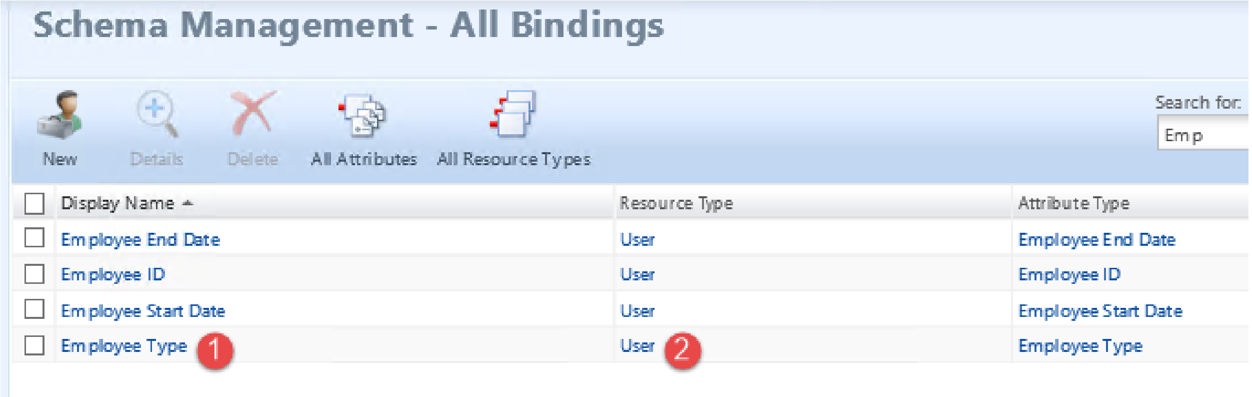
^(Contractor|Intern|Full Time Employee)?$



String pattern

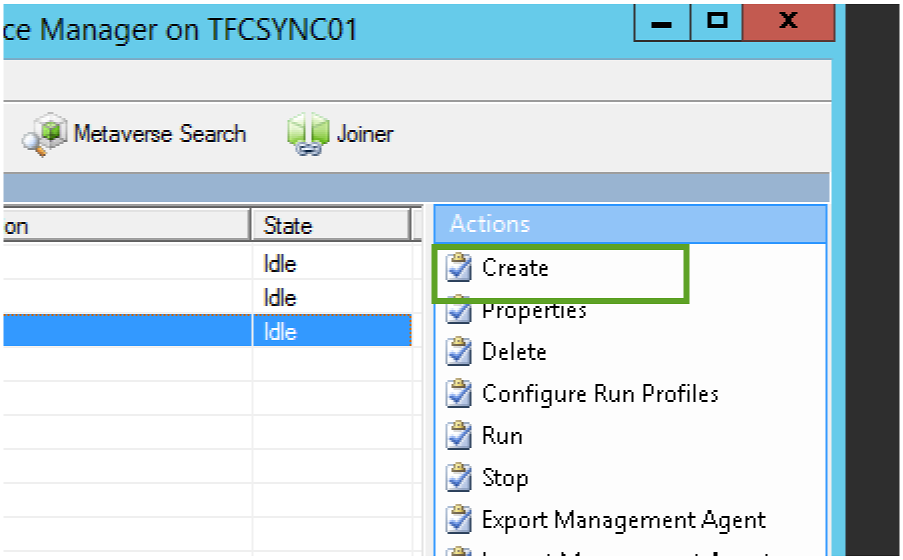
Enter a regular expression in the text box

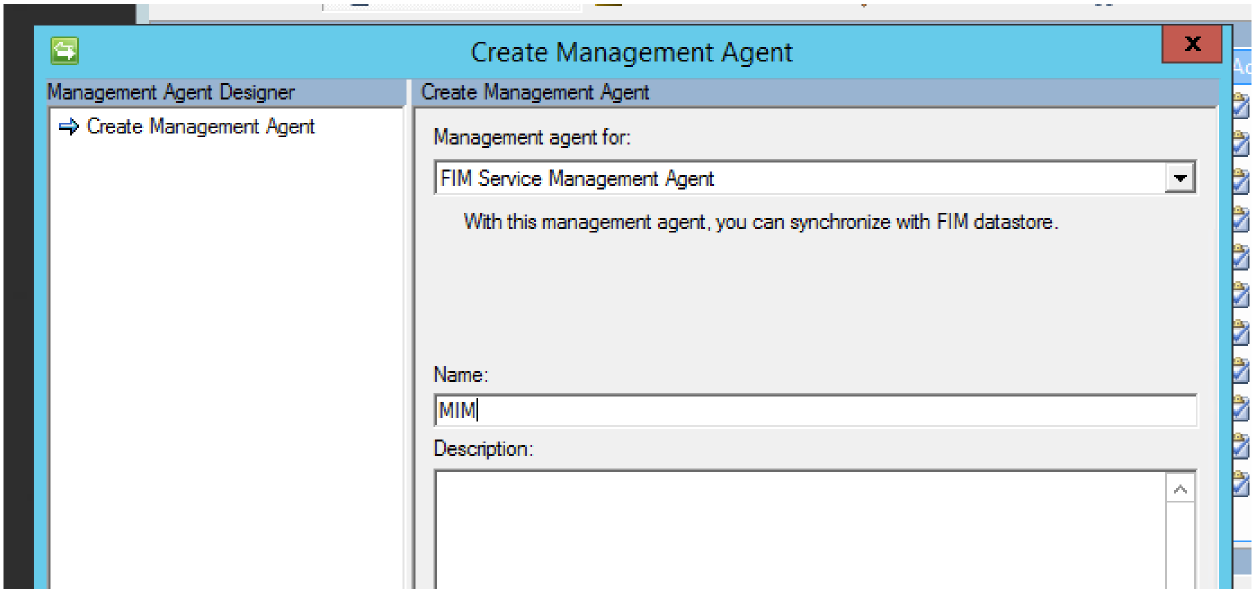
^(Contractor|Employee)?$



Search for: Emp

□	Display Name	Resource Type	Attribute Type
□	Employee End Date	User	Employee End Date
□	Employee ID	User	Employee ID
□	Employee Start Date	User	Employee Start Date
□	Employee Type	User	Employee Type



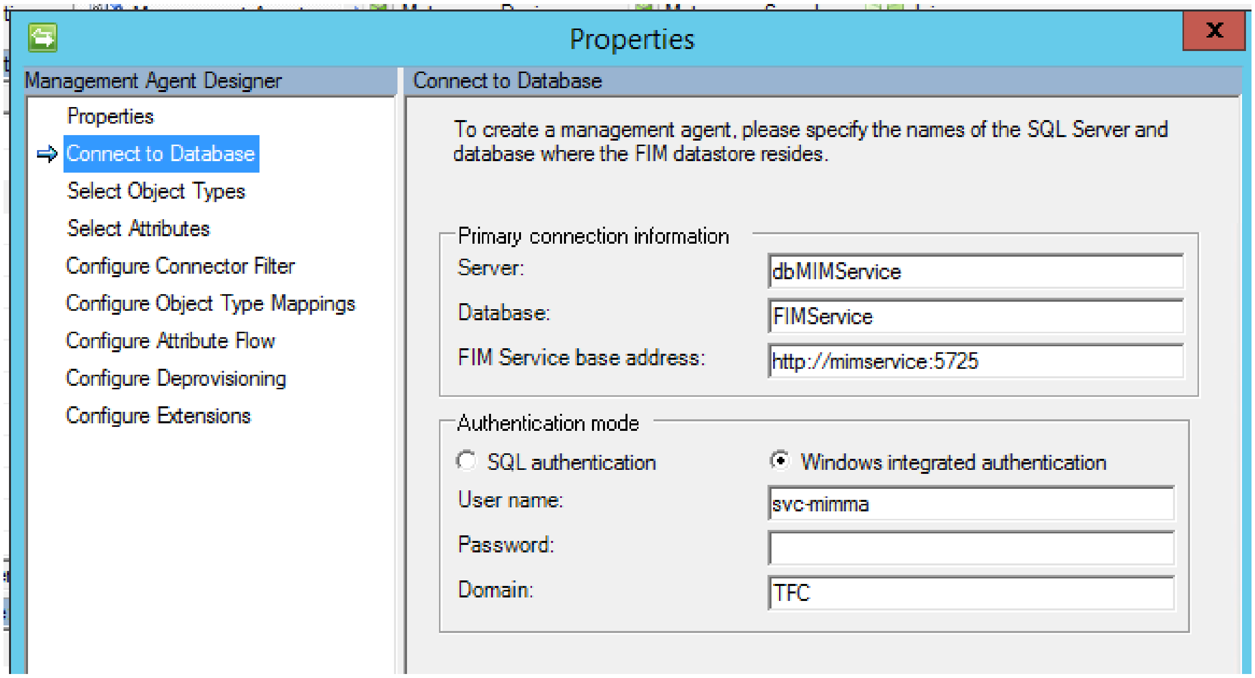


Management agent for: FIM Service Management Agent

With this management agent, you can synchronize with FIM datastore.

Name: MIM

Description:



Connect to Database

To create a management agent, please specify the names of the SQL Server and database where the FIM datastore resides.

Primary connection information

Server: dbMIMService

Database: FIMService

FIM Service base address: http://mimservice:5725

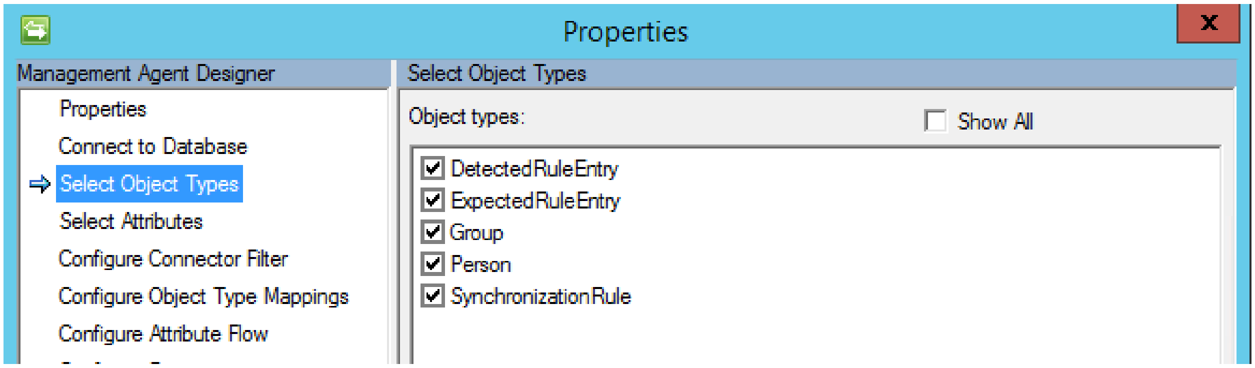
Authentication mode

○ SQL authentication ● Windows integrated authentication

User name: svc-mimma

Password:

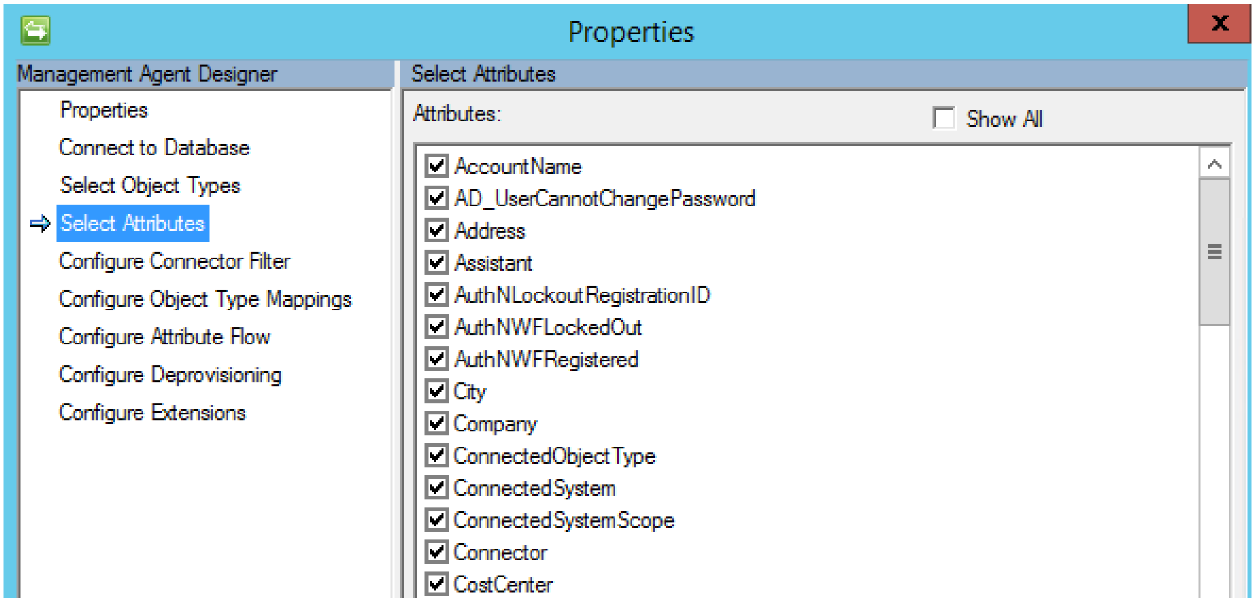
Domain: TFC



Select Object Types

Object types: □ Show All

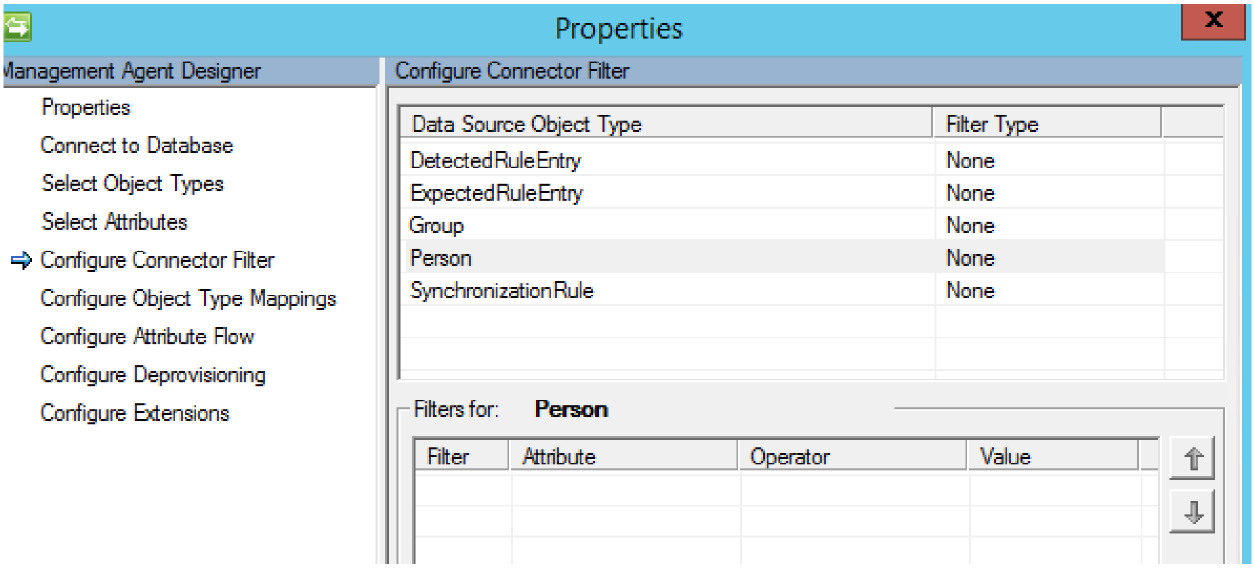
☑ DetectedRuleEntry
☑ ExpectedRuleEntry
☑ Group
☑ Person
☑ SynchronizationRule



Select Attributes

Attributes: □ Show All

☑ AccountName
☑ AD_UserCannotChangePassword
☑ Address
☑ Assistant
☑ AuthNLockoutRegistrationID
☑ AuthNWFLockedOut
☑ AuthNWFRegistered
☑ City
☑ Company
☑ ConnectedObjectType
☑ ConnectedSystem
☑ ConnectedSystemScope
☑ Connector
☑ CostCenter



Properties

Management Agent Designer

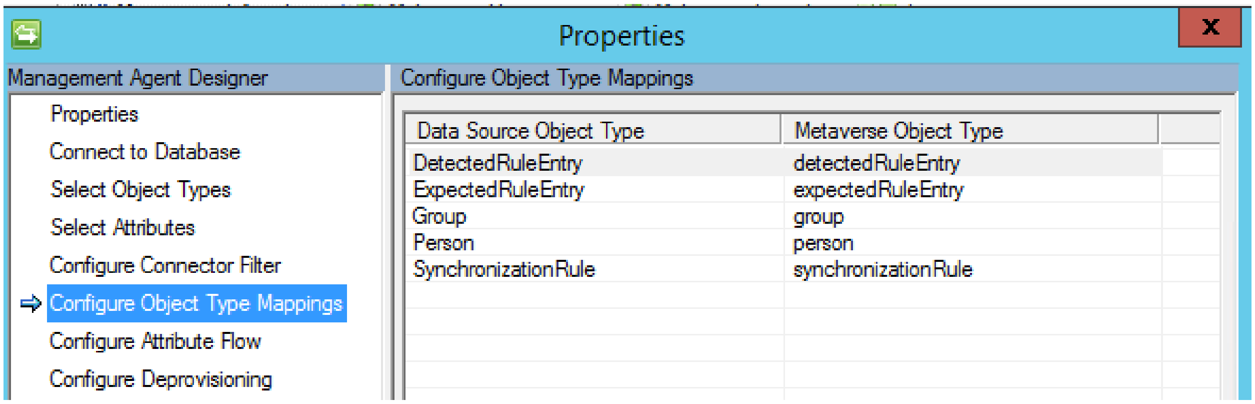
- Properties
- Connect to Database
- Select Object Types
- Select Attributes
- Configure Connector Filter
- Configure Object Type Mappings
- Configure Attribute Flow
- Configure Deprovisioning
- Configure Extensions

Configure Connector Filter

Data Source Object Type	Filter Type
DetectedRuleEntry	None
ExpectedRuleEntry	None
Group	None
Person	None
SynchronizationRule	None

Filters for: **Person**

Filter	Attribute	Operator	Value



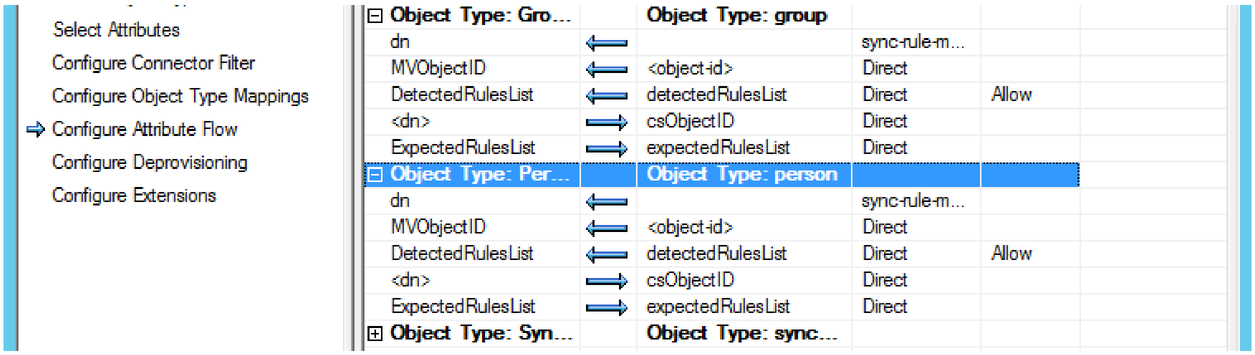
Properties

Management Agent Designer

- Properties
- Connect to Database
- Select Object Types
- Select Attributes
- Configure Connector Filter
- Configure Object Type Mappings
- Configure Attribute Flow
- Configure Deprovisioning

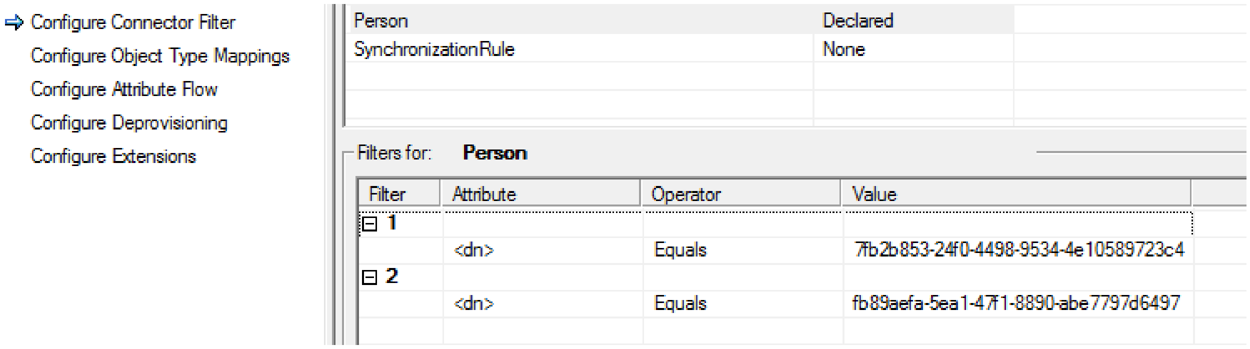
Configure Object Type Mappings

Data Source Object Type	Metaverse Object Type
DetectedRuleEntry	detectedRuleEntry
ExpectedRuleEntry	expectedRuleEntry
Group	group
Person	person
SynchronizationRule	synchronizationRule



- Select Attributes
- Configure Connector Filter
- Configure Object Type Mappings
- Configure Attribute Flow
- Configure Deprovisioning
- Configure Extensions

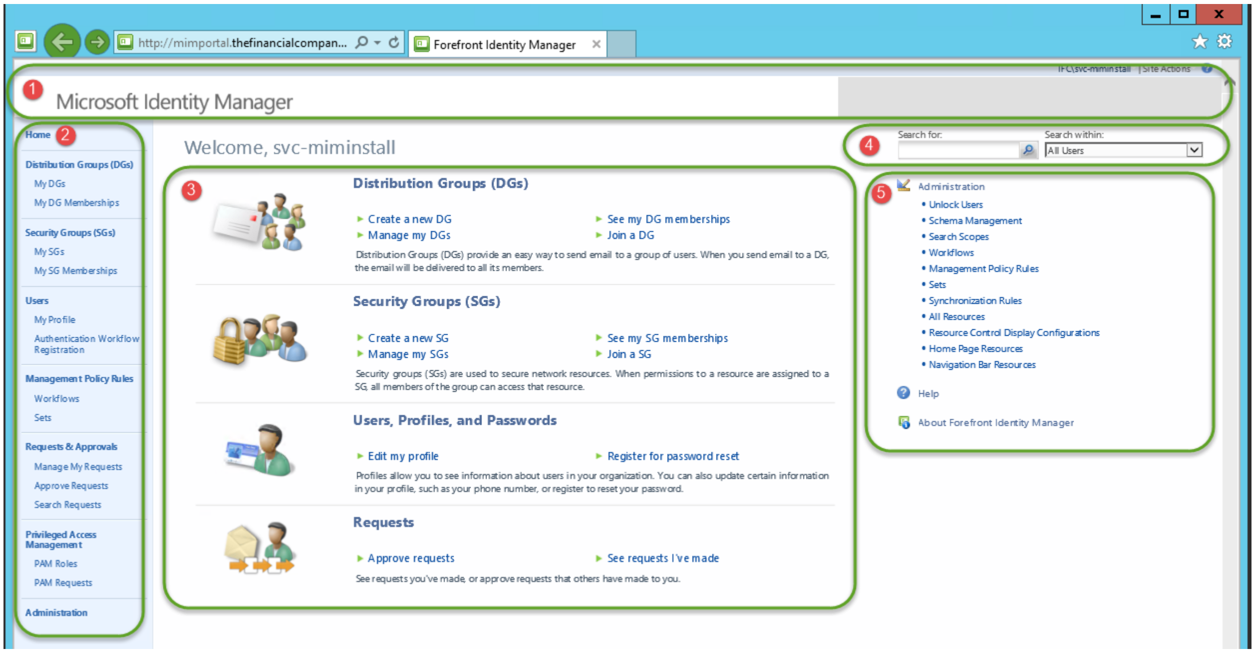
⊟ **Object Type: Gro...**		**Object Type: group**		
dn	←		sync-rule-m...	
MVObjectID	←	<object-id>	Direct	
DetectedRulesList	←	detectedRulesList	Direct	Allow
<dn>	→	csObjectID	Direct	
ExpectedRulesList	→	expectedRulesList	Direct	
⊟ **Object Type: Per...**		**Object Type: person**		
dn	←		sync-rule-m...	
MVObjectID	←	<object-id>	Direct	
DetectedRulesList	←	detectedRulesList	Direct	Allow
<dn>	→	csObjectID	Direct	
ExpectedRulesList	→	expectedRulesList	Direct	
⊞ **Object Type: Syn...**		**Object Type: sync...**		



Person	Declared
SynchronizationRule	None

Filters for: **Person**

Filter	Attribute	Operator	Value
⊟ 1			
	<dn>	Equals	7fb2b853-24f0-4498-9534-4e10589723c4
⊟ 2			
	<dn>	Equals	fb89aefa-5ea1-47f1-8890-abe7797d6497



Welcome, svc-miminstall

Distribution Groups (DGs)

- Create a new DG
- Manage my DGs
- See my DG memberships
- Join a DG

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.

Security Groups (SGs)

- Create a new SG
- Manage my SGs
- See my SG memberships
- Join a SG

Security groups (SGs) are used to secure network resources. When permissions to a resource are assigned to a SG, all members of the group can access that resource.

Users, Profiles, and Passwords

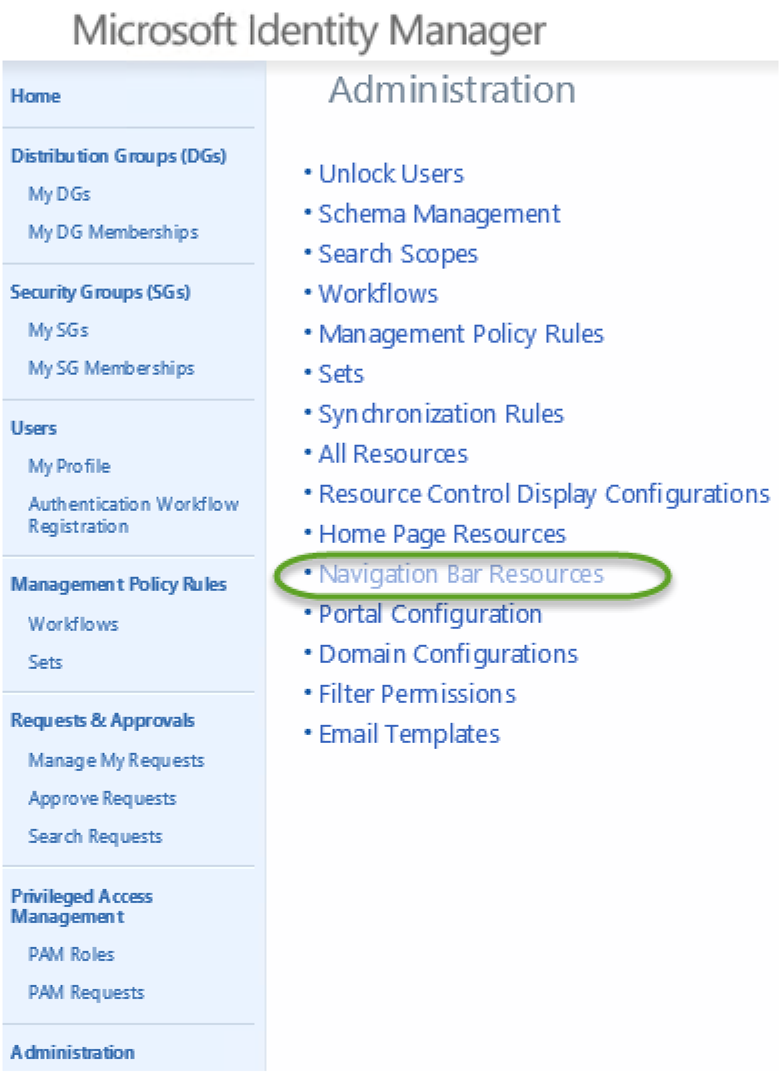
- Edit my profile
- Register for password reset

Profiles allow you to see information about users in your organization. You can also update certain information in your profile, such as your phone number, or register to reset your password.

Requests

- Approve requests
- See requests I've made

See requests you've made, or approve requests that others have made to you.

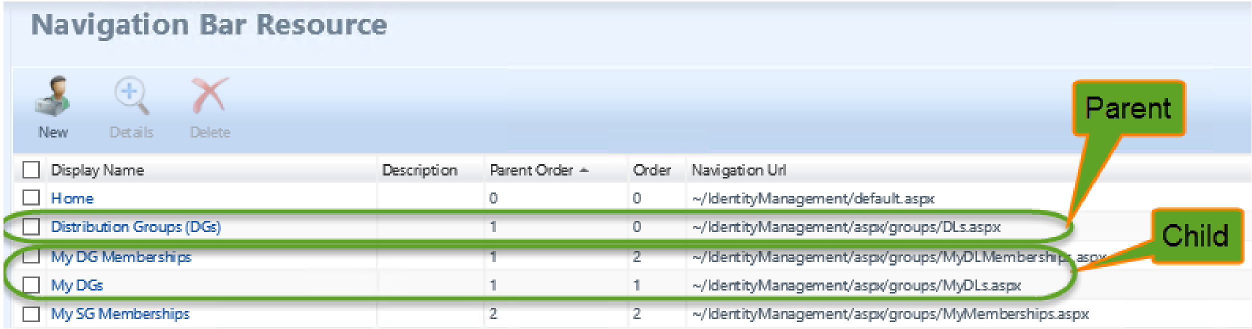


Microsoft Identity Manager

- Home
- Distribution Groups (DGs)
  - My DGs
  - My DG Memberships
- Security Groups (SGs)
  - My SGs
  - My SG Memberships
- Users
  - My Profile
  - Authentication Workflow Registration
- Management Policy Rules
  - Workflows
  - Sets
- Requests & Approvals
  - Manage My Requests
  - Approve Requests
  - Search Requests
- Privileged Access Management
  - PAM Roles
  - PAM Requests
- Administration

Administration

- Unlock Users
- Schema Management
- Search Scopes
- Workflows
- Management Policy Rules
- Sets
- Synchronization Rules
- All Resources
- Resource Control Display Configurations
- Home Page Resources
- Navigation Bar Resources
- Portal Configuration
- Domain Configurations
- Filter Permissions
- Email Templates

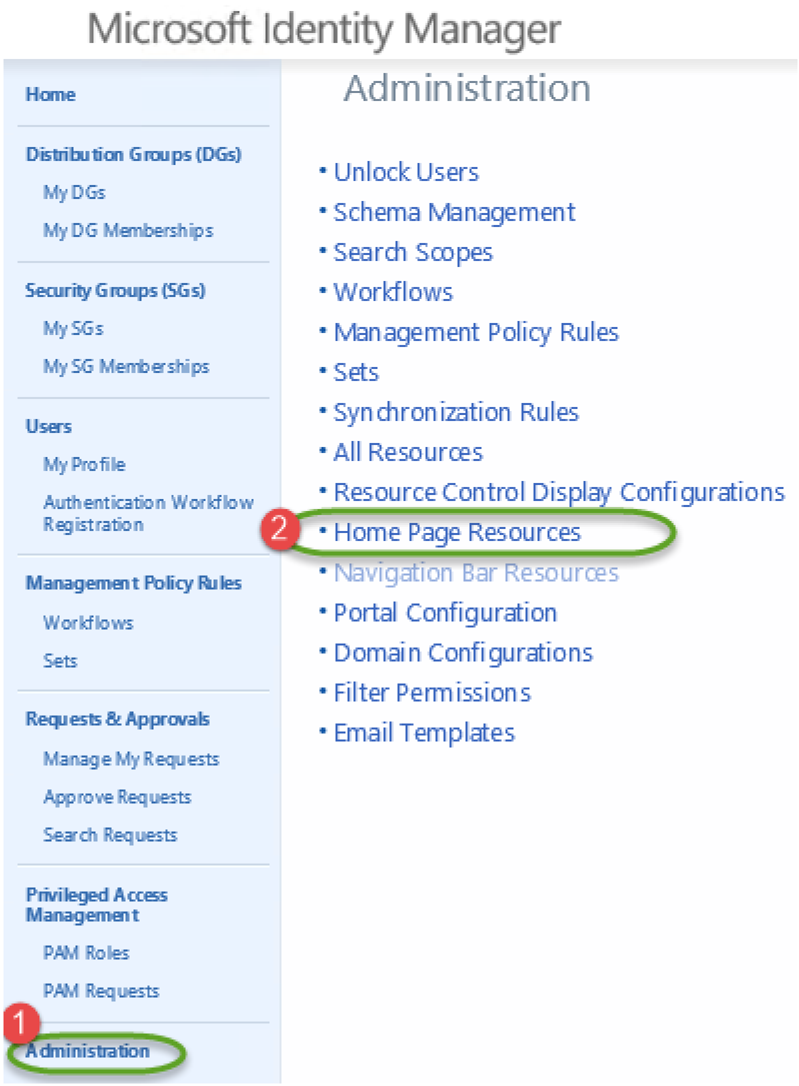


Navigation Bar Resource

☐	Display Name	Description	Parent Order ▲	Order	Navigation Url
☐	Home		0	0	~/IdentityManagement/default.aspx
☐	Distribution Groups (DGs)		1	0	~/IdentityManagement/aspx/groups/DLs.aspx
☐	My DG Memberships		1	2	~/IdentityManagement/aspx/groups/MyDLMemberships.aspx
☐	My DGs		1	1	~/IdentityManagement/aspx/groups/MyDLs.aspx
☐	My SG Memberships		2	2	~/IdentityManagement/aspx/groups/MyMemberships.aspx

Parent

Child

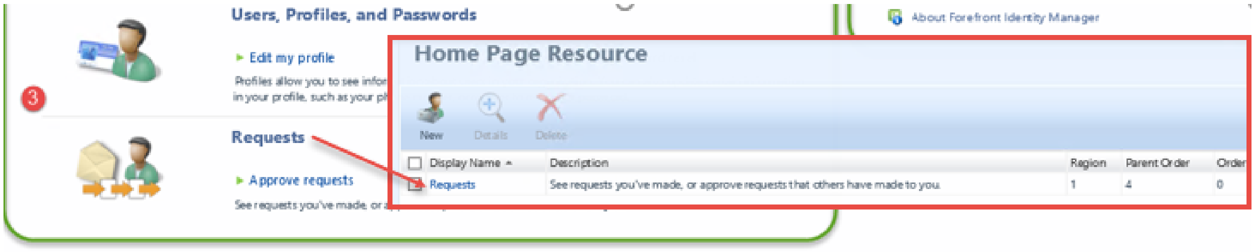


Microsoft Identity Manager

Administration

- Home
- Distribution Groups (DGs)
  - My DGs
  - My DG Memberships
- Security Groups (SGs)
  - My SGs
  - My SG Memberships
- Users
  - My Profile
  - Authentication Workflow Registration
- Management Policy Rules
  - Workflows
  - Sets
- Requests & Approvals
  - Manage My Requests
  - Approve Requests
  - Search Requests
- Privileged Access Management
  - PAM Roles
  - PAM Requests
- 1 Administration

- Unlock Users
- Schema Management
- Search Scopes
- Workflows
- Management Policy Rules
- Sets
- Synchronization Rules
- All Resources
- Resource Control Display Configurations
- 2 Home Page Resources
- Navigation Bar Resources
- Portal Configuration
- Domain Configurations
- Filter Permissions
- Email Templates



Users, Profiles, and Passwords

▸ Edit my profile

Profiles allow you to see infor
in your profile, such as your pl

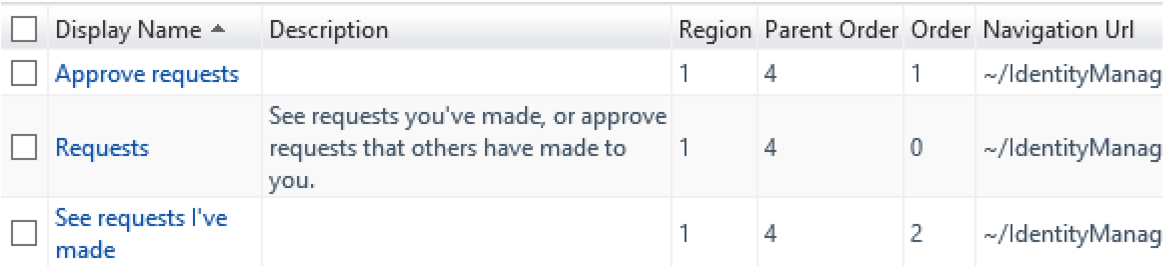
Requests

▸ Approve requests

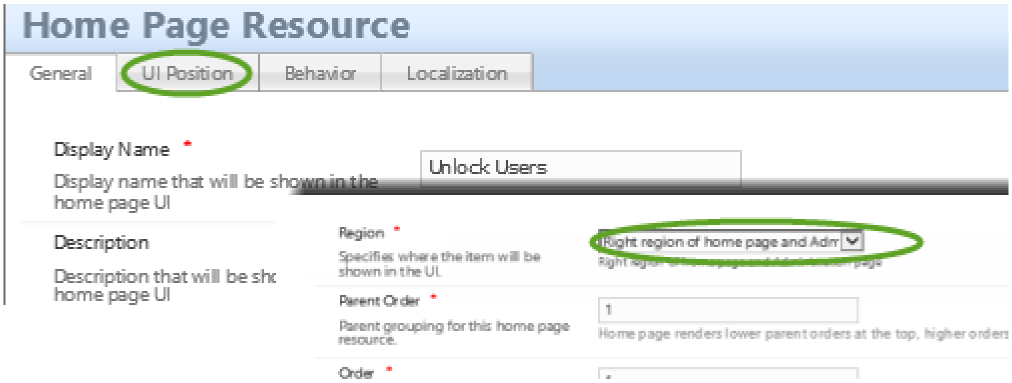
See requests you've made, or a

Home Page Resource

□	Display Name ▲	Description	Region	Parent Order	Order
□	Requests	See requests you've made, or approve requests that others have made to you.	1	4	0



□	Display Name ▲	Description	Region	Parent Order	Order	Navigation Url
□	Approve requests		1	4	1	~/IdentityManag
□	Requests	See requests you've made, or approve requests that others have made to you.	1	4	0	~/IdentityManag
□	See requests I've made		1	4	2	~/IdentityManag



Home Page Resource

Display Name *

Display name that will be shown in the home page UI

Unlock Users

Description

Description that will be shc home page UI

Region *

Specifies where the item will be shown in the UI.

Right region of home page and Adm

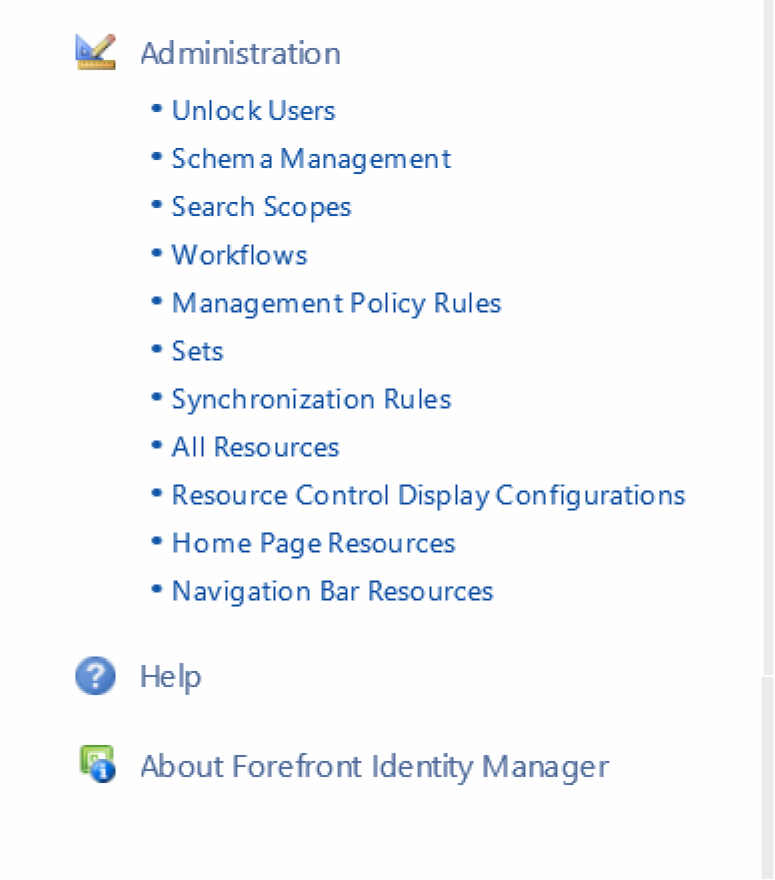
Parent Order *

Parent grouping for this home page resource.

1

Home page renders lower parent orders at the top, higher orders

Order *

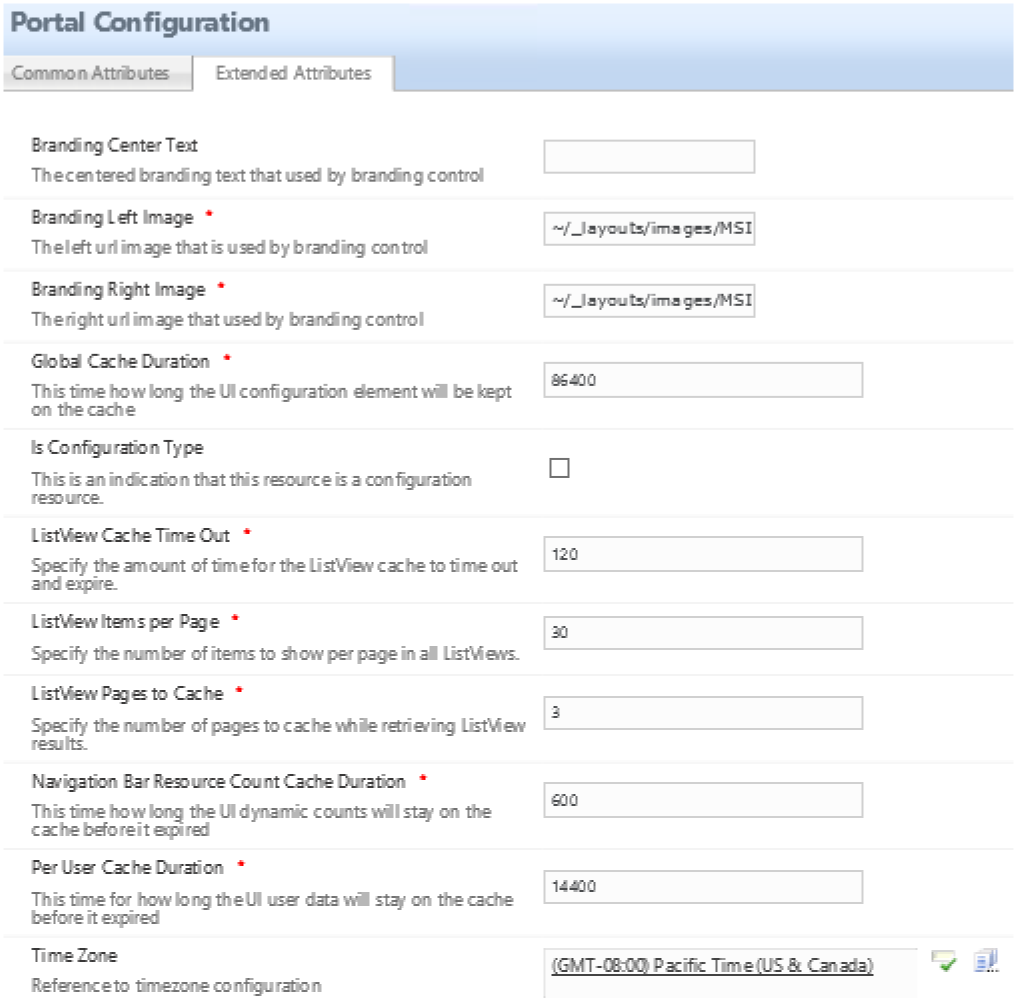


Administration

- Unlock Users
- Schema Management
- Search Scopes
- Workflows
- Management Policy Rules
- Sets
- Synchronization Rules
- All Resources
- Resource Control Display Configurations
- Home Page Resources
- Navigation Bar Resources

Help

About Forefront Identity Manager



Portal Configuration

Common Attributes | Extended Attributes

Branding Center Text
The centered branding text that used by branding control

Branding Left Image *
The left url image that is used by branding control
~/_layouts/images/MSI

Branding Right Image *
The right url image that used by branding control
~/_layouts/images/MSI

Global Cache Duration *
This time how long the UI configuration element will be kept on the cache
86400

Is Configuration Type
This is an indication that this resource is a configuration resource.
□

ListView Cache Time Out *
Specify the amount of time for the ListView cache to time out and expire.
120

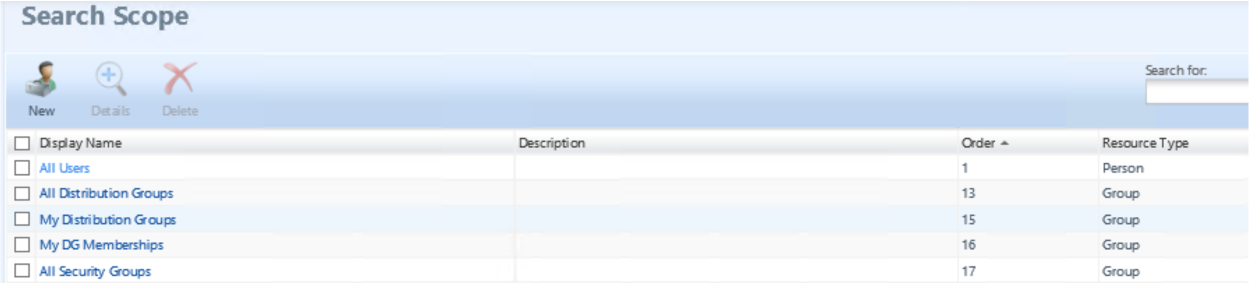
ListView Items per Page *
Specify the number of items to show per page in all ListViews.
30

ListView Pages to Cache *
Specify the number of pages to cache while retrieving ListView results.
3

Navigation Bar Resource Count Cache Duration *
This time how long the UI dynamic counts will stay on the cache before it expired
600

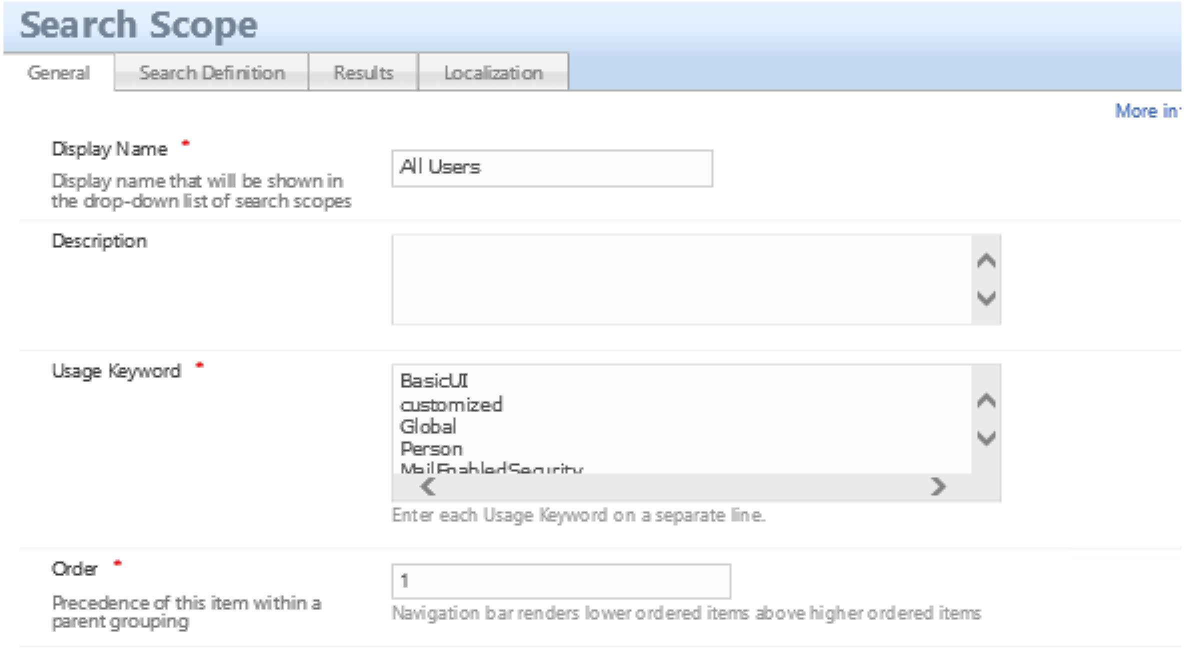
Per User Cache Duration *
This time for how long the UI user data will stay on the cache before it expired
14400

Time Zone
Reference to timezone configuration
(GMT-08:00) Pacific Time (US & Canada)



Search Scope

□ Display Name	Description	Order ▲	Resource Type
□ All Users		1	Person
□ All Distribution Groups		13	Group
□ My Distribution Groups		15	Group
□ My DG Memberships		16	Group
□ All Security Groups		17	Group



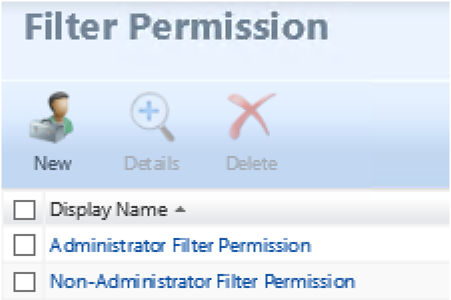
Search Scope

Display Name *
Display name that will be shown in the drop-down list of search scopes
All Users

Description

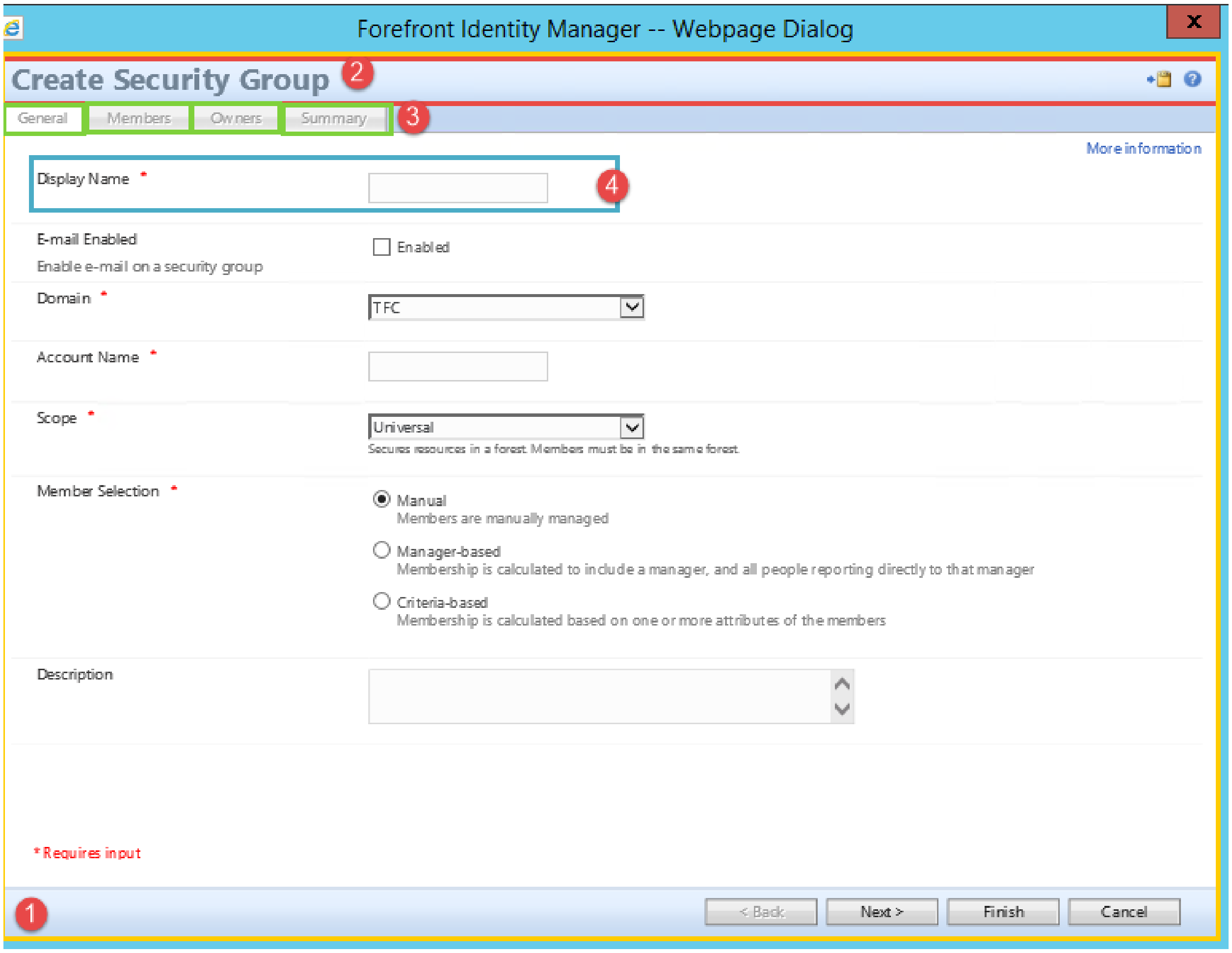
Usage Keyword *
BasicUI
customized
Global
Person
MailEnabledSecurity
Enter each Usage Keyword on a separate line.

Order *
Precedence of this item within a parent grouping
1
Navigation bar renders lower ordered items above higher ordered items



Filter Permission

□	Display Name ▲
□	Administrator Filter Permission
□	Non-Administrator Filter Permission



Forefront Identity Manager -- Webpage Dialog

Create Security Group

Display Name *

E-mail Enabled
Enable e-mail on a security group
□ Enabled

Domain * TFC

Account Name *

Scope * Universal
Secures resources in a forest. Members must be in the same forest.

Member Selection *

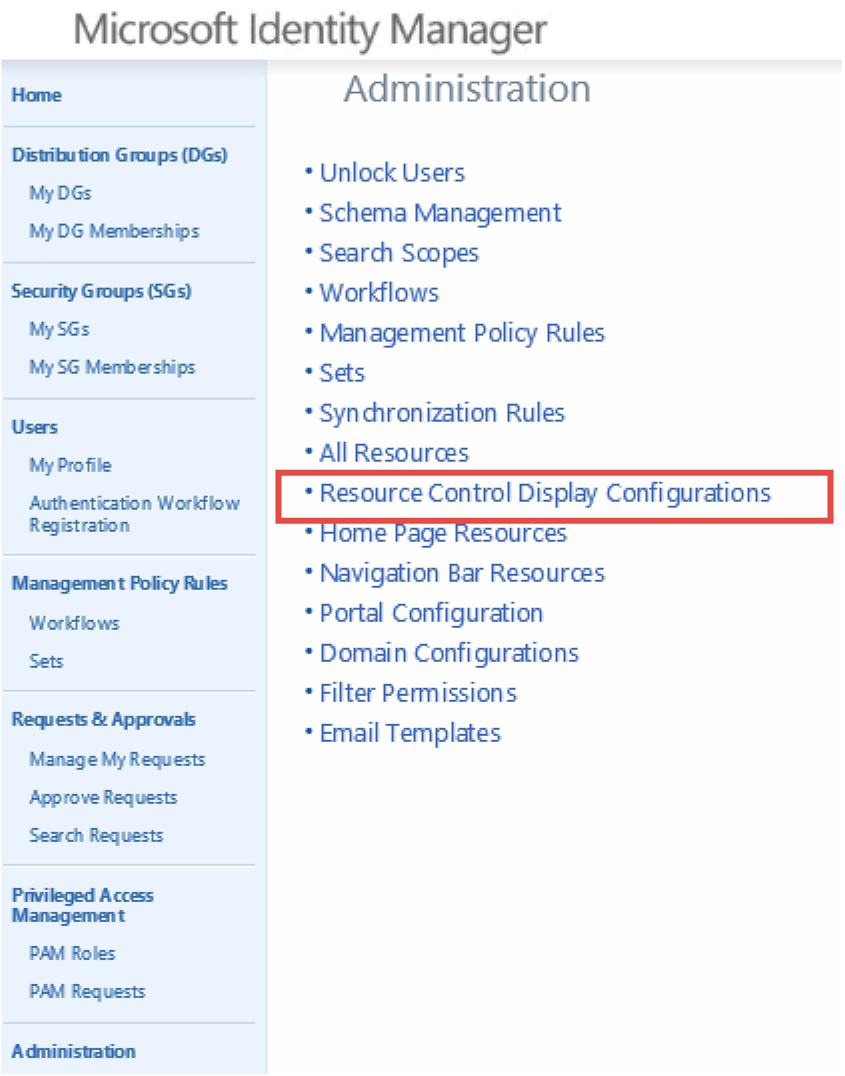
● Manual
Members are manually managed

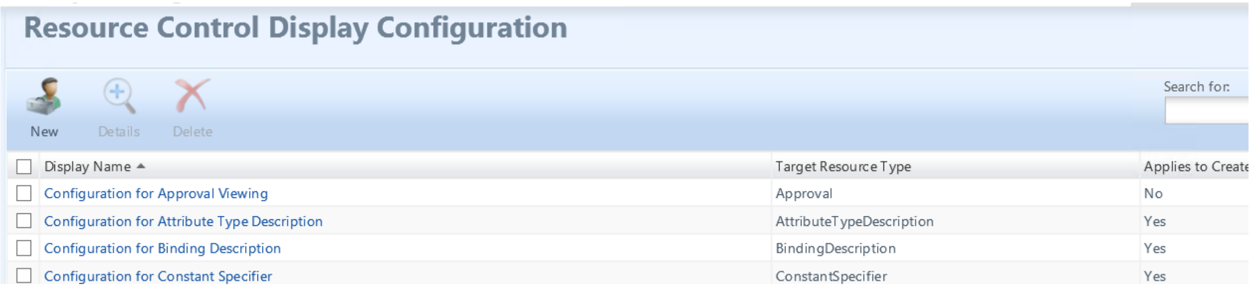
○ Manager-based
Membership is calculated to include a manager, and all people reporting directly to that manager

○ Criteria-based
Membership is calculated based on one or more attributes of the members

Description

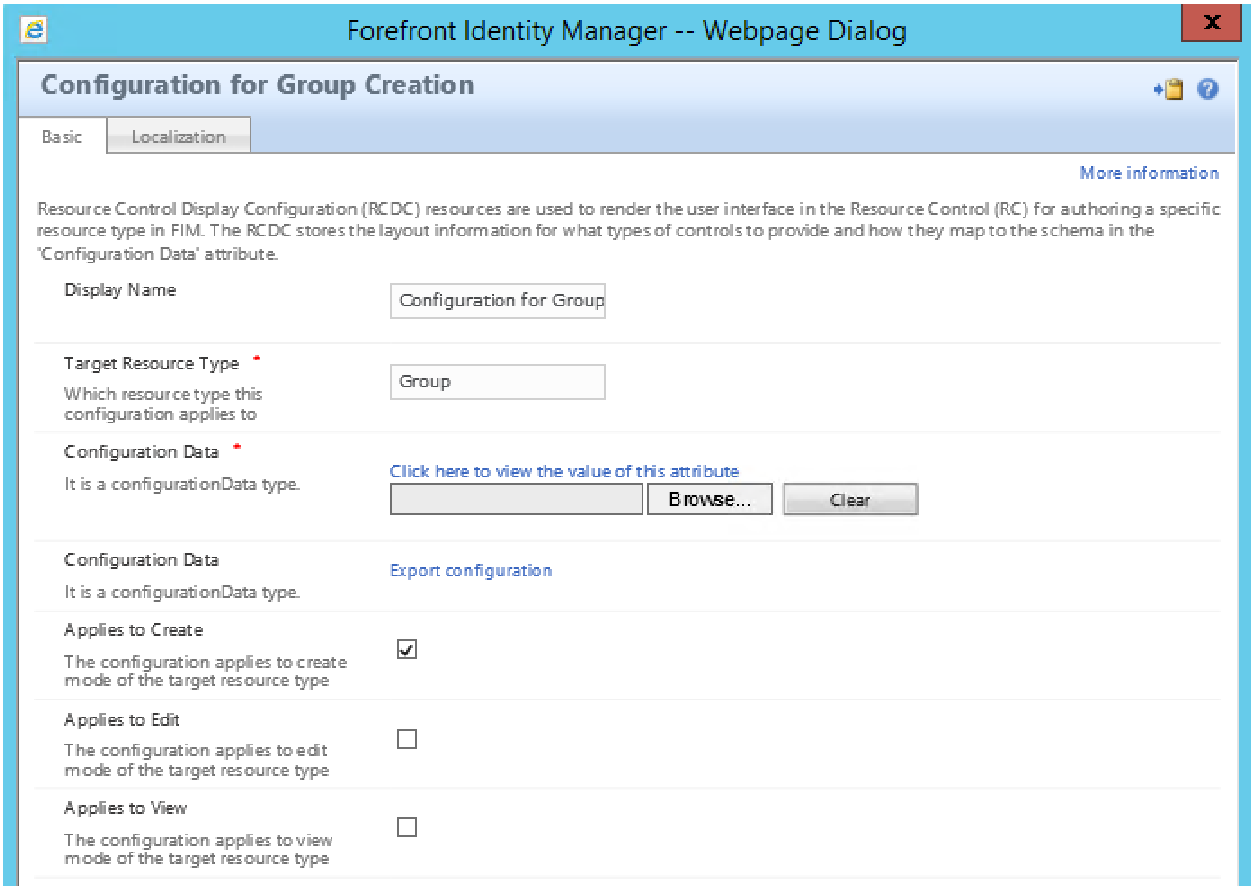
* Requires input





Resource Control Display Configuration

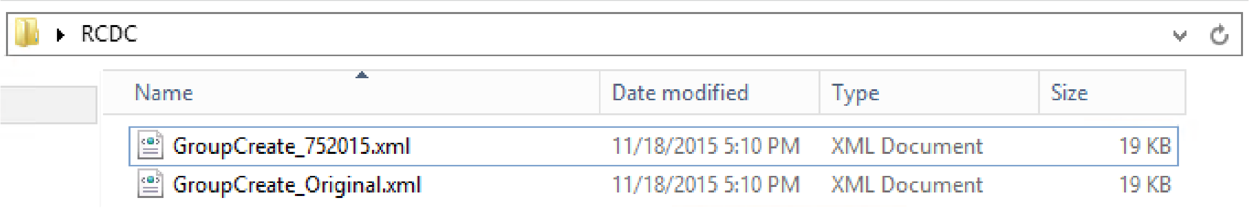
□ Display Name ▲	Target Resource Type	Applies to Create
□ Configuration for Approval Viewing	Approval	No
□ Configuration for Attribute Type Description	AttributeTypeDescription	Yes
□ Configuration for Binding Description	BindingDescription	Yes
□ Configuration for Constant Specifier	ConstantSpecifier	Yes



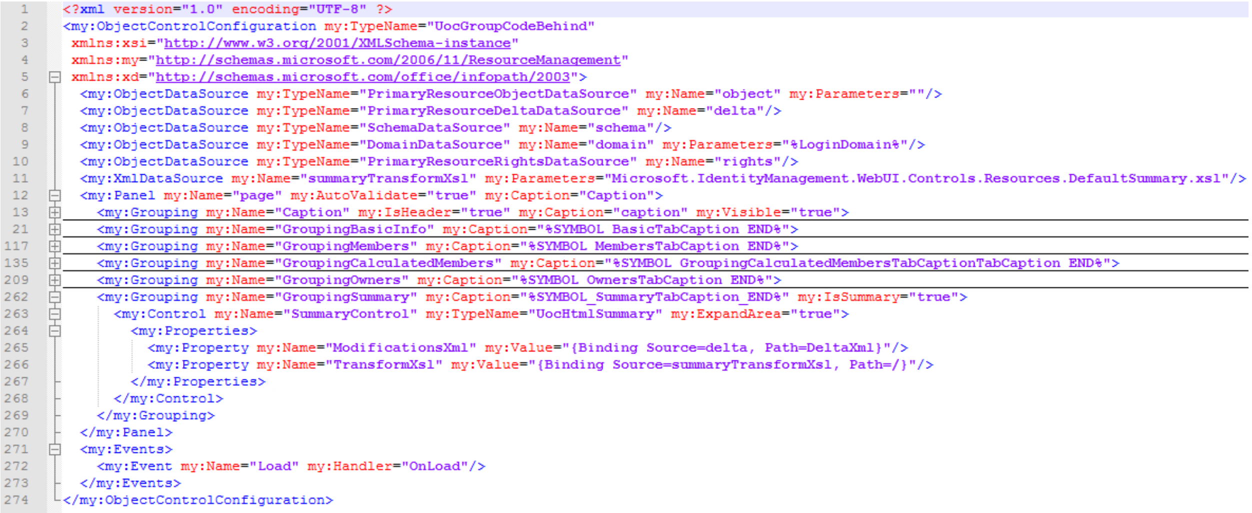
Configuration for Group Creation

Resource Control Display Configuration (RCDC) resources are used to render the user interface in the Resource Control (RC) for authoring a specific resource type in FIM. The RCDC stores the layout information for what types of controls to provide and how they map to the schema in the 'Configuration Data' attribute.

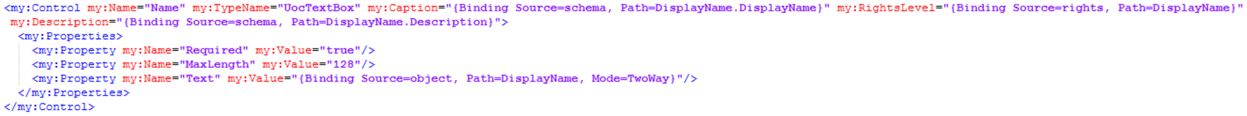
Display Name	Configuration for Group
Target Resource Type * Which resource type this configuration applies to	Group
Configuration Data * It is a configurationData type.	Click here to view the value of this attribute Browse... Clear
Configuration Data It is a configurationData type.	Export configuration
Applies to Create The configuration applies to create mode of the target resource type	☑
Applies to Edit The configuration applies to edit mode of the target resource type	☐
Applies to View The configuration applies to view mode of the target resource type	☐



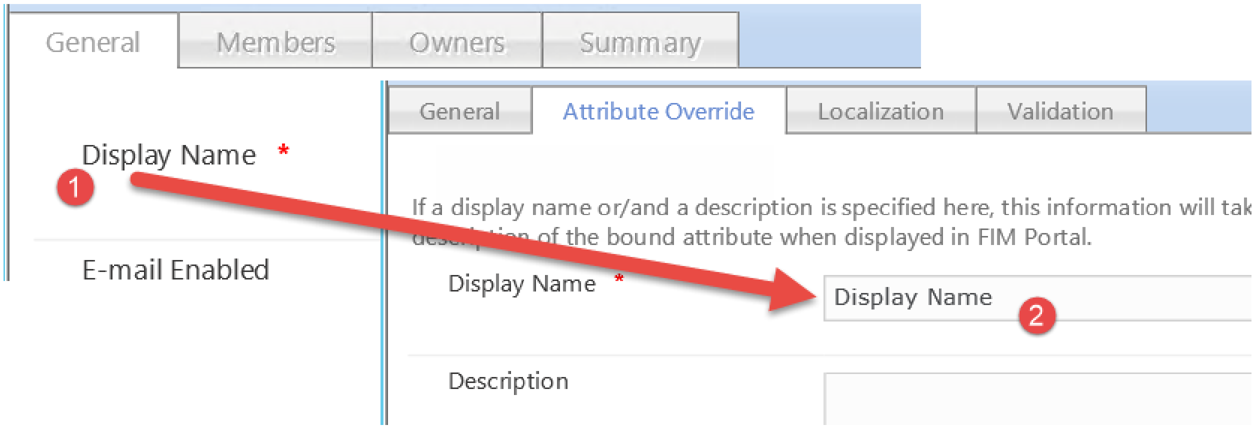
Name	Date modified	Type	Size
GroupCreate_752015.xml	11/18/2015 5:10 PM	XML Document	19 KB
GroupCreate_Original.xml	11/18/2015 5:10 PM	XML Document	19 KB



```
<?xml version="1.0" encoding="UTF-8" ?>
<my:ObjectControlConfiguration my:TypeName="UocGroupCodeBehind"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xmlns:my="http://schemas.microsoft.com/2006/11/ResourceManagement"
 xmlns:xd="http://schemas.microsoft.com/office/infopath/2003">
  <my:ObjectDataSource my:TypeName="PrimaryResourceObjectDataSource" my:Name="object" my:Parameters=""/>
  <my:ObjectDataSource my:TypeName="PrimaryResourceDeltaDataSource" my:Name="delta"/>
  <my:ObjectDataSource my:TypeName="SchemaDataSource" my:Name="schema"/>
  <my:ObjectDataSource my:TypeName="DomainDataSource" my:Name="domain" my:Parameters="%LoginDomain%"/>
  <my:ObjectDataSource my:TypeName="PrimaryResourceRightsDataSource" my:Name="rights"/>
  <my:XmlDataSource my:Name="summaryTransformXsl" my:Parameters="Microsoft.IdentityManagement.WebUI.Controls.Resources.DefaultSummary.xsl"/>
  <my:Panel my:Name="page" my:AutoValidate="true" my:Caption="Caption">
    <my:Grouping my:Name="Caption" my:IsHeader="true" my:Caption="caption" my:Visible="true">
    <my:Grouping my:Name="GroupingBasicInfo" my:Caption="%SYMBOL BasicTabCaption END%">
    <my:Grouping my:Name="GroupingMembers" my:Caption="%SYMBOL MembersTabCaption END%">
    <my:Grouping my:Name="GroupingCalculatedMembers" my:Caption="%SYMBOL GroupingCalculatedMembersTabCaptionTabCaption END%">
    <my:Grouping my:Name="GroupingOwners" my:Caption="%SYMBOL OwnersTabCaption END%">
    <my:Grouping my:Name="GroupingSummary" my:Caption="%SYMBOL_SummaryTabCaption_END%" my:IsSummary="true">
      <my:Control my:Name="SummaryControl" my:TypeName="UocHtmlSummary" my:ExpandArea="true">
        <my:Properties>
          <my:Property my:Name="ModificationsXml" my:Value="{Binding Source=delta, Path=DeltaXml}"/>
          <my:Property my:Name="TransformXsl" my:Value="{Binding Source=summaryTransformXsl, Path=/}"/>
        </my:Properties>
      </my:Control>
    </my:Grouping>
  </my:Panel>
  <my:Events>
    <my:Event my:Name="Load" my:Handler="OnLoad"/>
  </my:Events>
</my:ObjectControlConfiguration>
```



```
<my:Control my:Name="Name" my:TypeName="UocTextBox" my:Caption="{Binding Source=schema, Path=DisplayName.DisplayName}" my:RightsLevel="{Binding Source=rights, Path=DisplayName}"
 my:Description="{Binding Source=schema, Path=DisplayName.Description}">
  <my:Properties>
    <my:Property my:Name="Required" my:Value="true"/>
    <my:Property my:Name="MaxLength" my:Value="128"/>
    <my:Property my:Name="Text" my:Value="{Binding Source=object, Path=DisplayName, Mode=TwoWay}"/>
  </my:Properties>
</my:Control>
```



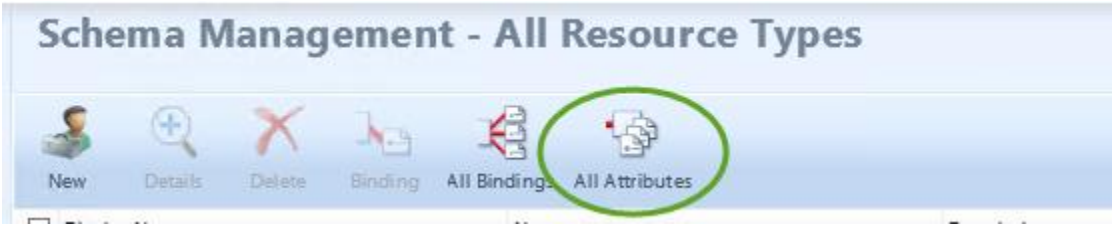
Display Name *

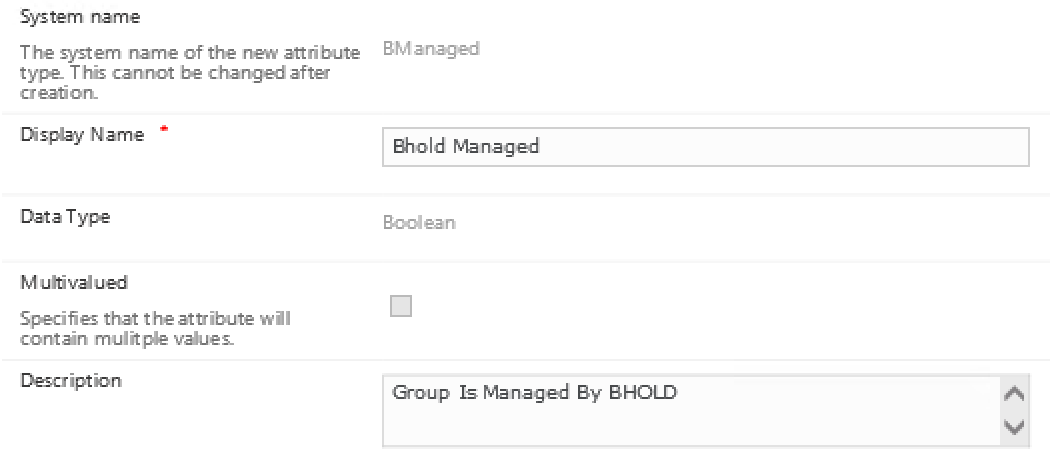
E-mail Enabled

If a display name or/and a description is specified here, this information will tak
description of the bound attribute when displayed in FIM Portal.

Display Name * Display Name

Description





System name

The system name of the new attribute type. This cannot be changed after creation.

BManaged

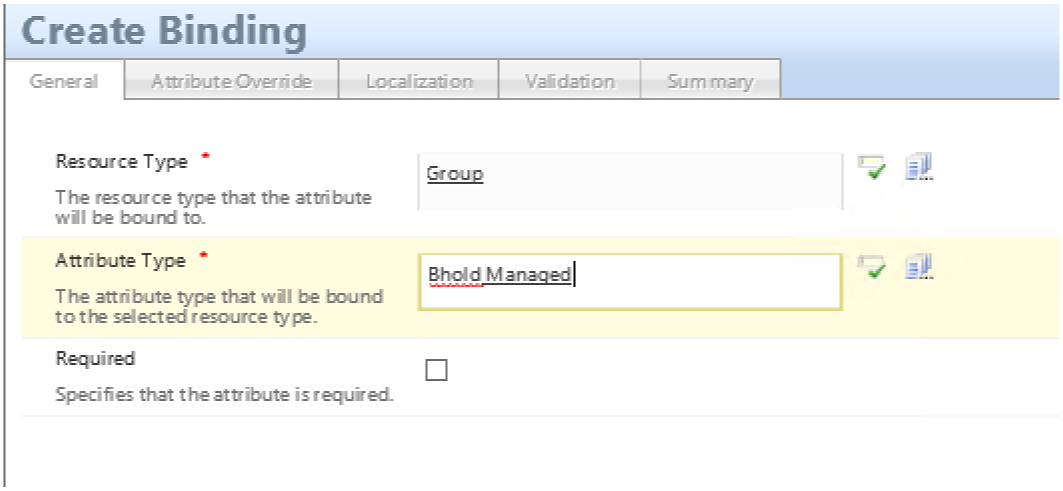
Display Name * Bhold Managed

Data Type Boolean

Multivalued □

Specifies that the attribute will contain mulitple values.

Description Group Is Managed By BHOLD



Create Binding

Resource Type *

The resource type that the attribute will be bound to.

Group

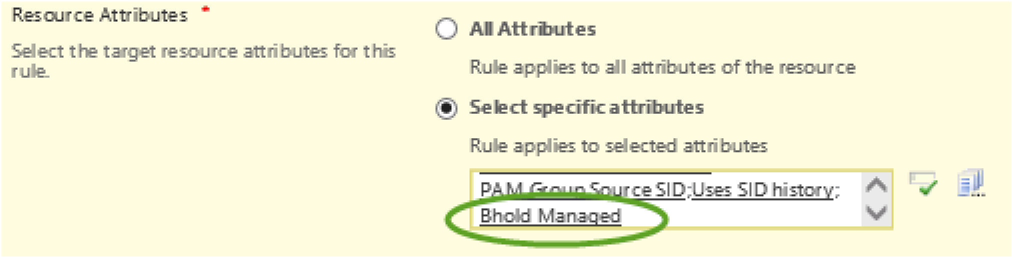
Attribute Type *

The attribute type that will be bound to the selected resource type.

Bhold Managed

Required □

Specifies that the attribute is required.



Resource Attributes *

Select the target resource attributes for this rule.

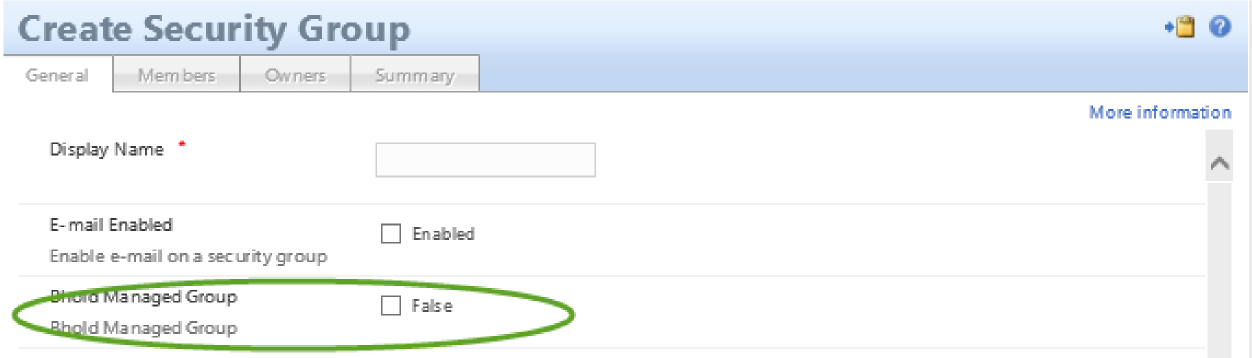
○ **All Attributes**

Rule applies to all attributes of the resource

● **Select specific attributes**

Rule applies to selected attributes

PAM Group Source SID;Uses SID history; Bhold Managed



Create Security Group

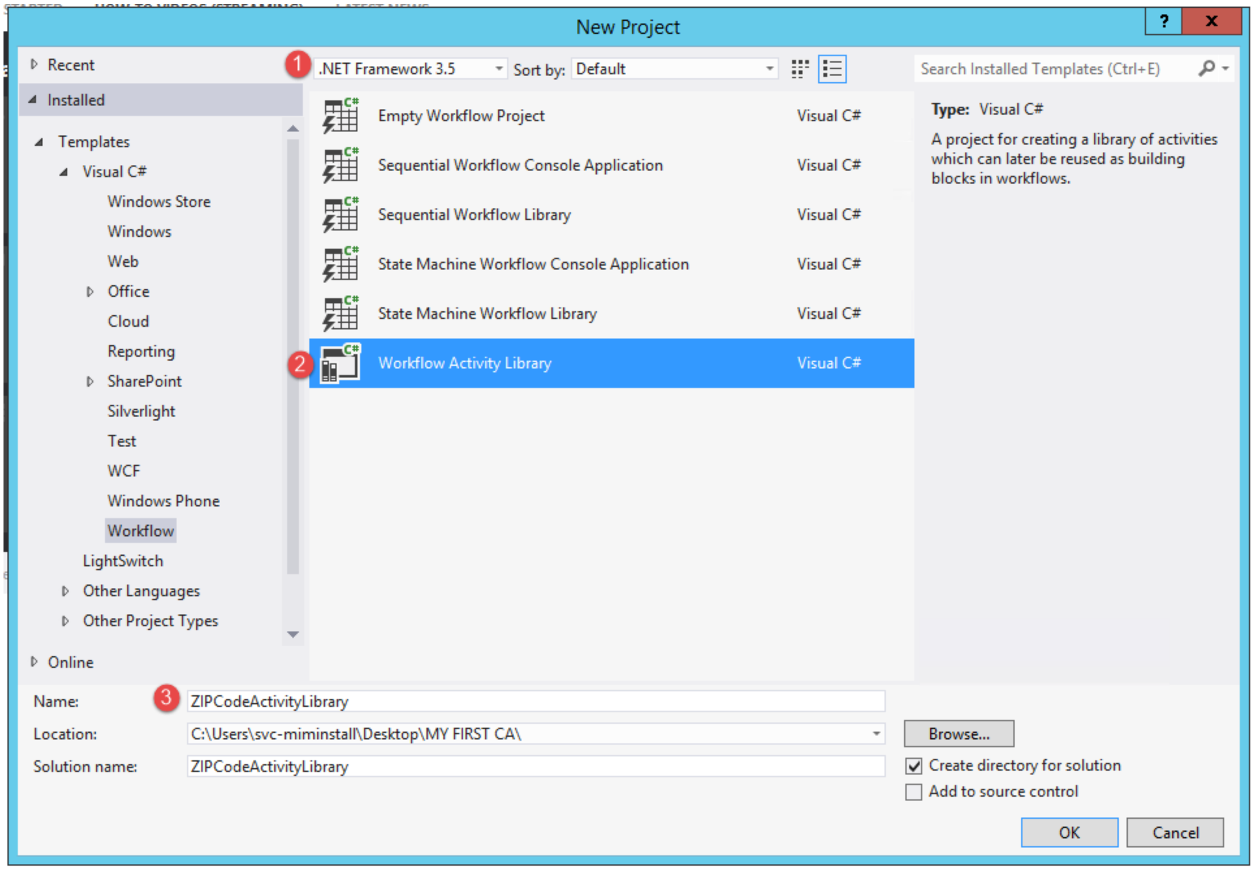
Display Name *

E-mail Enabled □ Enabled

Enable e-mail on a security group

Bhold Managed Group □ False

Bhold Managed Group



New Project

.NET Framework 3.5 Sort by: Default

Empty Workflow Project	Visual C#
Sequential Workflow Console Application	Visual C#
Sequential Workflow Library	Visual C#
State Machine Workflow Console Application	Visual C#
State Machine Workflow Library	Visual C#
Workflow Activity Library	Visual C#

Type: Visual C#

A project for creating a library of activities which can later be reused as building blocks in workflows.

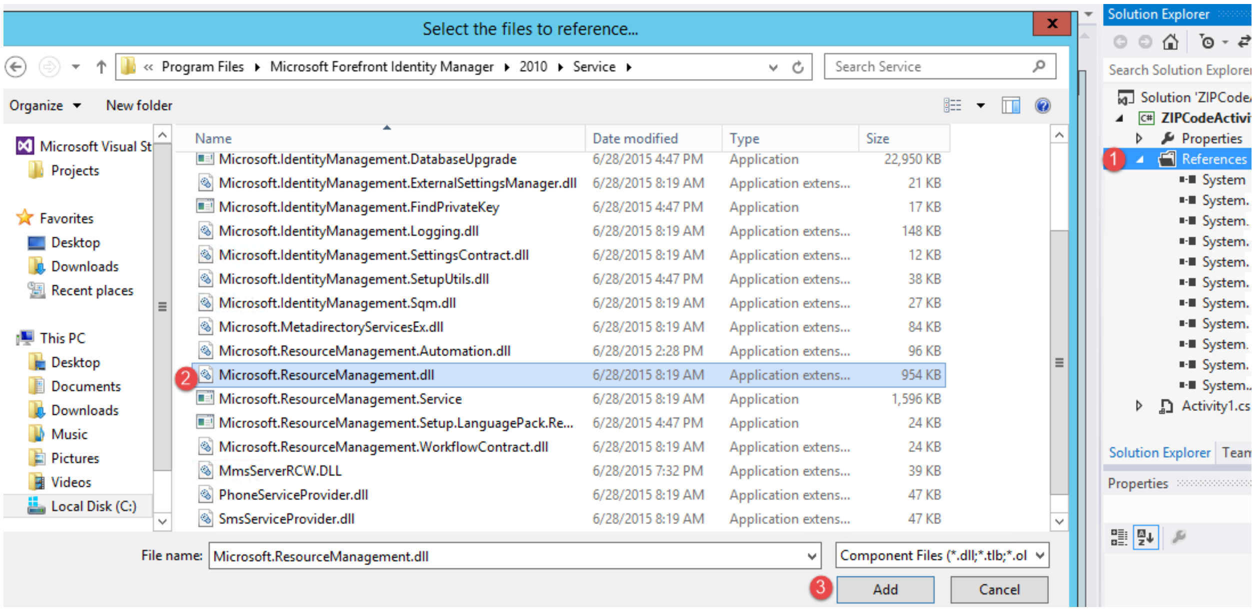
Name: ZIPCodeActivityLibrary

Location: C:\Users\svc-miminstall\Desktop\MY FIRST CA\

Solution name: ZIPCodeActivityLibrary

☑ Create directory for solution

☐ Add to source control



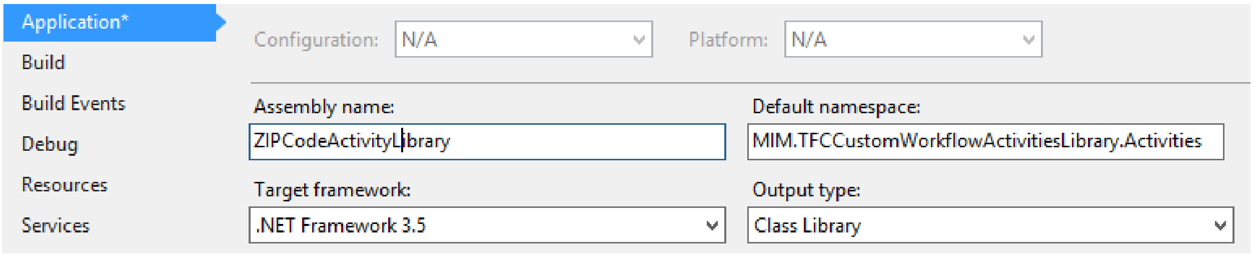
Select the files to reference...

« Program Files ▸ Microsoft Forefront Identity Manager ▸ 2010 ▸ Service ▸

Name	Date modified	Type	Size
Microsoft.IdentityManagement.DatabaseUpgrade	6/28/2015 4:47 PM	Application	22,950 KB
Microsoft.IdentityManagement.ExternalSettingsManager.dll	6/28/2015 8:19 AM	Application extens...	21 KB
Microsoft.IdentityManagement.FindPrivateKey	6/28/2015 4:47 PM	Application	17 KB
Microsoft.IdentityManagement.Logging.dll	6/28/2015 8:19 AM	Application extens...	148 KB
Microsoft.IdentityManagement.SettingsContract.dll	6/28/2015 8:19 AM	Application extens...	12 KB
Microsoft.IdentityManagement.SetupUtils.dll	6/28/2015 4:47 PM	Application extens...	38 KB
Microsoft.IdentityManagement.Sqm.dll	6/28/2015 8:19 AM	Application extens...	27 KB
Microsoft.MetadirectoryServicesEx.dll	6/28/2015 8:19 AM	Application extens...	84 KB
Microsoft.ResourceManagement.Automation.dll	6/28/2015 2:28 PM	Application extens...	96 KB
Microsoft.ResourceManagement.dll	6/28/2015 8:19 AM	Application extens...	954 KB
Microsoft.ResourceManagement.Service	6/28/2015 8:19 AM	Application	1,596 KB
Microsoft.ResourceManagement.Setup.LanguagePack.Re...	6/28/2015 4:47 PM	Application	24 KB
Microsoft.ResourceManagement.WorkflowContract.dll	6/28/2015 8:19 AM	Application extens...	24 KB
MmsServerRCW.DLL	6/28/2015 7:32 PM	Application extens...	39 KB
PhoneServiceProvider.dll	6/28/2015 8:19 AM	Application extens...	47 KB
SmsServiceProvider.dll	6/28/2015 8:19 AM	Application extens...	47 KB

File name: Microsoft.ResourceManagement.dll

Component Files (*.dll;*.tlb;*.ol



Configuration: N/A

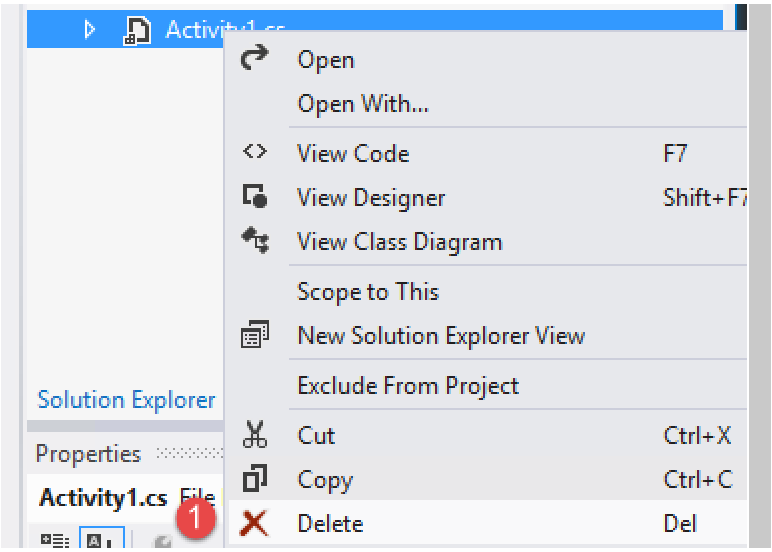
Platform: N/A

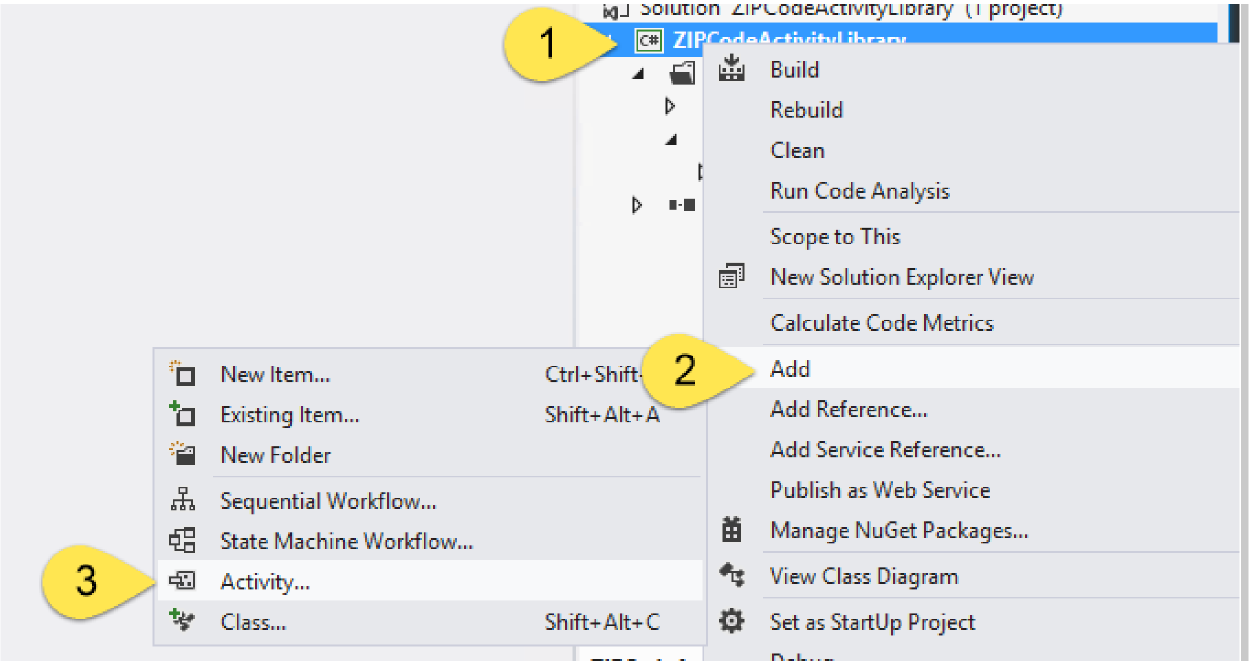
Assembly name: ZIPCodeActivityLibrary

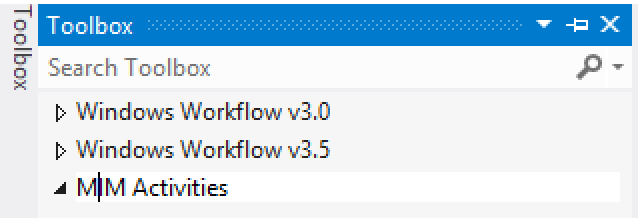
Default namespace: MIM.TFCCustomWorkflowActivitiesLibrary.Activities

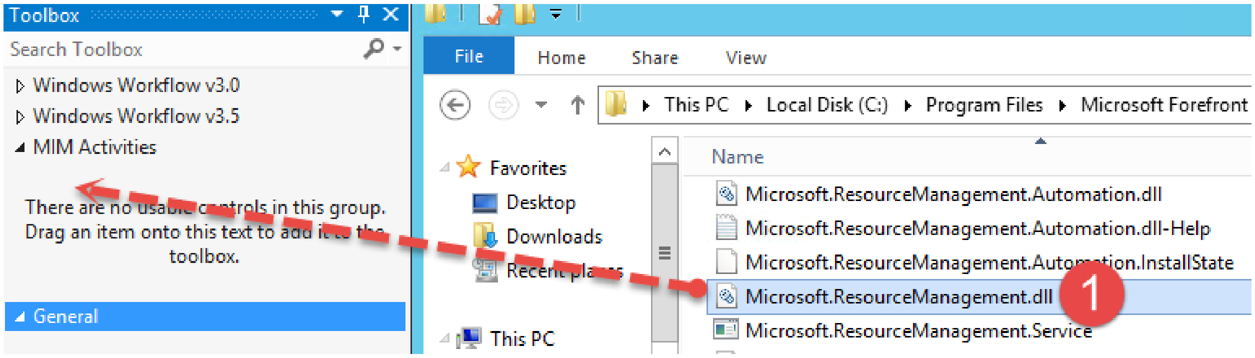
Target framework: .NET Framework 3.5

Output type: Class Library

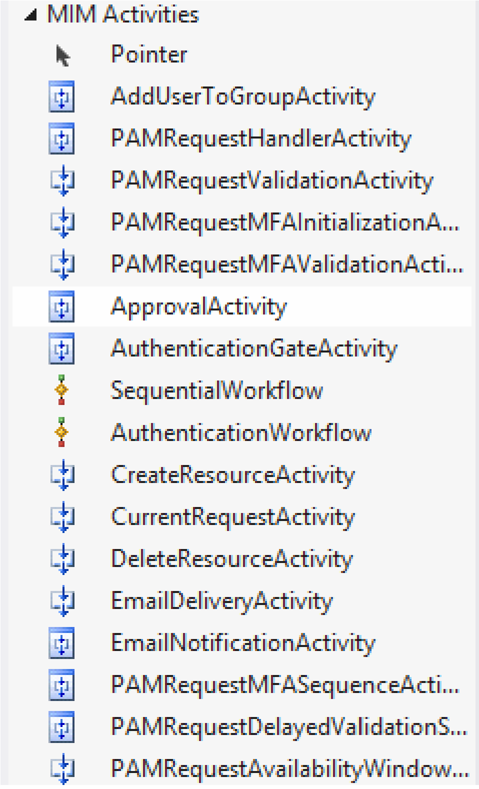


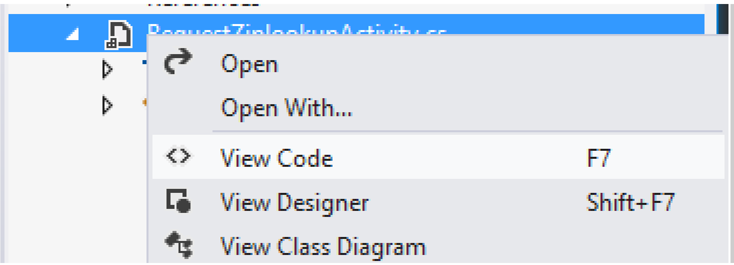


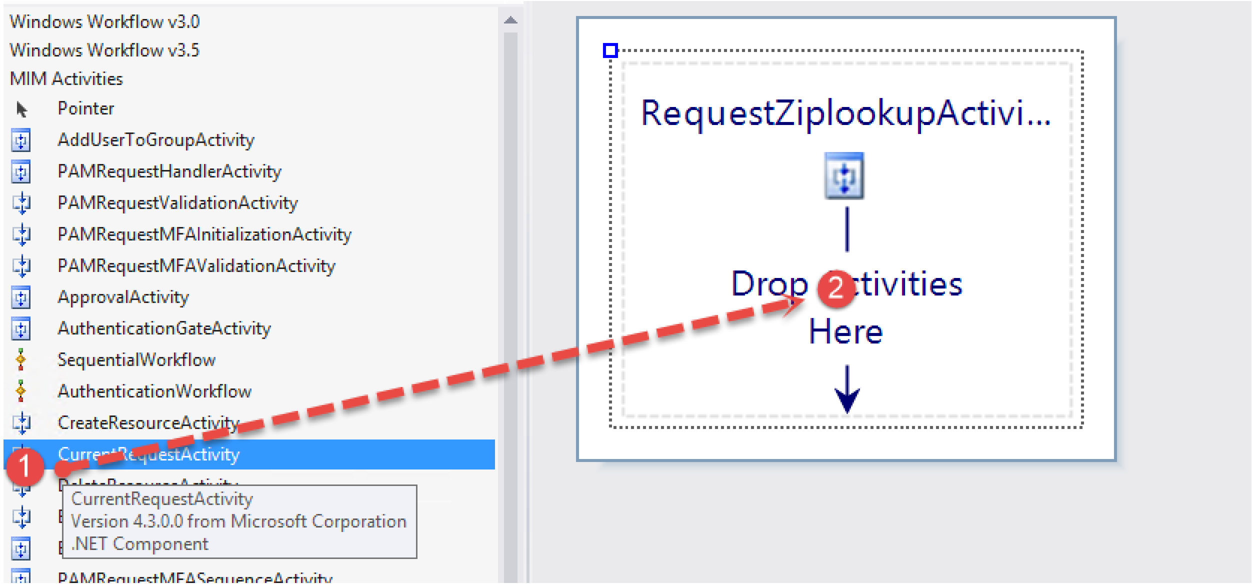



Toolbox
Search Toolbox
Windows Workflow v3.0
Windows Workflow v3.5
MIM Activities
General
File
Home
Share
View
This PC
Local Disk (C:)
Program Files
Microsoft Forefront
Favorites
Desktop
Downloads
Recent places
This PC
Name
Microsoft.ResourceManagement.Automation.dll
Microsoft.ResourceManagement.Automation.dll-Help
Microsoft.ResourceManagement.Automation.InstallState
Microsoft.ResourceManagement.dll
Microsoft.ResourceManagement.Service
1

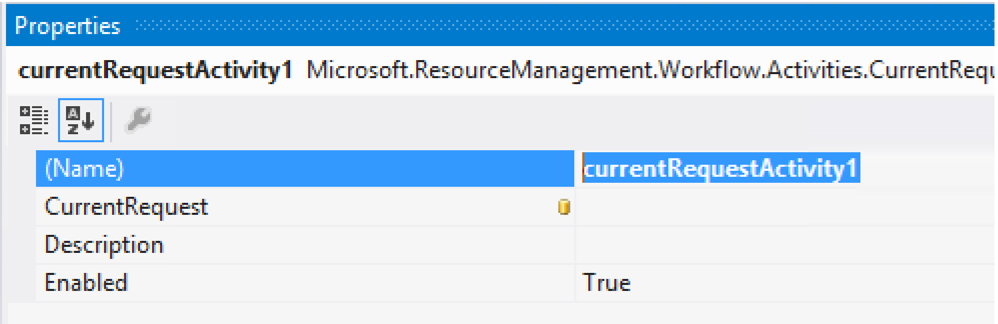
There are no usable controls in this group. Drag an item onto this text to add it to the toolbox.


MIM Activities
Pointer
AddUserToGroupActivity
PAMRequestHandlerActivity
PAMRequestValidationActivity
PAMRequestMFAInitializationA...
PAMRequestMFAValidationActi...
ApprovalActivity
AuthenticationGateActivity
SequentialWorkflow
AuthenticationWorkflow
CreateResourceActivity
CurrentRequestActivity
DeleteResourceActivity
EmailDeliveryActivity
EmailNotificationActivity
PAMRequestMFASequenceActi...
PAMRequestDelayedValidationS...
PAMRequestAvailabilityWindow...



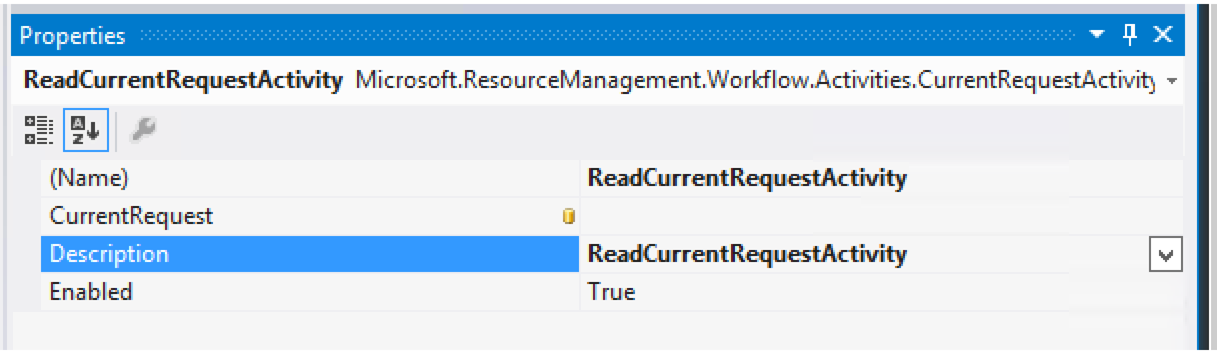


CurrentRequestActivity
Version 4.3.0.0 from Microsoft Corporation
.NET Component



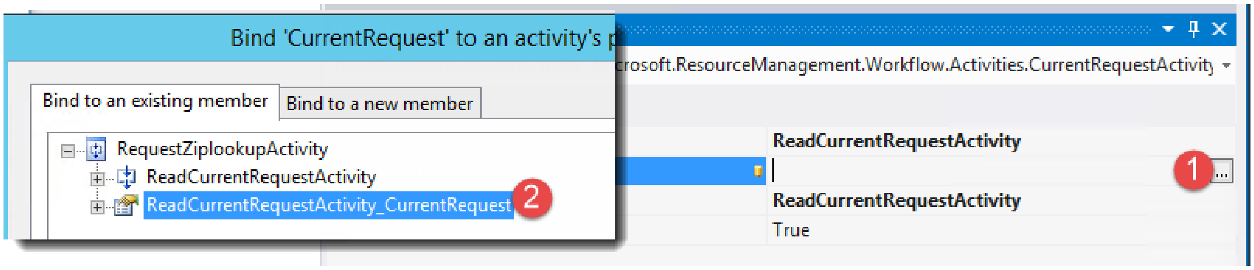
currentRequestActivity1 Microsoft.ResourceManagement.Workflow.Activities.CurrentRequ

(Name)	currentRequestActivity1
CurrentRequest	
Description	
Enabled	True



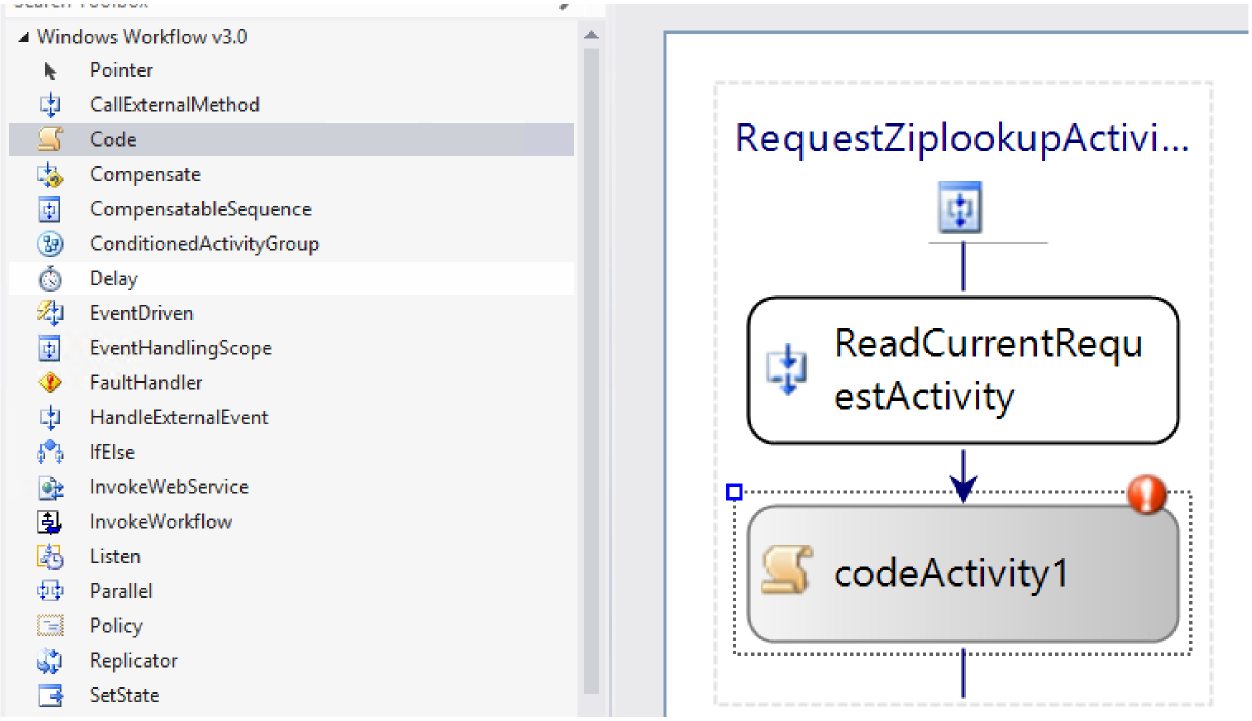
ReadCurrentRequestActivity Microsoft.ResourceManagement.Workflow.Activities.CurrentRequestActivity

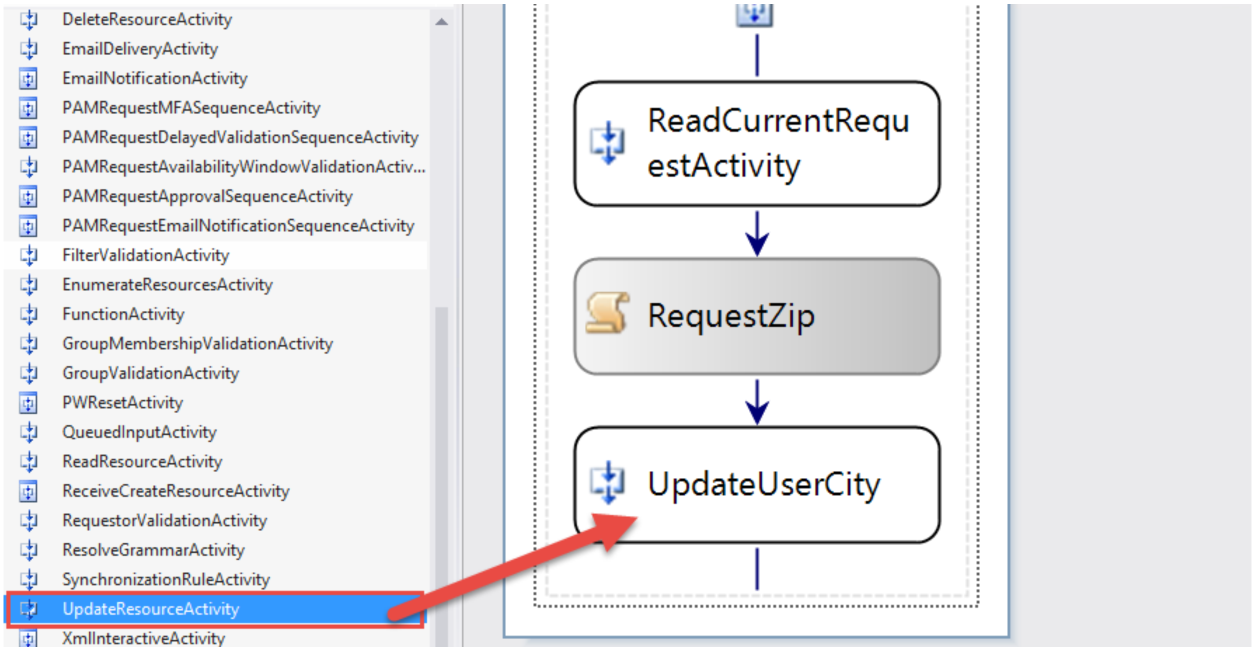
(Name)	ReadCurrentRequestActivity
CurrentRequest	
Description	ReadCurrentRequestActivity
Enabled	True

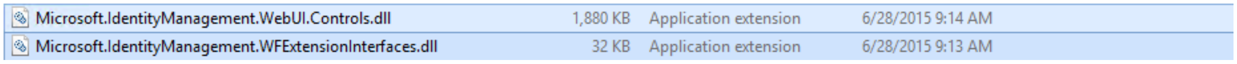

Bind 'CurrentRequest' to an activity's p
Bind to an existing member
Bind to a new member
RequestZiplookupActivity
ReadCurrentRequestActivity
ReadCurrentRequestActivity_CurrentRequest
2
1
...

rosoft.ResourceManagement.Workflow.Activities.CurrentRequestActivity

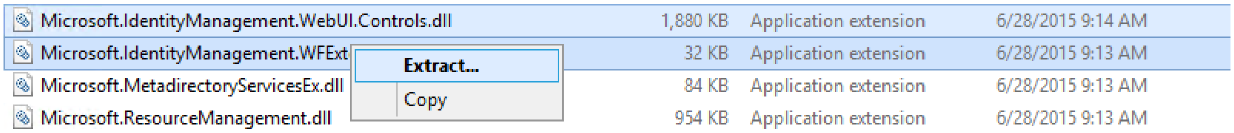
	ReadCurrentRequestActivity
	ReadCurrentRequestActivity
	True



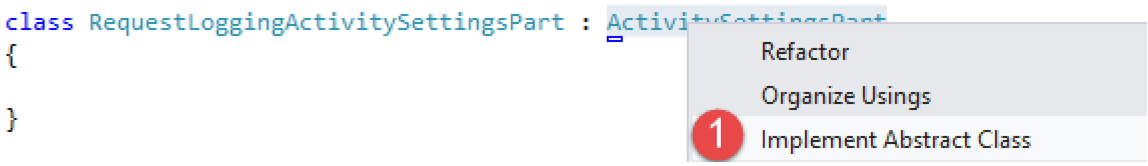

DeleteResourceActivity
EmailDeliveryActivity
EmailNotificationActivity
PAMRequestMFASequenceActivity
PAMRequestDelayedValidationSequenceActivity
PAMRequestAvailabilityWindowValidationActiv...
PAMRequestApprovalSequenceActivity
PAMRequestEmailNotificationSequenceActivity
FilterValidationActivity
EnumerateResourcesActivity
FunctionActivity
GroupMembershipValidationActivity
GroupValidationActivity
PWResetActivity
QueuedInputActivity
ReadResourceActivity
ReceiveCreateResourceActivity
RequestorValidationActivity
ResolveGrammarActivity
SynchronizationRuleActivity
UpdateResourceActivity
XmlInteractiveActivity
ReadCurrentRequestActivity
RequestZip
UpdateUserCity



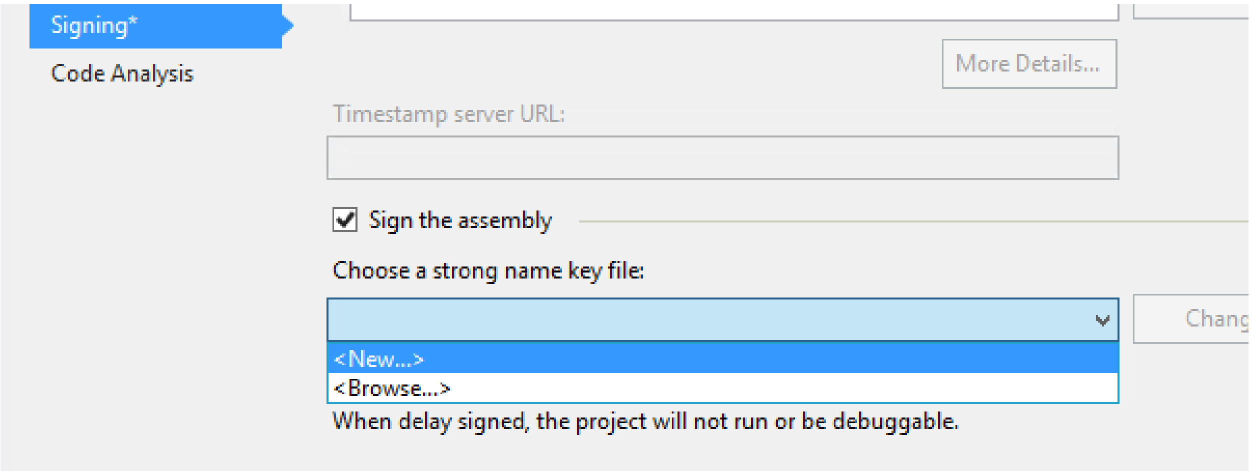
Microsoft.IdentityManagement.WebUI.Controls.dll	1,880 KB	Application extension	6/28/2015 9:14 AM
Microsoft.IdentityManagement.WFExtensionInterfaces.dll	32 KB	Application extension	6/28/2015 9:13 AM



Microsoft.IdentityManagement.WebUI.Controls.dll	1,880 KB	Application extension	6/28/2015 9:14 AM
Microsoft.IdentityManagement.WFExt	32 KB	Application extension	6/28/2015 9:13 AM
Microsoft.MetadirectoryServicesEx.dll	84 KB	Application extension	6/28/2015 9:13 AM
Microsoft.ResourceManagement.dll	954 KB	Application extension	6/28/2015 9:13 AM



```
class RequestLoggingActivitySettingsPart : ActivitySettingsPart
{

}
```

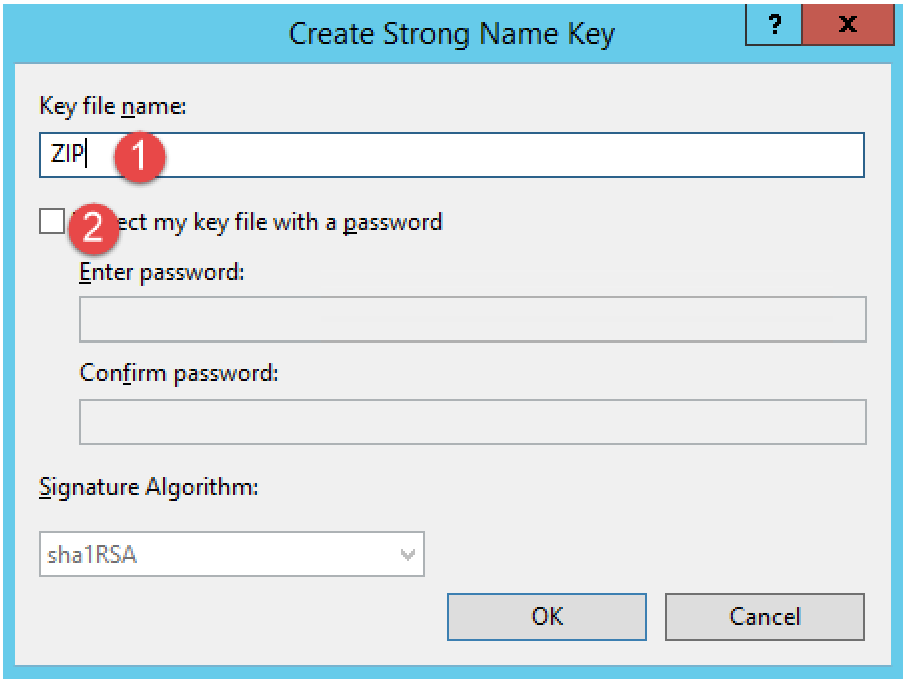


Timestamp server URL:

☑ Sign the assembly

Choose a strong name key file:

When delay signed, the project will not run or be debuggable.



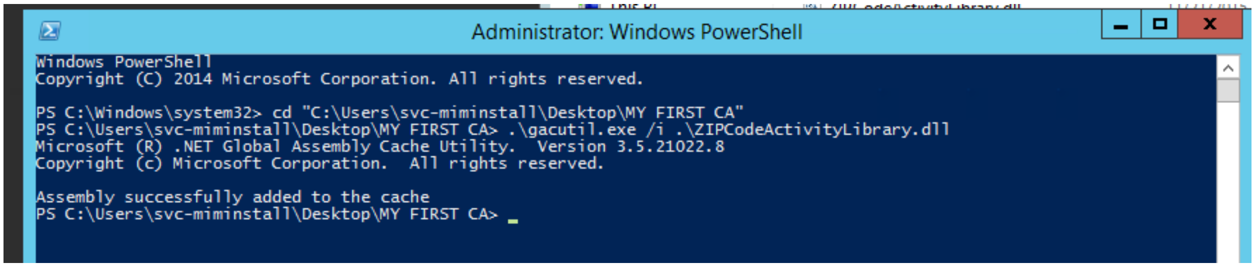
Key file name: ZIP

□ ect my key file with a password

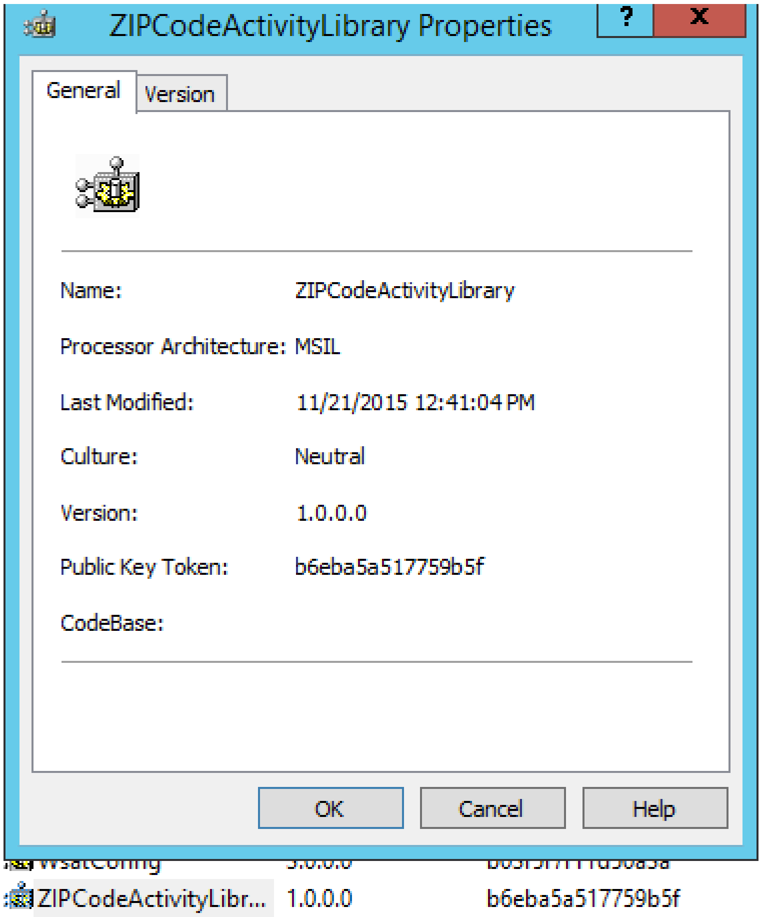
Enter password:

Confirm password:

Signature Algorithm: sha1RSA



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

PS C:\Windows\system32> cd "C:\Users\svc-miminstall\Desktop\MY FIRST CA"
PS C:\Users\svc-miminstall\Desktop\MY FIRST CA> .\gacutil.exe /i .\ZIPCodeActivityLibrary.dll
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
PS C:\Users\svc-miminstall\Desktop\MY FIRST CA> _
```



Name: ZIPCodeActivityLibrary

Processor Architecture: MSIL

Last Modified: 11/21/2015 12:41:04 PM

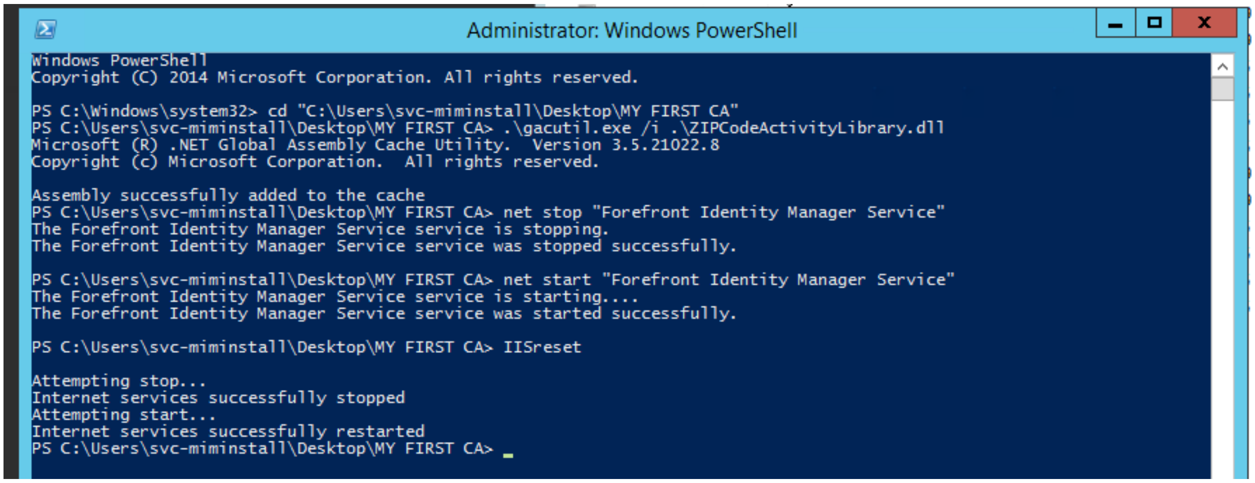
Culture: Neutral

Version: 1.0.0.0

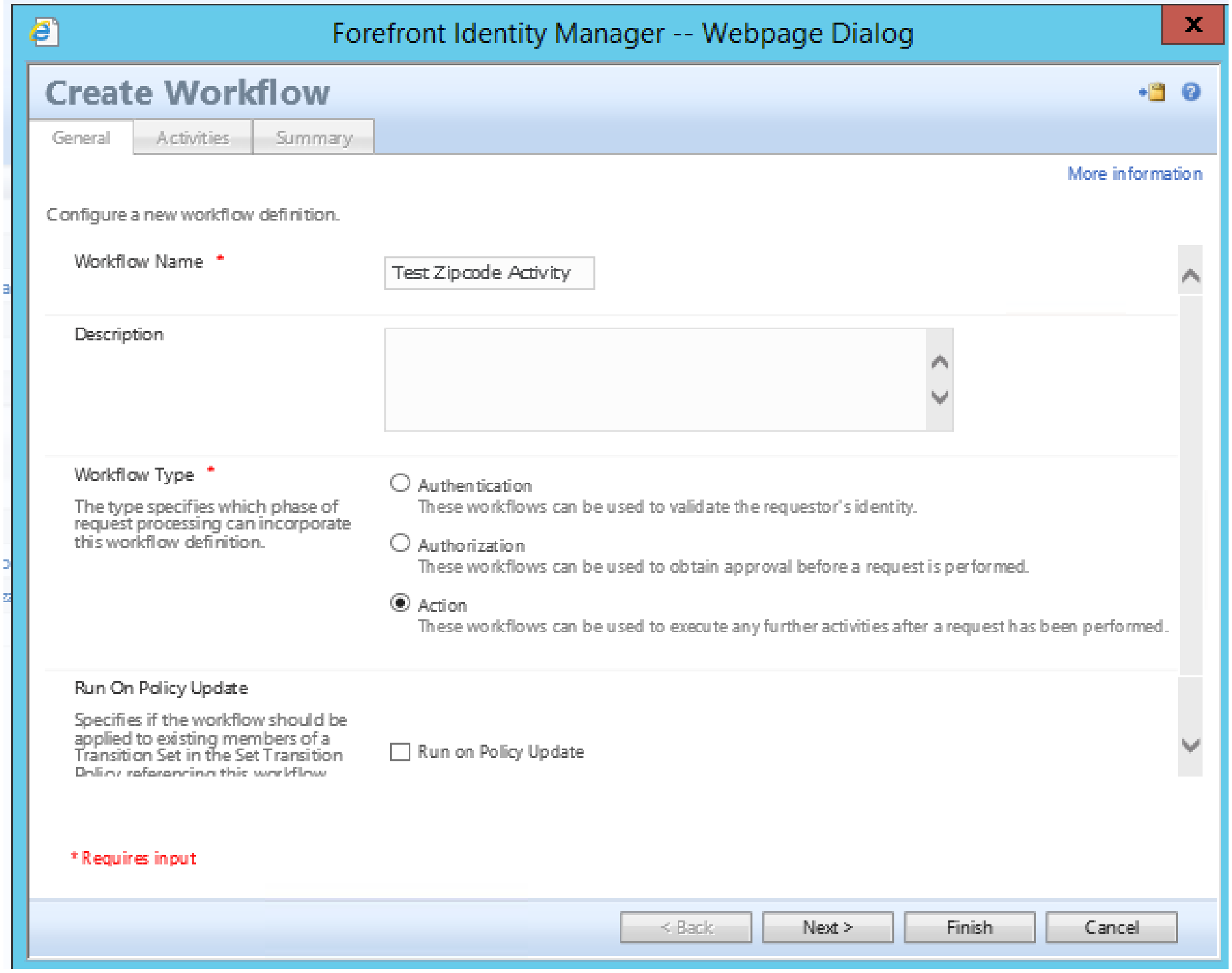
Public Key Token: b6eba5a517759b5f

CodeBase:

ZIPCodeActivityLibr... 1.0.0.0 b6eba5a517759b5f



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

PS C:\Windows\system32> cd "C:\Users\svc-miminstall\Desktop\MY FIRST CA"
PS C:\Users\svc-miminstall\Desktop\MY FIRST CA> .\gacutil.exe /i .\ZIPCodeActivityLibrary.dll
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
PS C:\Users\svc-miminstall\Desktop\MY FIRST CA> net stop "Forefront Identity Manager Service"
The Forefront Identity Manager Service service is stopping.
The Forefront Identity Manager Service service was stopped successfully.

PS C:\Users\svc-miminstall\Desktop\MY FIRST CA> net start "Forefront Identity Manager Service"
The Forefront Identity Manager Service service is starting....
The Forefront Identity Manager Service service was started successfully.

PS C:\Users\svc-miminstall\Desktop\MY FIRST CA> IISreset

Attempting stop...
Internet services successfully stopped
Attempting start...
Internet services successfully restarted
PS C:\Users\svc-miminstall\Desktop\MY FIRST CA> _
```



Forefront Identity Manager -- Webpage Dialog

Create Workflow

Configure a new workflow definition.

Workflow Name * : Test Zipcode Activity

Description

Workflow Type *

The type specifies which phase of request processing can incorporate this workflow definition.

○ Authentication
These workflows can be used to validate the requestor's identity.

○ Authorization
These workflows can be used to obtain approval before a request is performed.

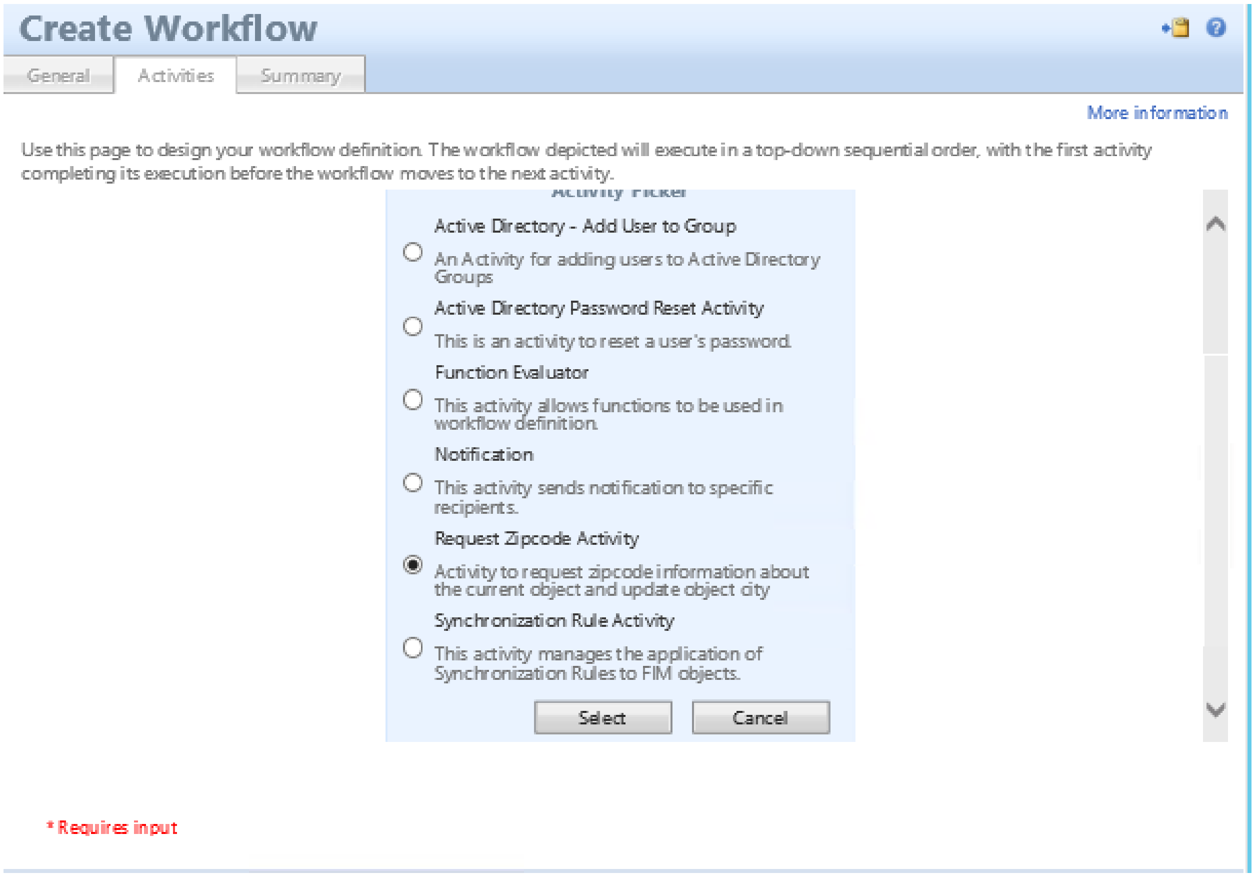
● Action
These workflows can be used to execute any further activities after a request has been performed.

Run On Policy Update

Specifies if the workflow should be applied to existing members of a Transition Set in the Set Transition Policy referencing this workflow

□ Run on Policy Update

* Requires input



Create Workflow

Use this page to design your workflow definition. The workflow depicted will execute in a top-down sequential order, with the first activity completing its execution before the workflow moves to the next activity.

Activity Picker

○ Active Directory - Add User to Group
An Activity for adding users to Active Directory Groups

○ Active Directory Password Reset Activity
This is an activity to reset a user's password.

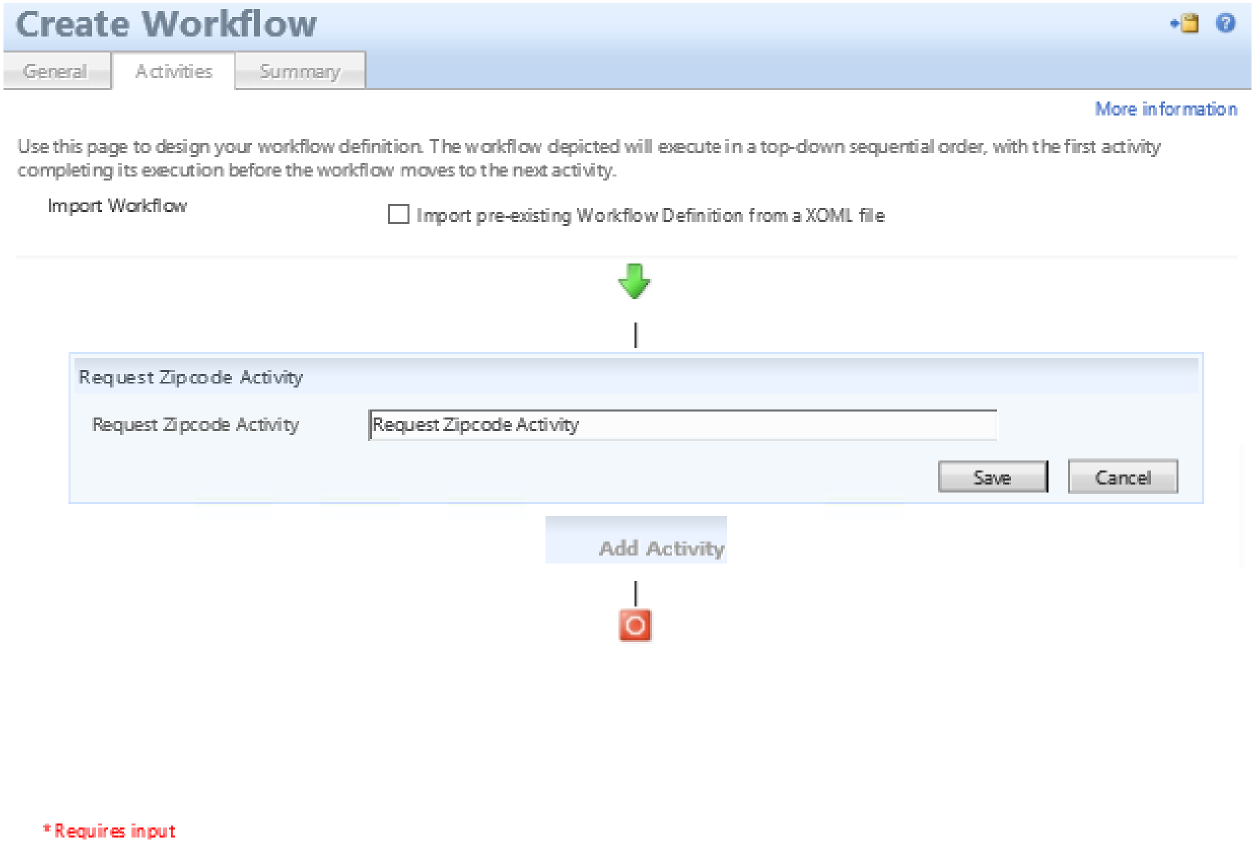
○ Function Evaluator
This activity allows functions to be used in workflow definition.

○ Notification
This activity sends notification to specific recipients.

● Request Zipcode Activity
Activity to request zipcode information about the current object and update object city

○ Synchronization Rule Activity
This activity manages the application of Synchronization Rules to FIM objects.

* Requires input

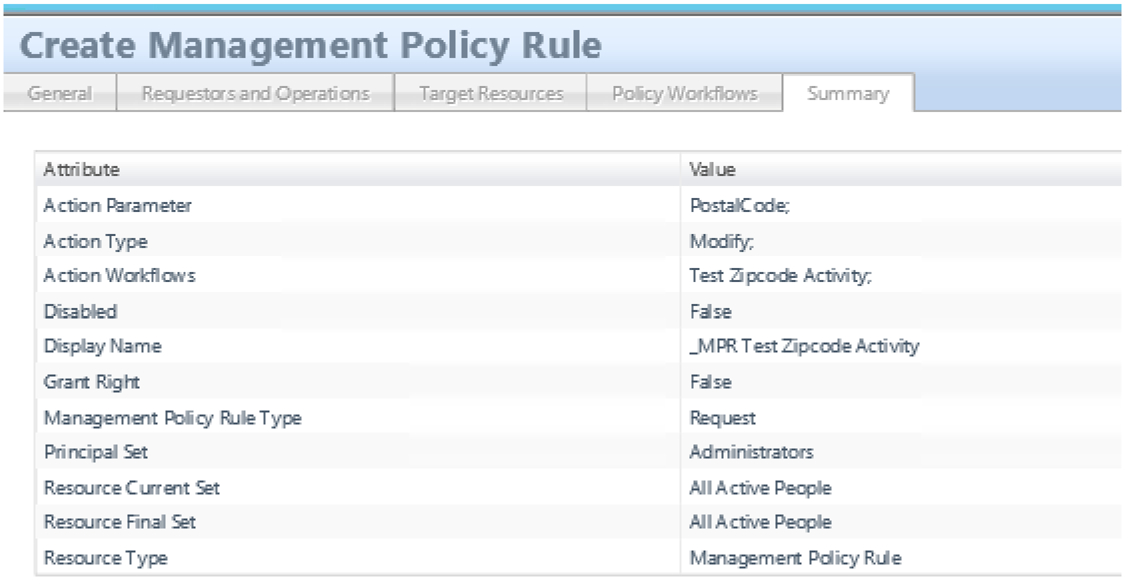


Use this page to design your workflow definition. The workflow depicted will execute in a top-down sequential order, with the first activity completing its execution before the workflow moves to the next activity.

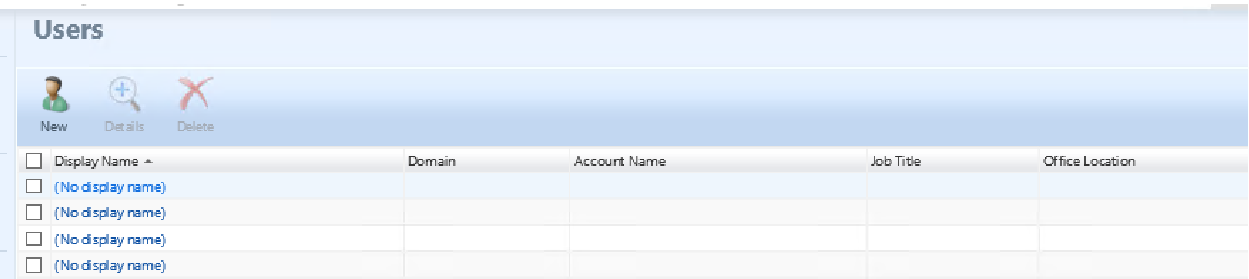
Import Workflow □ Import pre-existing Workflow Definition from a XOML file

Request Zipcode Activity

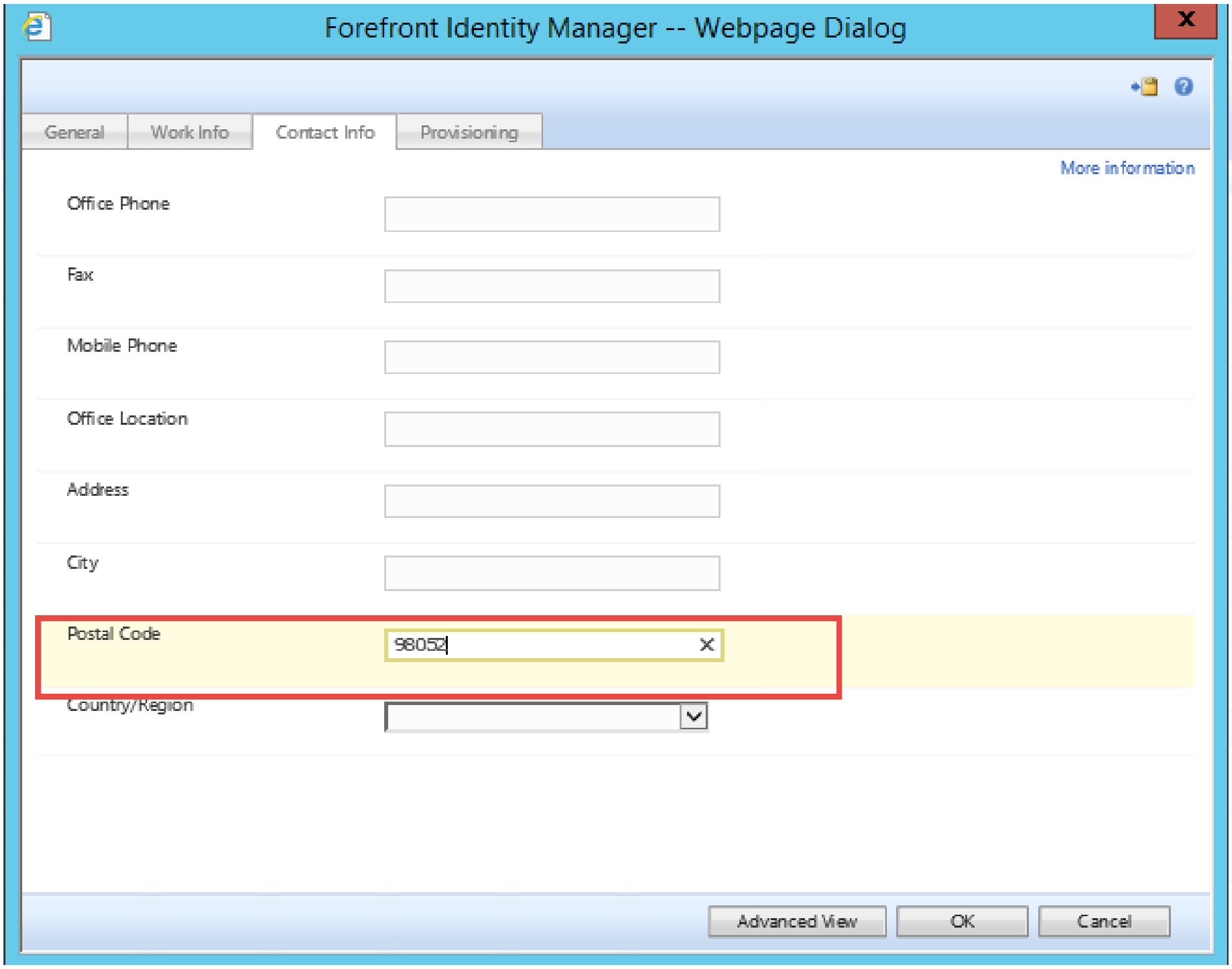
Request Zipcode Activity: Request Zipcode Activity



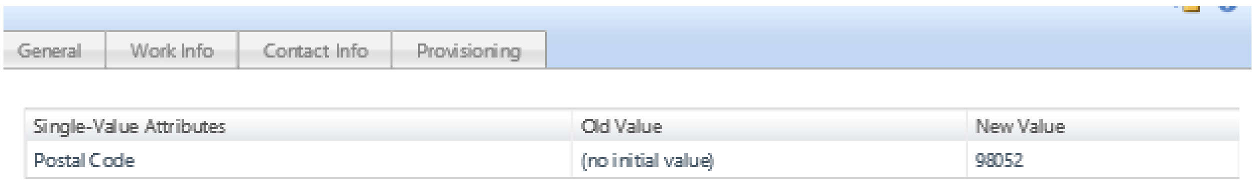
Attribute	Value
Action Parameter	PostalCode;
Action Type	Modify;
Action Workflows	Test Zipcode Activity;
Disabled	False
Display Name	_MPR Test Zipcode Activity
Grant Right	False
Management Policy Rule Type	Request
Principal Set	Administrators
Resource Current Set	All Active People
Resource Final Set	All Active People
Resource Type	Management Policy Rule



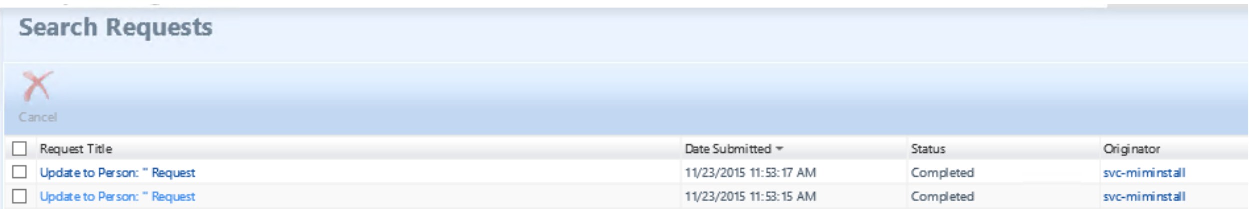
□	Display Name ▲	Domain	Account Name	Job Title	Office Location
□	(No display name)				
□	(No display name)				
□	(No display name)				
□	(No display name)				



Office Phone	
Fax	
Mobile Phone	
Office Location	
Address	
City	
Postal Code	98052
Country/Region	

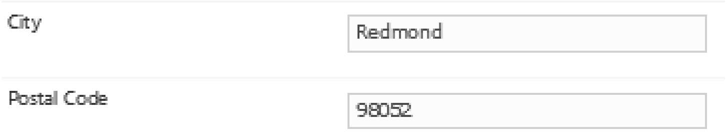


Single-Value Attributes	Old Value	New Value
Postal Code	(no initial value)	98052

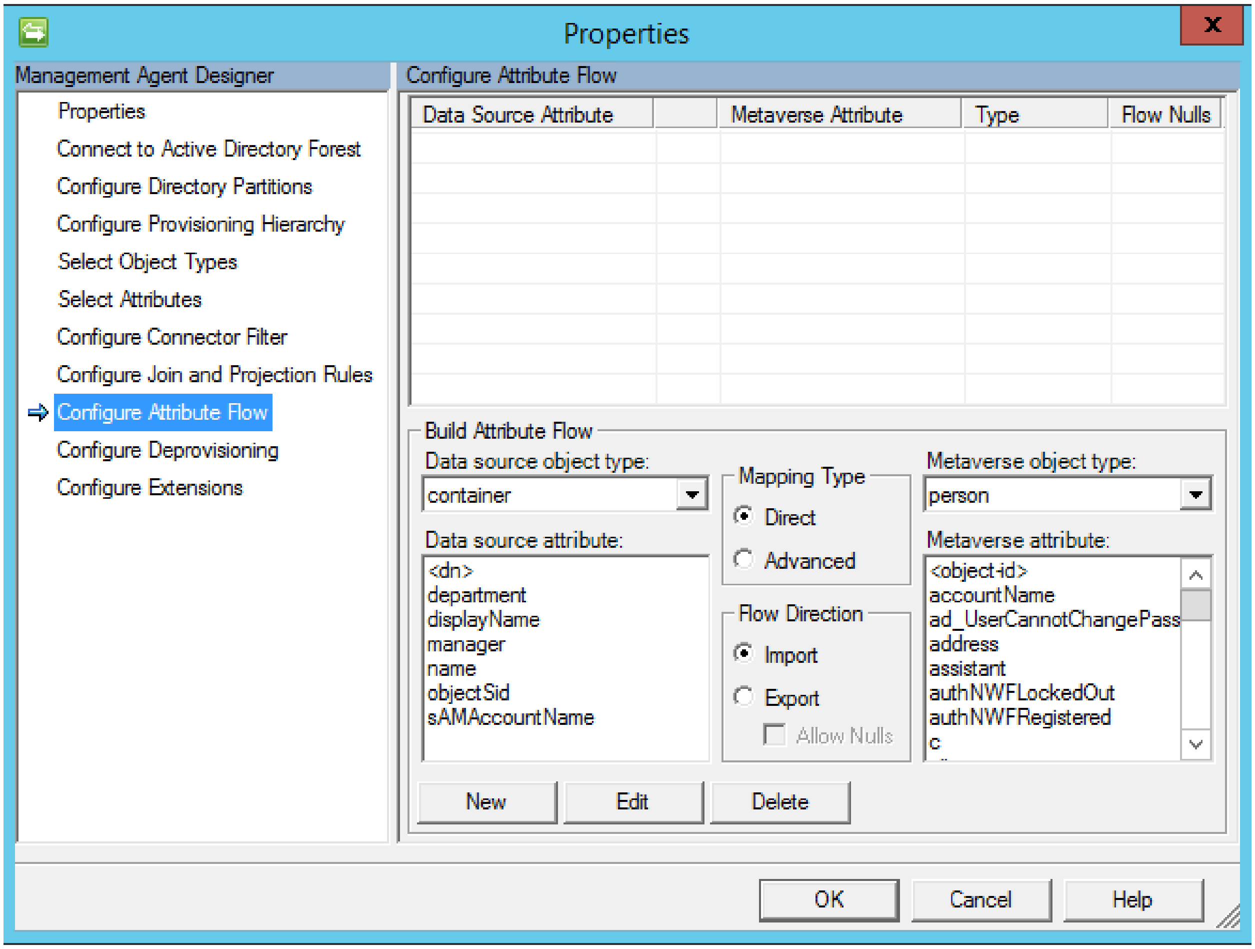


Search Requests

□	Request Title	Date Submitted	Status	Originator
□	Update to Person: '' Request	11/23/2015 11:53:17 AM	Completed	svc-miminstall
□	Update to Person: '' Request	11/23/2015 11:53:15 AM	Completed	svc-miminstall



City	Redmond
Postal Code	98052



Data source object type: container

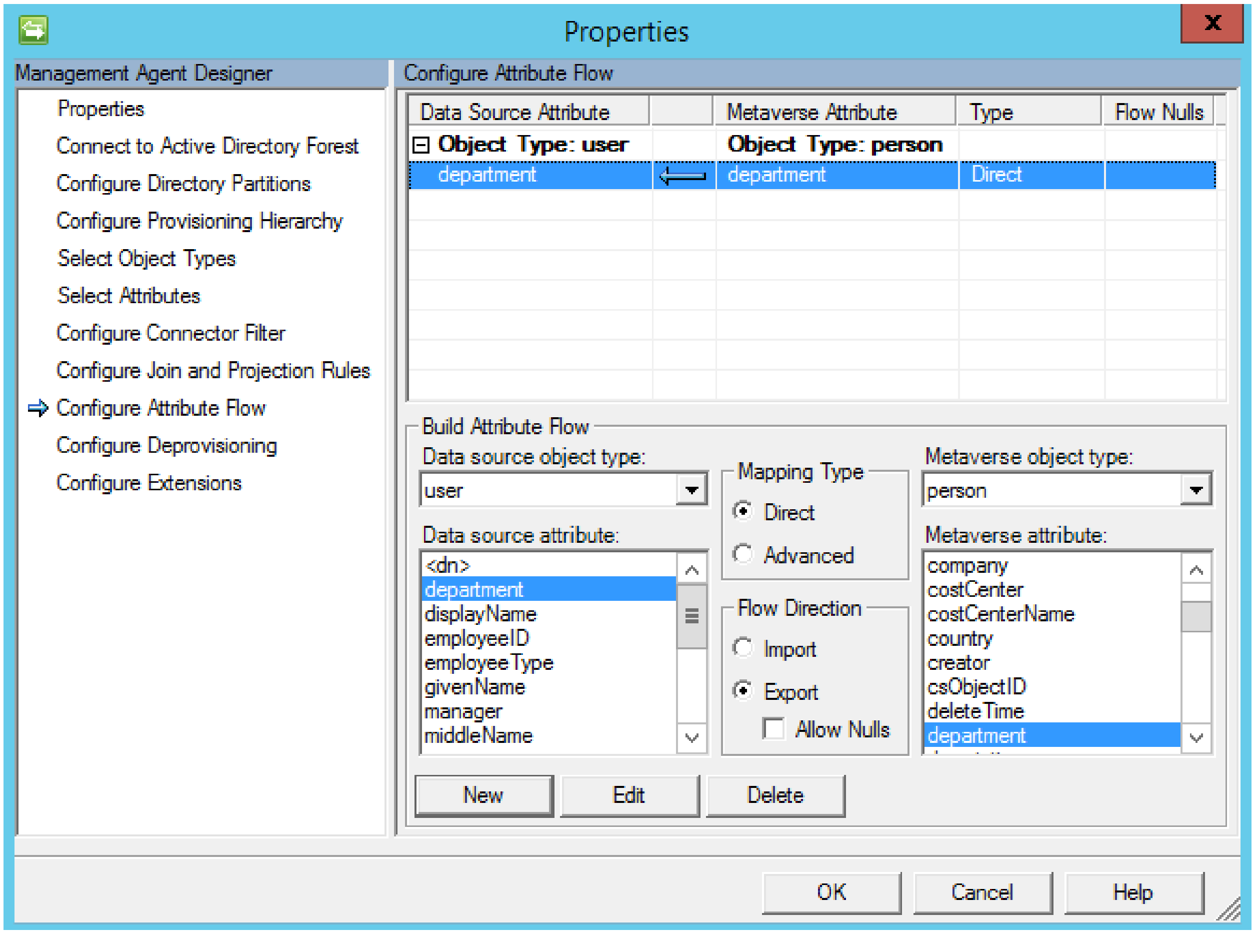
Mapping Type
● Direct
○ Advanced

Flow Direction
● Import
○ Export
□ Allow Nulls

Metaverse object type: person

Data source attribute:
<dn>
department
displayName
manager
name
objectSid
sAMAccountName

Metaverse attribute:
<object-id>
accountName
ad_UserCannotChangePass
address
assistant
authNWFLockedOut
authNWFRegistered
c



Data Source Attribute		Metaverse Attribute	Type	Flow Nulls
⊟ **Object Type: user**		**Object Type: person**		
department	⟵	department	Direct	

Data source object type: user

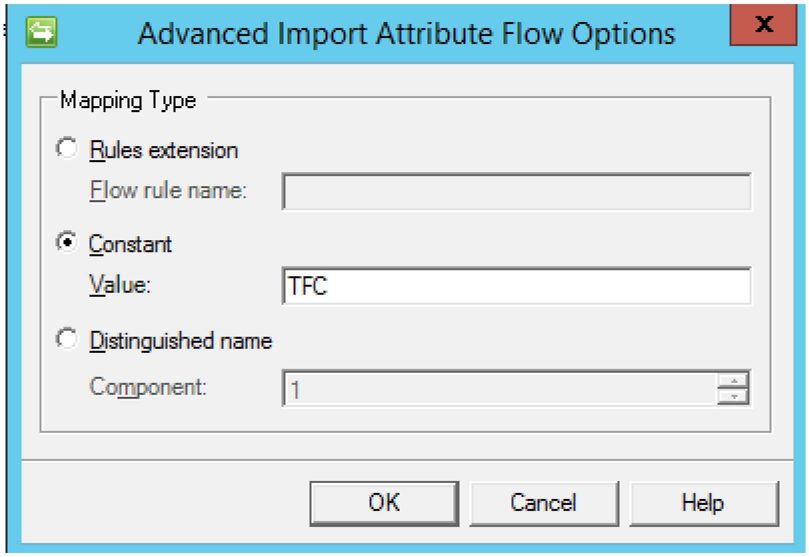
Data source attribute: <dn>, department, displayName, employeeID, employeeType, givenName, manager, middleName

Mapping Type: ● Direct ○ Advanced

Flow Direction: ○ Import ● Export □ Allow Nulls

Metaverse object type: person

Metaverse attribute: company, costCenter, costCenterName, country, creator, csObjectID, deleteTime, department



○ Rules extension

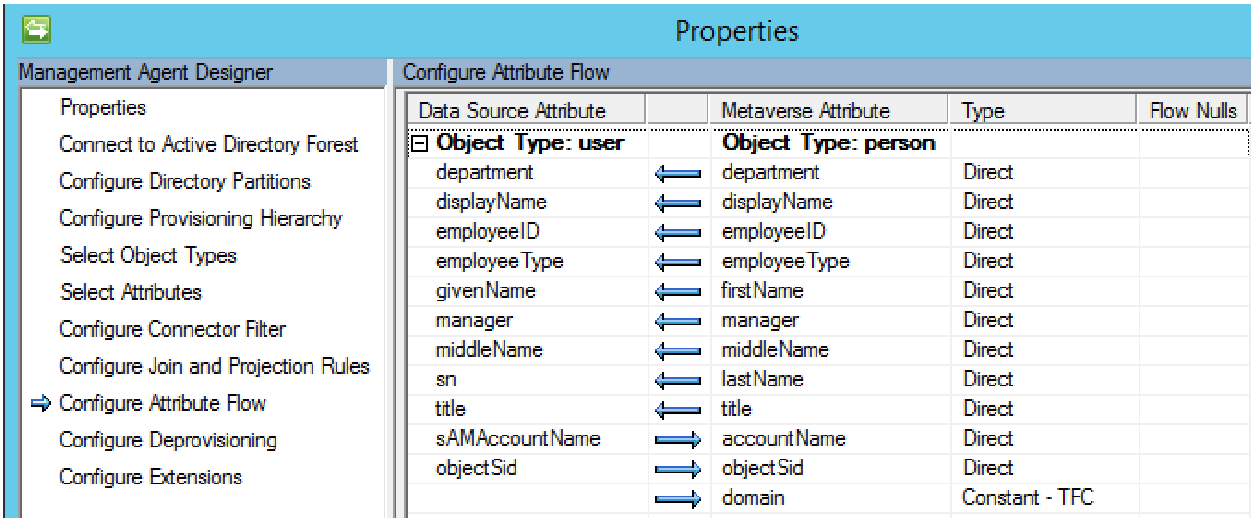
Flow rule name:

● Constant

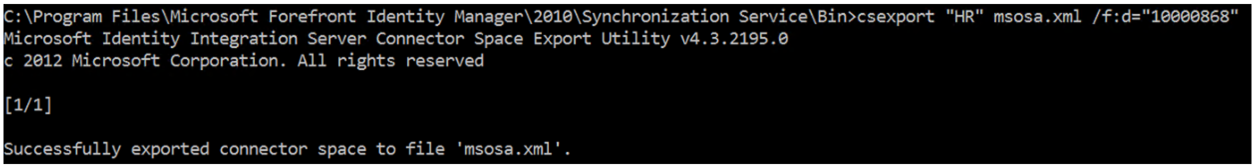
Value: TFC

○ Distinguished name

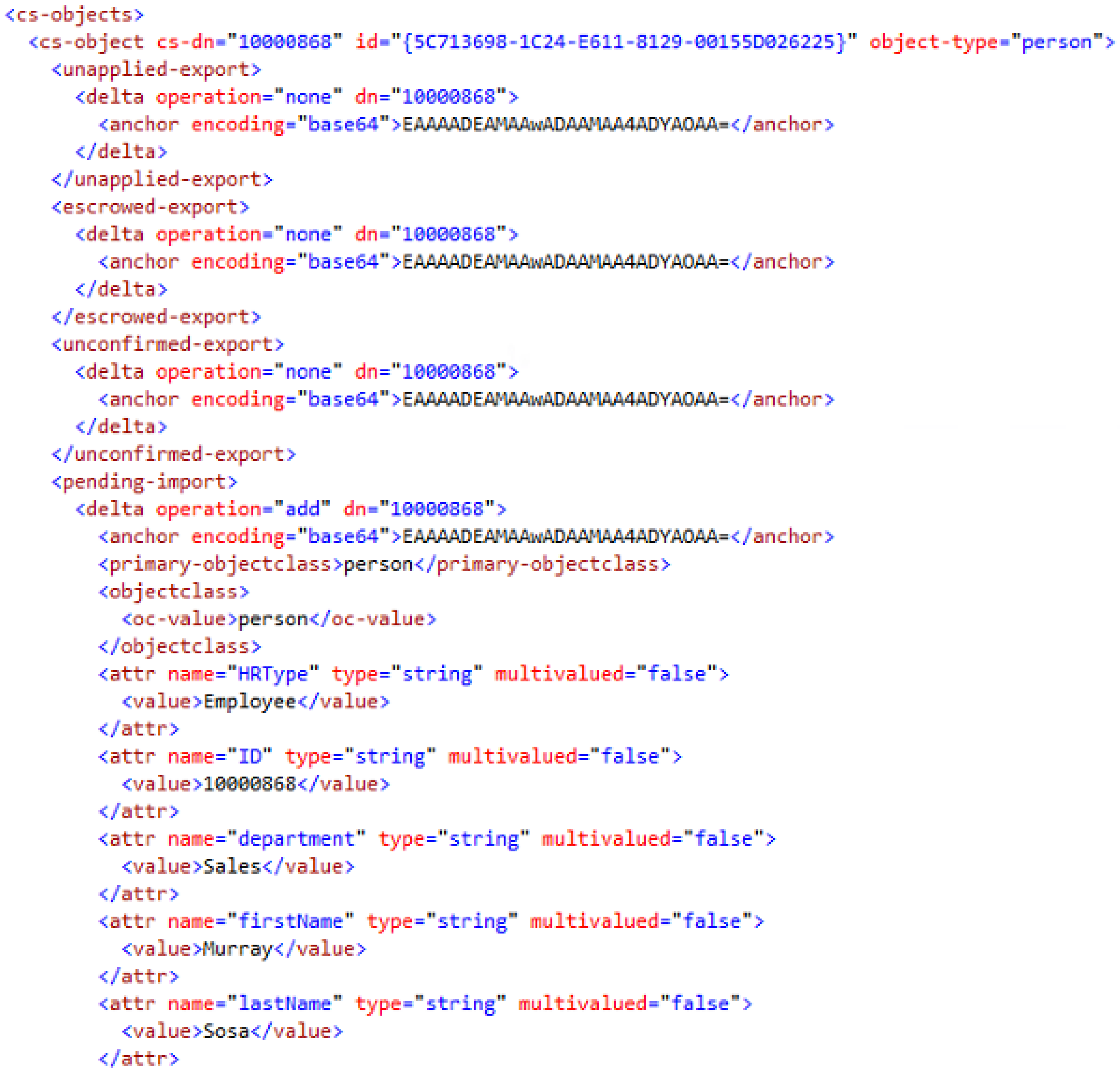
Component: 1


Properties
Management Agent Designer
Properties
Connect to Active Directory Forest
Configure Directory Partitions
Configure Provisioning Hierarchy
Select Object Types
Select Attributes
Configure Connector Filter
Configure Join and Projection Rules
⇨ Configure Attribute Flow
Configure Deprovisioning
Configure Extensions
Configure Attribute Flow

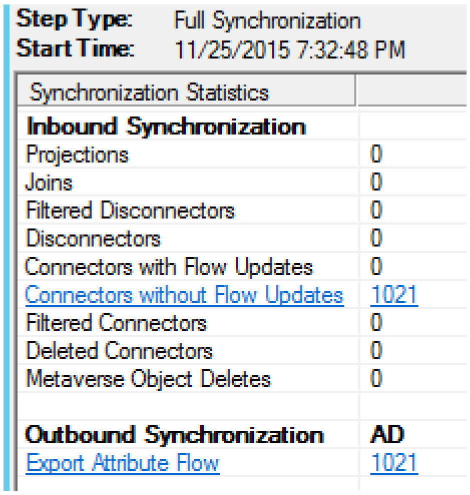
Data Source Attribute		Metaverse Attribute	Type	Flow Nulls
⊟ **Object Type: user**		**Object Type: person**		
department	⟵	department	Direct	
displayName	⟵	displayName	Direct	
employeeID	⟵	employeeID	Direct	
employeeType	⟵	employeeType	Direct	
givenName	⟵	firstName	Direct	
manager	⟵	manager	Direct	
middleName	⟵	middleName	Direct	
sn	⟵	lastName	Direct	
title	⟵	title	Direct	
sAMAccountName	⟶	accountName	Direct	
objectSid	⟶	objectSid	Direct	
	⟶	domain	Constant - TFC	



```
C:\Program Files\Microsoft Forefront Identity Manager\2010\Synchronization Service\Bin>csexport "HR" msosa.xml /f:d="10000868"
Microsoft Identity Integration Server Connector Space Export Utility v4.3.2195.0
c 2012 Microsoft Corporation. All rights reserved

[1/1]

Successfully exported connector space to file 'msosa.xml'.
```

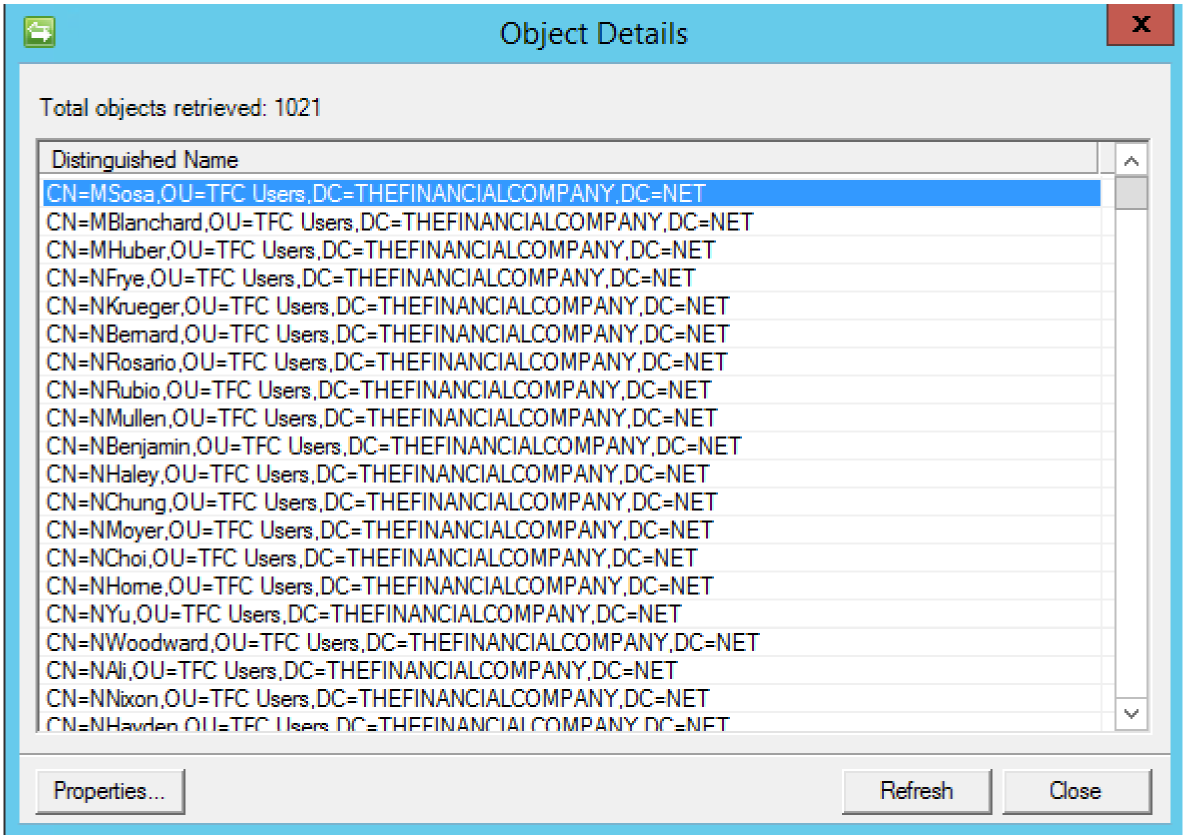


```
<cs-objects>
  <cs-object cs-dn="10000868" id="{5C713698-1C24-E611-8129-00155D026225}" object-type="person">
    <unapplied-export>
      <delta operation="none" dn="10000868">
        <anchor encoding="base64">EAAAADEAMAAwADAAMAA4ADYAOAA=</anchor>
      </delta>
    </unapplied-export>
    <escrowed-export>
      <delta operation="none" dn="10000868">
        <anchor encoding="base64">EAAAADEAMAAwADAAMAA4ADYAOAA=</anchor>
      </delta>
    </escrowed-export>
    <unconfirmed-export>
      <delta operation="none" dn="10000868">
        <anchor encoding="base64">EAAAADEAMAAwADAAMAA4ADYAOAA=</anchor>
      </delta>
    </unconfirmed-export>
    <pending-import>
      <delta operation="add" dn="10000868">
        <anchor encoding="base64">EAAAADEAMAAwADAAMAA4ADYAOAA=</anchor>
        <primary-objectclass>person</primary-objectclass>
        <objectclass>
          <oc-value>person</oc-value>
        </objectclass>
        <attr name="HRType" type="string" multivalued="false">
          <value>Employee</value>
        </attr>
        <attr name="ID" type="string" multivalued="false">
          <value>10000868</value>
        </attr>
        <attr name="department" type="string" multivalued="false">
          <value>Sales</value>
        </attr>
        <attr name="firstName" type="string" multivalued="false">
          <value>Murray</value>
        </attr>
        <attr name="lastName" type="string" multivalued="false">
          <value>Sosa</value>
        </attr>
```



Step Type: Full Synchronization
Start Time: 11/25/2015 7:32:48 PM

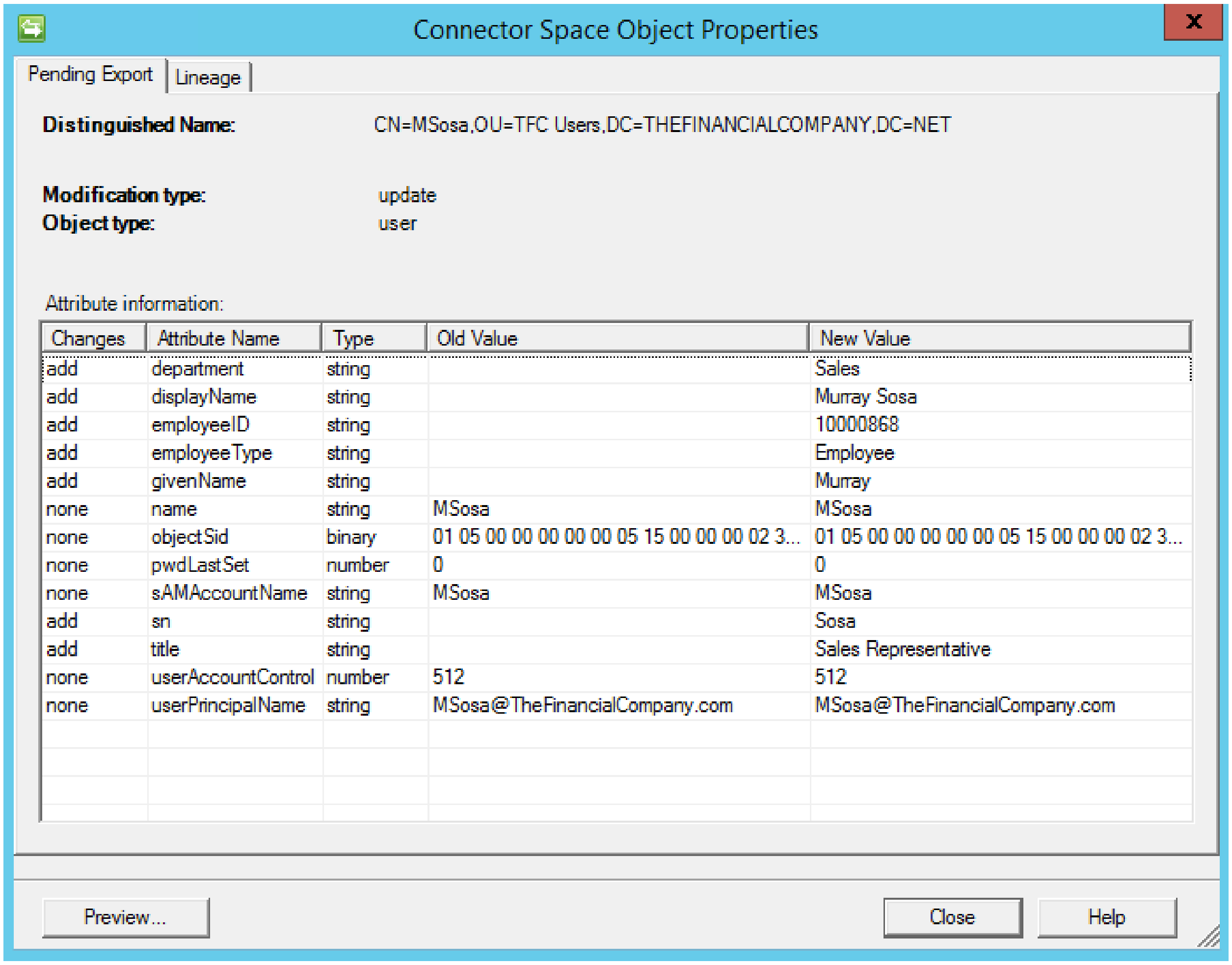
Synchronization Statistics	
Inbound Synchronization	
Projections	0
Joins	0
Filtered Disconnectors	0
Disconnectors	0
Connectors with Flow Updates	0
Connectors without Flow Updates	1021
Filtered Connectors	0
Deleted Connectors	0
Metaverse Object Deletes	0
Outbound Synchronization	**AD**
Export Attribute Flow	1021



Total objects retrieved: 1021

Distinguished Name

```
CN=MSosa,OU=TFC Users,DC=THEFINANCIALCOMPANY,DC=NET
CN=MBlanchard,OU=TFC Users,DC=THEFINANCIALCOMPANY,DC=NET
CN=MHuber,OU=TFC Users,DC=THEFINANCIALCOMPANY,DC=NET
CN=NFrye,OU=TFC Users,DC=THEFINANCIALCOMPANY,DC=NET
CN=NKrueger,OU=TFC Users,DC=THEFINANCIALCOMPANY,DC=NET
CN=NBernard,OU=TFC Users,DC=THEFINANCIALCOMPANY,DC=NET
CN=NRosario,OU=TFC Users,DC=THEFINANCIALCOMPANY,DC=NET
CN=NRubio,OU=TFC Users,DC=THEFINANCIALCOMPANY,DC=NET
CN=NMullen,OU=TFC Users,DC=THEFINANCIALCOMPANY,DC=NET
CN=NBenjamin,OU=TFC Users,DC=THEFINANCIALCOMPANY,DC=NET
CN=NHaley,OU=TFC Users,DC=THEFINANCIALCOMPANY,DC=NET
CN=NChung,OU=TFC Users,DC=THEFINANCIALCOMPANY,DC=NET
CN=NMoyer,OU=TFC Users,DC=THEFINANCIALCOMPANY,DC=NET
CN=NChoi,OU=TFC Users,DC=THEFINANCIALCOMPANY,DC=NET
CN=NHorne,OU=TFC Users,DC=THEFINANCIALCOMPANY,DC=NET
CN=NYu,OU=TFC Users,DC=THEFINANCIALCOMPANY,DC=NET
CN=NWoodward,OU=TFC Users,DC=THEFINANCIALCOMPANY,DC=NET
CN=NAli,OU=TFC Users,DC=THEFINANCIALCOMPANY,DC=NET
CN=NNixon,OU=TFC Users,DC=THEFINANCIALCOMPANY,DC=NET
CN=NHayden,OU=TFC Users,DC=THEFINANCIALCOMPANY,DC=NET
```

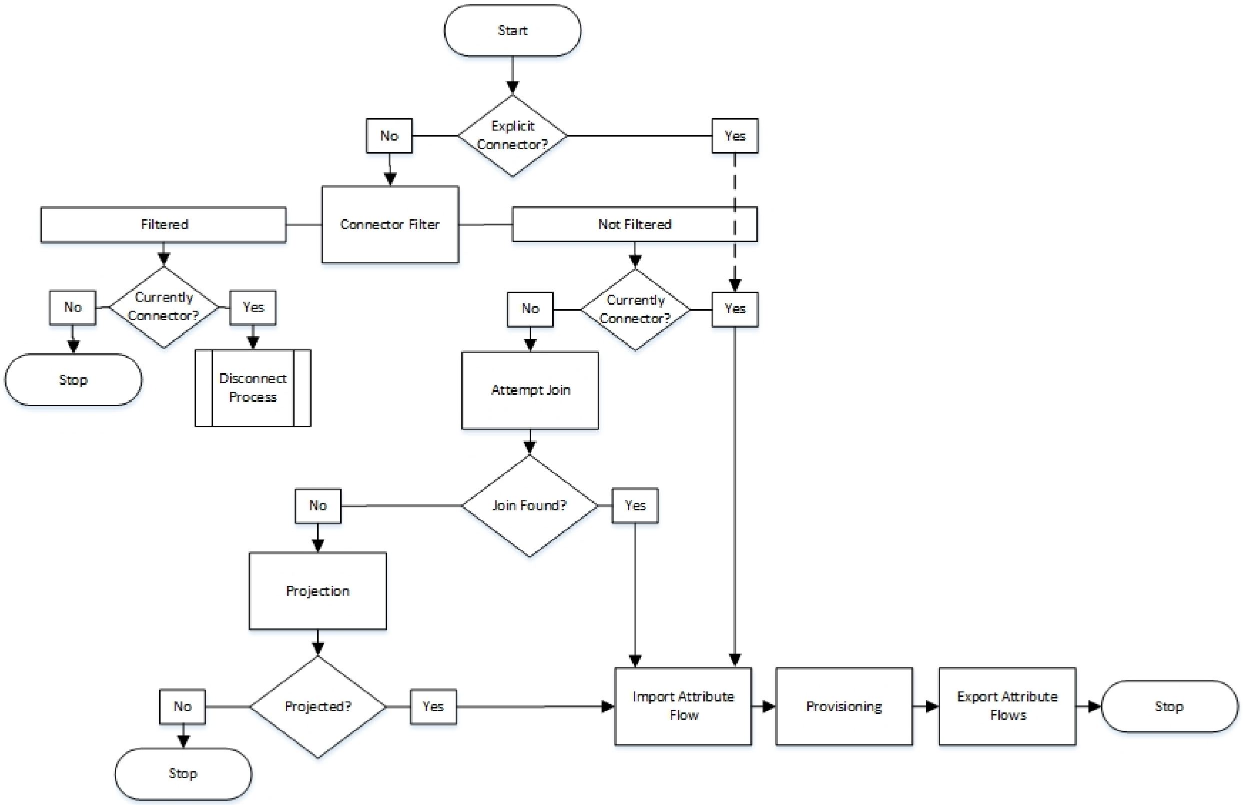


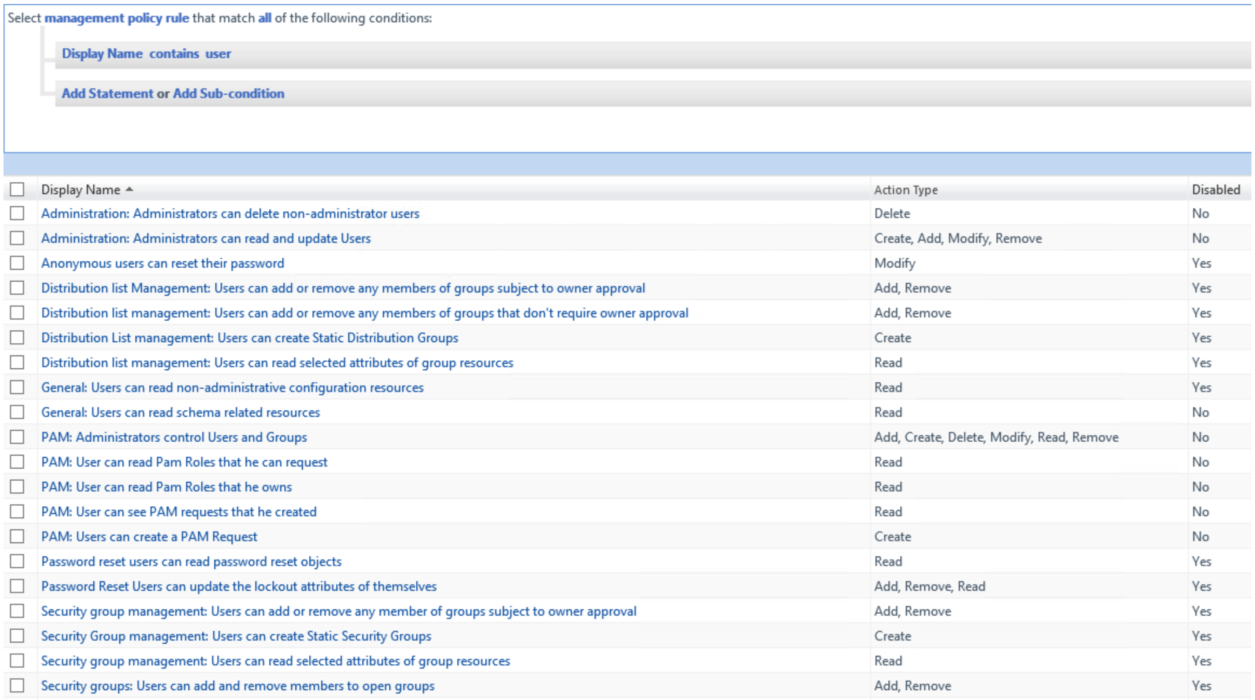
Distinguished Name: CN=MSosa,OU=TFC Users,DC=THEFINANCIALCOMPANY,DC=NET

Modification type: update
Object type: user

Attribute information:

Changes	Attribute Name	Type	Old Value	New Value
add	department	string		Sales
add	displayName	string		Murray Sosa
add	employeeID	string		10000868
add	employeeType	string		Employee
add	givenName	string		Murray
none	name	string	MSosa	MSosa
none	objectSid	binary	01 05 00 00 00 00 00 05 15 00 00 00 02 3...	01 05 00 00 00 00 00 05 15 00 00 00 02 3...
none	pwdLastSet	number	0	0
none	sAMAccountName	string	MSosa	MSosa
add	sn	string		Sosa
add	title	string		Sales Representative
none	userAccountControl	number	512	512
none	userPrincipalName	string	MSosa@TheFinancialCompany.com	MSosa@TheFinancialCompany.com

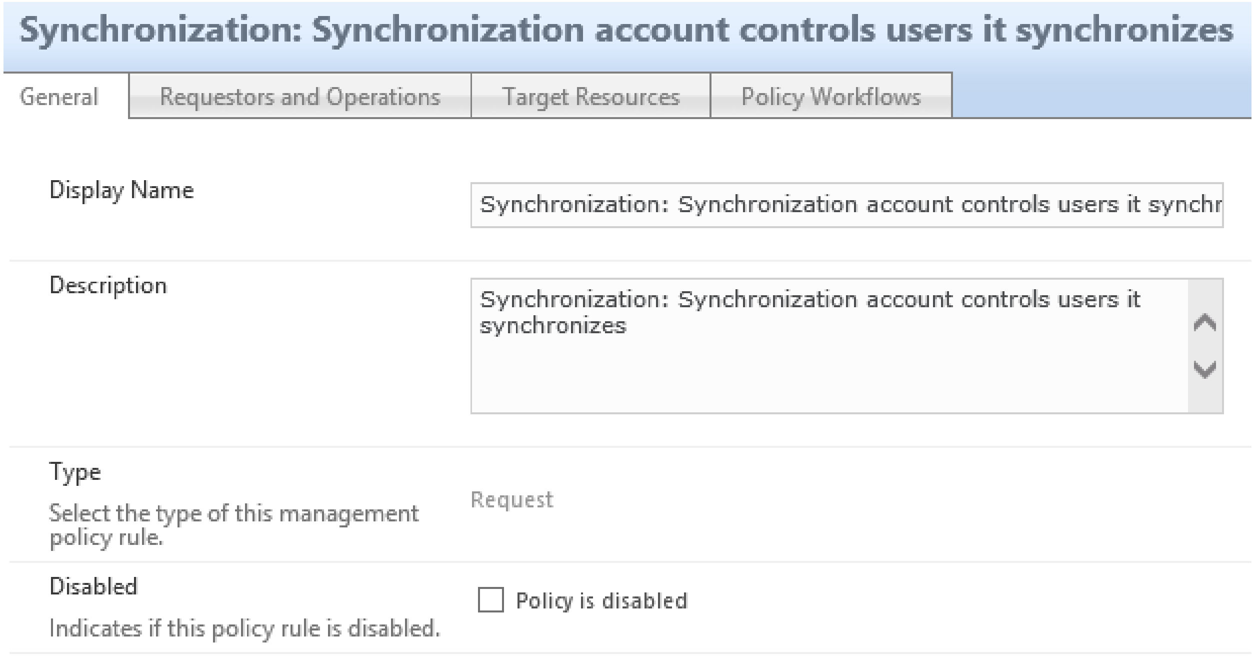



Select **management policy rule** that match **all** of the following conditions:

Display Name contains user

Add Statement or **Add Sub-condition**

□	Display Name ▲	Action Type	Disabled
□	Administration: Administrators can delete non-administrator users	Delete	No
□	Administration: Administrators can read and update Users	Create, Add, Modify, Remove	No
□	Anonymous users can reset their password	Modify	Yes
□	Distribution list Management: Users can add or remove any members of groups subject to owner approval	Add, Remove	Yes
□	Distribution list management: Users can add or remove any members of groups that don't require owner approval	Add, Remove	Yes
□	Distribution List management: Users can create Static Distribution Groups	Create	Yes
□	Distribution list management: Users can read selected attributes of group resources	Read	Yes
□	General: Users can read non-administrative configuration resources	Read	Yes
□	General: Users can read schema related resources	Read	No
□	PAM: Administrators control Users and Groups	Add, Create, Delete, Modify, Read, Remove	No
□	PAM: User can read Pam Roles that he can request	Read	No
□	PAM: User can read Pam Roles that he owns	Read	No
□	PAM: User can see PAM requests that he created	Read	No
□	PAM: Users can create a PAM Request	Create	No
□	Password reset users can read password reset objects	Read	Yes
□	Password Reset Users can update the lockout attributes of themselves	Add, Remove, Read	Yes
□	Security group management: Users can add or remove any member of groups subject to owner approval	Add, Remove	Yes
□	Security Group management: Users can create Static Security Groups	Create	Yes
□	Security group management: Users can read selected attributes of group resources	Read	Yes
□	Security groups: Users can add and remove members to open groups	Add, Remove	Yes



Synchronization: Synchronization account controls users it synchronizes

Display Name

Synchronization: Synchronization account controls users it synchr

Description

Synchronization: Synchronization account controls users it synchronizes

Type

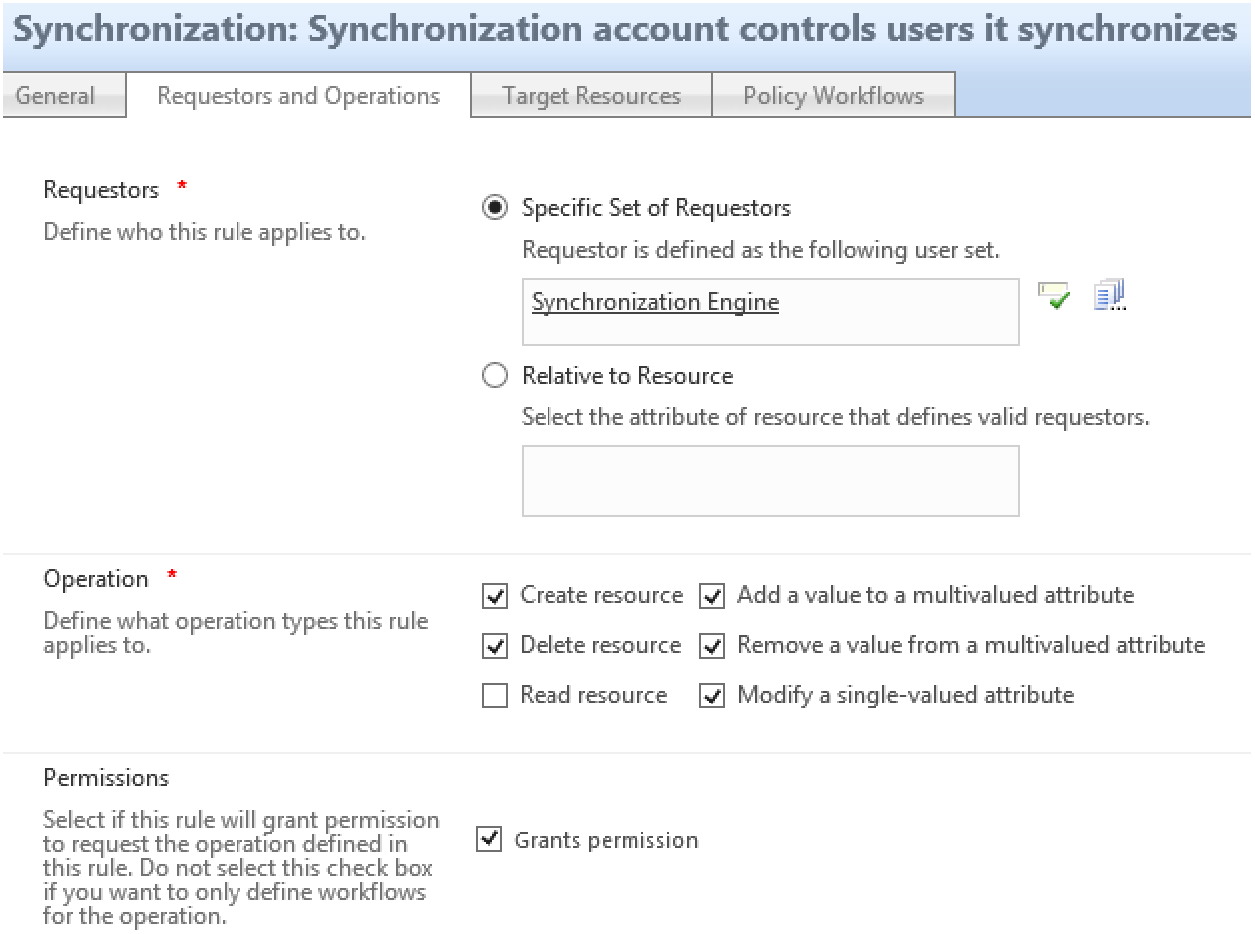
Select the type of this management policy rule.

Request

Disabled

Indicates if this policy rule is disabled.

□ Policy is disabled



Synchronization: Synchronization account controls users it synchronizes

Requestors *

Define who this rule applies to.

● Specific Set of Requestors

Requestor is defined as the following user set.

Synchronization Engine

○ Relative to Resource

Select the attribute of resource that defines valid requestors.

Operation *

Define what operation types this rule applies to.

☑ Create resource ☑ Add a value to a multivalued attribute

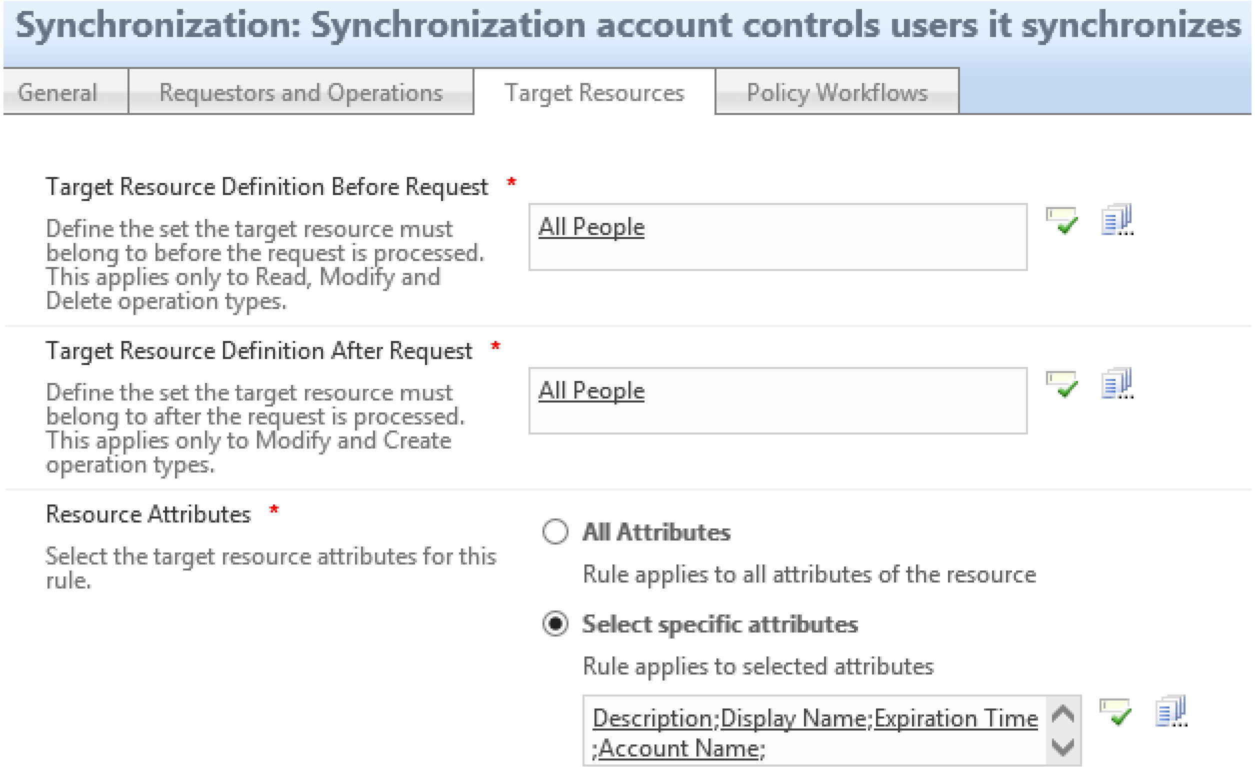
☑ Delete resource ☑ Remove a value from a multivalued attribute

□ 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



Synchronization: Synchronization account controls users it synchronizes

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 People

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 People

Resource Attributes *

Select the target resource attributes for this rule.

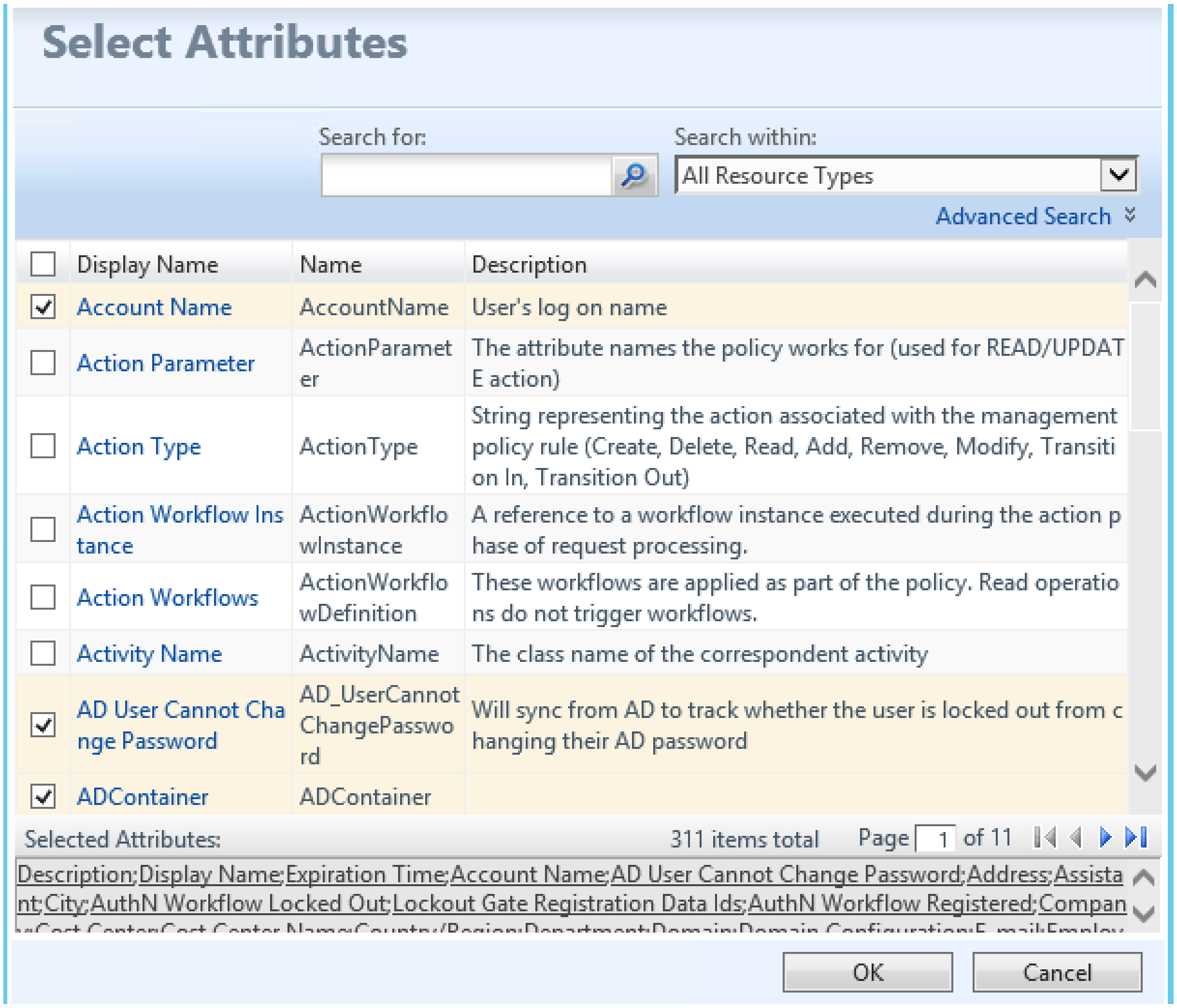
○ **All Attributes**

Rule applies to all attributes of the resource

● **Select specific attributes**

Rule applies to selected attributes

Description;Display Name;Expiration Time;Account Name;



Select Attributes

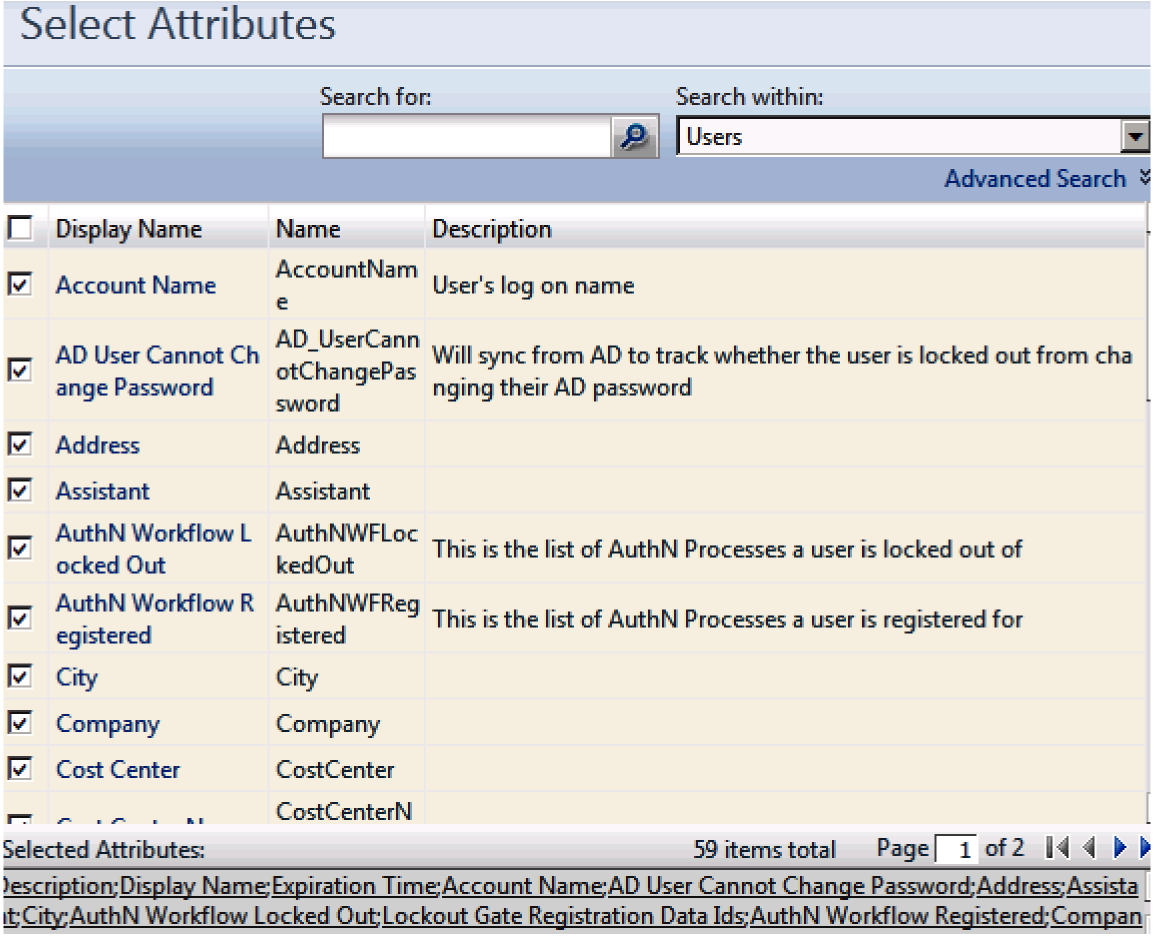
Search for: [ ]

Search within: All Resource Types

□	Display Name	Name	Description
☑	Account Name	AccountName	User's log on name
□	Action Parameter	ActionParameter	The attribute names the policy works for (used for READ/UPDATE action)
□	Action Type	ActionType	String representing the action associated with the management policy rule (Create, Delete, Read, Add, Remove, Modify, Transition In, Transition Out)
□	Action Workflow Instance	ActionWorkflowInstance	A reference to a workflow instance executed during the action phase of request processing.
□	Action Workflows	ActionWorkflowDefinition	These workflows are applied as part of the policy. Read operations do not trigger workflows.
□	Activity Name	ActivityName	The class name of the correspondent activity
☑	AD User Cannot Change Password	AD_UserCannotChangePassword	Will sync from AD to track whether the user is locked out from changing their AD password
☑	ADContainer	ADContainer	

Selected Attributes: 311 items total Page 1 of 11

Description;Display Name;Expiration Time;Account Name;AD User Cannot Change Password;Address;Assistant;City;AuthN Workflow Locked Out;Lockout Gate Registration Data Ids;AuthN Workflow Registered;Company;Cost Center;Cost Center Name;Country/Region;Department;Domain;Domain Configuration;E-mail;Employ

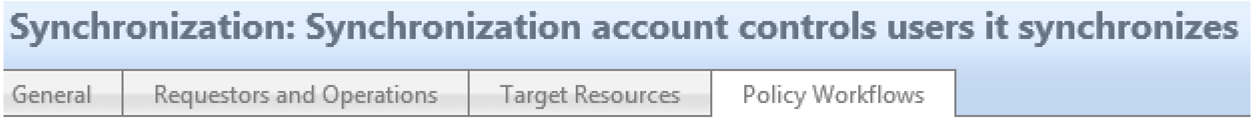


Select Attributes

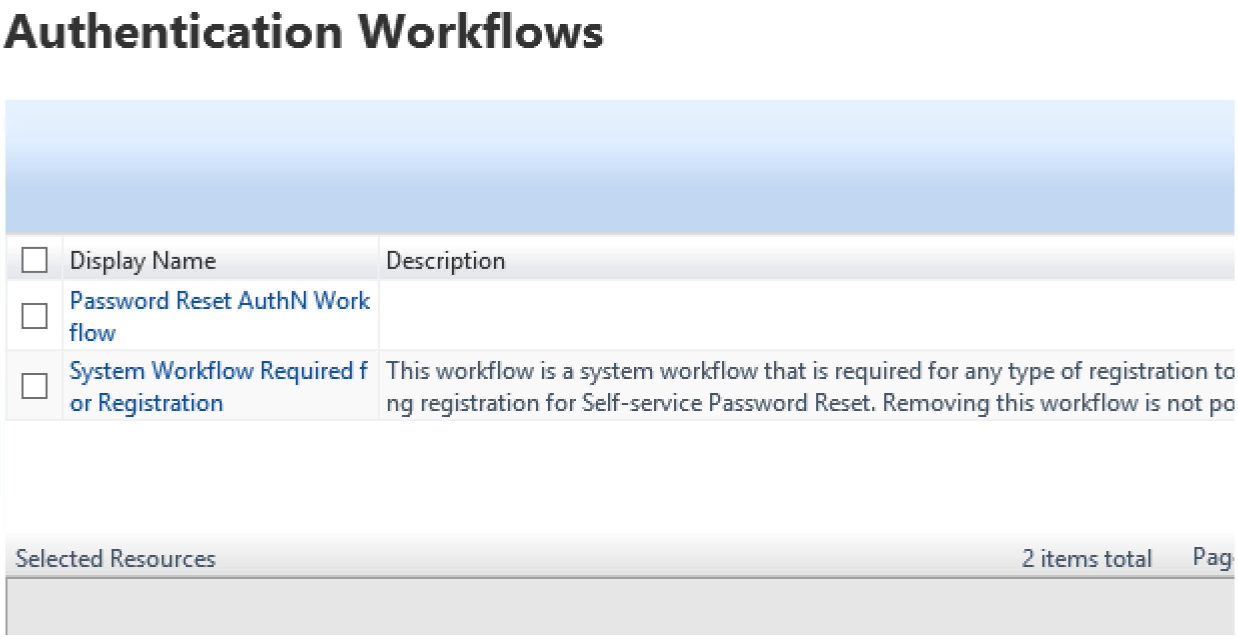
☐	Display Name	Name	Description
☑	Account Name	AccountName	User's log on name
☑	AD User Cannot Change Password	AD_UserCannotChangePassword	Will sync from AD to track whether the user is locked out from changing their AD password
☑	Address	Address	
☑	Assistant	Assistant	
☑	AuthN Workflow Locked Out	AuthNWFLockedOut	This is the list of AuthN Processes a user is locked out of
☑	AuthN Workflow Registered	AuthNWFRegistered	This is the list of AuthN Processes a user is registered for
☑	City	City	
☑	Company	Company	
☑	Cost Center	CostCenter	
☑	Cost Center N	CostCenterN	

Selected Attributes: 59 items total Page 1 of 2

escription;Display Name;Expiration Time;Account Name;AD User Cannot Change Password;Address;Assista
t;City;AuthN Workflow Locked Out;Lockout Gate Registration Data Ids;AuthN Workflow Registered;Compan



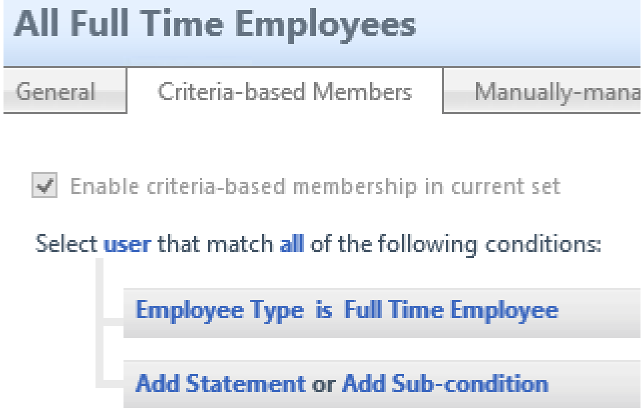
Synchronization: Synchronization account controls users it synchronizes



Authentication Workflows

□	Display Name	Description
□	Password Reset AuthN Workflow	
□	System Workflow Required for Registration	This workflow is a system workflow that is required for any type of registration to ng registration for Self-service Password Reset. Removing this workflow is not po

Selected Resources 2 items total Pag

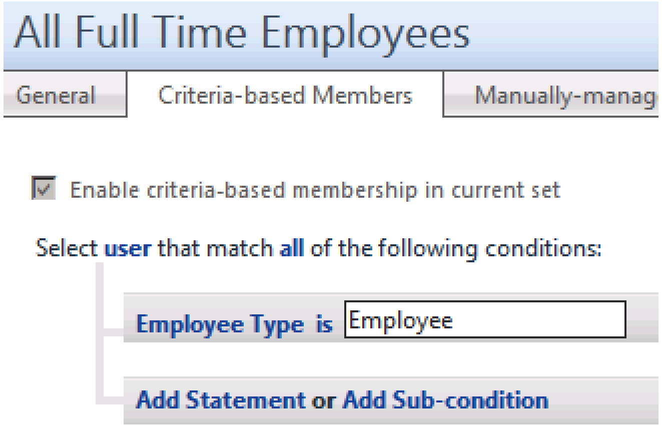


All Full Time Employees

☑ Enable criteria-based membership in current set

Select user that match all of the following conditions:

Employee Type is Full Time Employee

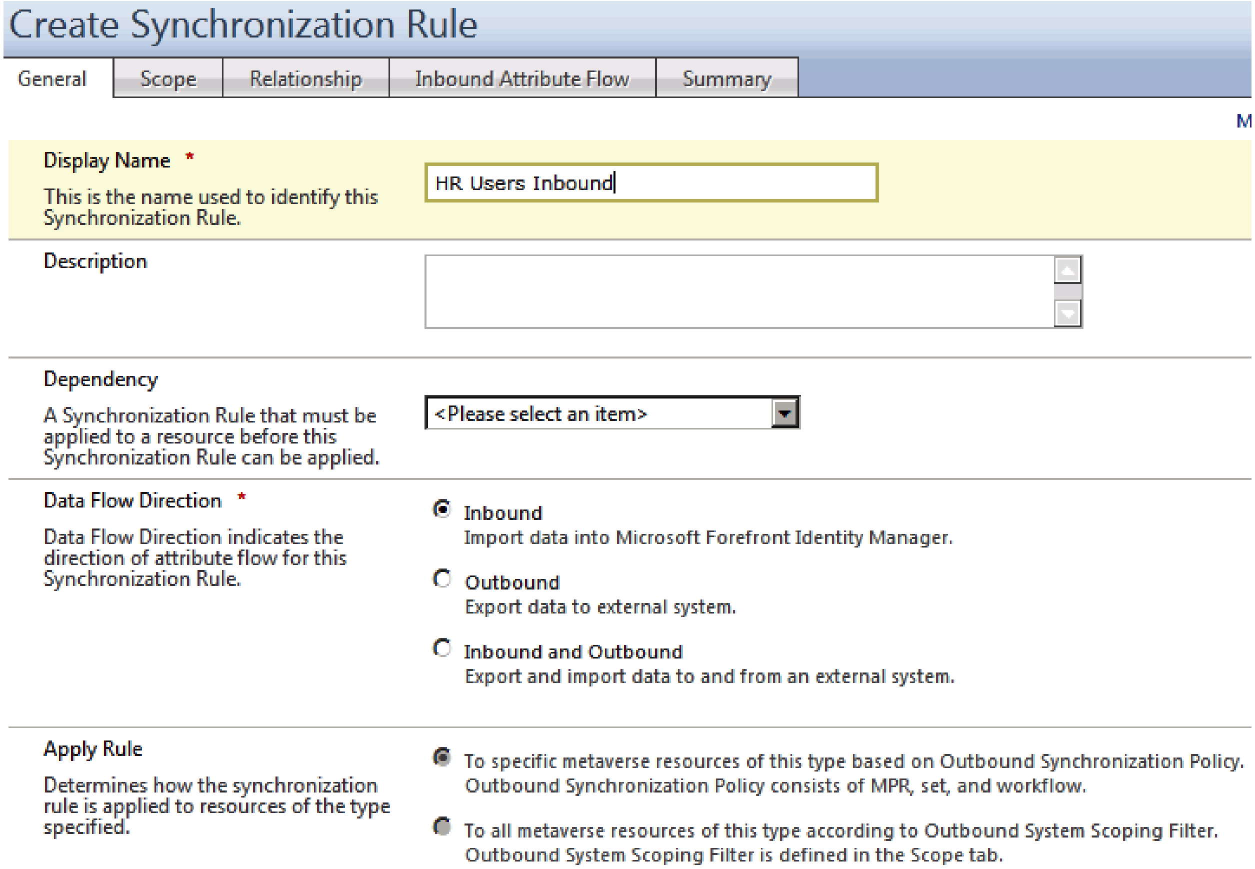


All Full Time Employees

☑ Enable criteria-based membership in current set

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

Employee Type is Employee



Create Synchronization Rule

Display Name *

This is the name used to identify this Synchronization Rule.

HR Users Inbound

Description

Dependency

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

<Please select an item>

Data Flow Direction *

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

● Inbound
Import data into Microsoft Forefront Identity Manager.

○ Outbound
Export data to external system.

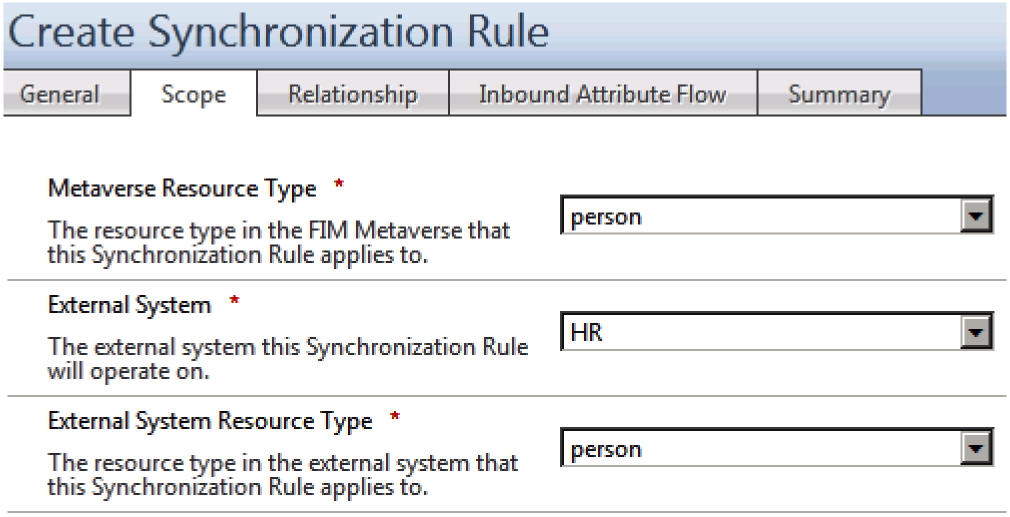
○ Inbound and Outbound
Export and import data to and from an external system.

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.



Create Synchronization Rule

Metaverse Resource Type *

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

person

External System *

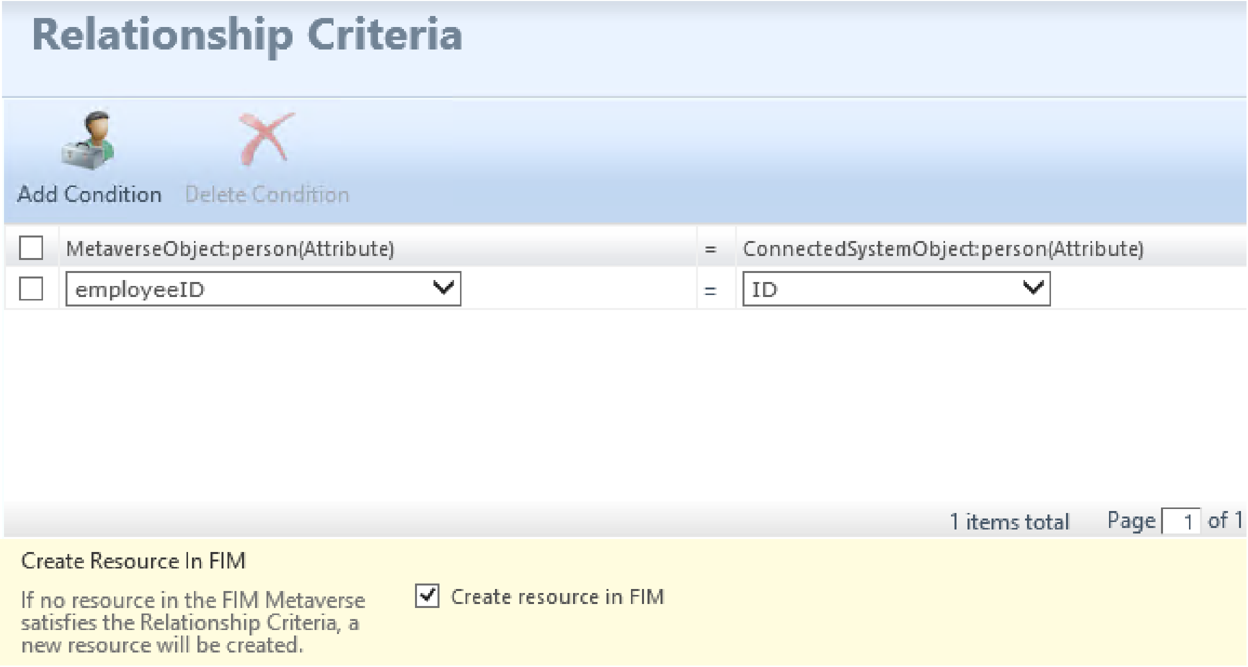
The external system this Synchronization Rule will operate on.

HR

External System Resource Type *

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

person



Relationship Criteria

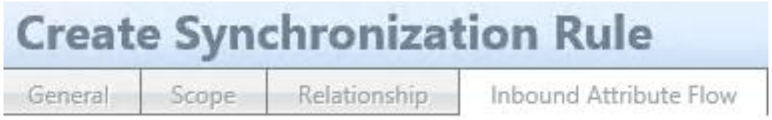
□	MetaverseObject:person(Attribute)	=	ConnectedSystemObject:person(Attribute)
□	employeeID	=	ID

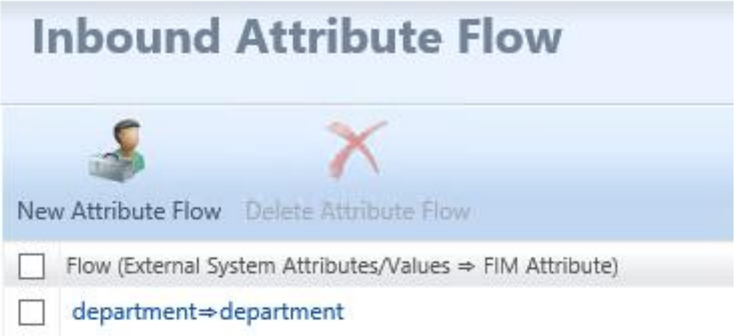
1 items total   Page 1 of 1

Create Resource In FIM

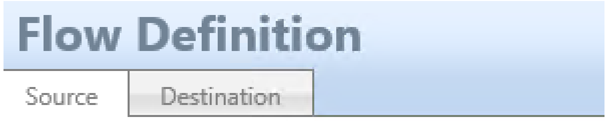
If no resource in the FIM Metaverse satisfies the Relationship Criteria, a new resource will be created.

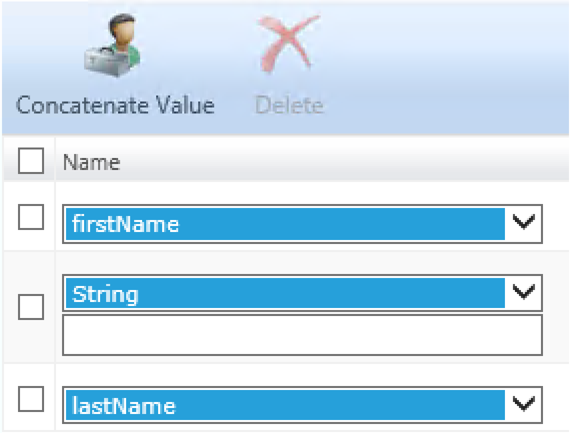
☑ Create resource in FIM



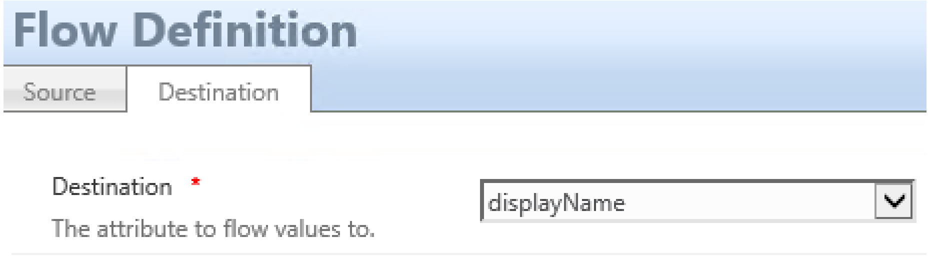


□	Flow (External System Attributes/Values ⇒ FIM Attribute)
□	department⇒department



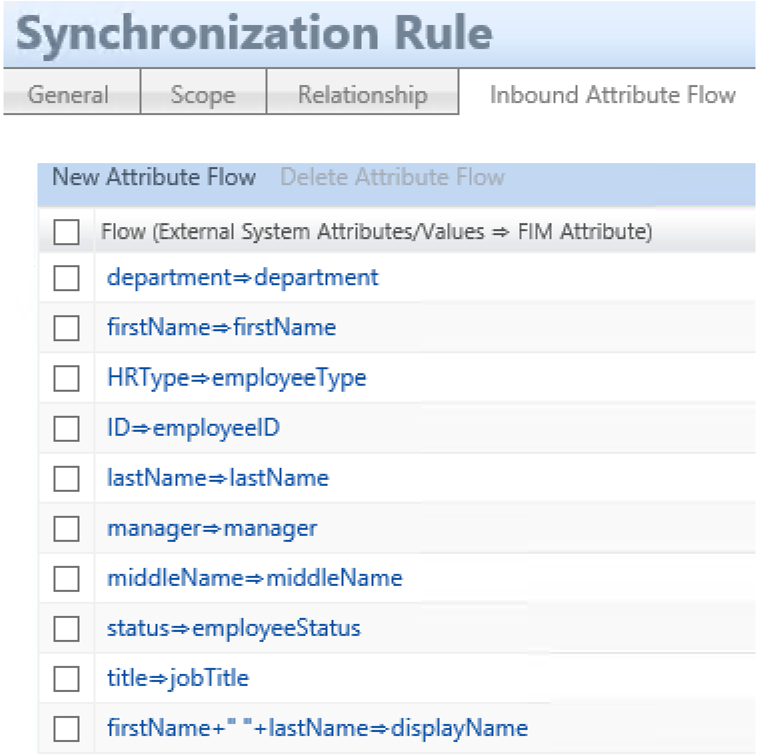


□	Name
□	firstName
□	String
□	lastName



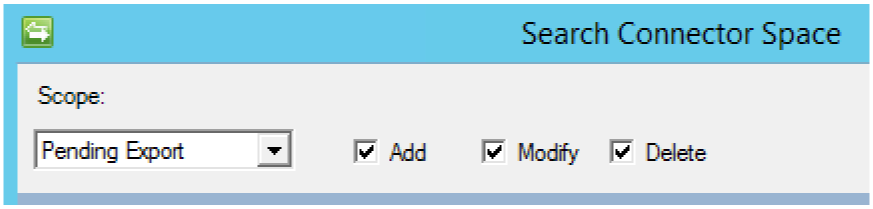
Destination *
The attribute to flow values to.

displayName



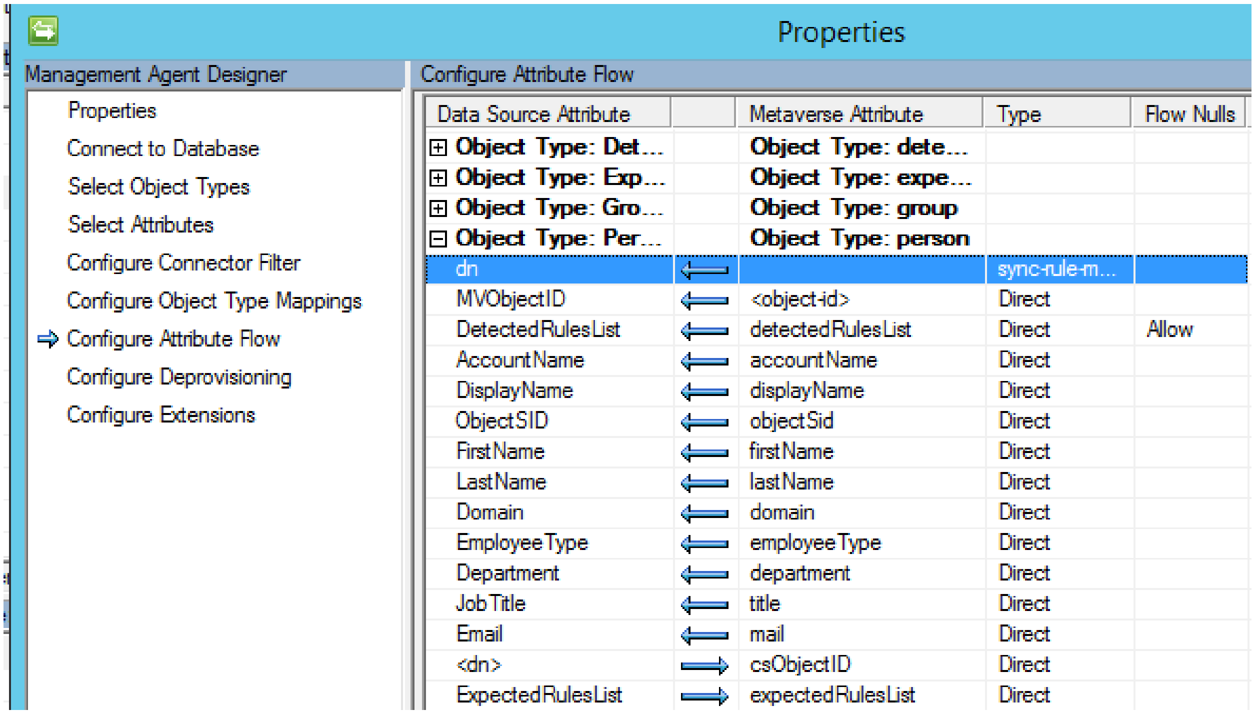
Synchronization Rule

□	Flow (External System Attributes/Values ⇒ FIM Attribute)
□	department⇒department
□	firstName⇒firstName
□	HRType⇒employeeType
□	ID⇒employeeID
□	lastName⇒lastName
□	manager⇒manager
□	middleName⇒middleName
□	status⇒employeeStatus
□	title⇒jobTitle
□	firstName+" "+lastName⇒displayName



Search Connector Space

Scope: Pending Export ☑ Add ☑ Modify ☑ Delete

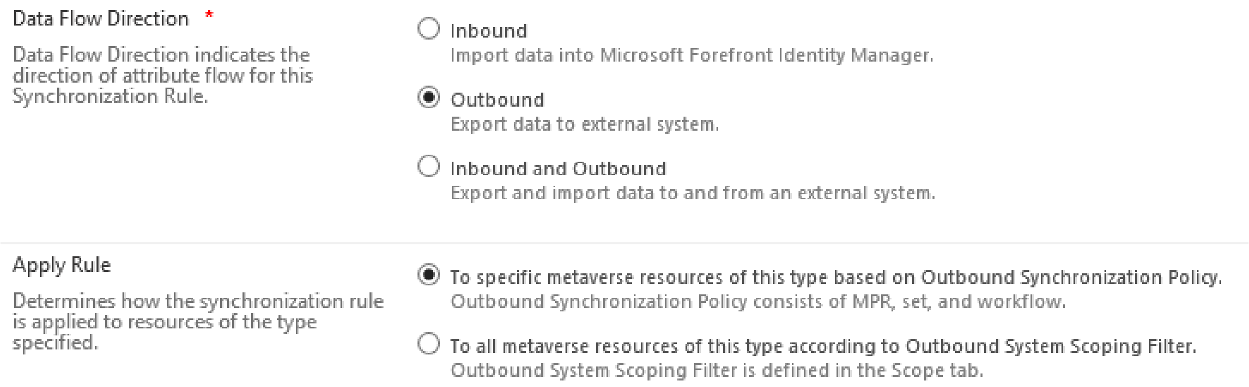


Properties

Management Agent Designer

Configure Attribute Flow

Data Source Attribute		Metaverse Attribute	Type	Flow Nulls
⊞ **Object Type: Det...**		**Object Type: dete...**		
⊞ **Object Type: Exp...**		**Object Type: expe...**		
⊞ **Object Type: Gro...**		**Object Type: group**		
⊟ **Object Type: Per...**		**Object Type: person**		
dn	⟵		sync-rule-m...	
MVObjectID	⟵	<object-id>	Direct	
DetectedRulesList	⟵	detectedRulesList	Direct	Allow
AccountName	⟵	accountName	Direct	
DisplayName	⟵	displayName	Direct	
ObjectSID	⟵	objectSid	Direct	
FirstName	⟵	firstName	Direct	
LastName	⟵	lastName	Direct	
Domain	⟵	domain	Direct	
EmployeeType	⟵	employeeType	Direct	
Department	⟵	department	Direct	
JobTitle	⟵	title	Direct	
Email	⟵	mail	Direct	
<dn>	⟶	csObjectID	Direct	
ExpectedRulesList	⟶	expectedRulesList	Direct	



Data Flow Direction *

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

○ Inbound
Import data into Microsoft Forefront Identity Manager.

● Outbound
Export data to external system.

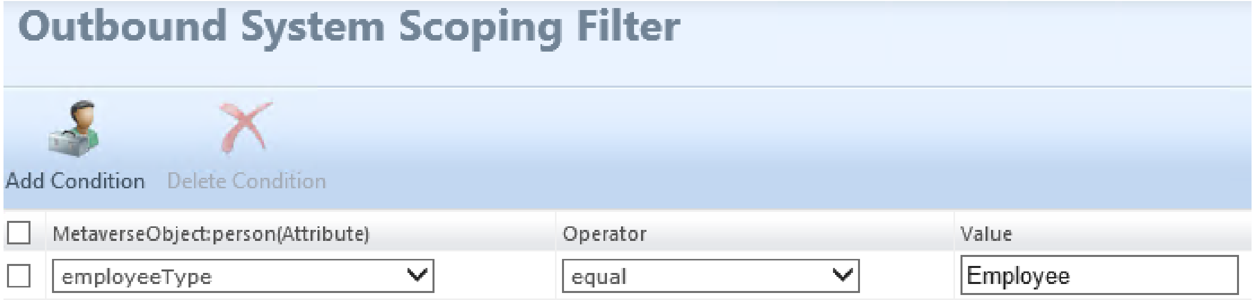
○ Inbound and Outbound
Export and import data to and from an external system.

Apply Rule

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

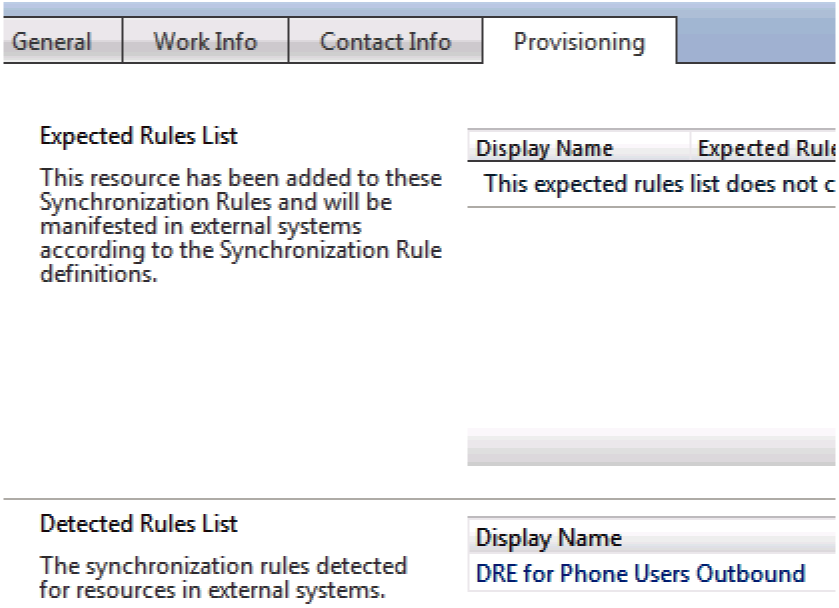
● To specific metaverse resources of this type based on Outbound Synchronization Policy.
Outbound Synchronization Policy consists of MPR, set, and workflow.

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



Outbound System Scoping Filter

□	MetaverseObject:person(Attribute)	Operator	Value
□	employeeType	equal	Employee



Expected Rules List

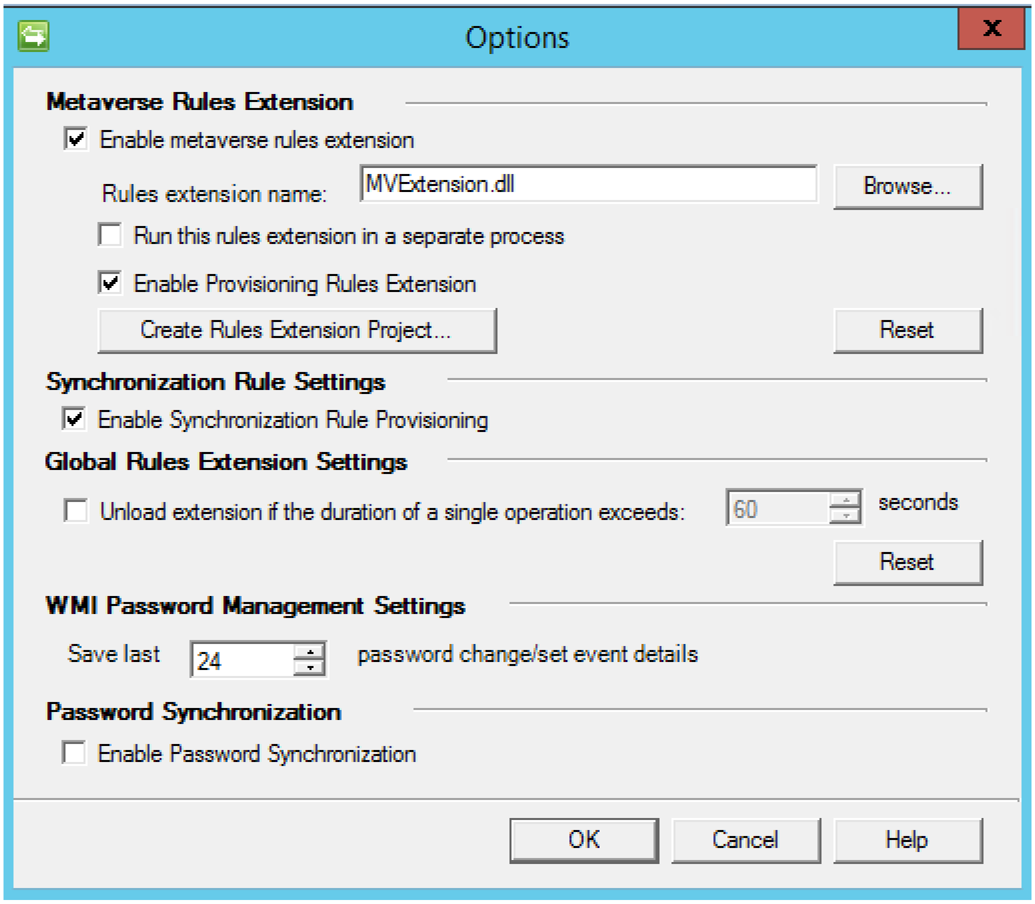
This resource has been added to these Synchronization Rules and will be manifested in external systems according to the Synchronization Rule definitions.

Display Name	Expected Rul
This expected rules list does not c	

Detected Rules List

The synchronization rules detected for resources in external systems.

Display Name
DRE for Phone Users Outbound



Options

Metaverse Rules Extension

☑ Enable metaverse rules extension

Rules extension name: MVExtension.dll

☐ Run this rules extension in a separate process

☑ Enable Provisioning Rules Extension

Synchronization Rule Settings

☑ Enable Synchronization Rule Provisioning

Global Rules Extension Settings

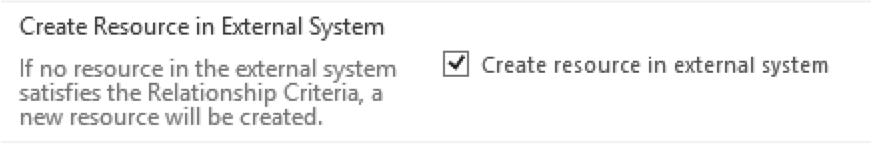
☐ Unload extension if the duration of a single operation exceeds: 60 seconds

WMI Password Management Settings

Save last 24 password change/set event details

Password Synchronization

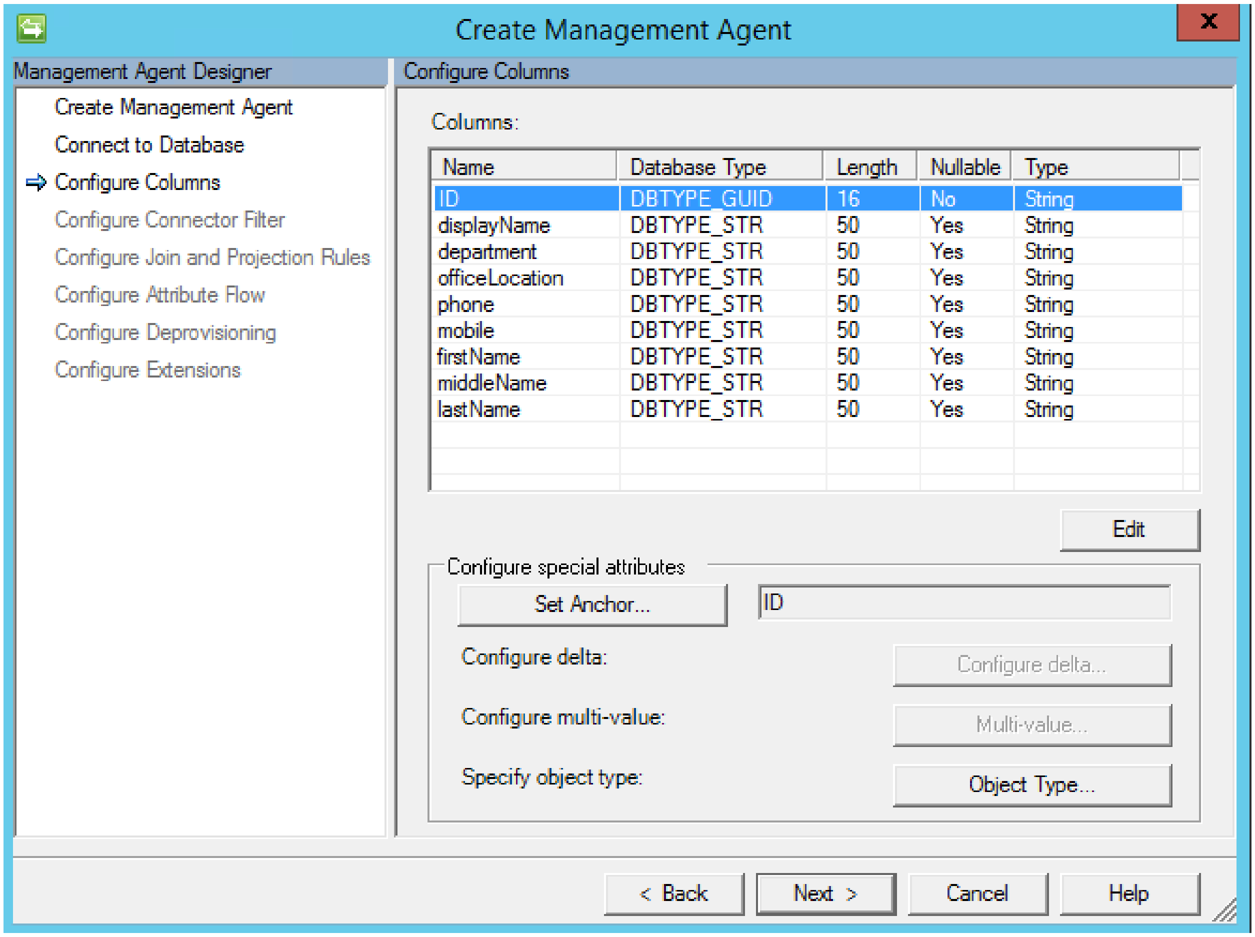
☐ Enable Password Synchronization



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



Columns:

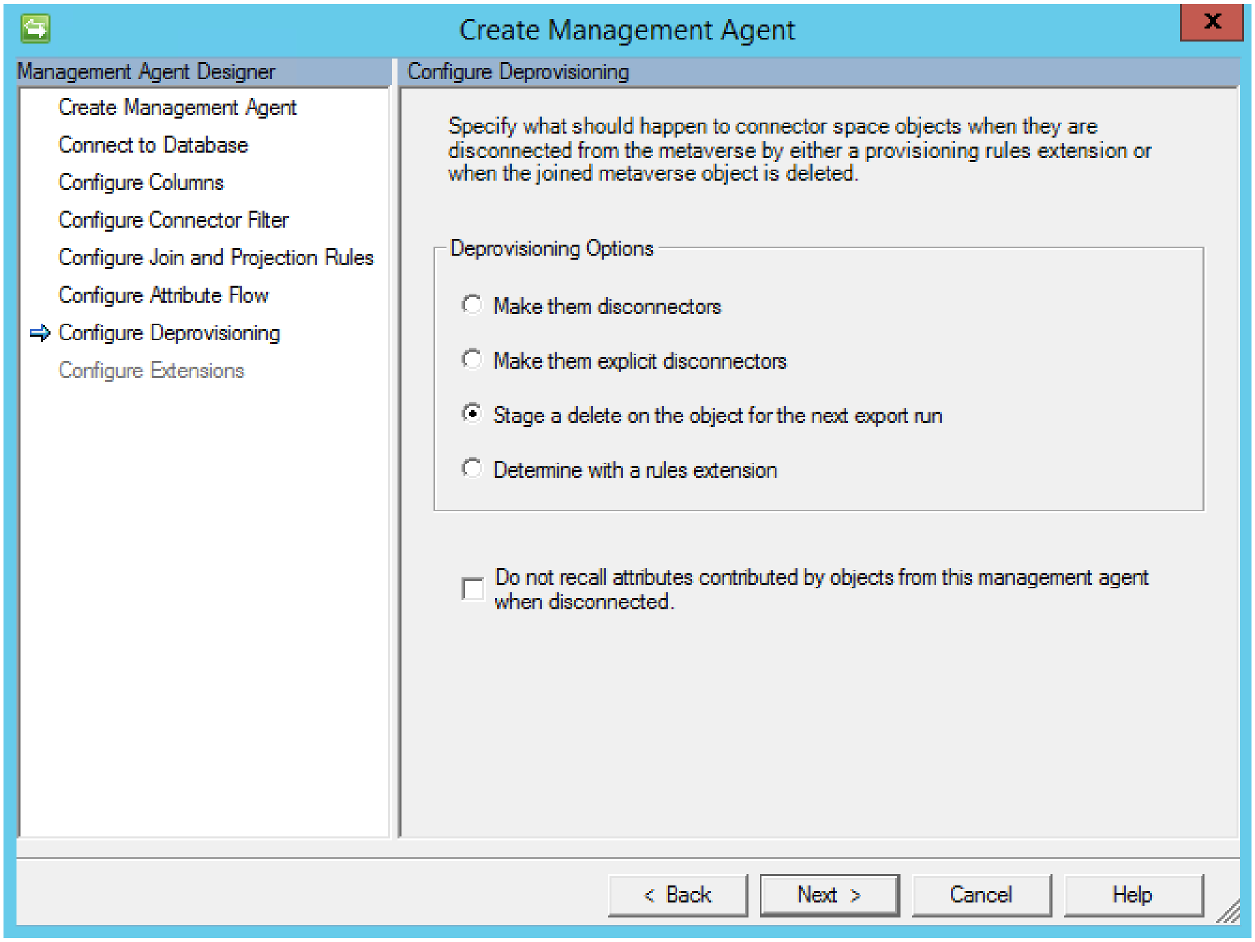
Name	Database Type	Length	Nullable	Type
ID	DBTYPE_GUID	16	No	String
displayName	DBTYPE_STR	50	Yes	String
department	DBTYPE_STR	50	Yes	String
officeLocation	DBTYPE_STR	50	Yes	String
phone	DBTYPE_STR	50	Yes	String
mobile	DBTYPE_STR	50	Yes	String
firstName	DBTYPE_STR	50	Yes	String
middleName	DBTYPE_STR	50	Yes	String
lastName	DBTYPE_STR	50	Yes	String

Set Anchor: ID

Configure delta:

Configure multi-value:

Specify object type:



Create Management Agent

Management Agent Designer

- Create Management Agent
- Connect to Database
- Configure Columns
- Configure Connector Filter
- Configure Join and Projection Rules
- Configure Attribute Flow
- ⇨ Configure Deprovisioning
- Configure Extensions

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

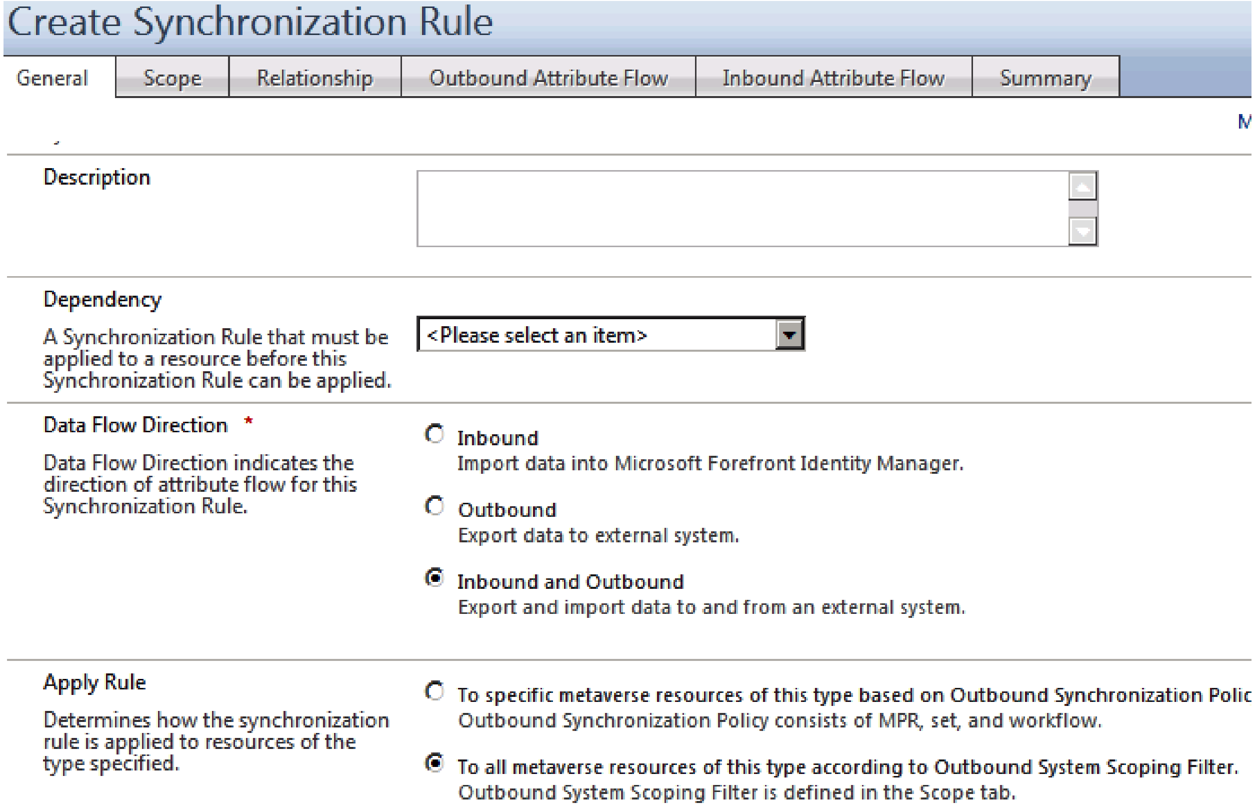
○ Make them disconnectors

○ 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.



Create Synchronization Rule

Description

Dependency

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

<Please select an item>

Data Flow Direction *

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

○ Inbound
Import data into Microsoft Forefront Identity Manager.

○ Outbound
Export data to external system.

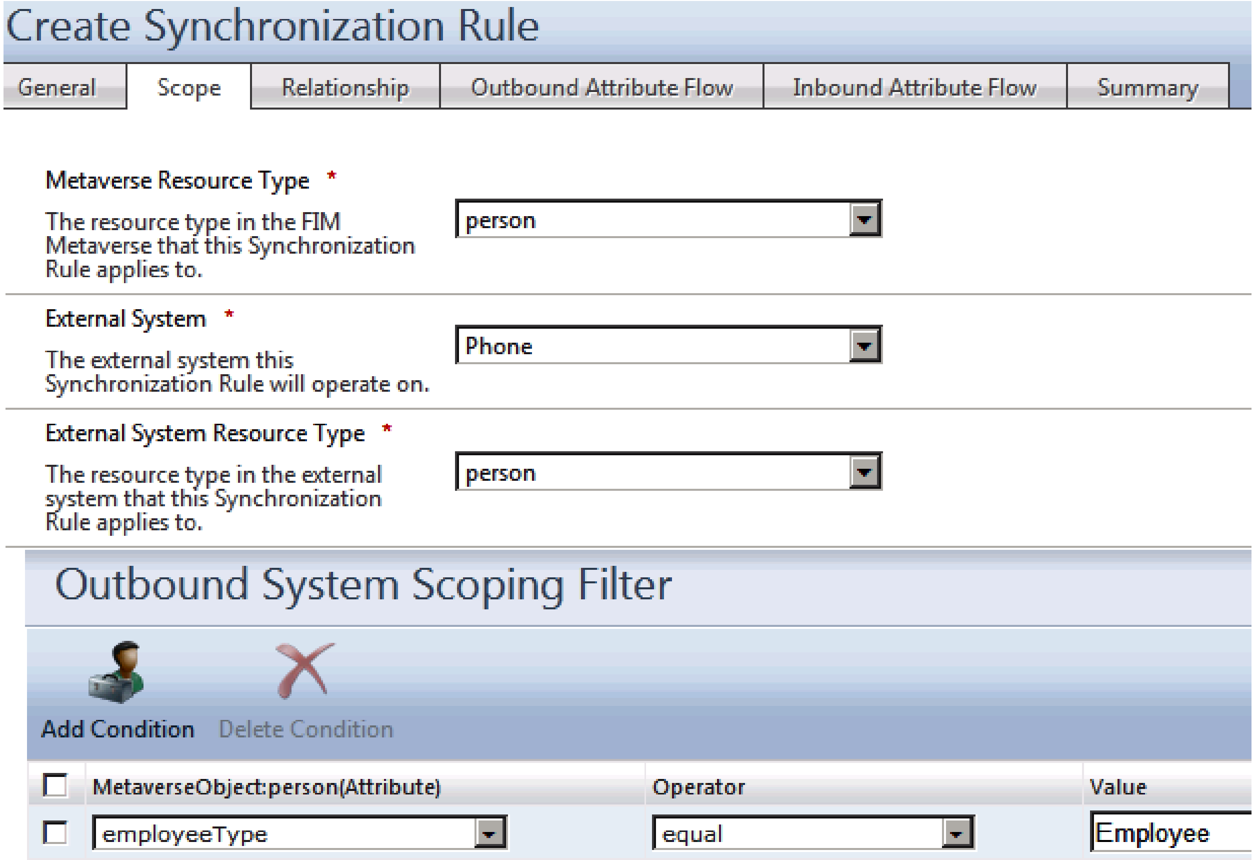
● Inbound and Outbound
Export and import data to and from an external system.

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 Polic
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.



Create Synchronization Rule

Metaverse Resource Type *

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

person

External System *

The external system this Synchronization Rule will operate on.

Phone

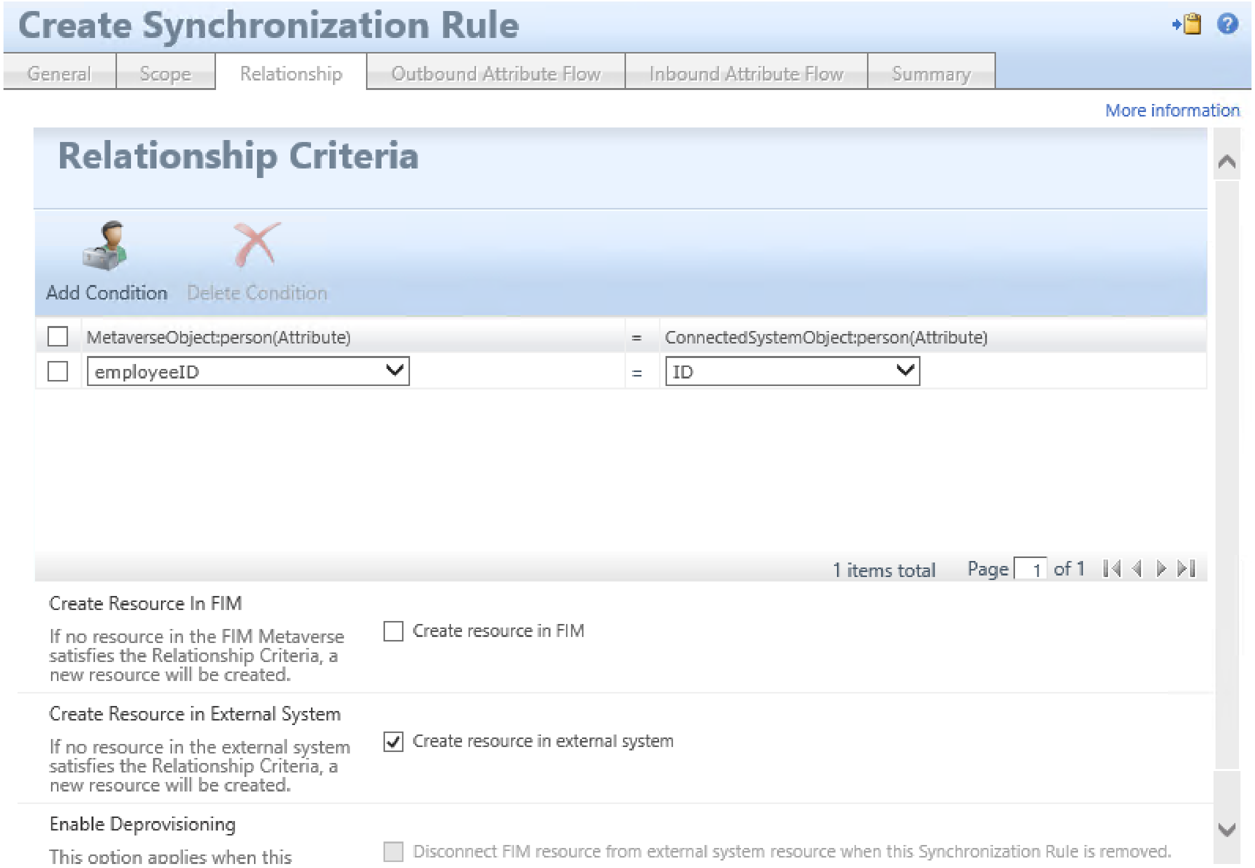
External System Resource Type *

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

person

Outbound System Scoping Filter

□	MetaverseObject:person(Attribute)	Operator	Value
□	employeeType	equal	Employee



Create Synchronization Rule

Relationship Criteria

□	MetaverseObject:person(Attribute)	=	ConnectedSystemObject:person(Attribute)
□	employeeID	=	ID

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

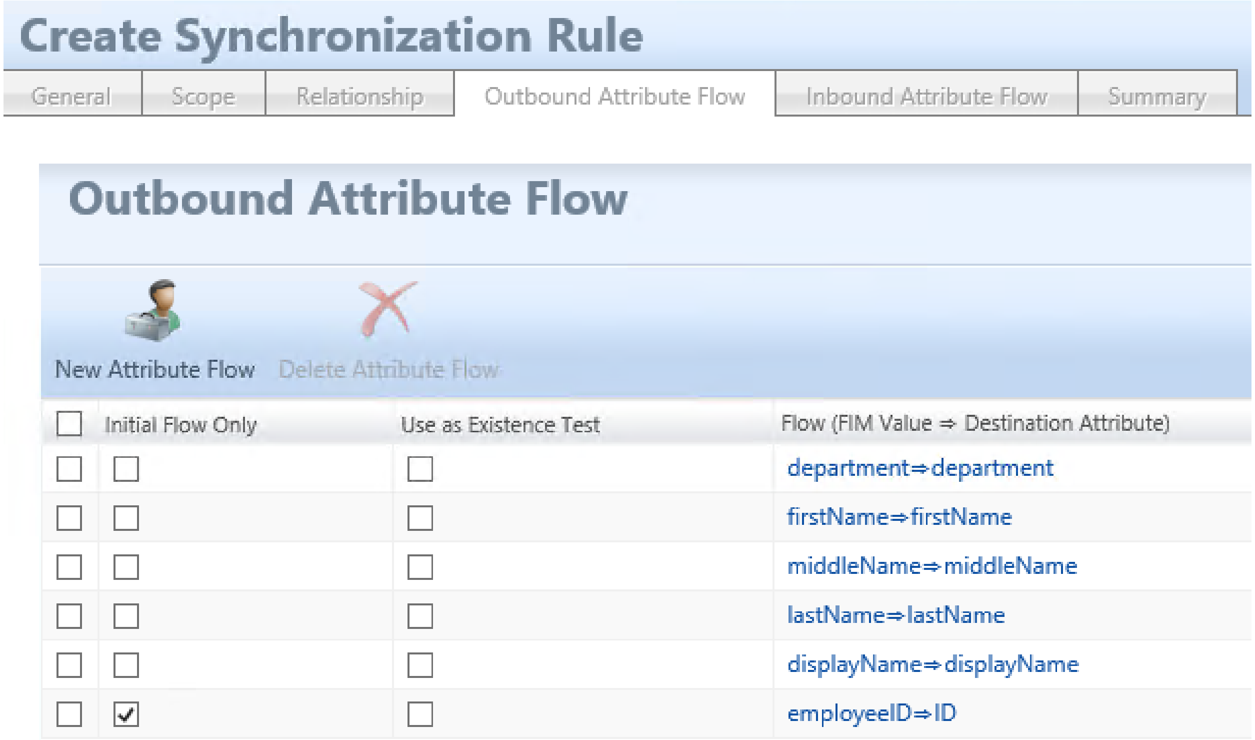
If no resource in the external system satisfies the Relationship Criteria, a new resource will be created.

☑ Create resource in external system

Enable Deprovisioning

This option applies when this

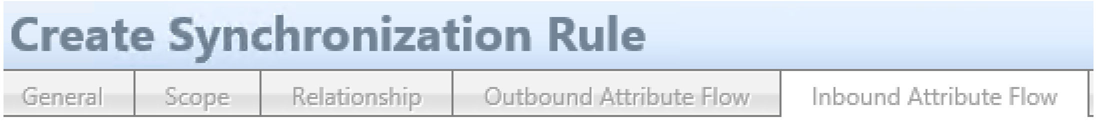
□ Disconnect FIM resource from external system resource when this Synchronization Rule is removed.



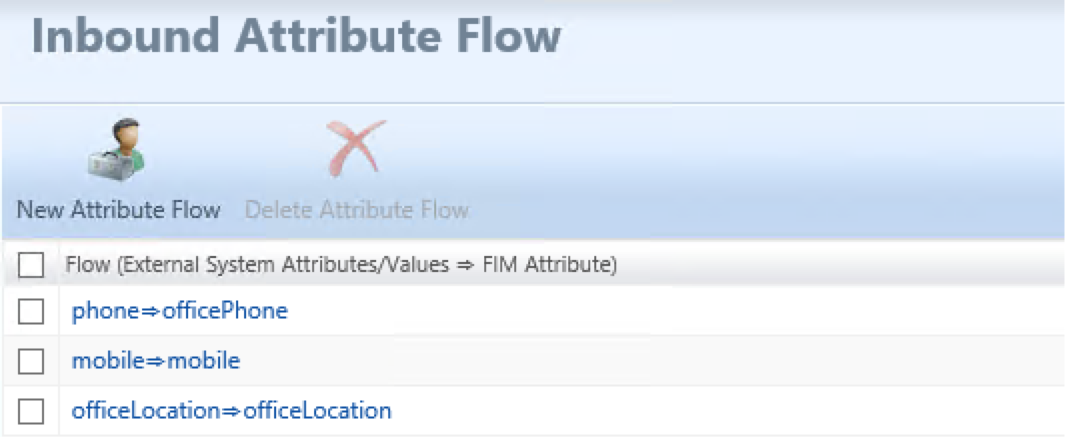
Create Synchronization Rule

Outbound Attribute Flow

□	Initial Flow Only	Use as Existence Test	Flow (FIM Value ⇒ Destination Attribute)
□	□	□	department⇒department
□	□	□	firstName⇒firstName
□	□	□	middleName⇒middleName
□	□	□	lastName⇒lastName
□	□	□	displayName⇒displayName
□	☑	□	employeeID⇒ID

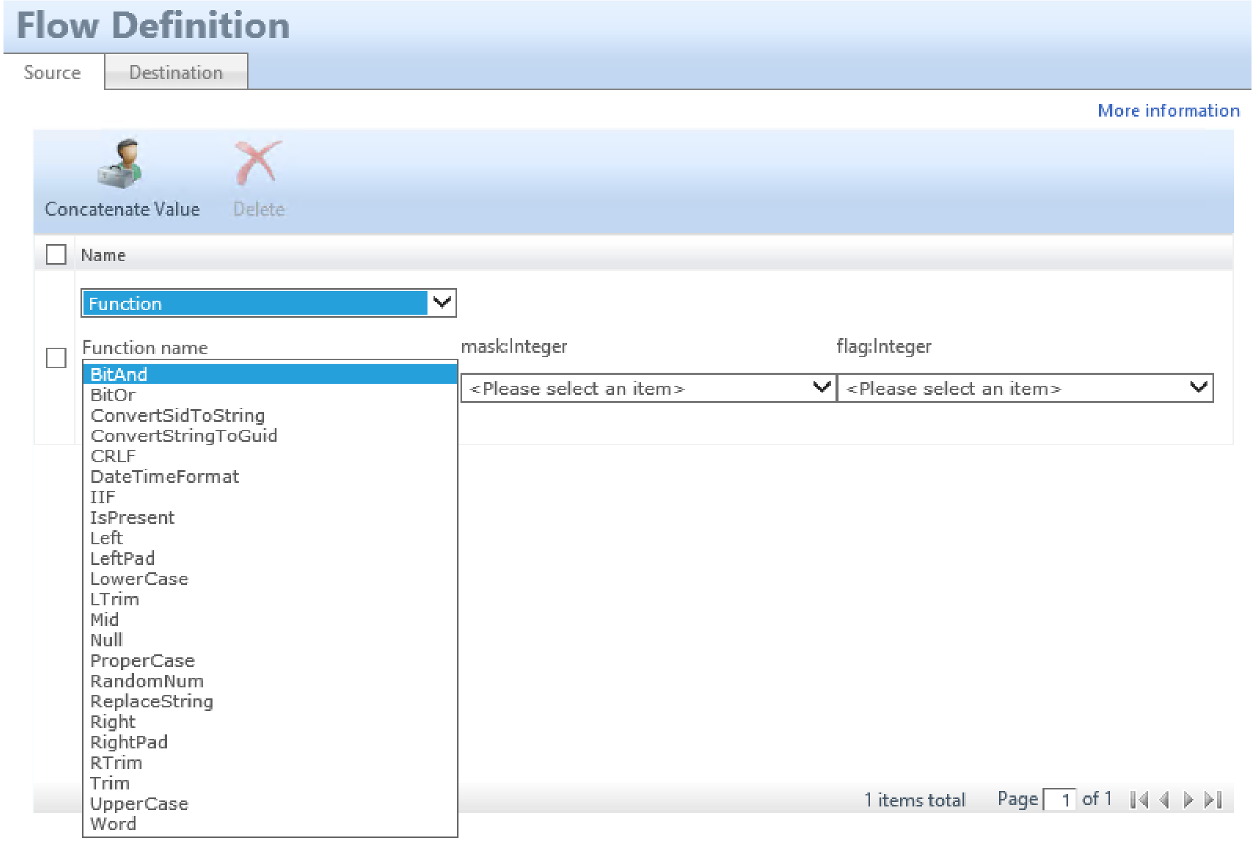


Create Synchronization Rule



Inbound Attribute Flow

□	Flow (External System Attributes/Values ⇒ FIM Attribute)
□	phone⇒officePhone
□	mobile⇒mobile
□	officeLocation⇒officeLocation



Flow Definition

□ Name

Function

□ Function name

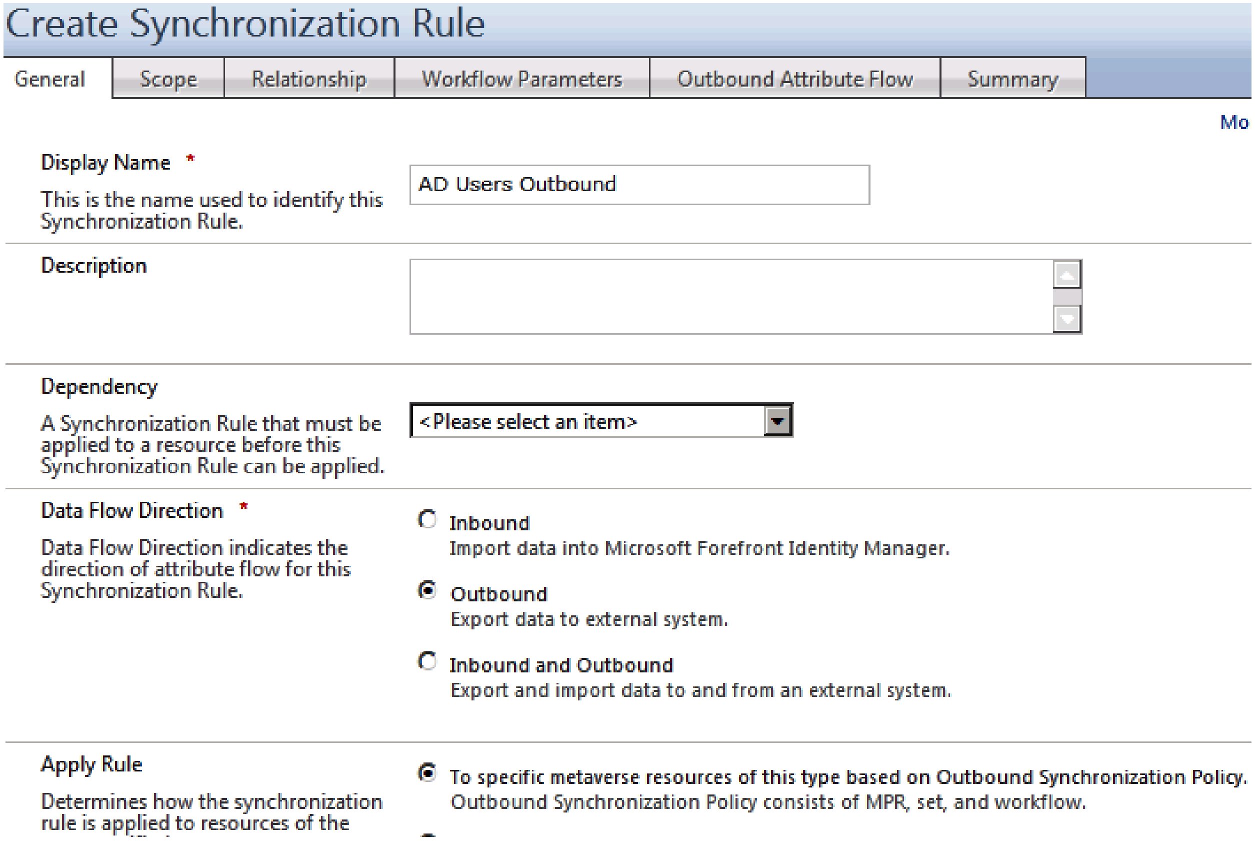
mask:Integer

<Please select an item>

flag:Integer

<Please select an item>

1 items total Page 1 of 1



Create Synchronization Rule

Display Name *

This is the name used to identify this Synchronization Rule.

AD Users Outbound

Description

Dependency

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

<Please select an item>

Data Flow Direction *

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

○ Inbound
Import data into Microsoft Forefront Identity Manager.

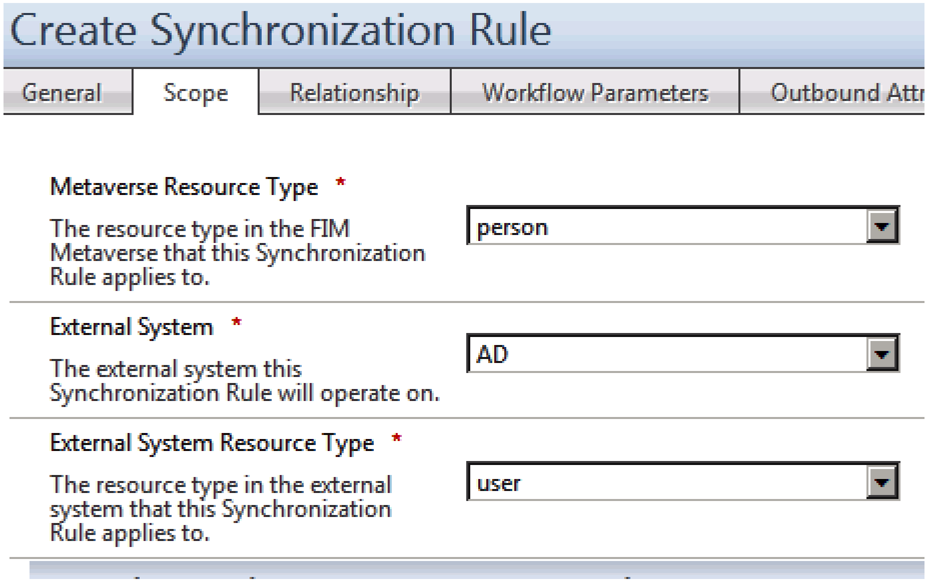
● Outbound
Export data to external system.

○ 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

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



Create Synchronization Rule

Metaverse Resource Type *

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

person

External System *

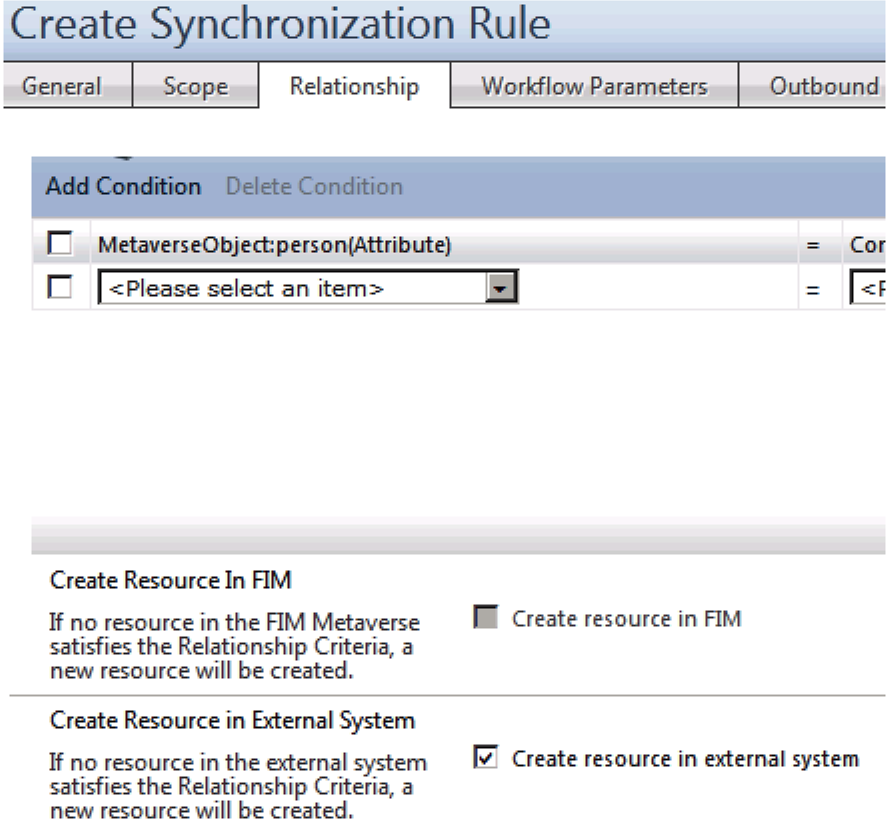
The external system this Synchronization Rule will operate on.

AD

External System Resource Type *

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

user



Create Synchronization Rule

□	MetaverseObject:person(Attribute)	=	Cor
□	<Please select an item>	=	<F

Create Resource In FIM

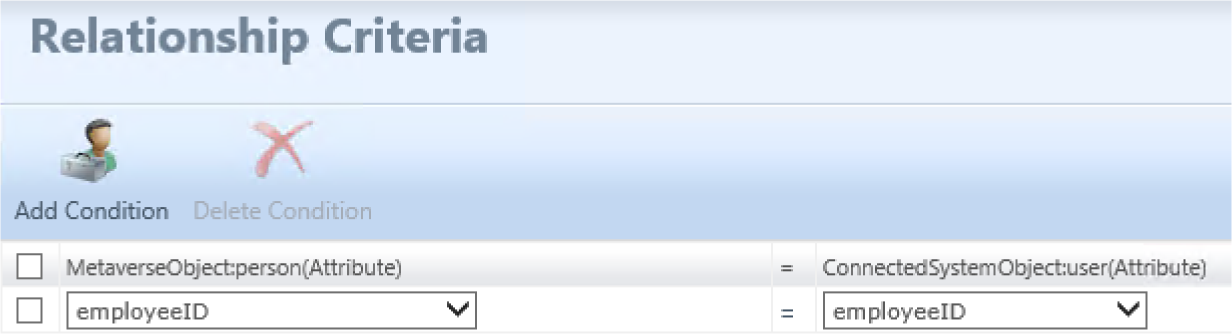
If no resource in the FIM Metaverse satisfies the Relationship Criteria, a new resource will be created.

□ Create resource in FIM

Create Resource in External System

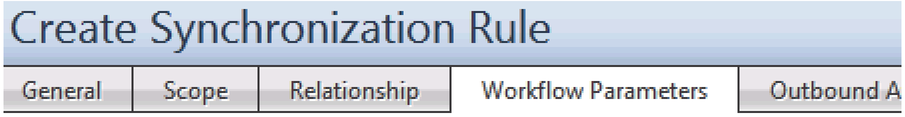
If no resource in the external system satisfies the Relationship Criteria, a new resource will be created.

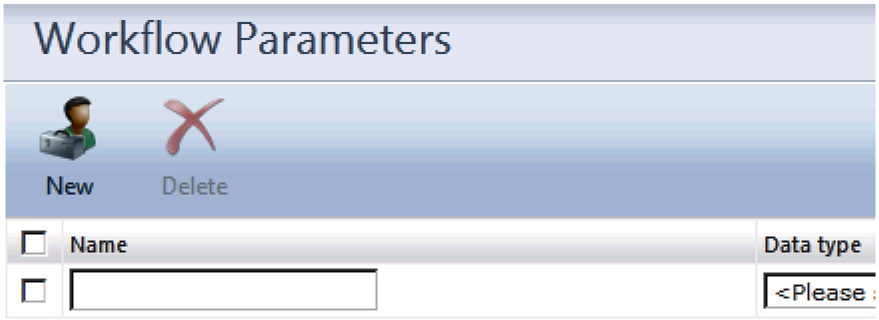
☑ Create resource in external system



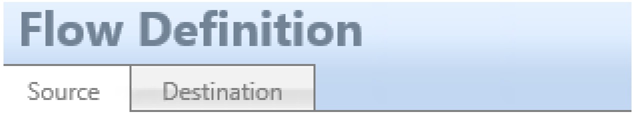
Relationship Criteria

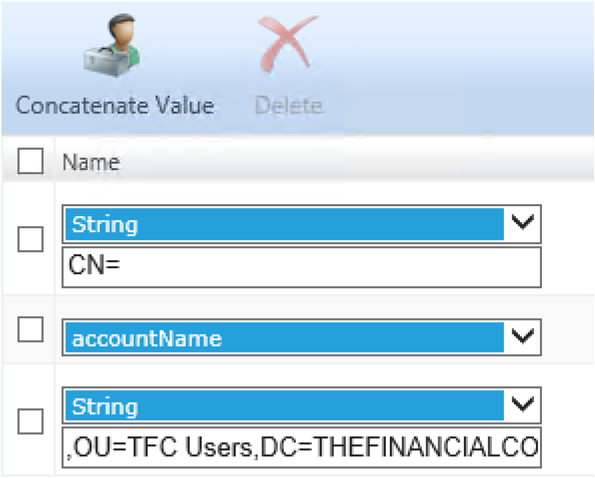
□	MetaverseObject:person(Attribute)	=	ConnectedSystemObject:user(Attribute)
□	employeeID	=	employeeID



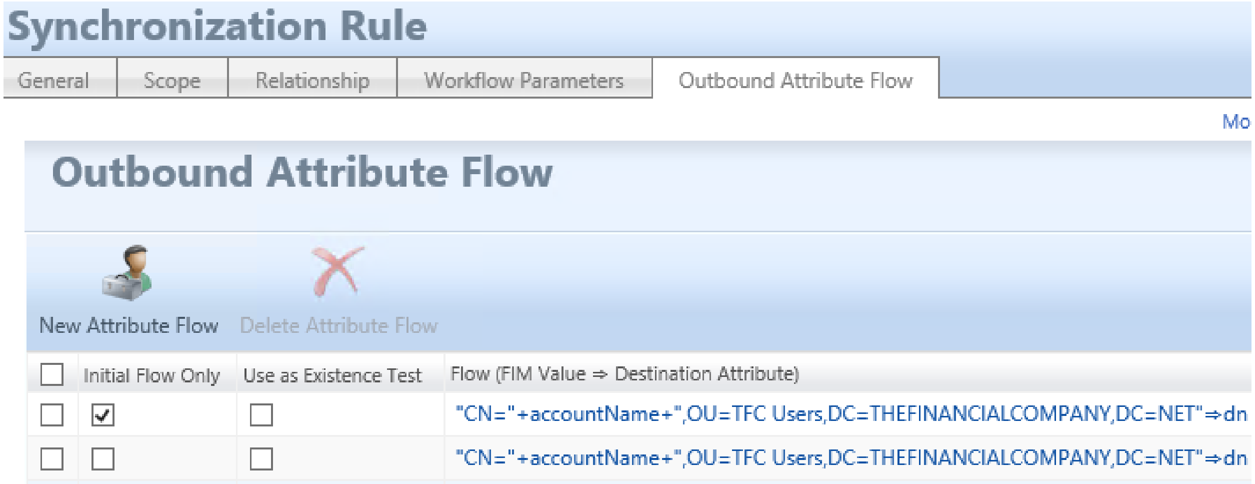


□	Name	Data type
□		<Please

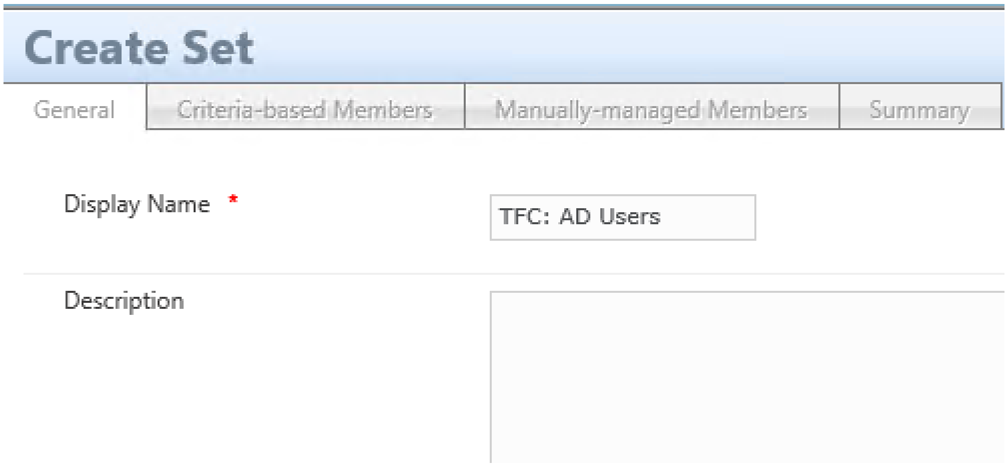




□	Name
□	String CN=
□	accountName
□	String ,OU=TFC Users,DC=THEFINANCIALCO



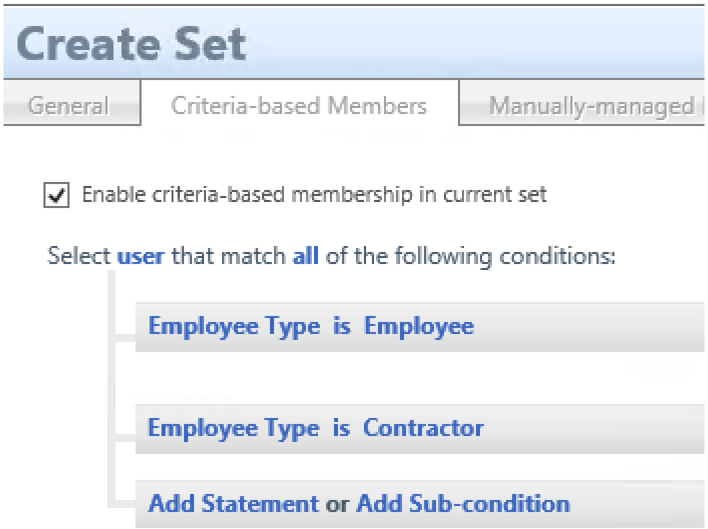
□	Initial Flow Only	Use as Existence Test	Flow (FIM Value ⇒ Destination Attribute)
□	☑	□	"CN="+accountName+",OU=TFC Users,DC=THEFINANCIALCOMPANY,DC=NET"⇒dn
□	□	□	"CN="+accountName+",OU=TFC Users,DC=THEFINANCIALCOMPANY,DC=NET"⇒dn



Create Set

Display Name * TFC: AD Users

Description



Create Set

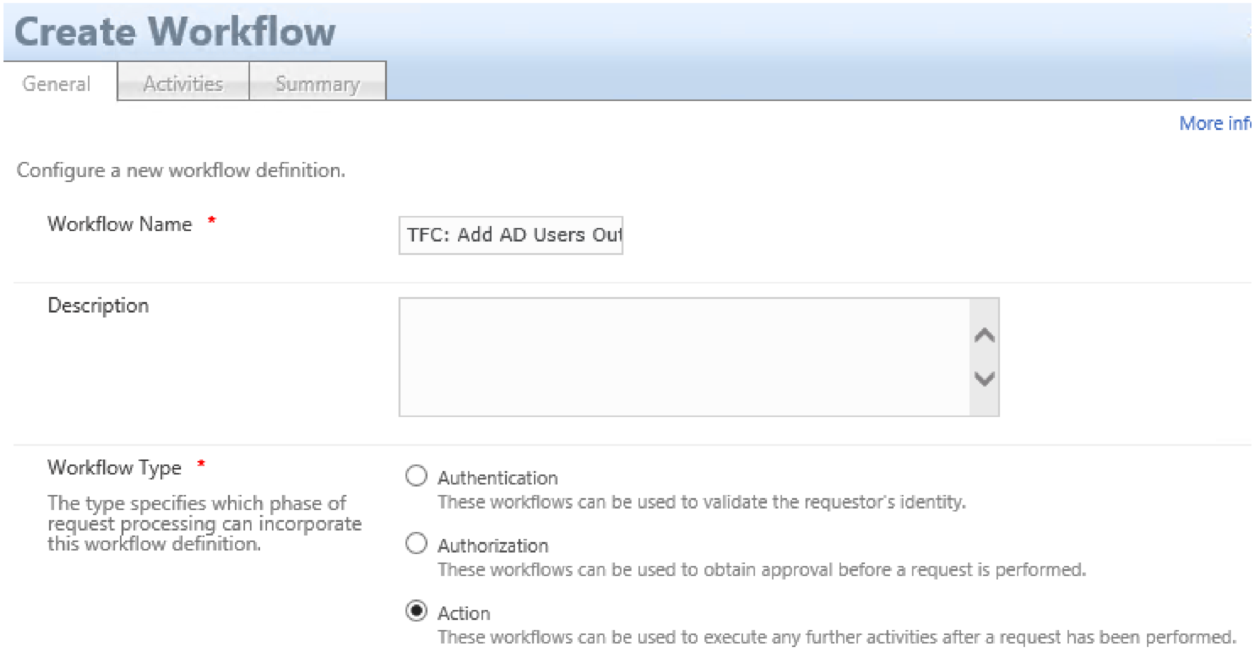
☑ Enable criteria-based membership in current set

Select user that match all of the following conditions:

Employee Type is Employee

Employee Type is Contractor

Add Statement or Add Sub-condition



Create Workflow

Configure a new workflow definition.

Workflow Name * TFC: Add AD Users Out

Description

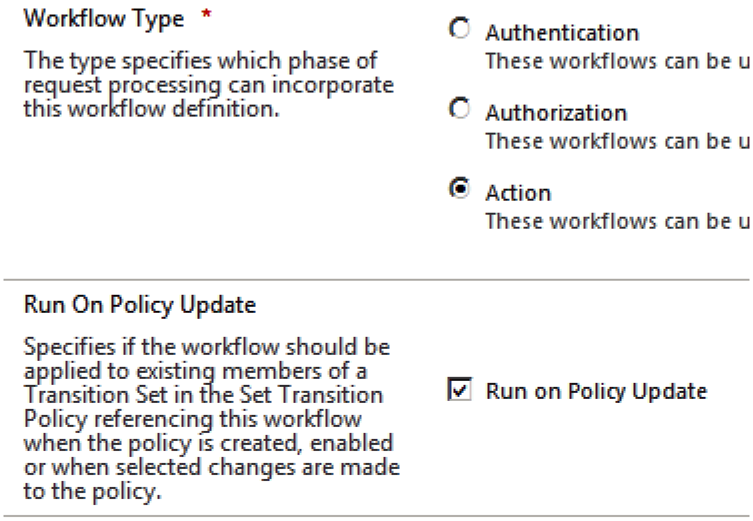
Workflow Type *

The type specifies which phase of request processing can incorporate this workflow definition.

○ Authentication
These workflows can be used to validate the requestor's identity.

○ Authorization
These workflows can be used to obtain approval before a request is performed.

● Action
These workflows can be used to execute any further activities after a request has been performed.



Workflow Type *

The type specifies which phase of request processing can incorporate this workflow definition.

○ Authentication
These workflows can be u

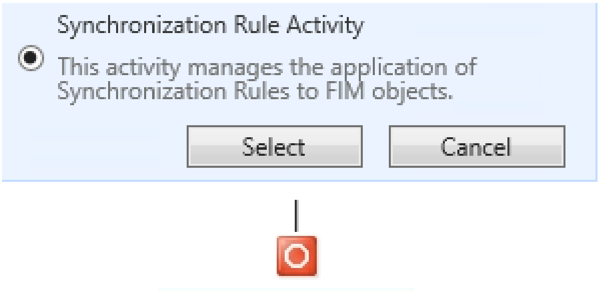
○ Authorization
These workflows can be u

● Action
These workflows can be u

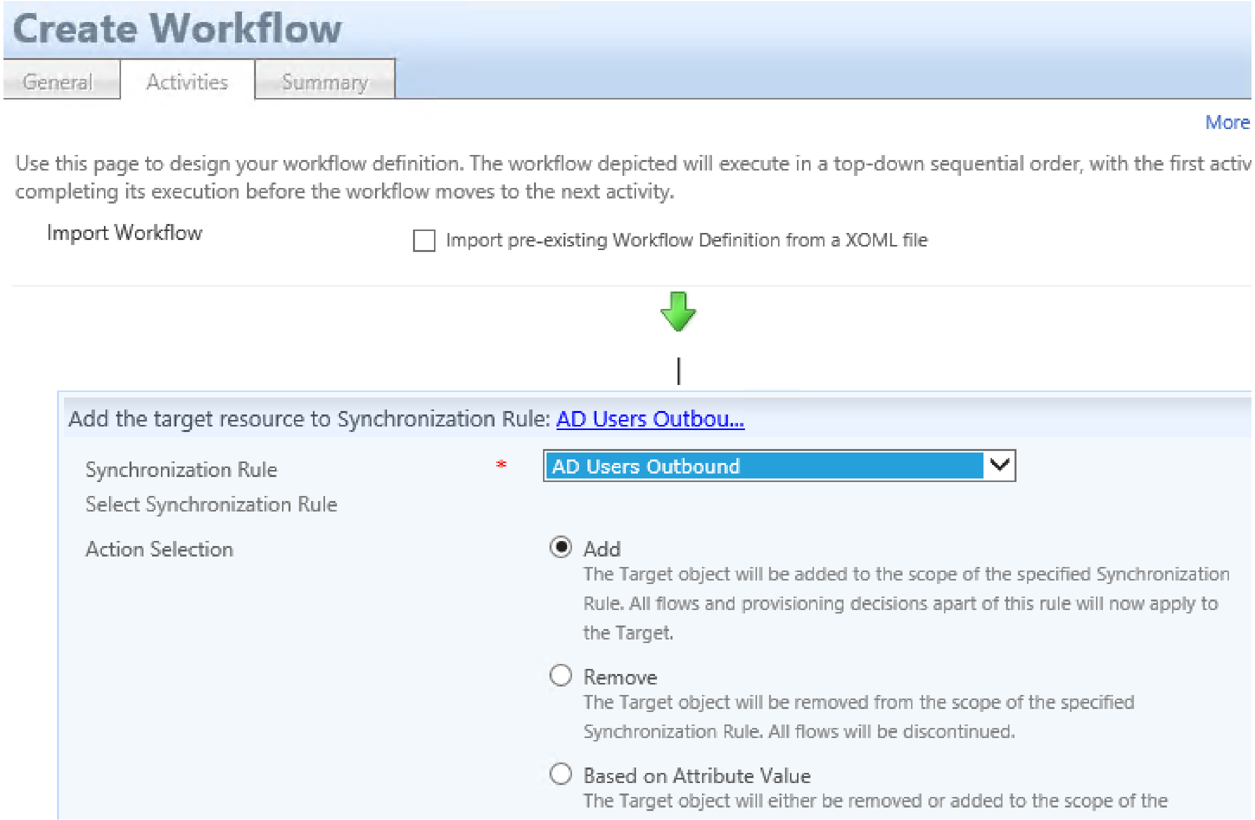
Run On Policy Update

Specifies if the workflow should be applied to existing members of a Transition Set in the Set Transition Policy referencing this workflow when the policy is created, enabled or when selected changes are made to the policy.

☑ Run on Policy Update



● Synchronization Rule Activity
This activity manages the application of Synchronization Rules to FIM objects.



Create Workflow

Use this page to design your workflow definition. The workflow depicted will execute in a top-down sequential order, with the first activ completing its execution before the workflow moves to the next activity.

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

Add the target resource to Synchronization Rule: AD Users Outbou...

Synchronization Rule * AD Users Outbound

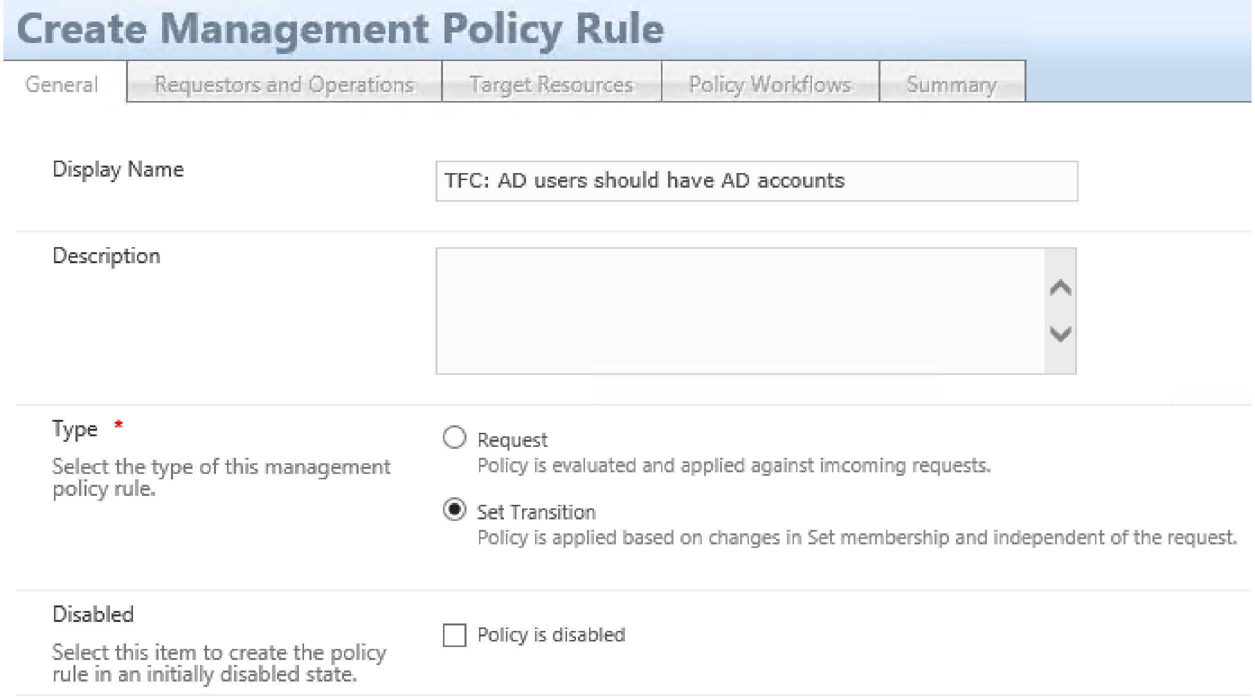
Select Synchronization Rule

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



Create Management Policy Rule

Display Name: TFC: AD users should have AD accounts

Description

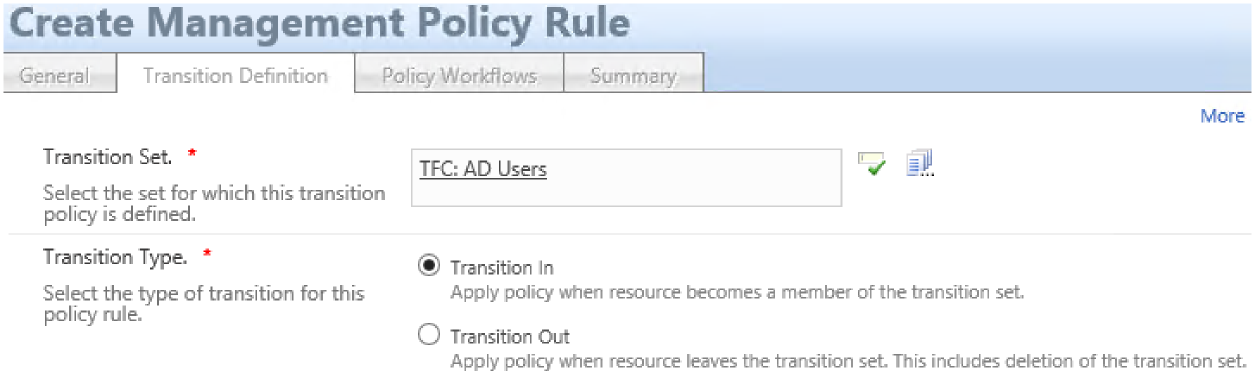
Type *
Select the type of this management policy rule.

○ Request
Policy is evaluated and applied against imcoming requests.

● Set Transition
Policy is applied based on changes in Set membership and independent of the request.

Disabled
Select this item to create the policy rule in an initially disabled state.

□ Policy is disabled



Create Management Policy Rule

Transition Set. *

Select the set for which this transition policy is defined.

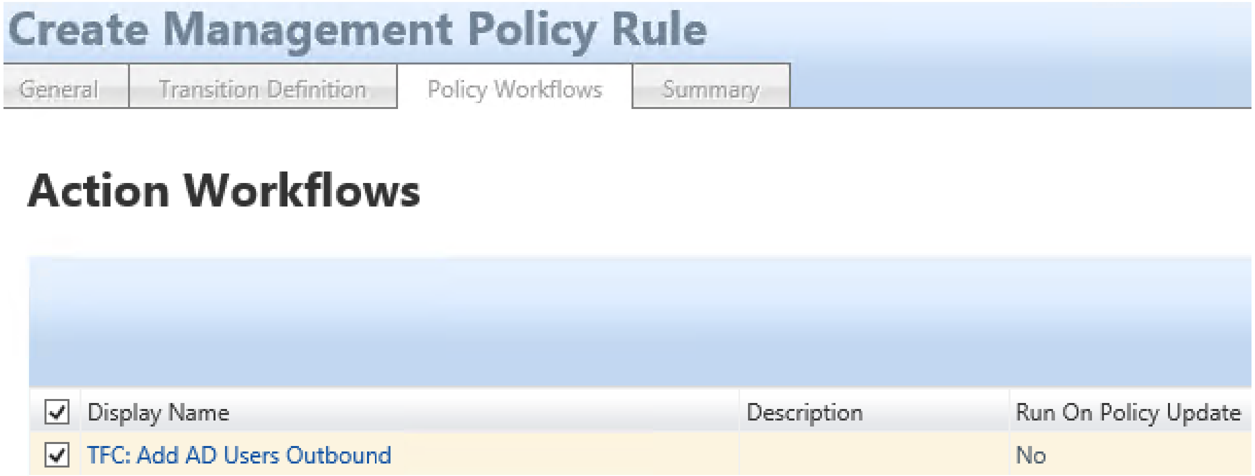
TFC: AD Users

Transition Type. *

Select the type of transition for this policy rule.

● Transition In
Apply policy when resource becomes a member of the transition set.

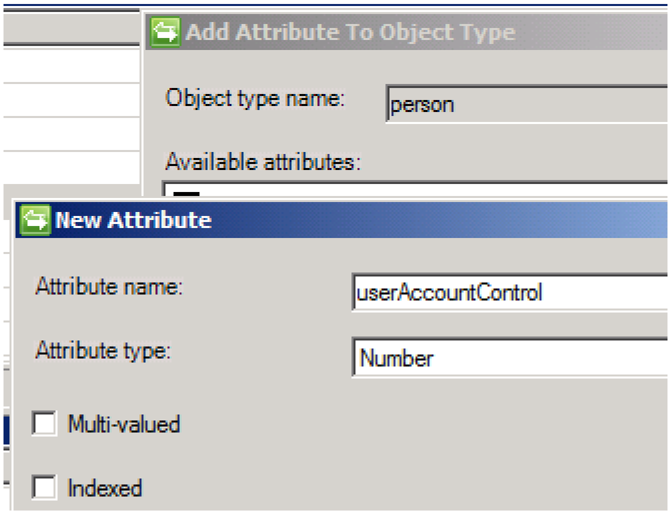
○ Transition Out
Apply policy when resource leaves the transition set. This includes deletion of the transition set.



Create Management Policy Rule

Action Workflows

☑	Display Name	Description	Run On Policy Update
☑	TFC: Add AD Users Outbound		No



Add Attribute To Object Type

Object type name: person

Available attributes:

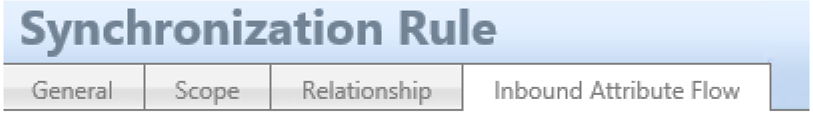
New Attribute

Attribute name: userAccountControl

Attribute type: Number

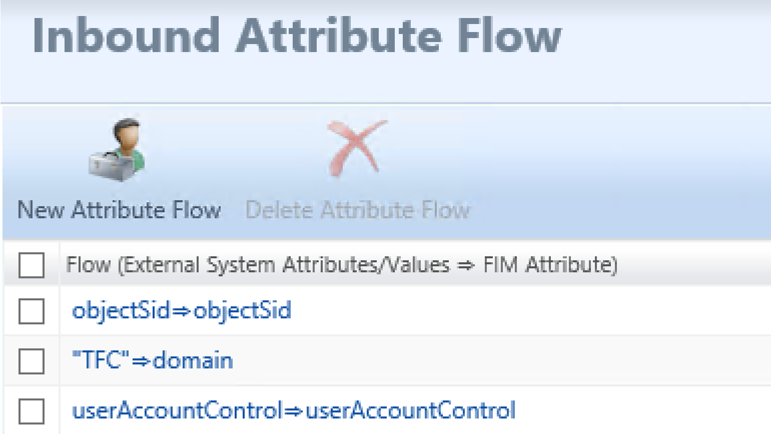
□ Multi-valued

□ Indexed



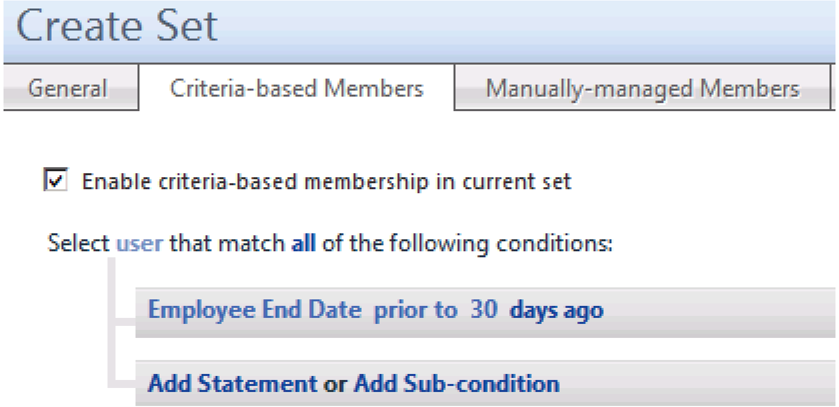
Synchronization Rule

General | Scope | Relationship | Inbound Attribute Flow



Inbound Attribute Flow

□	Flow (External System Attributes/Values ⇒ FIM Attribute)
□	objectSid⇒objectSid
□	"TFC"⇒domain
□	userAccountControl⇒userAccountControl



Create Set

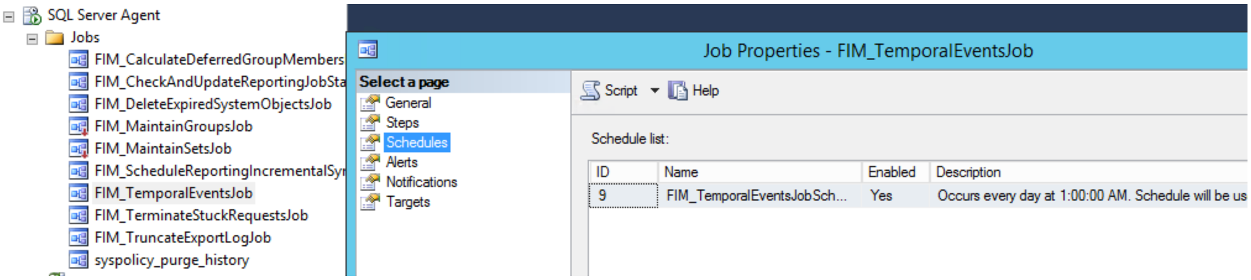
General | Criteria-based Members | Manually-managed Members

☑ Enable criteria-based membership in current set

Select user that match all of the following conditions:

Employee End Date prior to 30 days ago

Add Statement or Add Sub-condition

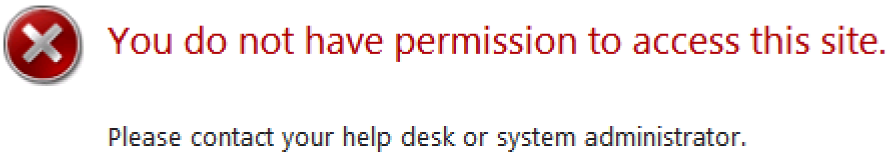


SQL Server Agent
- Jobs
  - FIM_CalculateDeferredGroupMembers
  - FIM_CheckAndUpdateReportingJobSta
  - FIM_DeleteExpiredSystemObjectsJob
  - FIM_MaintainGroupsJob
  - FIM_MaintainSetsJob
  - FIM_ScheduleReportingIncrementalSy
  - FIM_TemporalEventsJob
  - FIM_TerminateStuckRequestsJob
  - FIM_TruncateExportLogJob
  - syspolicy_purge_history

Job Properties - FIM_TemporalEventsJob

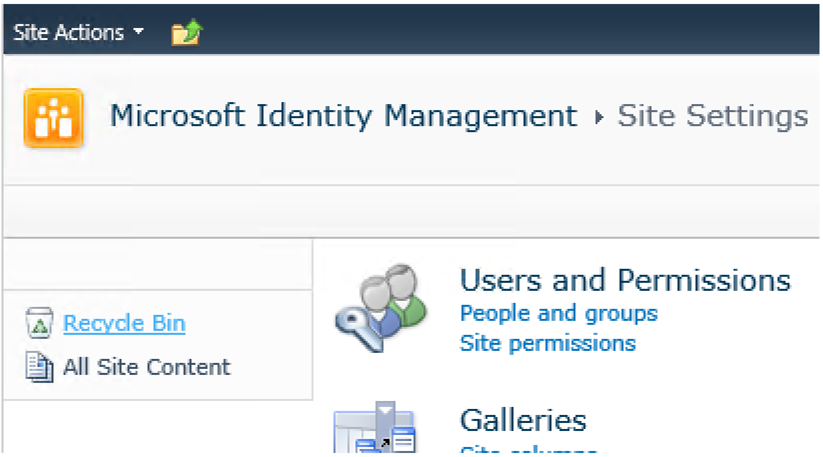
Schedule list:

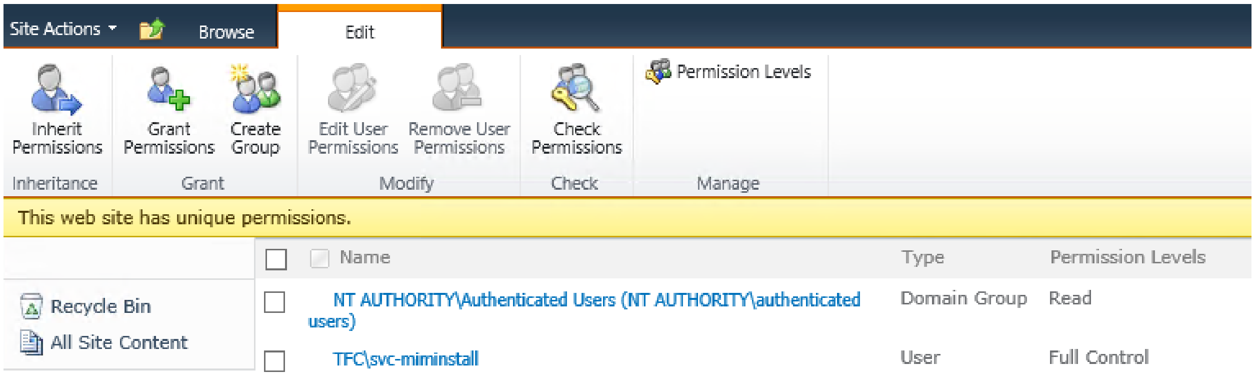
ID	Name	Enabled	Description
9	FIM_TemporalEventsJobSch...	Yes	Occurs every day at 1:00:00 AM. Schedule will be us



You do not have permission to access this site.

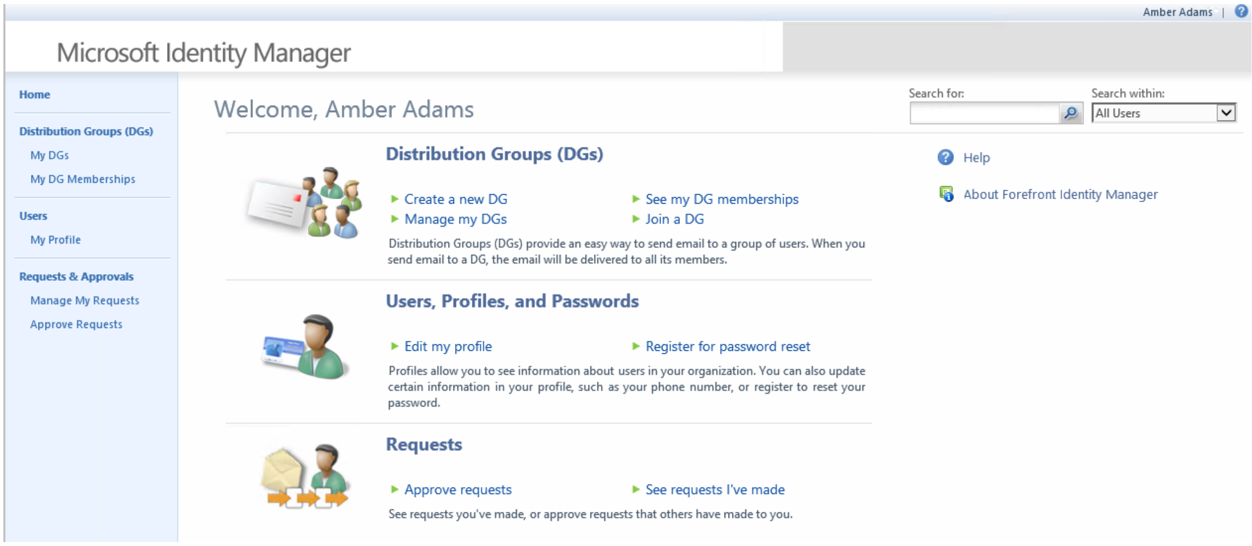
Please contact your help desk or system administrator.





This web site has unique permissions.

□	Name	Type	Permission Levels
□	NT AUTHORITY\Authenticated Users (NT AUTHORITY\authenticated users)	Domain Group	Read
□	TFC\svc-miminstall	User	Full Control



Welcome, Amber Adams

Distribution Groups (DGs)

- Create a new DG
- Manage my DGs
- See my DG memberships
- Join a DG

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.

Users, Profiles, and Passwords

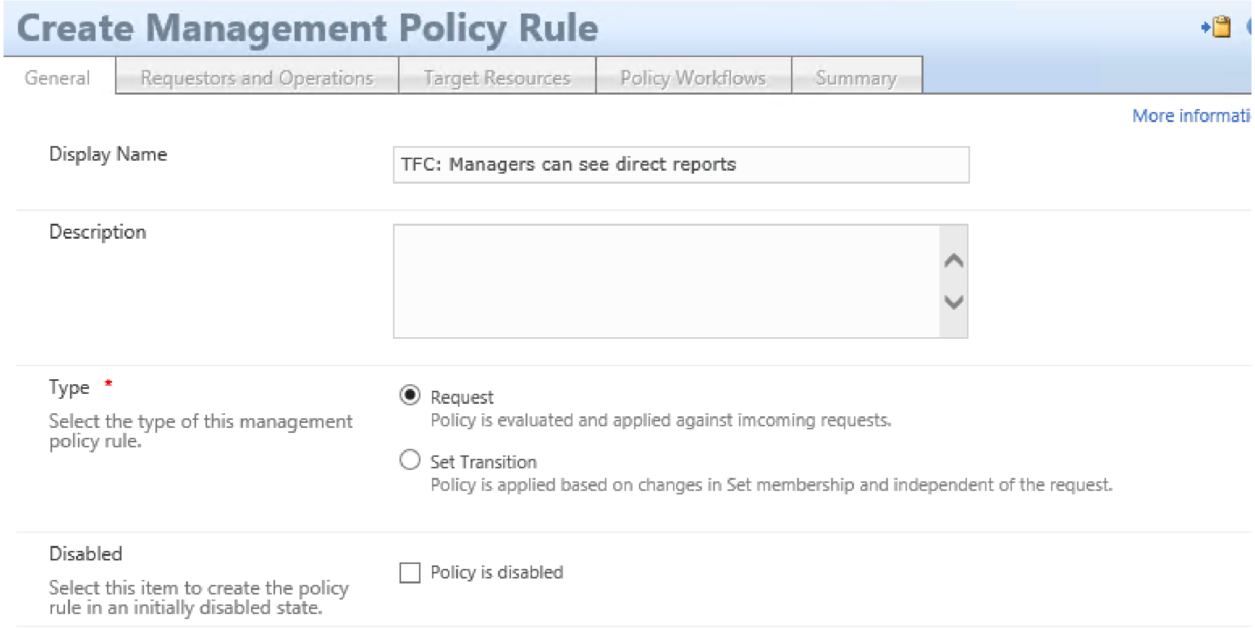
- Edit my profile
- Register for password reset

Profiles allow you to see information about users in your organization. You can also update certain information in your profile, such as your phone number, or register to reset your password.

Requests

- Approve requests
- See requests I've made

See requests you've made, or approve requests that others have made to you.



Create Management Policy Rule

Display Name: TFC: Managers can see direct reports

Description:

Type *

Select the type of this management policy rule.

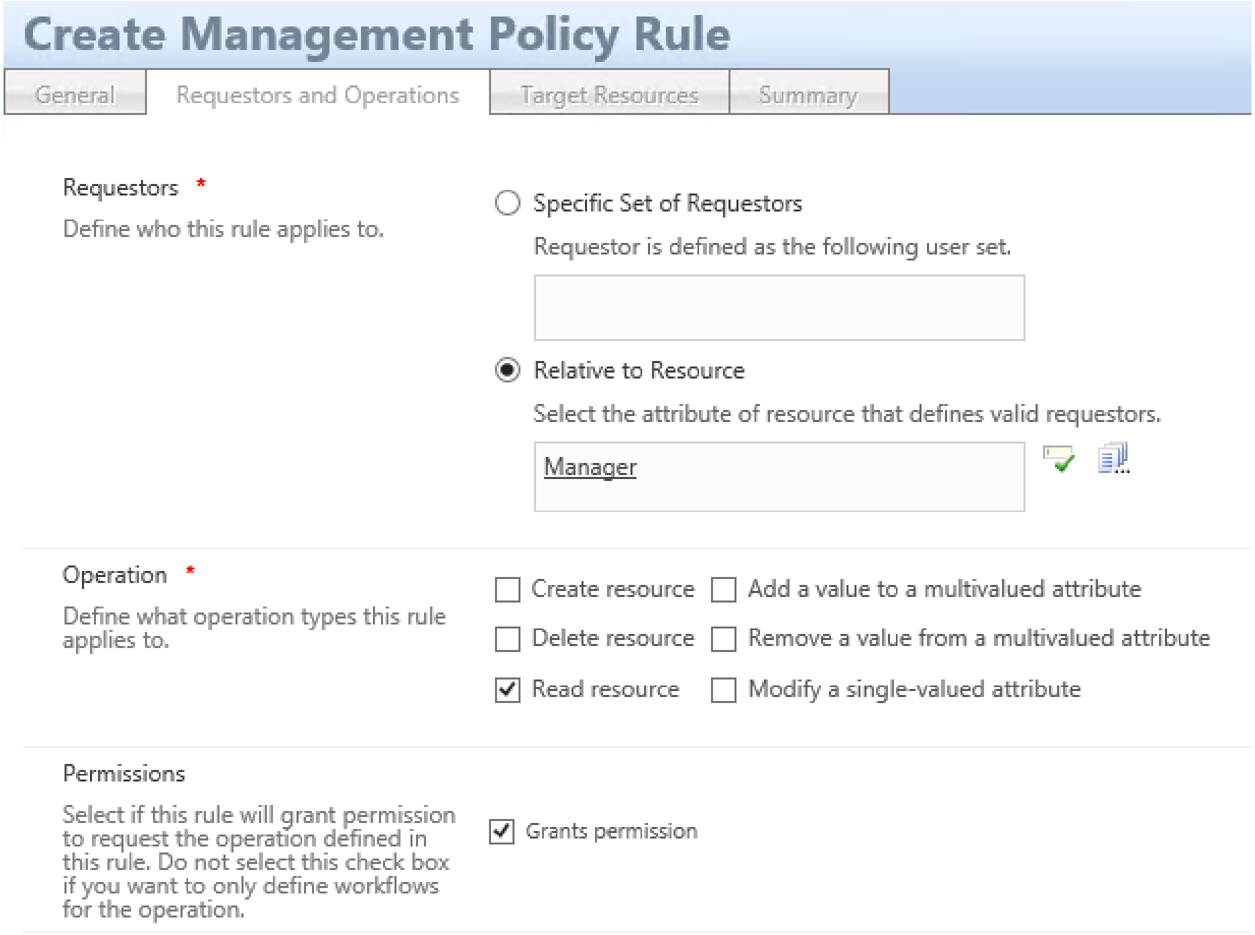
● Request
Policy is evaluated and applied against imcoming requests.

○ Set Transition
Policy is applied based on changes in Set membership and independent of the request.

Disabled

Select this item to create the policy rule in an initially disabled state.

□ Policy is disabled



Create Management Policy Rule

Requestors *

Define who this rule applies to.

○ Specific Set of Requestors
Requestor is defined as the following user set.

● Relative to Resource
Select the attribute of resource that defines valid requestors.

Manager

Operation *

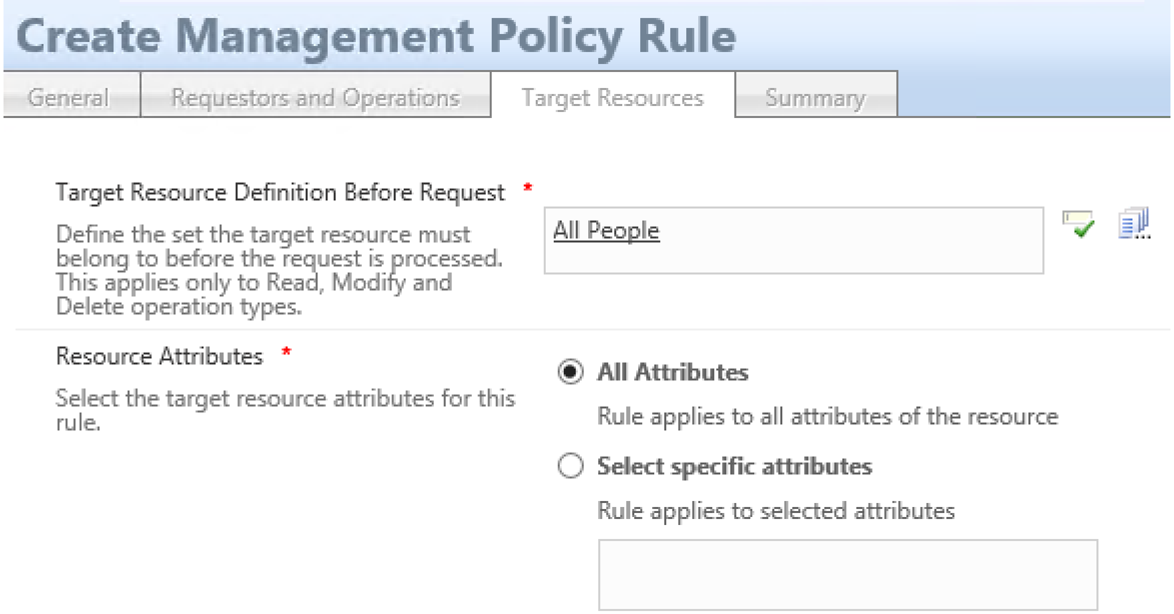
Define what operation types this rule applies to.

□ 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



Create Management Policy Rule

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 People

Resource Attributes *

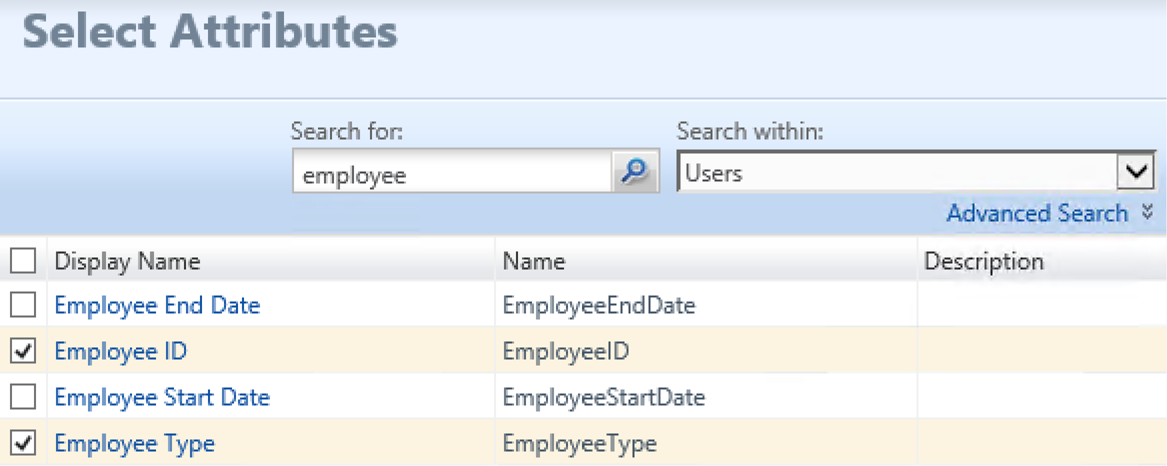
Select the target resource attributes for this rule.

● **All Attributes**

Rule applies to all attributes of the resource

○ **Select specific attributes**

Rule applies to selected attributes

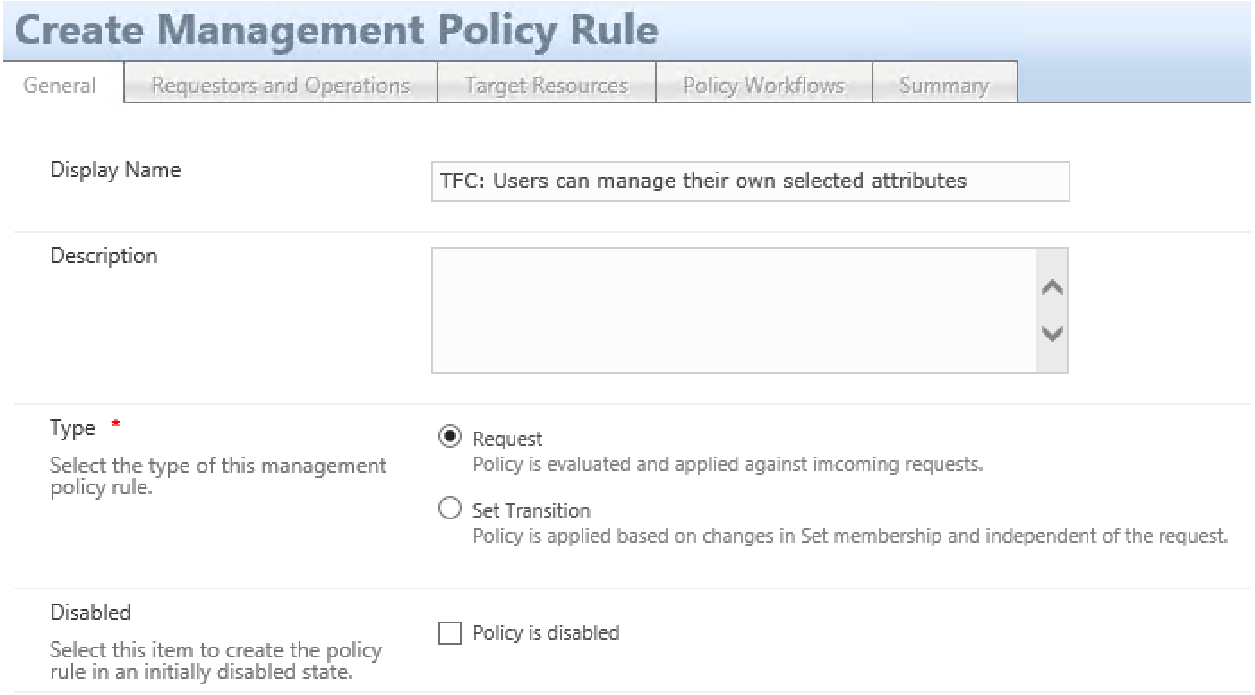


Select Attributes

Search for: employee

Search within: Users

□	Display Name	Name	Description
□	Employee End Date	EmployeeEndDate	
☑	Employee ID	EmployeeID	
□	Employee Start Date	EmployeeStartDate	
☑	Employee Type	EmployeeType	



Create Management Policy Rule

Display Name: TFC: Users can manage their own selected attributes

Description

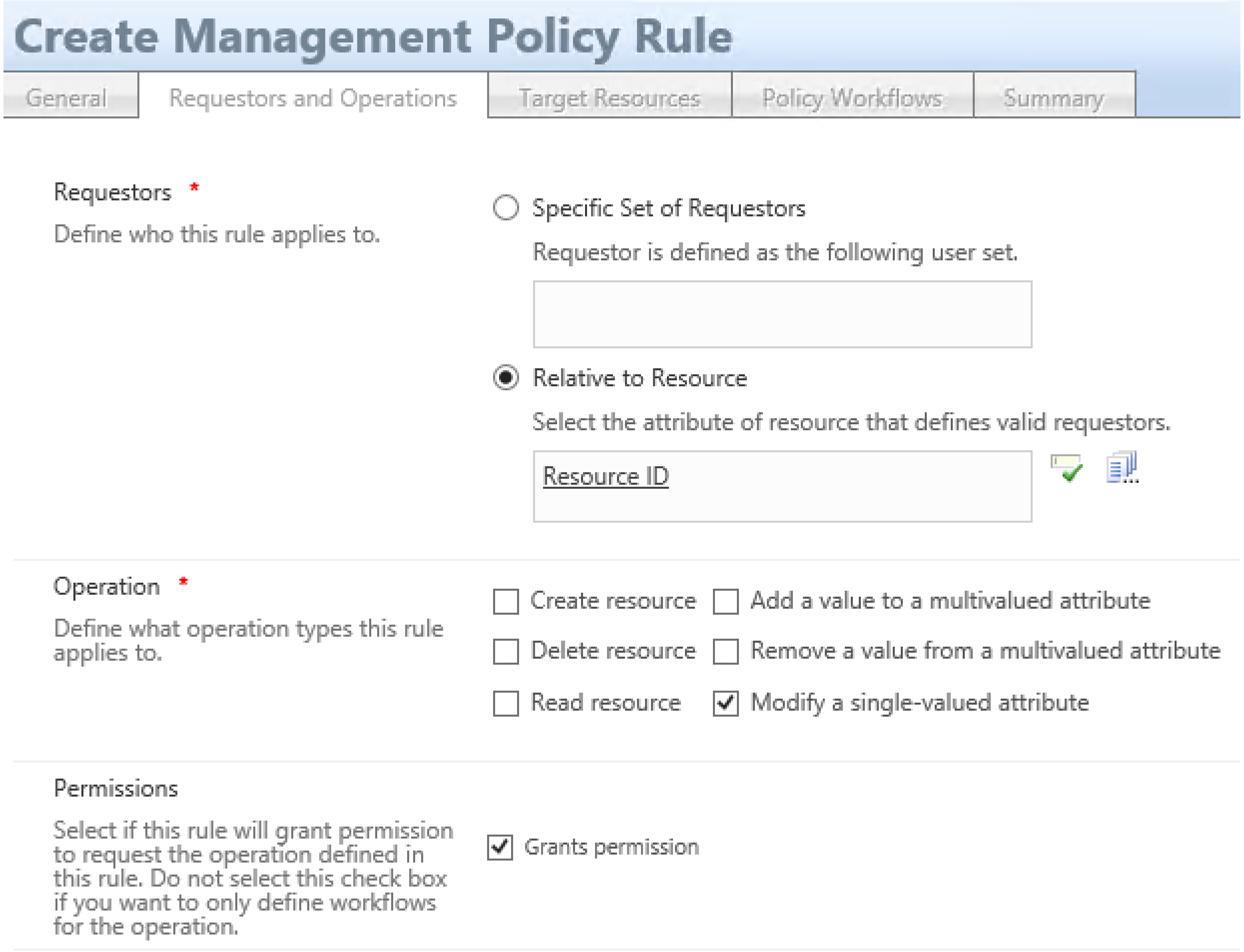
Type *
Select the type of this management policy rule.

● Request
Policy is evaluated and applied against imcoming requests.

○ Set Transition
Policy is applied based on changes in Set membership and independent of the request.

Disabled
Select this item to create the policy rule in an initially disabled state.

□ Policy is disabled



Create Management Policy Rule

Requestors *
Define who this rule applies to.

○ Specific Set of Requestors
Requestor is defined as the following user set.

● Relative to Resource
Select the attribute of resource that defines valid requestors.

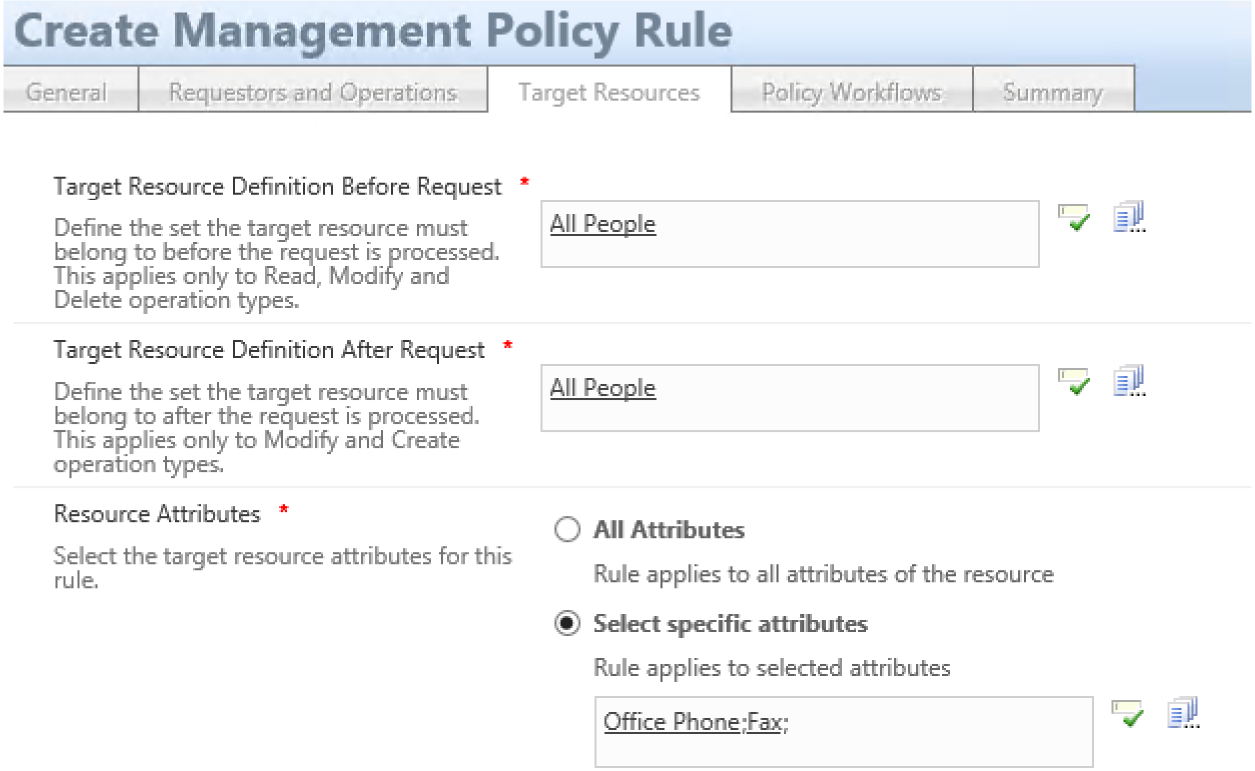
Resource ID

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



Create Management Policy Rule

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 People

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 People

Resource Attributes *

Select the target resource attributes for this rule.

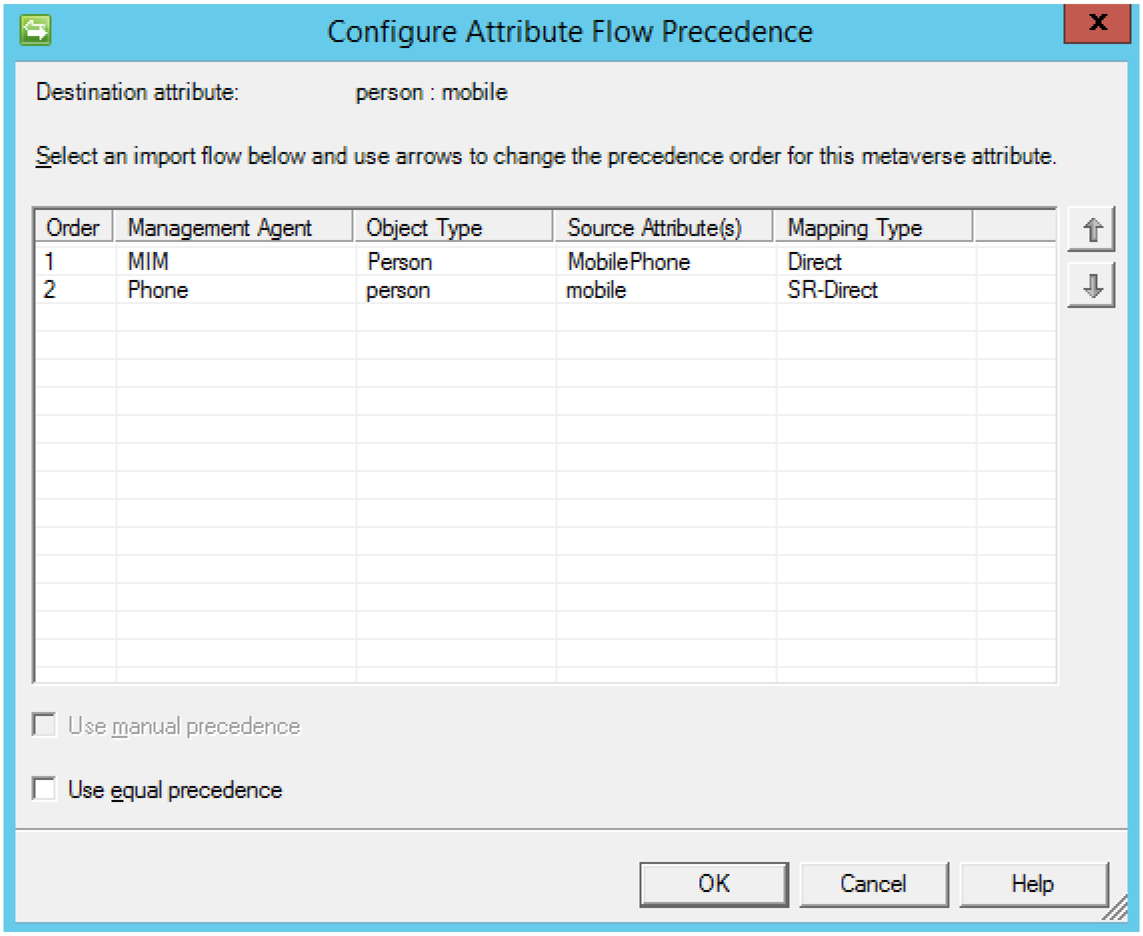
○ All Attributes

Rule applies to all attributes of the resource

● Select specific attributes

Rule applies to selected attributes

Office Phone;Fax;



Configure Attribute Flow Precedence

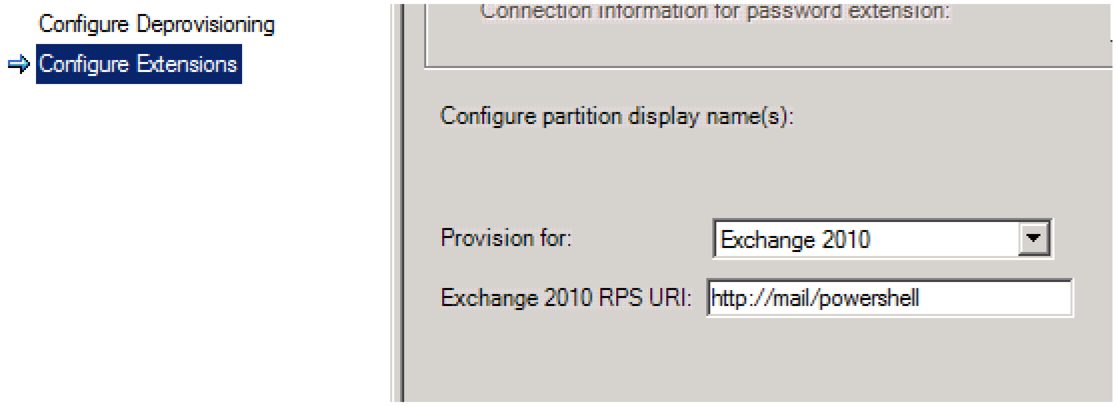
Destination attribute: person : mobile

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	MobilePhone	Direct
2	Phone	person	mobile	SR-Direct

□ Use manual precedence

□ Use equal precedence

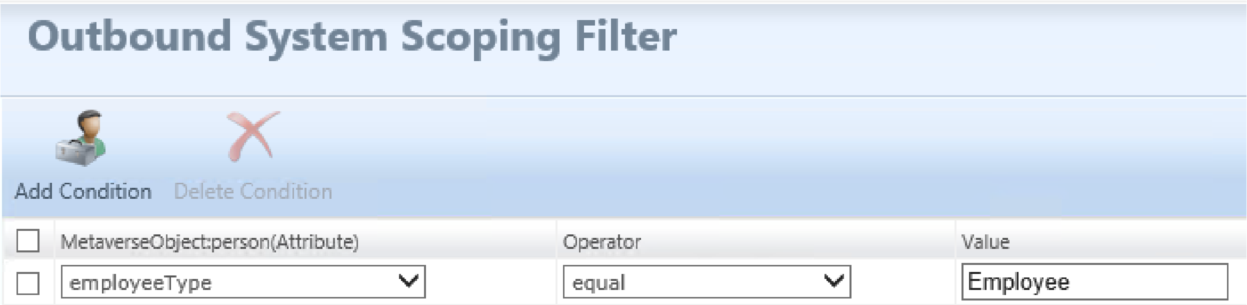


Connection information for password extension:

Configure partition display name(s):

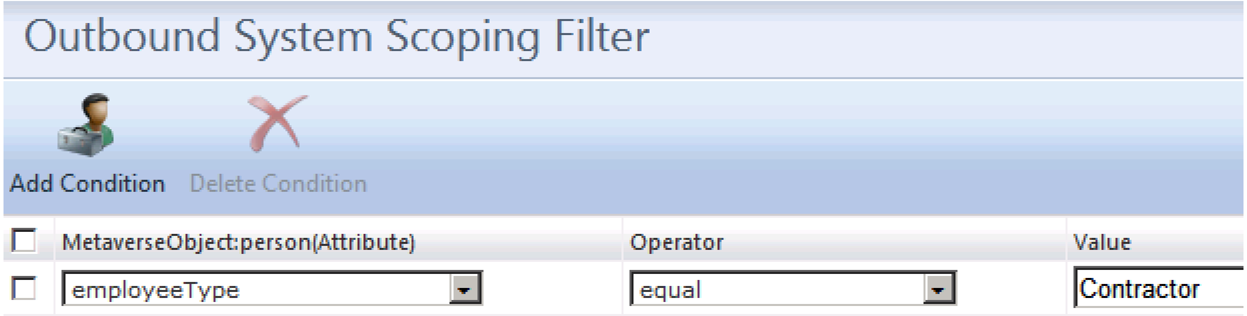
Provision for: Exchange 2010

Exchange 2010 RPS URI: http://mail/powershell



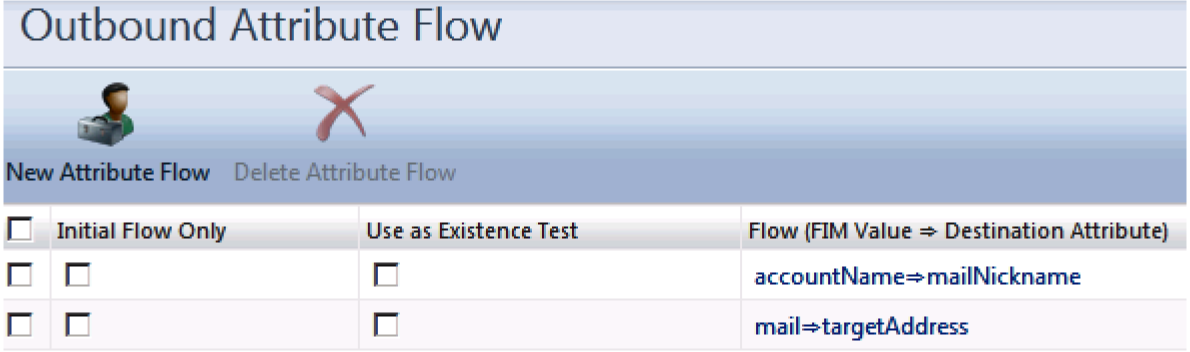
Outbound System Scoping Filter

□	MetaverseObject:person(Attribute)	Operator	Value
□	employeeType	equal	Employee



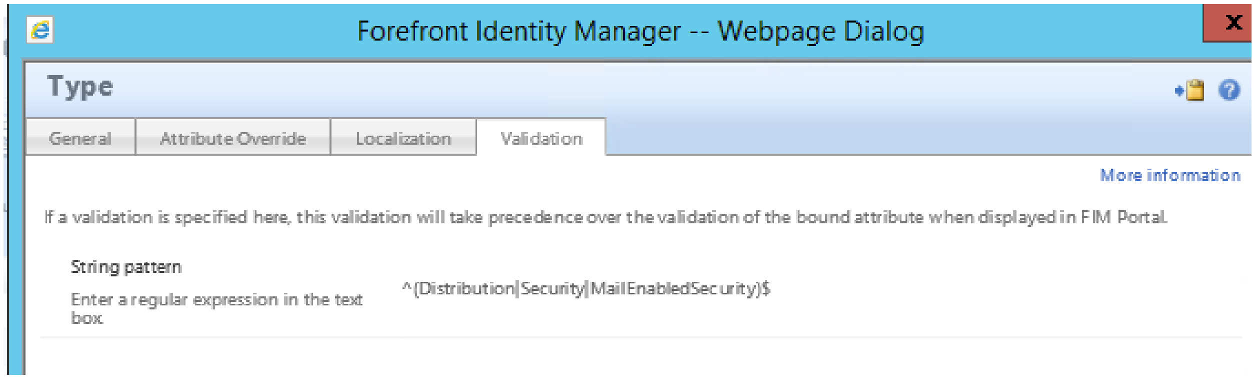
Outbound System Scoping Filter

□	MetaverseObject:person(Attribute)	Operator	Value
□	employeeType	equal	Contractor



Outbound Attribute Flow

□	Initial Flow Only	Use as Existence Test	Flow (FIM Value ⇒ Destination Attribute)
□	□	□	accountName⇒mailNickname
□	□	□	mail⇒targetAddress



Forefront Identity Manager -- Webpage Dialog

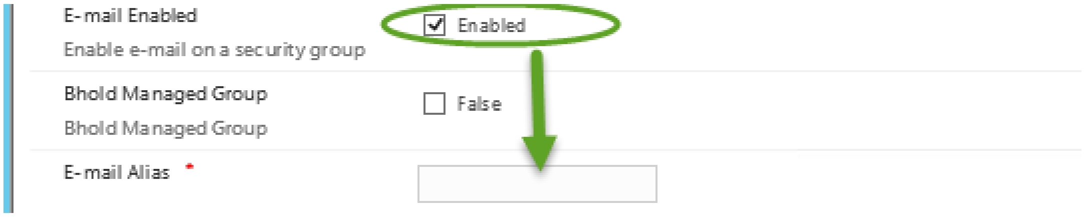
Type

If a validation is specified here, this validation will take precedence over the validation of the bound attribute when displayed in FIM Portal.

String pattern

Enter a regular expression in the text box

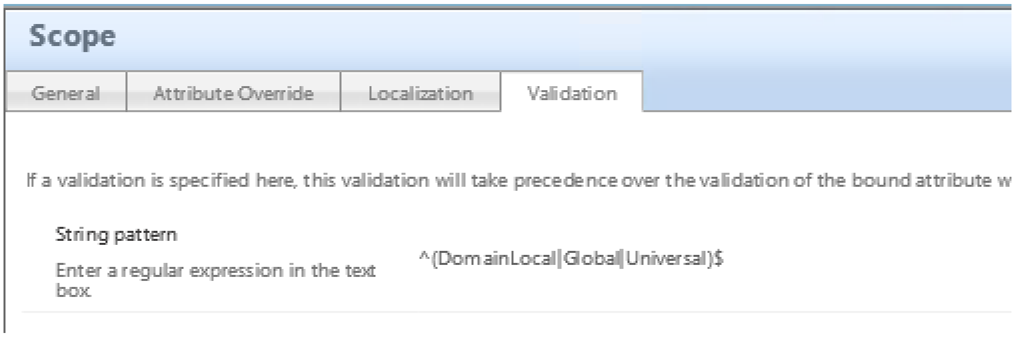
^(Distribution|Security|MailEnabledSecurity)$



E-mail Enabled
Enable e-mail on a security group
☑ Enabled

Bhold Managed Group
Bhold Managed Group
☐ False

E-mail Alias *



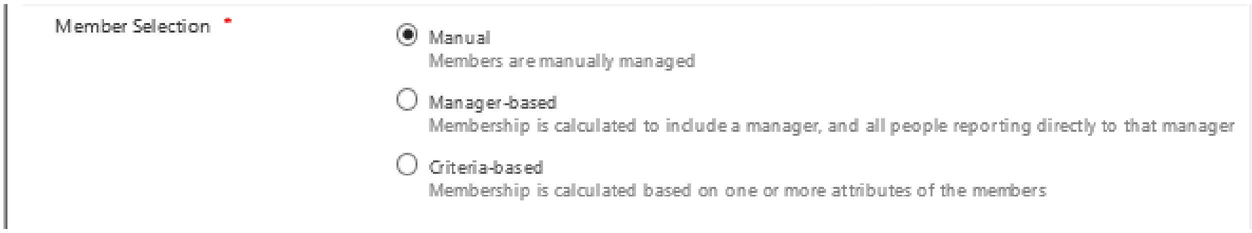
Scope

If a validation is specified here, this validation will take precedence over the validation of the bound attribute w

String pattern

Enter a regular expression in the text box

^(DomainLocal|Global|Universal)$

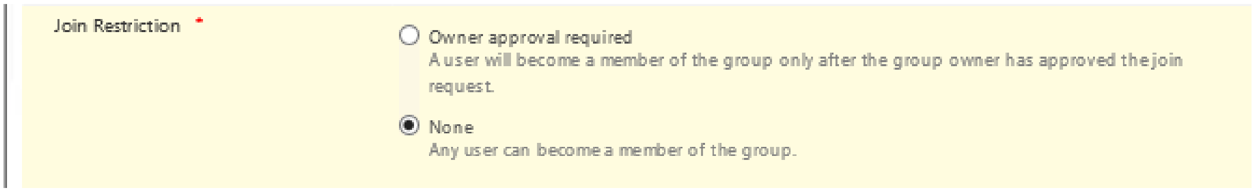


Member Selection *

● Manual
Members are manually managed

○ Manager-based
Membership is calculated to include a manager, and all people reporting directly to that manager

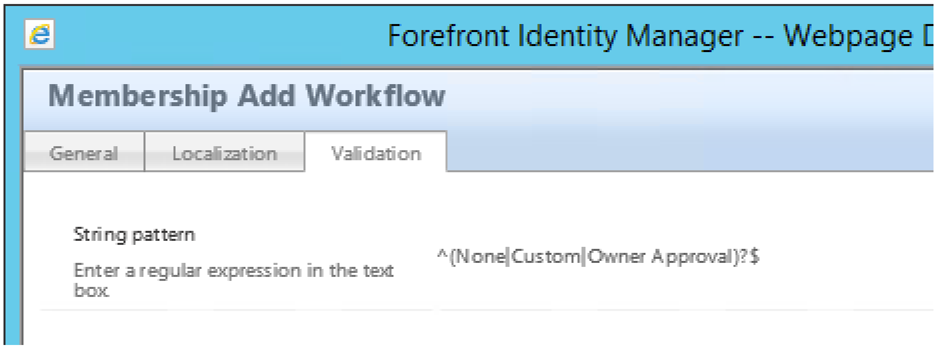
○ Criteria-based
Membership is calculated based on one or more attributes of the members



Join Restriction *

○ Owner approval required
A user will become a member of the group only after the group owner has approved the join request.

● None
Any user can become a member of the group.

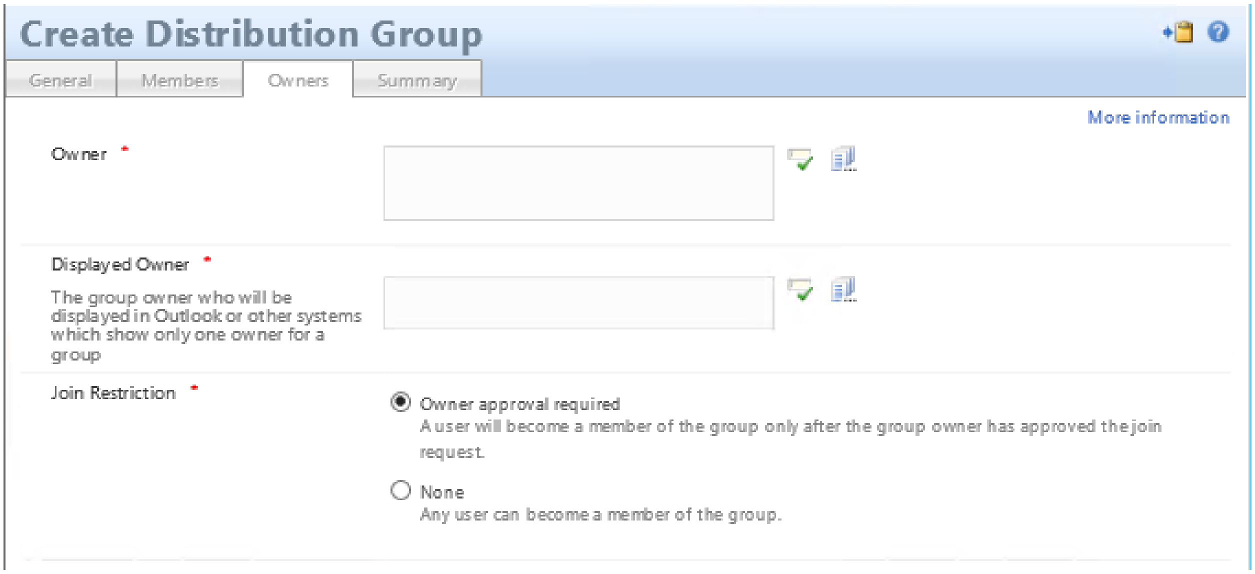


Membership Add Workflow

String pattern

Enter a regular expression in the text box.

^(None|Custom|Owner Approval)?$



Create Distribution Group

Owner *

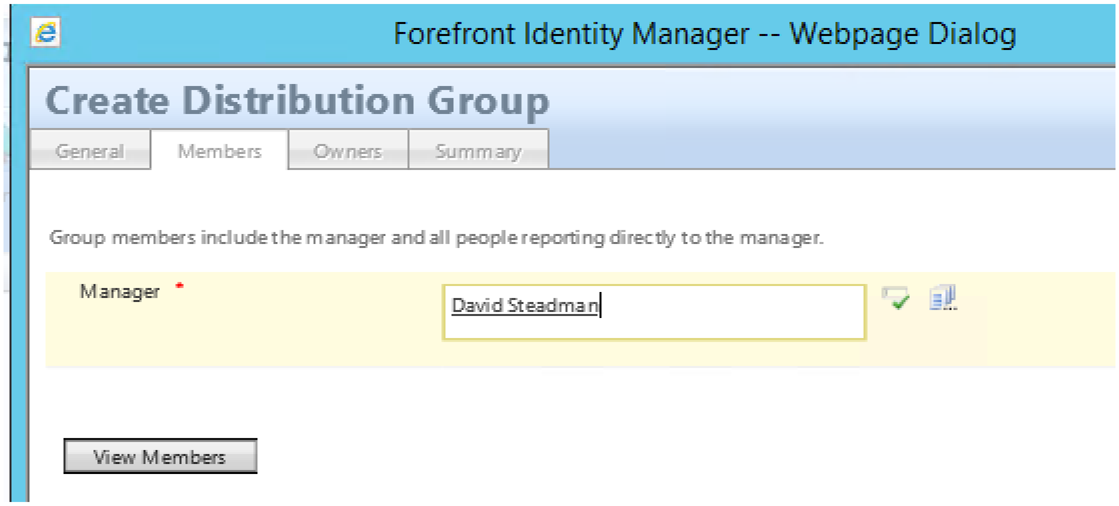
Displayed Owner *

The group owner who will be displayed in Outlook or other systems which show only one owner for a group

Join Restriction *

● Owner approval required
A user will become a member of the group only after the group owner has approved the join request.

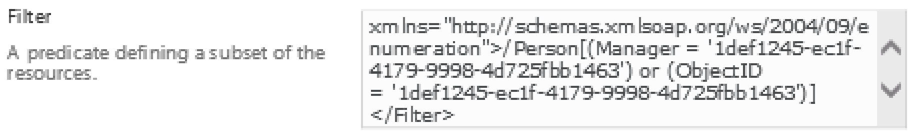
○ None
Any user can become a member of the group.



Create Distribution Group

Group members include the manager and all people reporting directly to the manager.

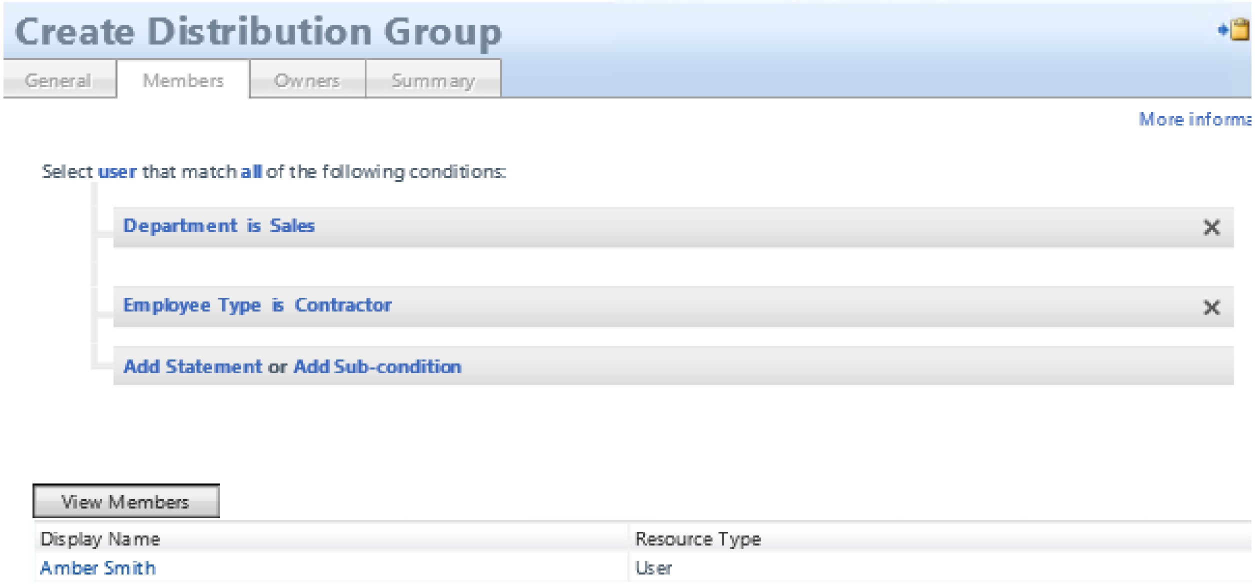
Manager * David Steadman



Filter

A predicate defining a subset of the resources.

```
xmlns="http://schemas.xmlsoap.org/ws/2004/09/enumeration">/Person[(Manager = '1def1245-ec1f-4179-9998-4d725fbb1463') or (ObjectID
= '1def1245-ec1f-4179-9998-4d725fbb1463')]
</Filter>
```

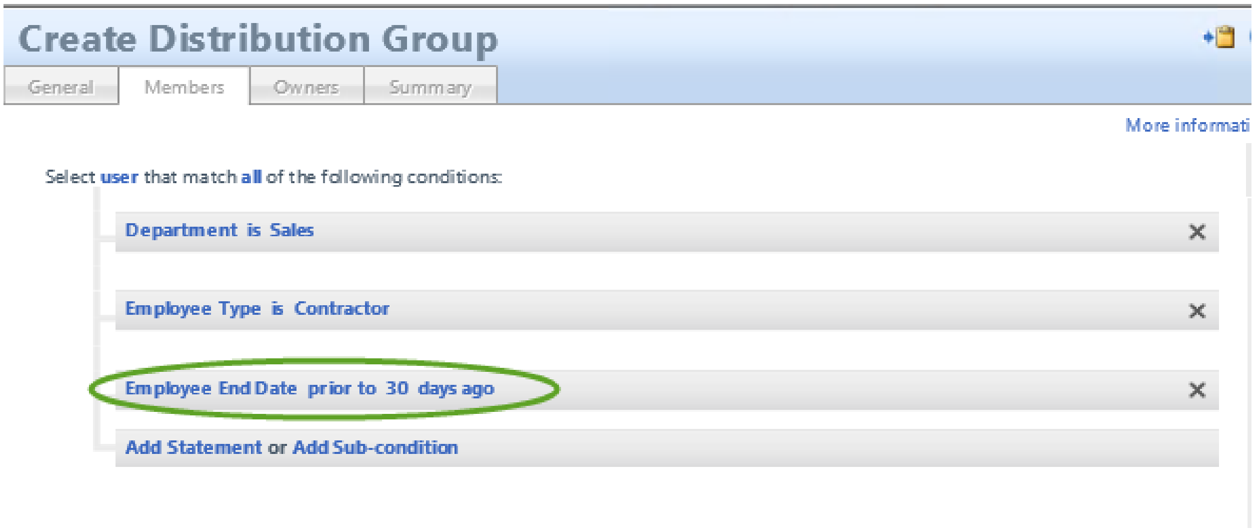


Create Distribution Group

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

- **Department is Sales** ✕
- **Employee Type is Contractor** ✕
- **Add Statement** or **Add Sub-condition**

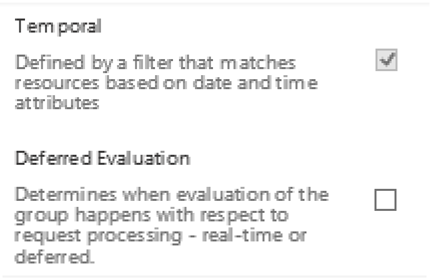
Display Name	Resource Type
Amber Smith	User



Create Distribution Group

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

- **Department is Sales** ✕
- **Employee Type is Contractor** ✕
- **Employee End Date prior to 30 days ago** ✕
- **Add Statement** or **Add Sub-condition**

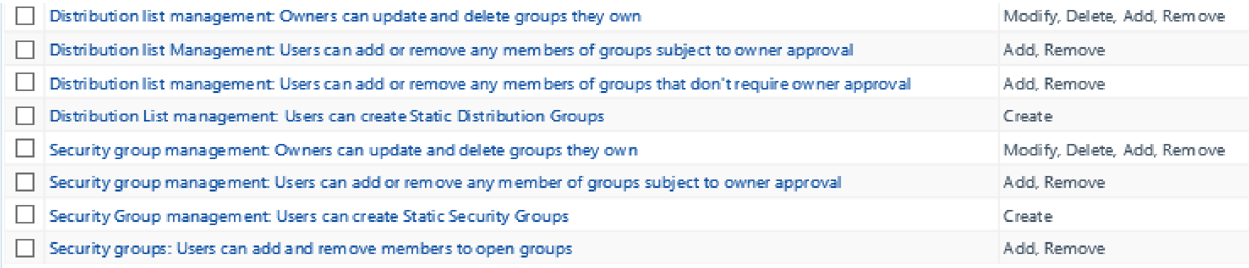


Temporal

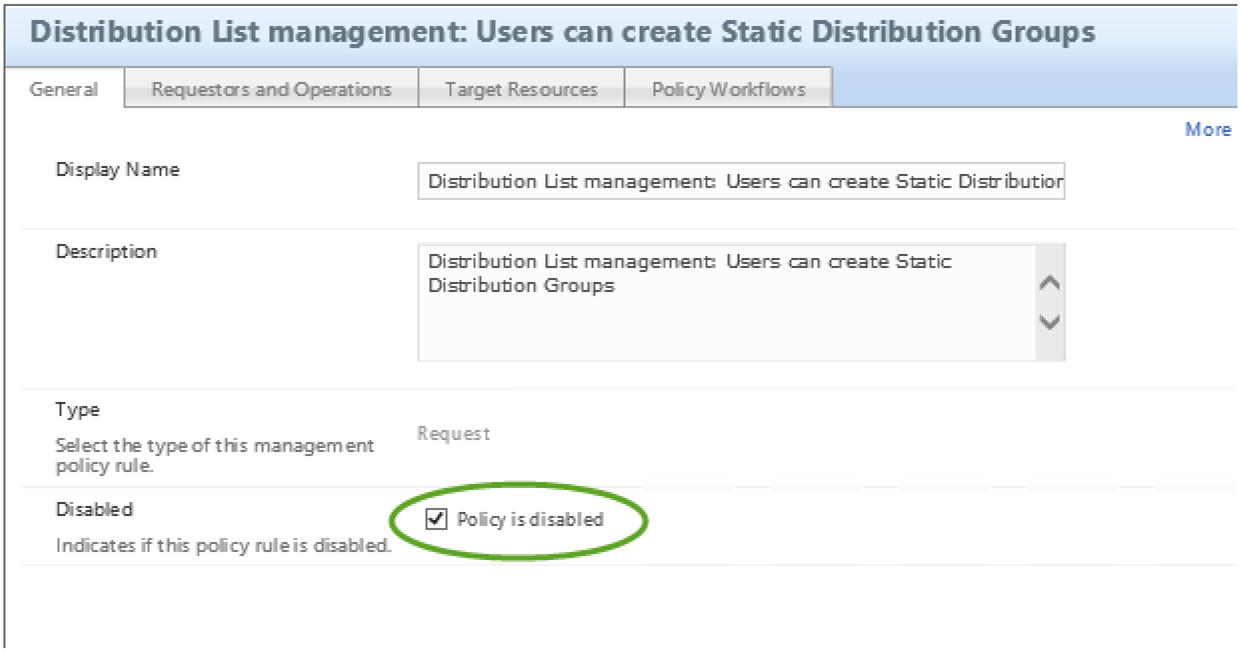
Defined by a filter that matches resources based on date and time attributes ☑

Deferred Evaluation

Determines when evaluation of the group happens with respect to request processing - real-time or deferred. □



□	Distribution list management: Owners can update and delete groups they own	Modify, Delete, Add, Remove
□	Distribution list Management: Users can add or remove any members of groups subject to owner approval	Add, Remove
□	Distribution list management: Users can add or remove any members of groups that don't require owner approval	Add, Remove
□	Distribution List management: Users can create Static Distribution Groups	Create
□	Security group management: Owners can update and delete groups they own	Modify, Delete, Add, Remove
□	Security group management: Users can add or remove any member of groups subject to owner approval	Add, Remove
□	Security Group management: Users can create Static Security Groups	Create
□	Security groups: Users can add and remove members to open groups	Add, Remove



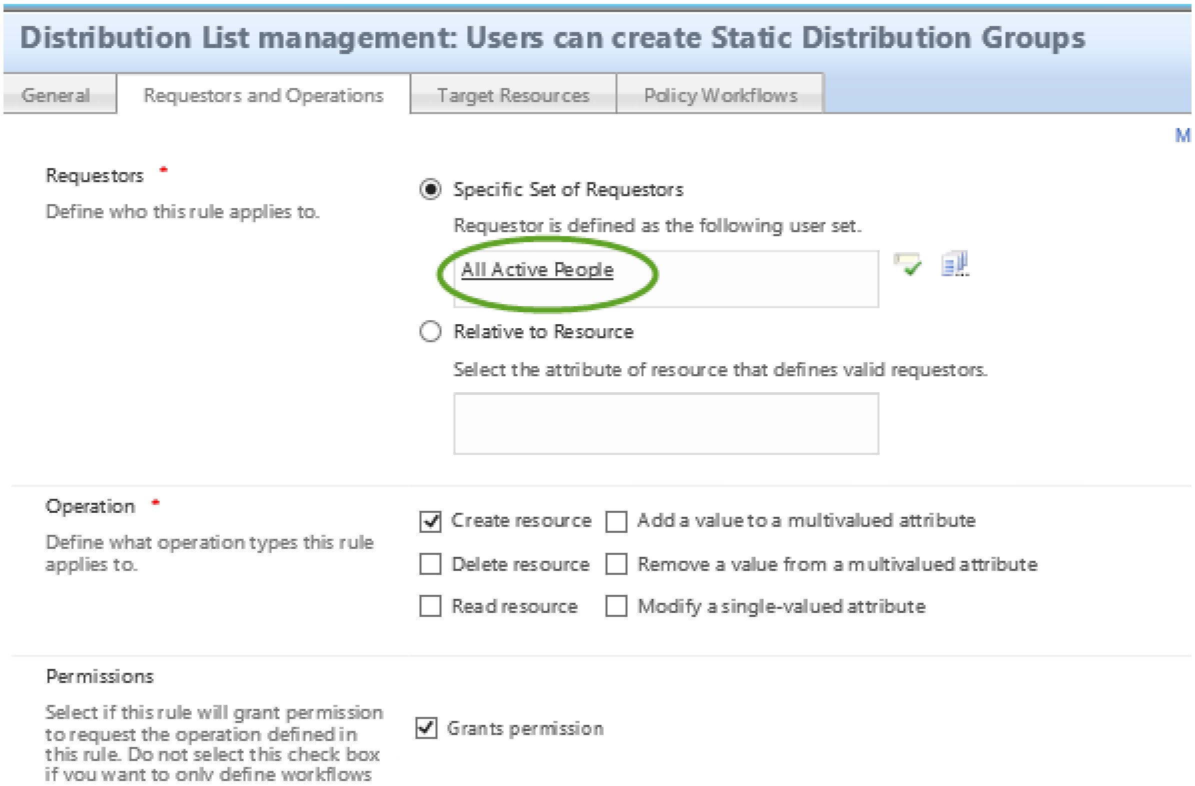
Distribution List management: Users can create Static Distribution Groups

Display Name: Distribution List management: Users can create Static Distributior

Description: Distribution List management: Users can create Static Distribution Groups

Type
Select the type of this management policy rule.
Request

Disabled
Indicates if this policy rule is disabled.
☑ Policy is disabled



Distribution List management: Users can create Static Distribution Groups

Requestors *

Define who this rule applies to.

● Specific Set of Requestors

Requestor is defined as the following user set.

All Active People

○ Relative to Resource

Select the attribute of resource that defines valid requestors.

Operation *

Define what operation types this rule applies to.

☑ Create resource ☐ Add a value to a multivalued attribute

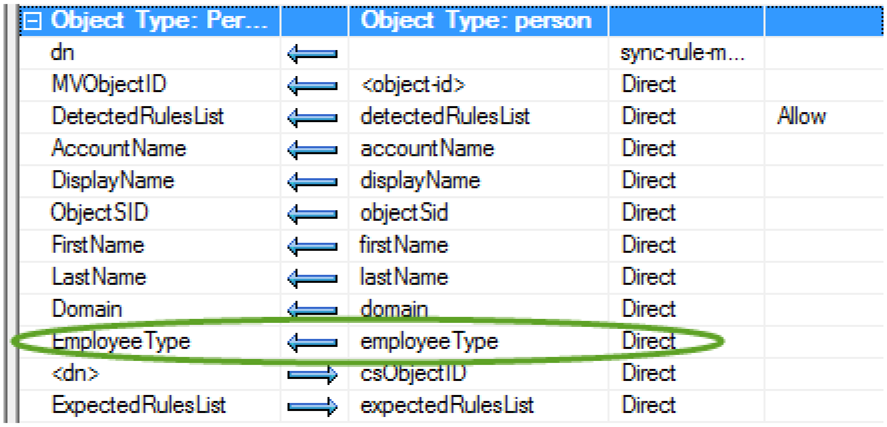
☐ Delete resource ☐ Remove a value from a multivalued attribute

☐ Read resource ☐ Modify a single-valued attribute

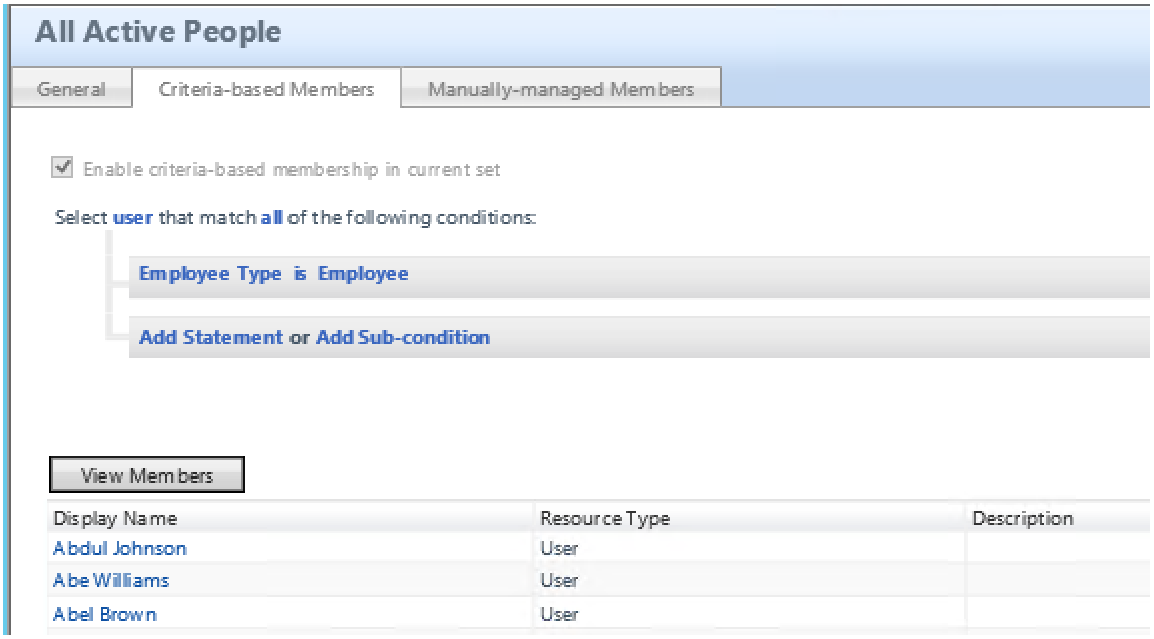
Permissions

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

☑ Grants permission



⊟ Object Type: Per...		Object Type: person		
dn	⟵		sync-rule-m...	
MVObjectID	⟵	<object-id>	Direct	
DetectedRulesList	⟵	detectedRulesList	Direct	Allow
AccountName	⟵	accountName	Direct	
DisplayName	⟵	displayName	Direct	
ObjectSID	⟵	objectSid	Direct	
FirstName	⟵	firstName	Direct	
LastName	⟵	lastName	Direct	
Domain	⟵	domain	Direct	
EmployeeType	⟵	employeeType	Direct	
<dn>	⟶	csObjectID	Direct	
ExpectedRulesList	⟶	expectedRulesList	Direct	



All Active People

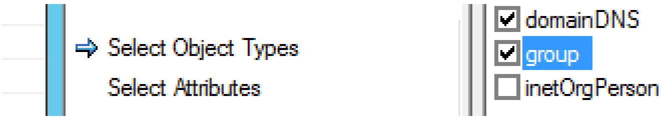
☑ Enable criteria-based membership in current set

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

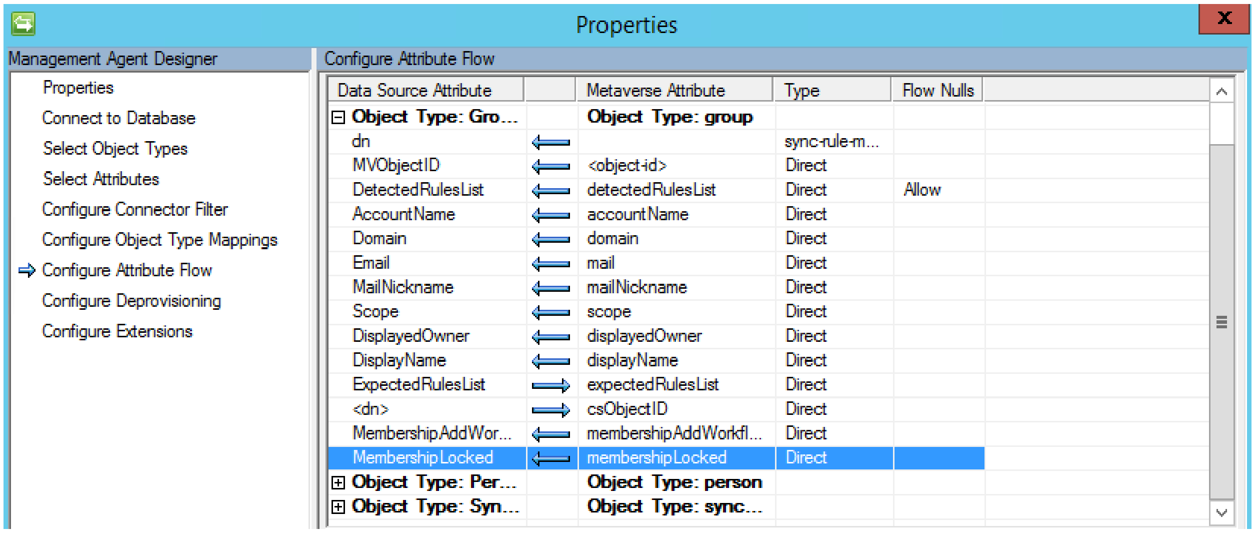
Employee Type is Employee

Add Statement or Add Sub-condition

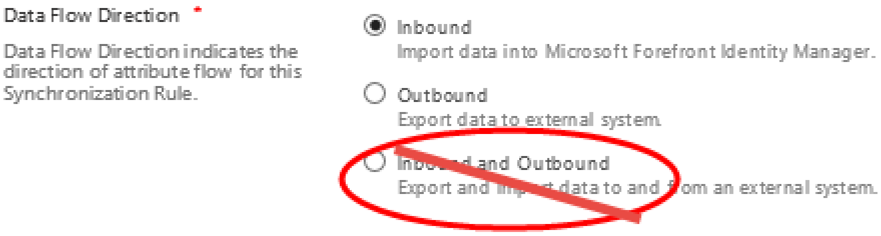
Display Name	Resource Type	Description
Abdul Johnson	User	
Abe Williams	User	
Abel Brown	User	



☑ domainDNS
☑ group
□ inetOrgPerson



Data Source Attribute		Metaverse Attribute	Type	Flow Nulls
⊟ **Object Type: Gro...**		**Object Type: group**		
dn	⟵		sync-rule-m...	
MVObjectID	⟵	<object-id>	Direct	
DetectedRulesList	⟵	detectedRulesList	Direct	Allow
AccountName	⟵	accountName	Direct	
Domain	⟵	domain	Direct	
Email	⟵	mail	Direct	
MailNickname	⟵	mailNickname	Direct	
Scope	⟵	scope	Direct	
DisplayedOwner	⟵	displayedOwner	Direct	
DisplayName	⟵	displayName	Direct	
ExpectedRulesList	⟶	expectedRulesList	Direct	
<dn>	⟶	csObjectID	Direct	
MembershipAddWor...	⟵	membershipAddWorkfl...	Direct	
MembershipLocked	⟵	membershipLocked	Direct	
⊞ **Object Type: Per...**		**Object Type: person**		
⊞ **Object Type: Syn...**		**Object Type: sync...**		



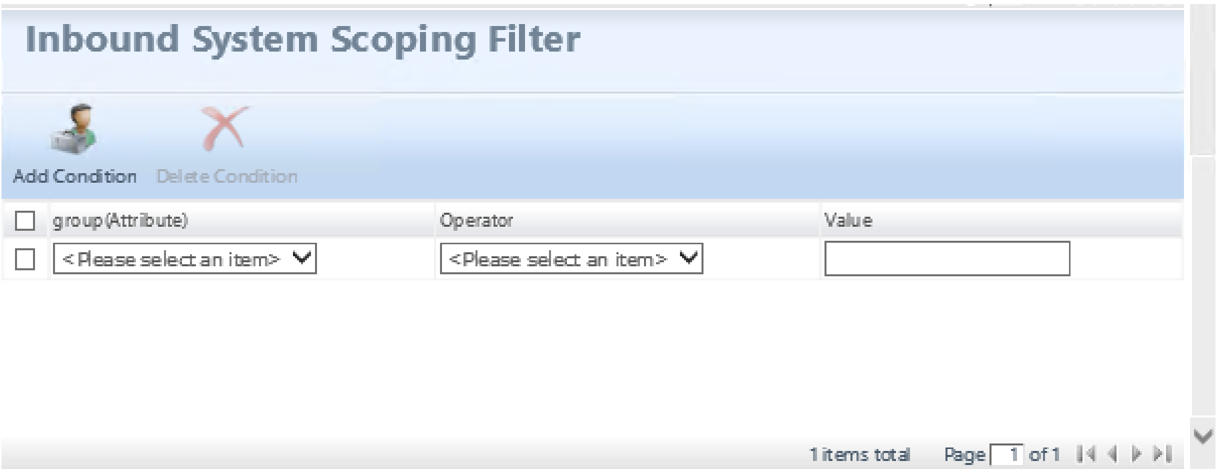
Data Flow Direction *

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

● Inbound
Import data into Microsoft Forefront Identity Manager.

○ Outbound
Export data to external system.

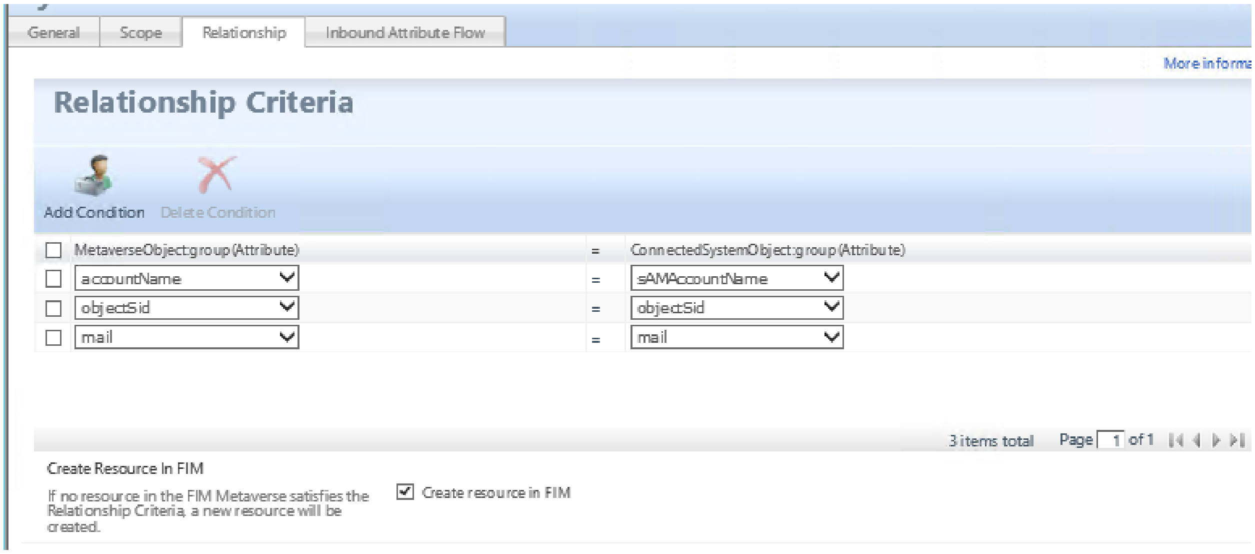
○ Inbound and Outbound
Export and import data to and from an external system.



Inbound System Scoping Filter

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

1 items total Page 1 of 1



Relationship Criteria

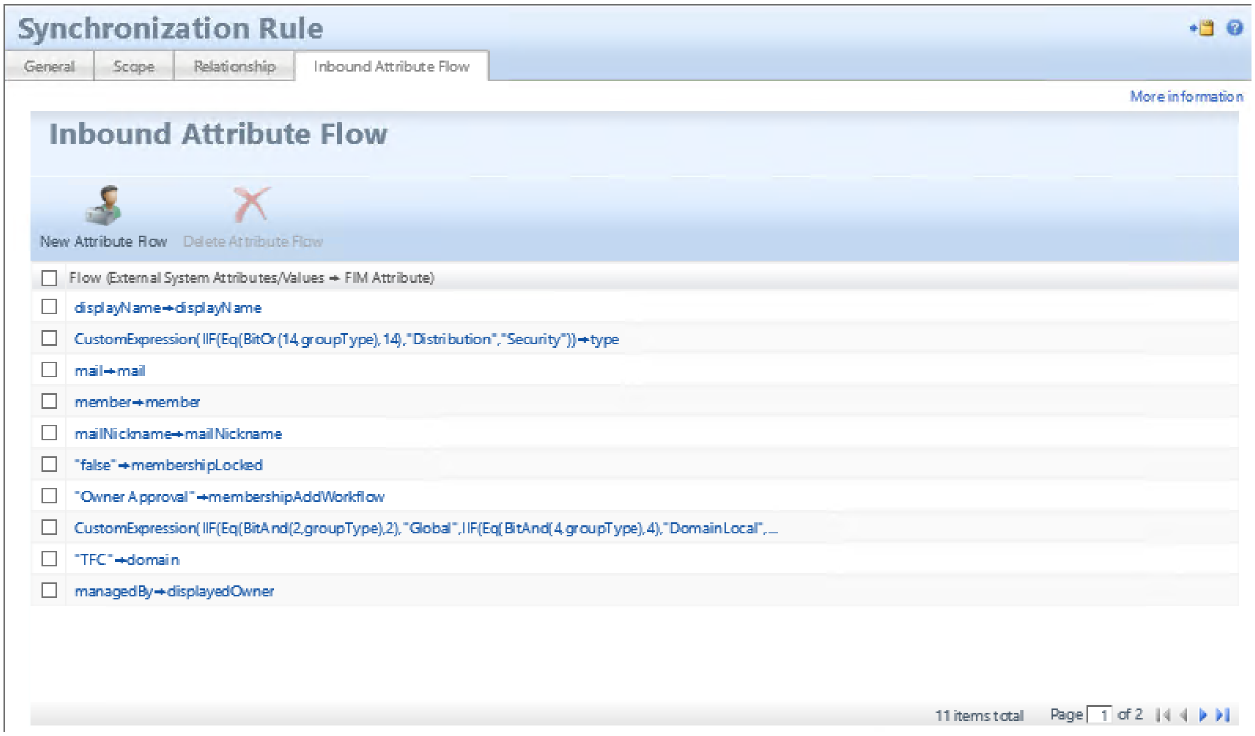
□	MetaverseObject:group (Attribute)	=	ConnectedSystemObject:group (Attribute)
□	accountName	=	sAMAccountName
□	objectSid	=	objectSid
□	mail	=	mail

3 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



Inbound Attribute Flow

□ Flow (External System Attributes/Values → FIM Attribute)

□ displayName→displayName

□ CustomExpression(IIF(Eq(BitOr(14,groupType),14),"Distribution","Security"))→type

□ mail→mail

□ member→member

□ mailNickname→mailNickname

□ "false"→membershipLocked

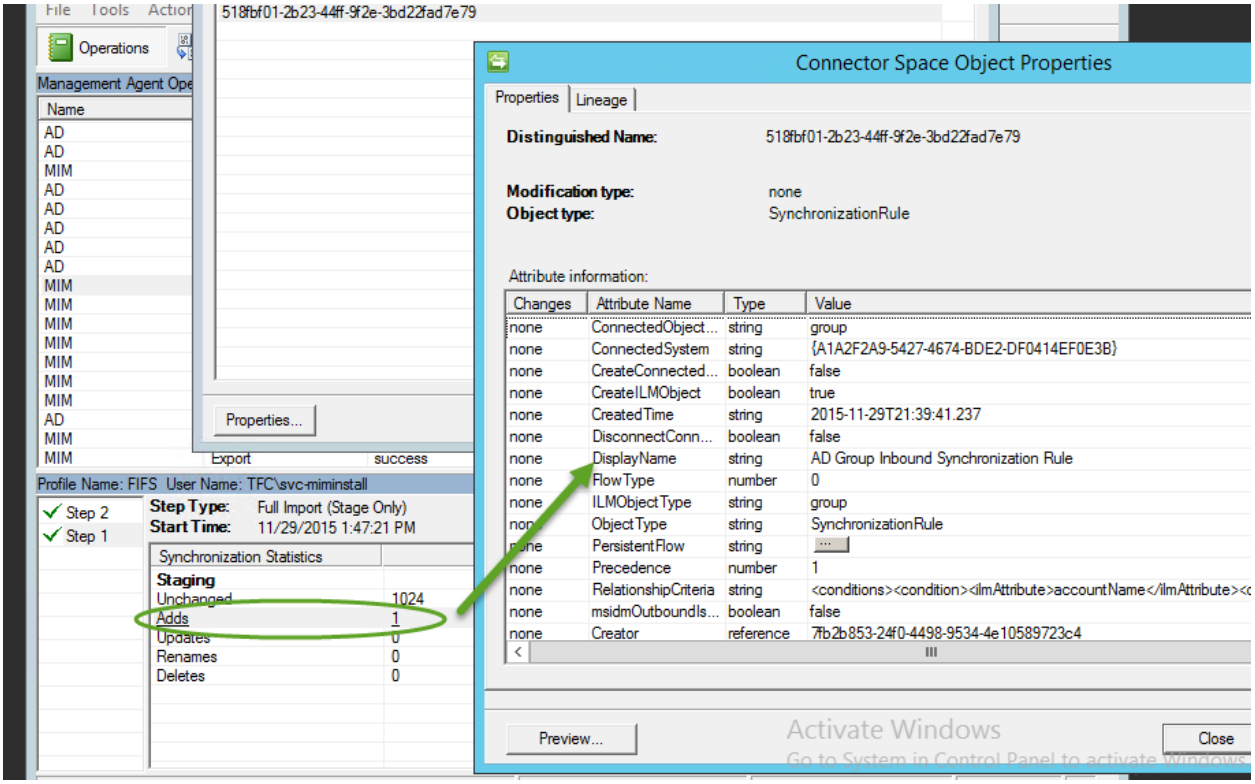
□ "Owner Approval"→membershipAddWorkflow

□ CustomExpression(IIF(Eq(BitAnd(2,groupType),2),"Global",IIF(Eq(BitAnd(4,groupType),4),"DomainLocal",...

□ "TFC"→domain

□ managedBy→displayedOwner

11 items total Page 1 of 2



518fbf01-2b23-44ff-9f2e-3bd22fad7e79

Name
AD
AD
MIM
AD
AD
AD
AD
AD
MIM
MIM
MIM
MIM
MIM
MIM
MIM
AD
MIM
MIM

Export success

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

✓ Step 2
✓ Step 1

Step Type: Full Import (Stage Only)
Start Time: 11/29/2015 1:47:21 PM

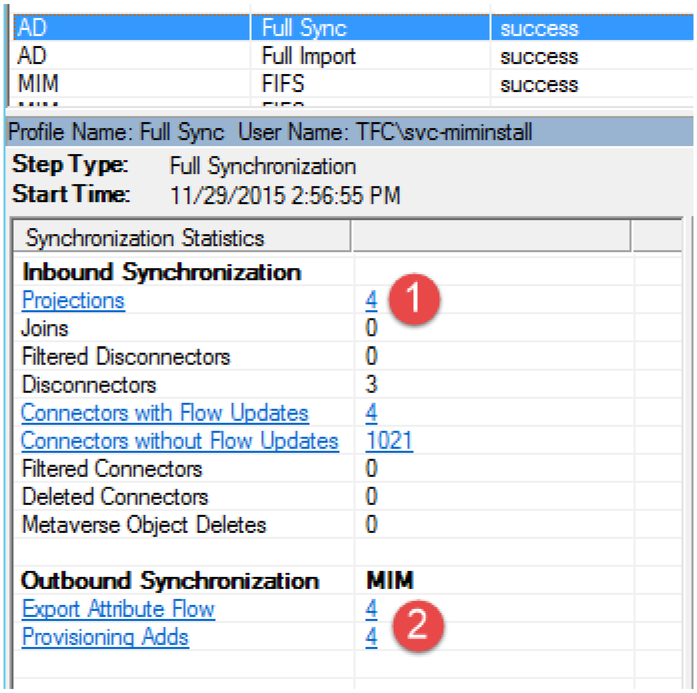
Synchronization Statistics	
Staging	
Unchanged	1024
Adds	1
Updates	0
Renames	0
Deletes	0

Distinguished Name: 518fbf01-2b23-44ff-9f2e-3bd22fad7e79

Modification type: none
Object type: SynchronizationRule

Attribute information:

Changes	Attribute Name	Type	Value
none	ConnectedObject...	string	group
none	ConnectedSystem	string	{A1A2F2A9-5427-4674-BDE2-DF0414EF0E3B}
none	CreateConnected...	boolean	false
none	CreateILMObject	boolean	true
none	CreatedTime	string	2015-11-29T21:39:41.237
none	DisconnectConn...	boolean	false
none	DisplayName	string	AD Group Inbound Synchronization Rule
none	FlowType	number	0
none	ILMObjectType	string	group
none	ObjectType	string	SynchronizationRule
none	PersistentFlow	string	...
none	Precedence	number	1
none	RelationshipCriteria	string	<conditions><condition><ilmAttribute>accountName</ilmAttribute><c
none	msidmOutboundIs...	boolean	false
none	Creator	reference	7fb2b853-24f0-4498-9534-4e10589723c4

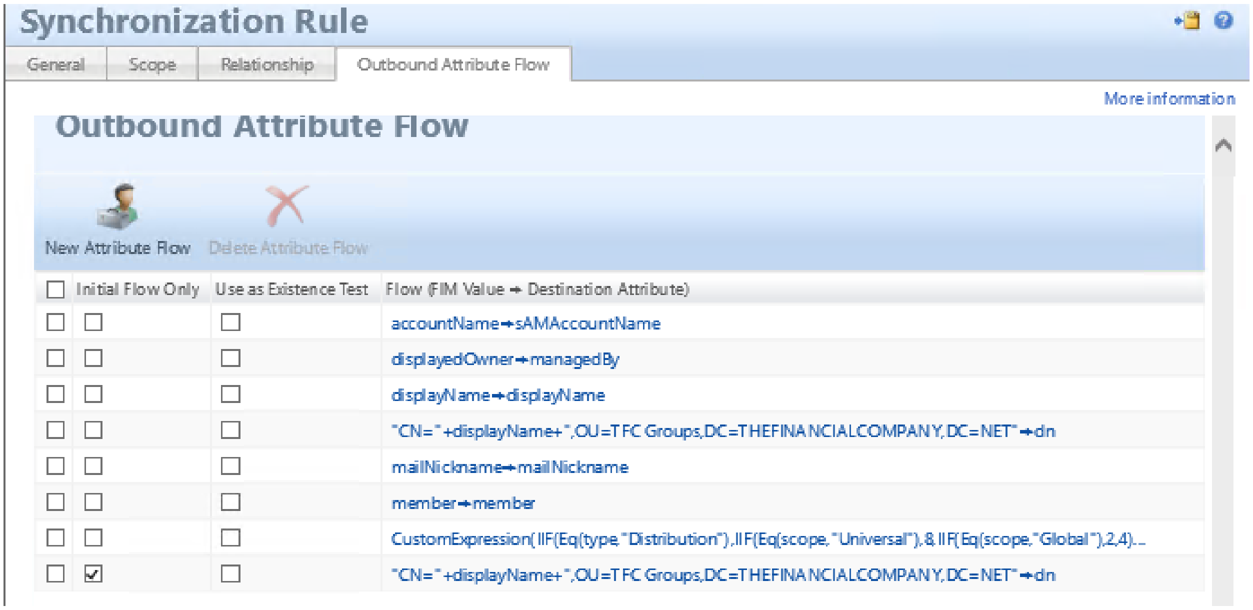


AD	Full Sync	success
AD	Full Import	success
MIM	FIFS	success

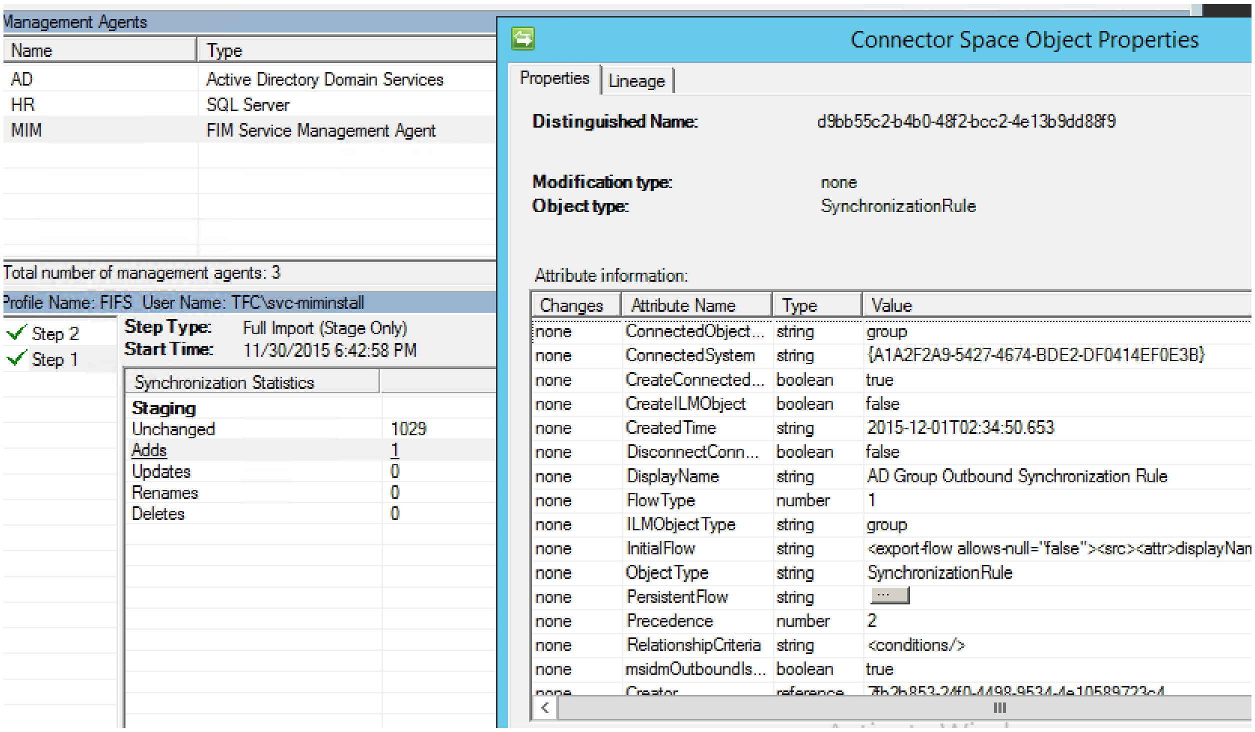
Profile Name: Full Sync User Name: TFC\svc-miminstall

Step Type: Full Synchronization
Start Time: 11/29/2015 2:56:55 PM

Synchronization Statistics	
Inbound Synchronization	
Projections	4
Joins	0
Filtered Disconnectors	0
Disconnectors	3
Connectors with Flow Updates	4
Connectors without Flow Updates	1021
Filtered Connectors	0
Deleted Connectors	0
Metaverse Object Deletes	0
Outbound Synchronization	**MIM**
Export Attribute Flow	4
Provisioning Adds	4



□	Initial Flow Only	Use as Existence Test	Flow (FIM Value → Destination Attribute)
□	□	□	accountName→sAMAccountName
□	□	□	displayedOwner→managedBy
□	□	□	displayName→displayName
□	□	□	"CN="+displayName+",OU=TFC Groups,DC=THEFINANCIALCOMPANY,DC=NET"→dn
□	□	□	mailNickname→mailNickname
□	□	□	member→member
□	□	□	CustomExpression(IIF(Eq(type,"Distribution"),IIF(Eq(scope,"Universal"),8,IIF(Eq(scope,"Global"),2,4)...
□	☑	□	"CN="+displayName+",OU=TFC Groups,DC=THEFINANCIALCOMPANY,DC=NET"→dn



Management Agents

Name	Type
AD	Active Directory Domain Services
HR	SQL Server
MIM	FIM Service Management Agent

Total number of management agents: 3

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

✓ Step 2
✓ Step 1

Step Type: Full Import (Stage Only)
Start Time: 11/30/2015 6:42:58 PM

Synchronization Statistics	
Staging	
Unchanged	1029
Adds	1
Updates	0
Renames	0
Deletes	0

Connector Space Object Properties

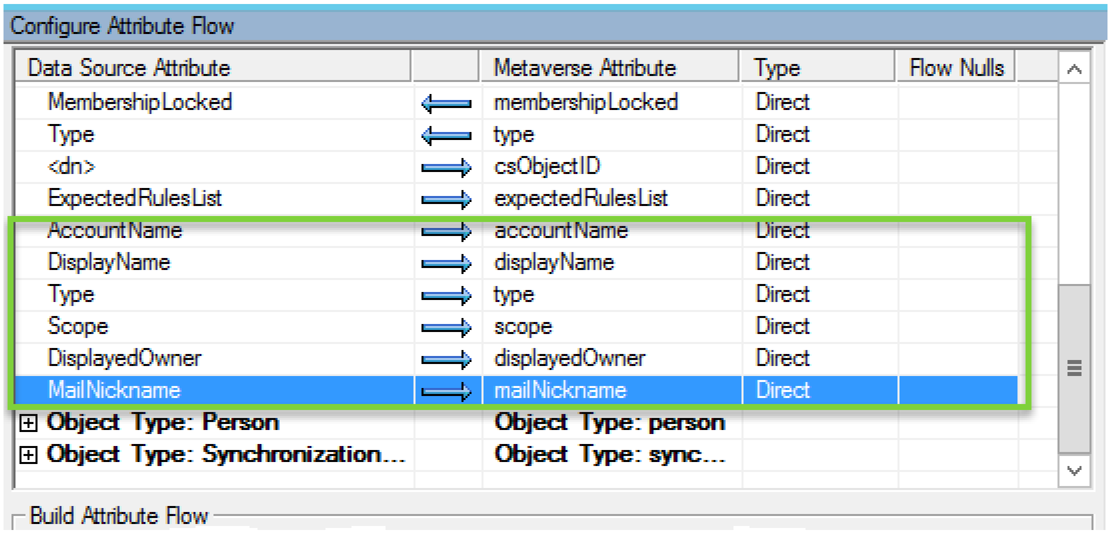
Properties | Lineage

Distinguished Name: d9bb55c2-b4b0-48f2-bcc2-4e13b9dd88f9

Modification type: none
Object type: SynchronizationRule

Attribute information:

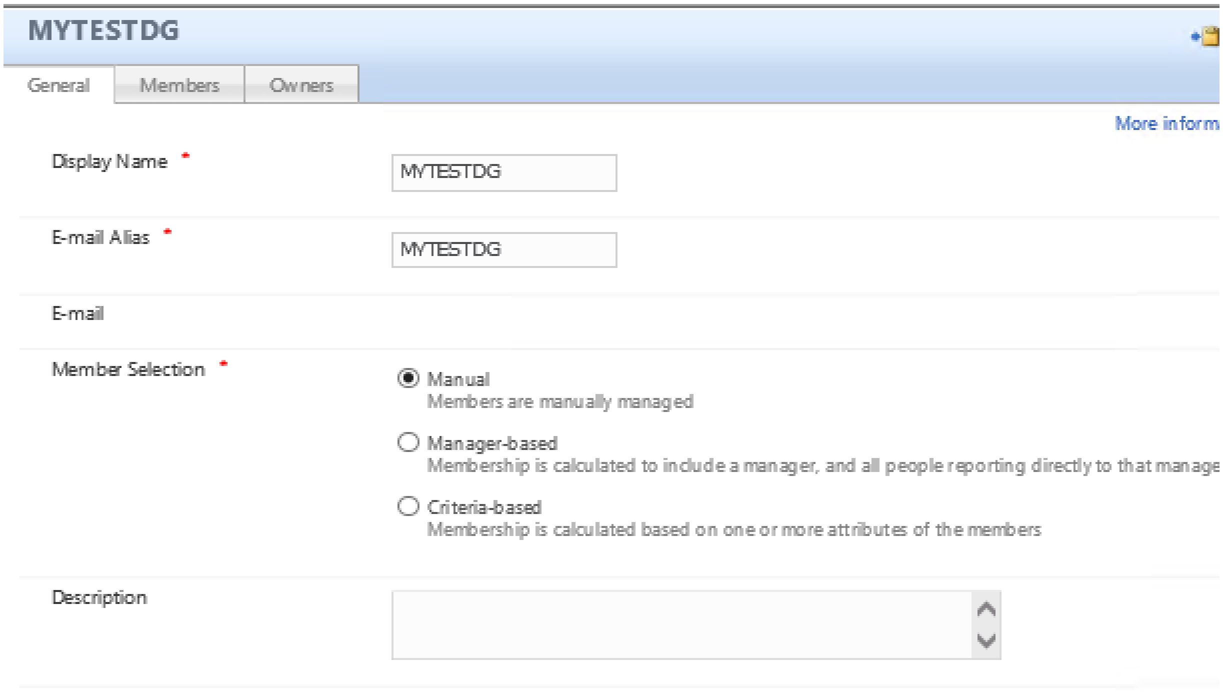
Changes	Attribute Name	Type	Value
none	ConnectedObject...	string	group
none	ConnectedSystem	string	{A1A2F2A9-5427-4674-BDE2-DF0414EF0E3B}
none	CreateConnected...	boolean	true
none	CreateILMObject	boolean	false
none	CreatedTime	string	2015-12-01T02:34:50.653
none	DisconnectConn...	boolean	false
none	DisplayName	string	AD Group Outbound Synchronization Rule
none	FlowType	number	1
none	ILMObjectType	string	group
none	InitialFlow	string	<export-flow allows-null="false"><src><attr>displayNan
none	ObjectType	string	SynchronizationRule
none	PersistentFlow	string	...
none	Precedence	number	2
none	RelationshipCriteria	string	<conditions/>
none	msidmOutboundIs...	boolean	true
none	Creator	reference	7b2b853-24f0-4498-9534-4e10589723c4



Configure Attribute Flow

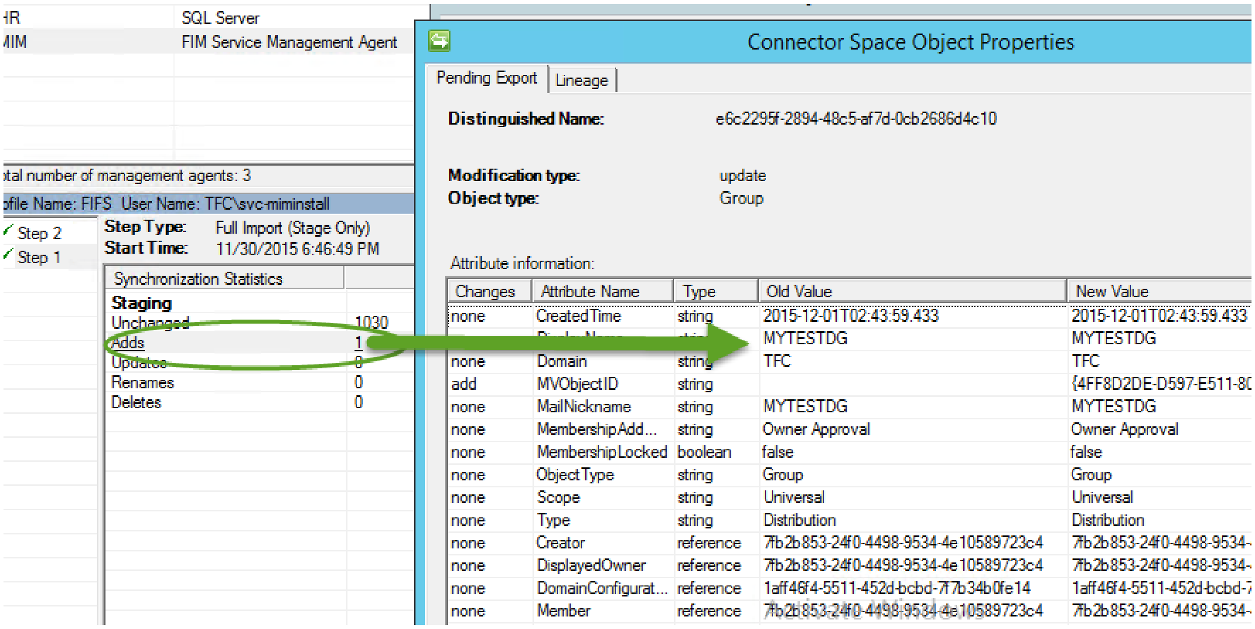
Data Source Attribute		Metaverse Attribute	Type	Flow Nulls
MembershipLocked	⟸	membershipLocked	Direct	
Type	⟸	type	Direct	
<dn>	⟹	csObjectID	Direct	
ExpectedRulesList	⟹	expectedRulesList	Direct	
AccountName	⟹	accountName	Direct	
DisplayName	⟹	displayName	Direct	
Type	⟹	type	Direct	
Scope	⟹	scope	Direct	
DisplayedOwner	⟹	displayedOwner	Direct	
MailNickname	⟹	mailNickname	Direct	
⊞ **Object Type: Person**		**Object Type: person**		
⊞ **Object Type: Synchronization...**		**Object Type: sync...**		

Build Attribute Flow



MYTESTDG

Display Name *	MYTESTDG
E-mail Alias *	MYTESTDG
E-mail	
Member Selection *	● Manual Members are manually managed ○ Manager-based Membership is calculated to include a manager, and all people reporting directly to that manage ○ Criteria-based Membership is calculated based on one or more attributes of the members
Description	



HR	SQL Server
MIM	FIM Service Management Agent

otal number of management agents: 3

ofile Name: FIFS User Name: TFC\svc-miminstall

Step Type: Full Import (Stage Only)
Start Time: 11/30/2015 6:46:49 PM

Synchronization Statistics	
Staging	
Unchanged	1030
Adds	1
Updates	0
Renames	0
Deletes	0

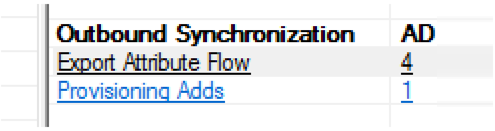
Connector Space Object Properties

Distinguished Name: e6c2295f-2894-48c5-af7d-0cb2686d4c10

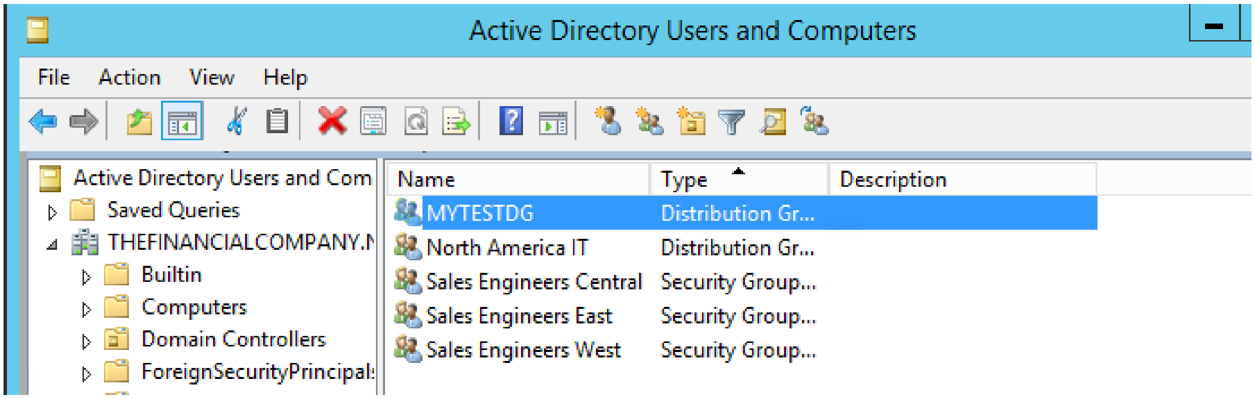
Modification type: update
Object type: Group

Attribute information:

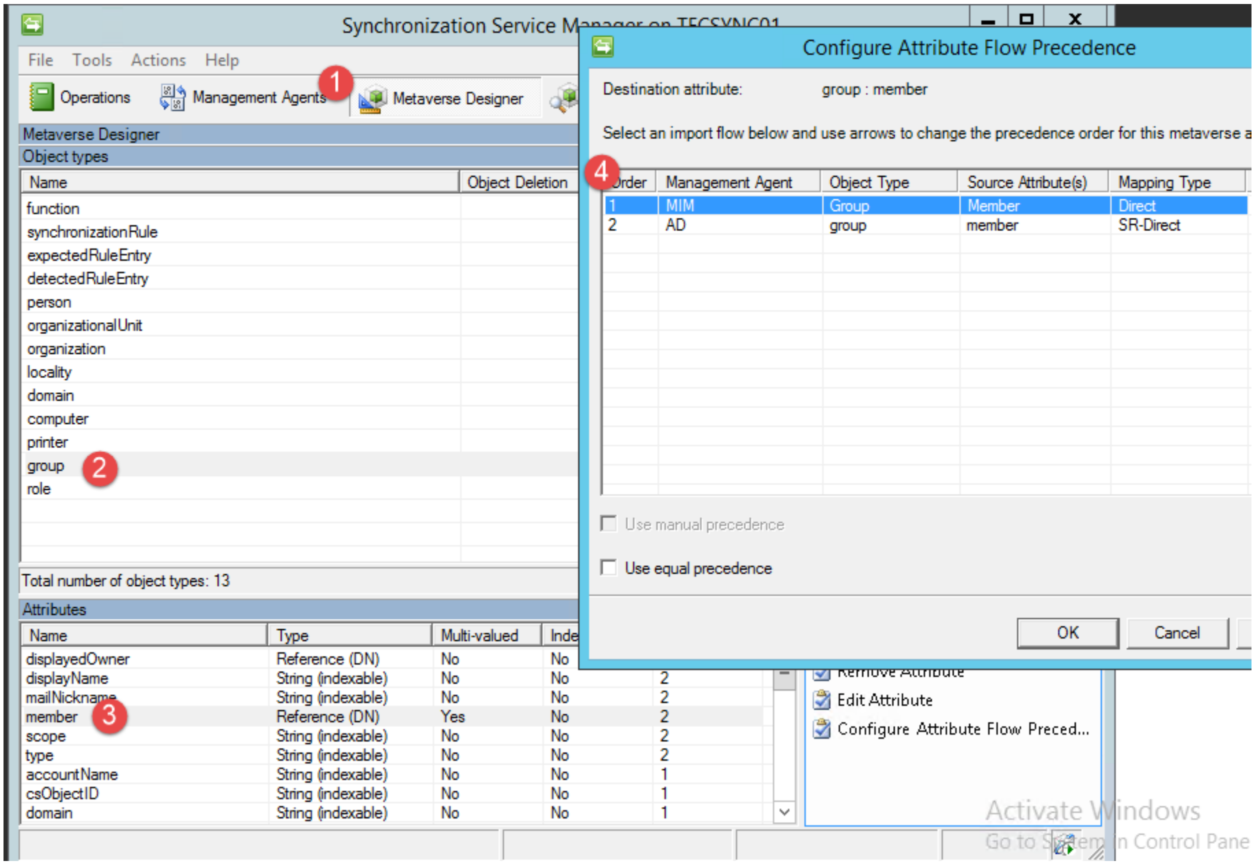
Changes	Attribute Name	Type	Old Value	New Value
none	CreatedTime	string	2015-12-01T02:43:59.433	2015-12-01T02:43:59.433
	DisplayName	string	MYTESTDG	MYTESTDG
none	Domain	string	TFC	TFC
add	MVObjectID	string		{4FF8D2DE-D597-E511-80
none	MailNickname	string	MYTESTDG	MYTESTDG
none	MembershipAdd...	string	Owner Approval	Owner Approval
none	MembershipLocked	boolean	false	false
none	ObjectType	string	Group	Group
none	Scope	string	Universal	Universal
none	Type	string	Distribution	Distribution
none	Creator	reference	7fb2b853-24f0-4498-9534-4e10589723c4	7fb2b853-24f0-4498-9534-
none	DisplayedOwner	reference	7fb2b853-24f0-4498-9534-4e10589723c4	7fb2b853-24f0-4498-9534-
none	DomainConfigurat...	reference	1aff46f4-5511-452d-bcbd-7f7b34b0fe14	1aff46f4-5511-452d-bcbd-7
none	Member	reference	7fb2b853-24f0-4498-9534-4e10589723c4	7fb2b853-24f0-4498-9534-



Outbound Synchronization	AD
Export Attribute Flow	4
Provisioning Adds	1


Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
THEFINANCIALCOMPANY.N
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals

Name	Type	Description
MYTESTDG	Distribution Gr...	
North America IT	Distribution Gr...	
Sales Engineers Central	Security Group...	
Sales Engineers East	Security Group...	
Sales Engineers West	Security Group...	



Name	Object Deletion
function	
synchronizationRule	
expectedRuleEntry	
detectedRuleEntry	
person	
organizationalUnit	
organization	
locality	
domain	
computer	
printer	
group	
role	

Total number of object types: 13

Name	Type	Multi-valued	Inde	
displayedOwner	Reference (DN)	No	No	
displayName	String (indexable)	No	No	2
mailNickname	String (indexable)	No	No	2
member	Reference (DN)	Yes	No	2
scope	String (indexable)	No	No	2
type	String (indexable)	No	No	2
accountName	String (indexable)	No	No	1
csObjectID	String (indexable)	No	No	1
domain	String (indexable)	No	No	1

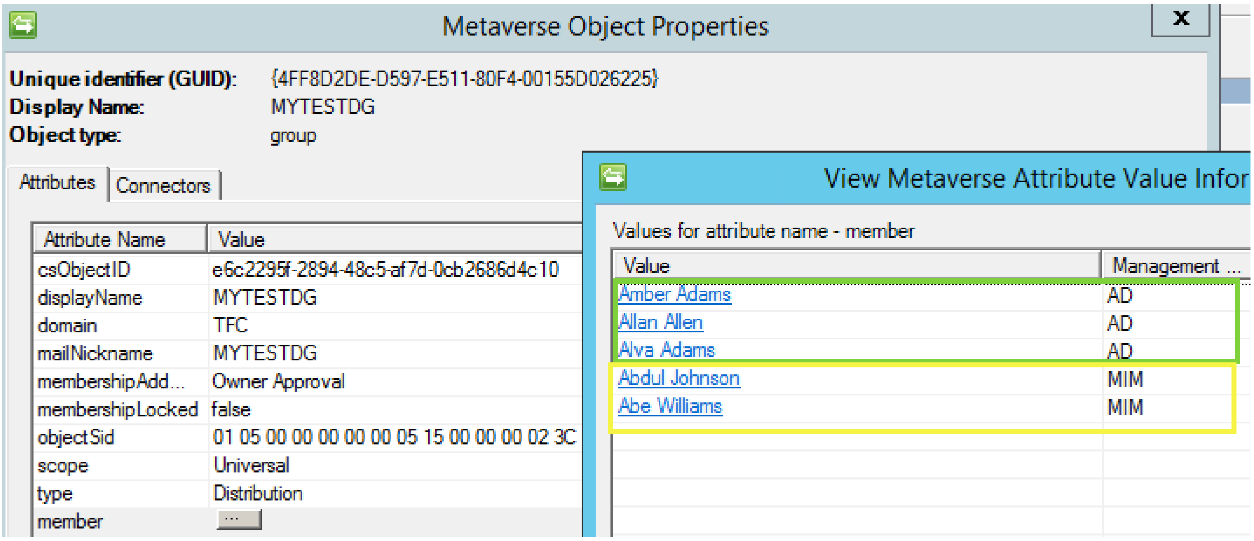
Destination attribute: group : member

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

Order	Management Agent	Object Type	Source Attribute(s)	Mapping Type
1	MIM	Group	Member	Direct
2	AD	group	member	SR-Direct

□ Use manual precedence

□ Use equal precedence



Metaverse Object Properties

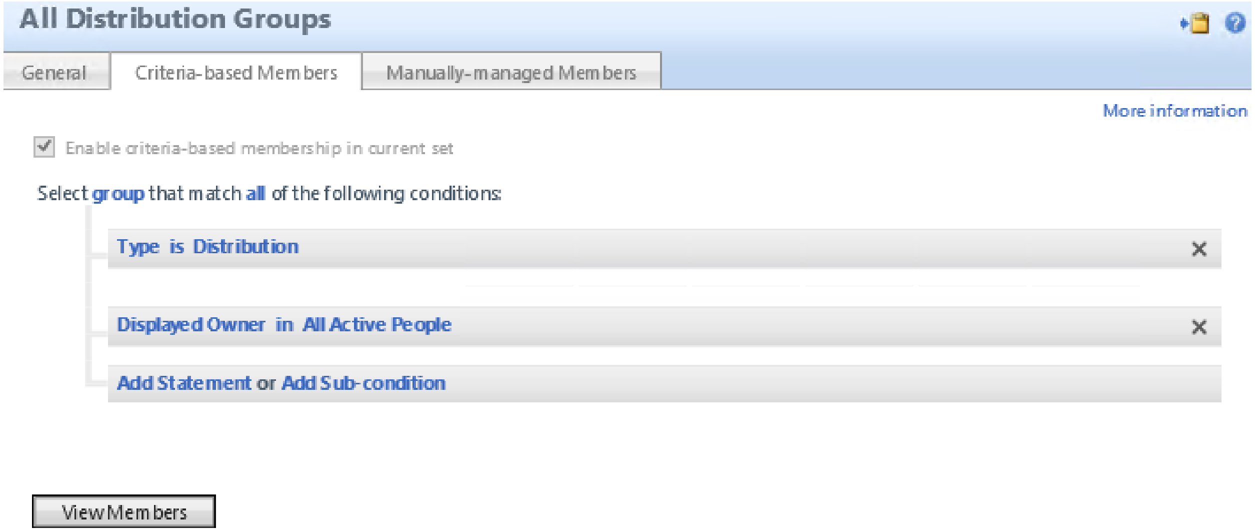
Unique identifier (GUID): {4FF8D2DE-D597-E511-80F4-00155D026225}
Display Name: MYTESTDG
Object type: group

Attribute Name	Value
csObjectID	e6c2295f-2894-48c5-af7d-0cb2686d4c10
displayName	MYTESTDG
domain	TFC
mailNickname	MYTESTDG
membershipAdd...	Owner Approval
membershipLocked	false
objectSid	01 05 00 00 00 00 00 05 15 00 00 00 02 3C
scope	Universal
type	Distribution
member	...

View Metaverse Attribute Value Infor

Values for attribute name - member

Value	Management ...
Amber Adams	AD
Allan Allen	AD
Alva Adams	AD
Abdul Johnson	MIM
Abe Williams	MIM

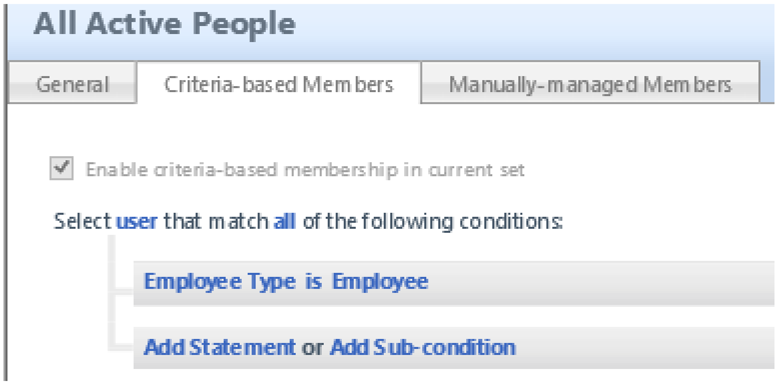


All Distribution Groups

☑ Enable criteria-based membership in current set

Select group that match all of the following conditions:

- Type is Distribution ✕
- Displayed Owner in All Active People ✕
- Add Statement or Add Sub-condition

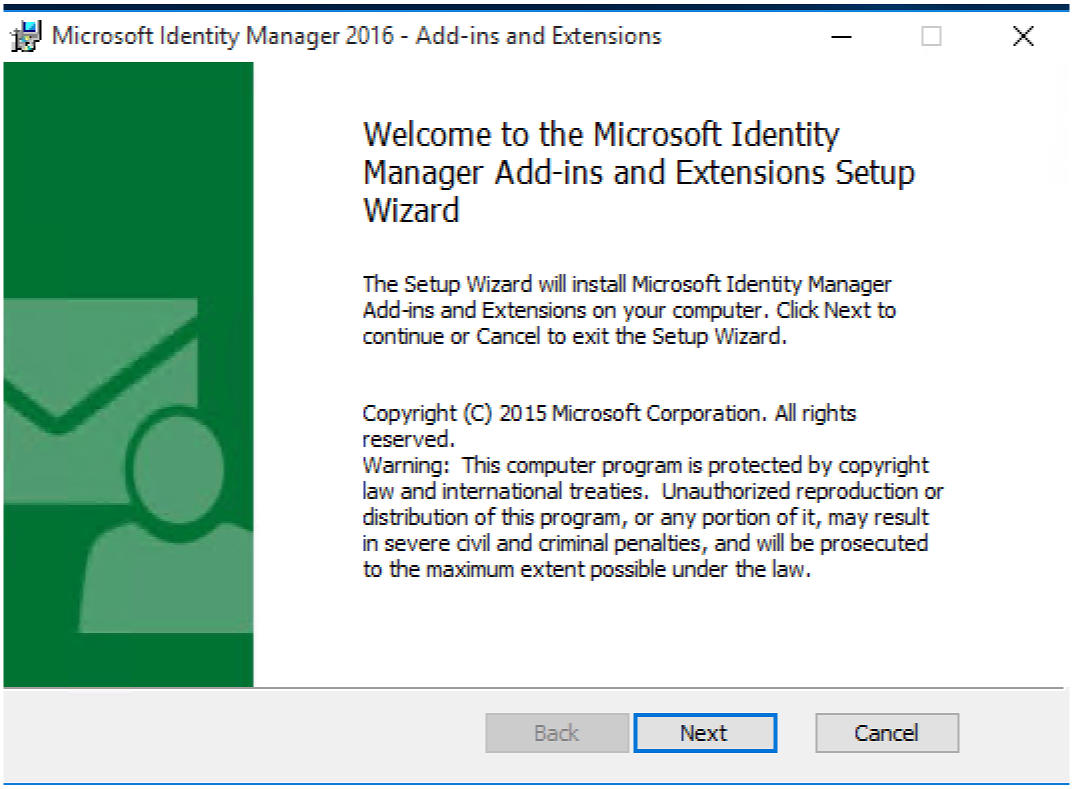


All Active People

☑ Enable criteria-based membership in current set

Select user that match all of the following conditions:

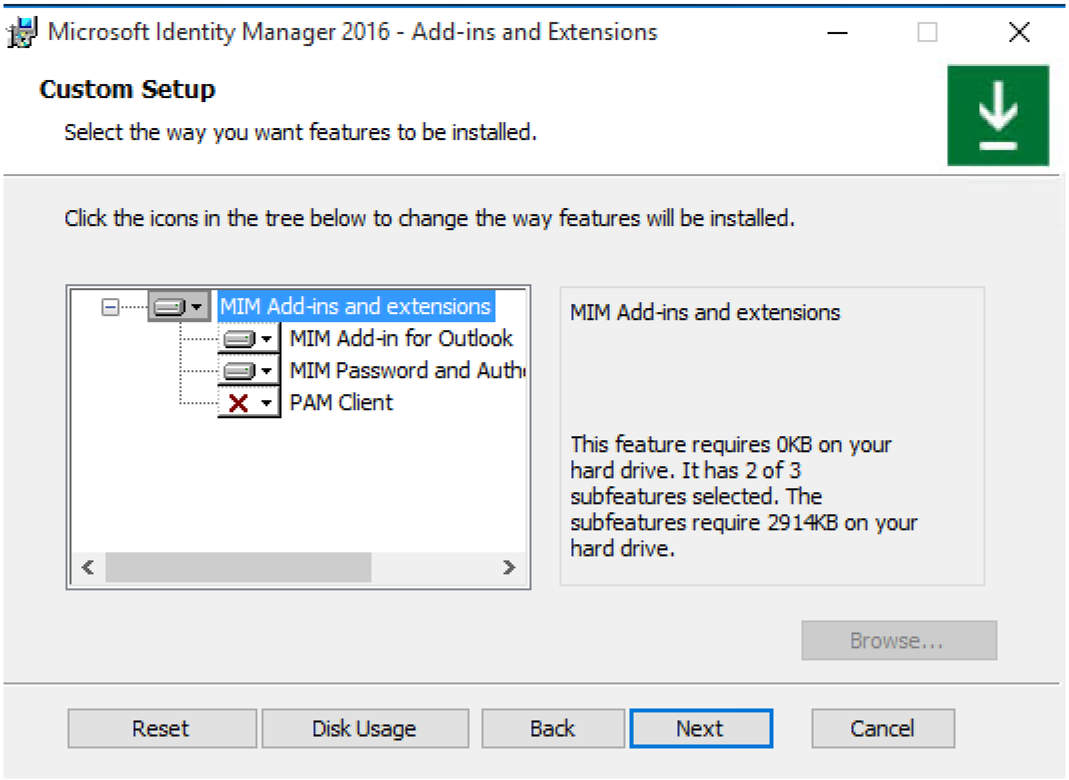
- Employee Type is Employee
- Add Statement or Add Sub-condition



Welcome to the Microsoft Identity Manager Add-ins and Extensions Setup Wizard

The Setup Wizard will install Microsoft Identity Manager Add-ins and Extensions on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Copyright (C) 2015 Microsoft Corporation. All rights reserved.
Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.



Custom Setup

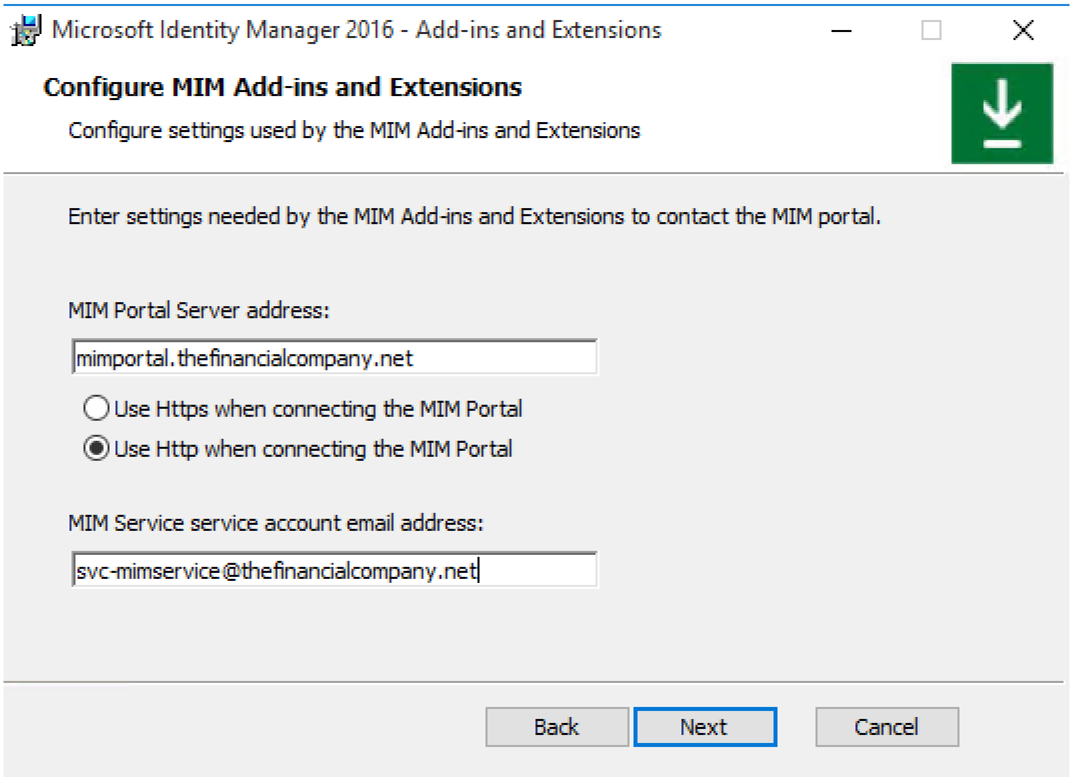
Select the way you want features to be installed.

Click the icons in the tree below to change the way features will be installed.

- MIM Add-ins and extensions
  - MIM Add-in for Outlook
  - MIM Password and Auth
  - ☒ PAM Client

MIM Add-ins and extensions

This feature requires 0KB on your hard drive. It has 2 of 3 subfeatures selected. The subfeatures require 2914KB on your hard drive.



Configure MIM Add-ins and Extensions

Configure settings used by the MIM Add-ins and Extensions

Enter settings needed by the MIM Add-ins and Extensions to contact the MIM portal.

MIM Portal Server address:

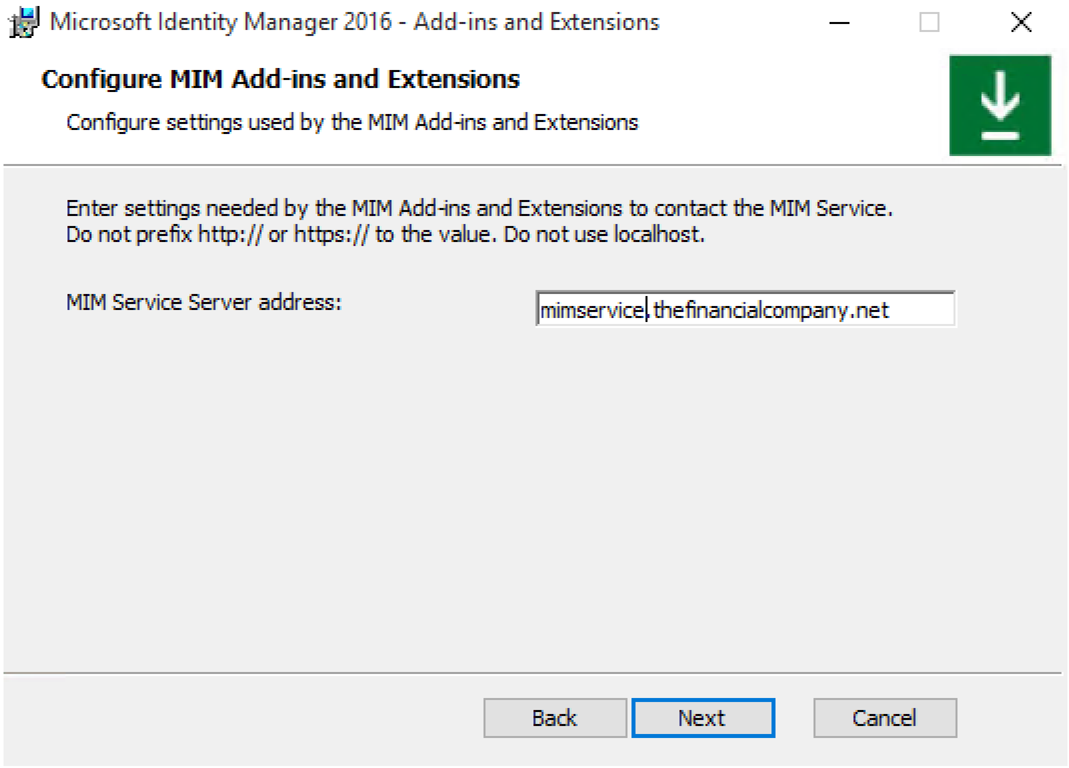
mimportal.thefinancialcompany.net

○ Use Https when connecting the MIM Portal

● Use Http when connecting the MIM Portal

MIM Service service account email address:

svc-mimservice@thefinancialcompany.net

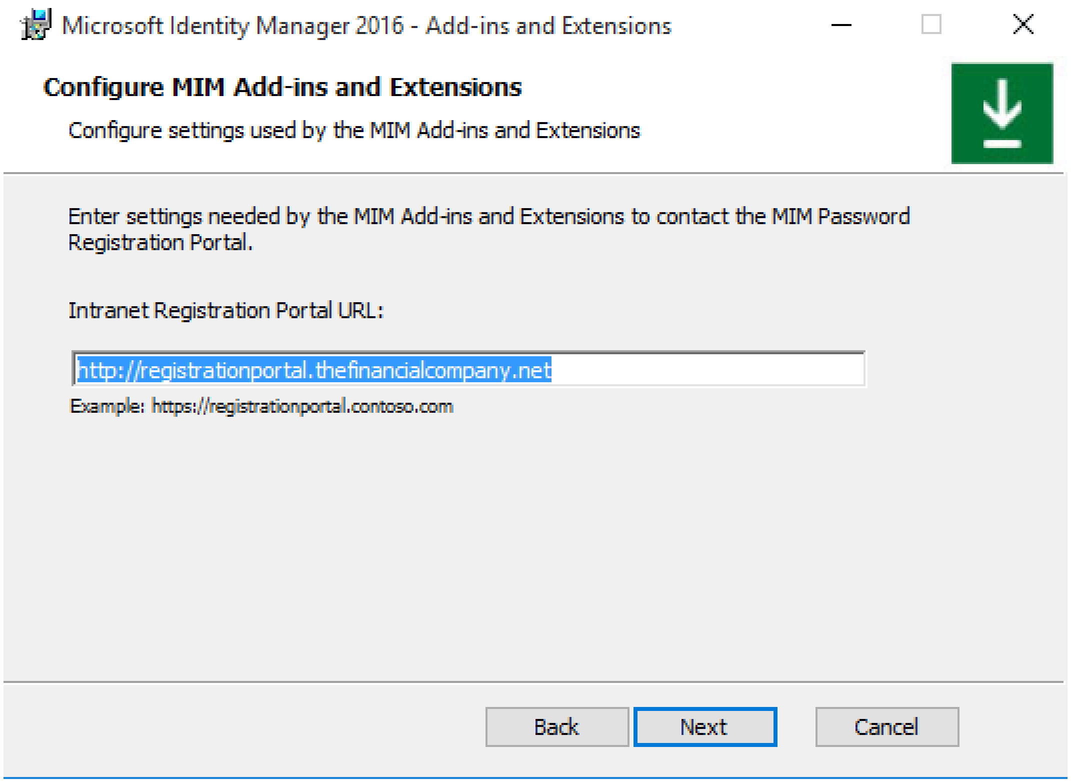


Configure MIM Add-ins and Extensions

Configure settings used by the MIM Add-ins and Extensions

Enter settings needed by the MIM Add-ins and Extensions to contact the MIM Service.
Do not prefix http:// or https:// to the value. Do not use localhost.

MIM Service Server address: mimservice.thefinancialcompany.net



Microsoft Identity Manager 2016 - Add-ins and Extensions

Configure MIM Add-ins and Extensions

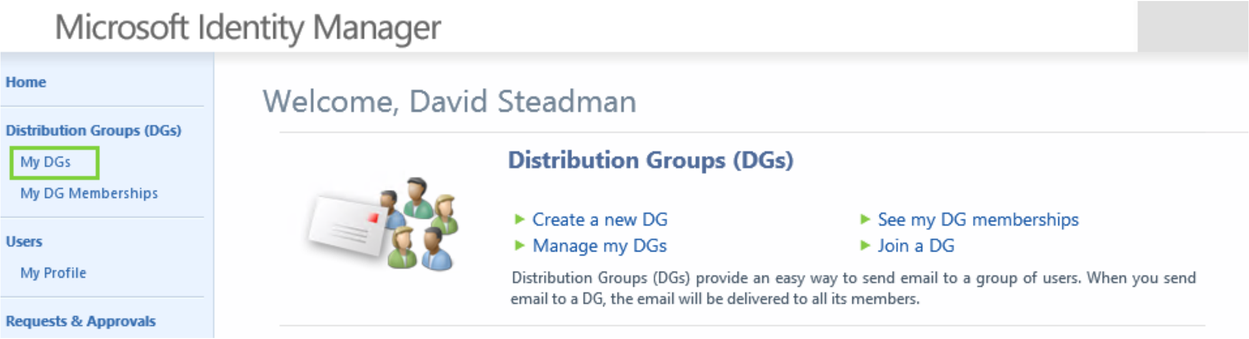
Configure settings used by the MIM Add-ins and Extensions

Enter settings needed by the MIM Add-ins and Extensions to contact the MIM Password Registration Portal.

Intranet Registration Portal URL:

http://registrationportal.thefinancialcompany.net

Example: https://registrationportal.contoso.com

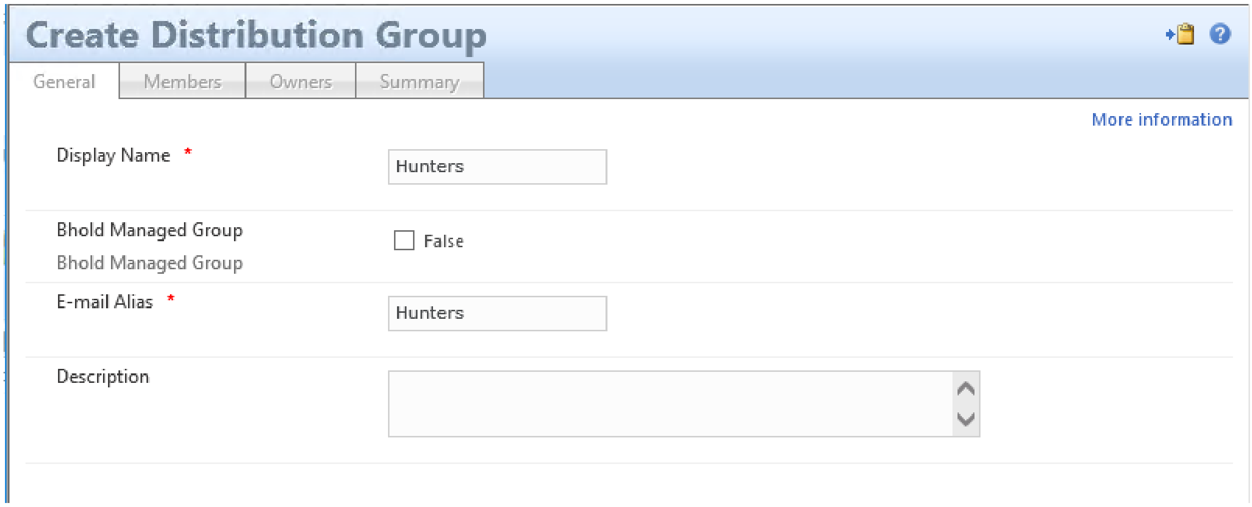


Microsoft Identity Manager

Welcome, David Steadman

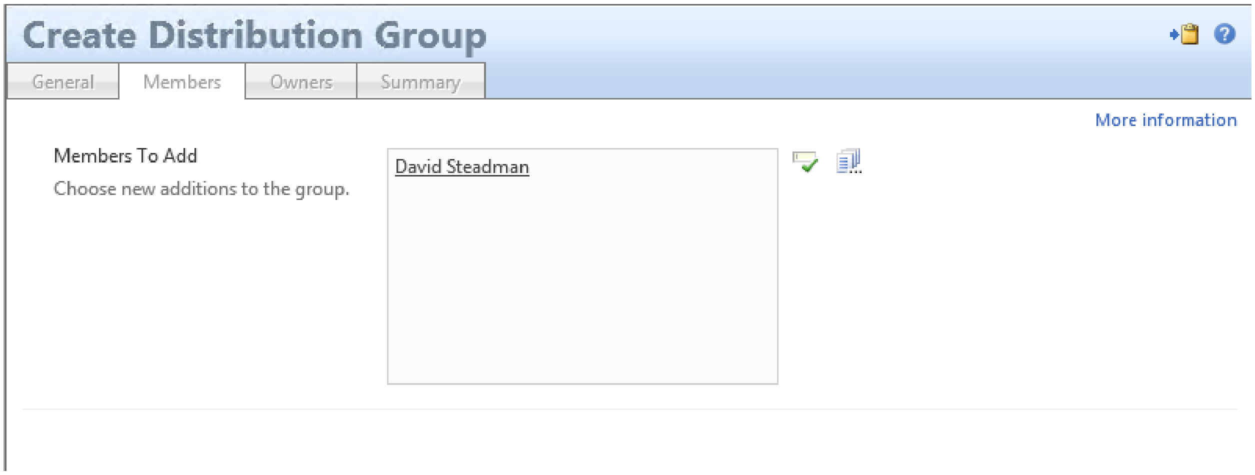
Distribution Groups (DGs)

Distribution Groups (DGs) provide an easy way to send email to a group of users. When you send email to a DG, the email will be delivered to all its members.



Create Distribution Group

Display Name *	Hunters
Bhold Managed Group Bhold Managed Group	□ False
E-mail Alias *	Hunters
Description	

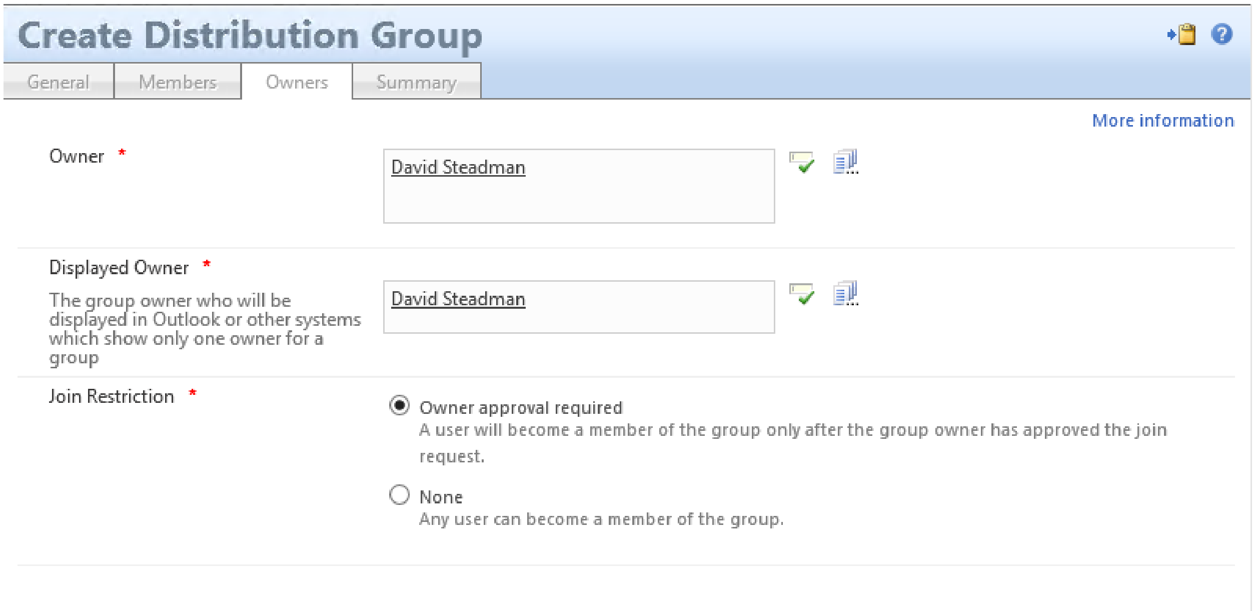


Create Distribution Group

Members To Add

Choose new additions to the group.

David Steadman



Create Distribution Group

Owner * David Steadman

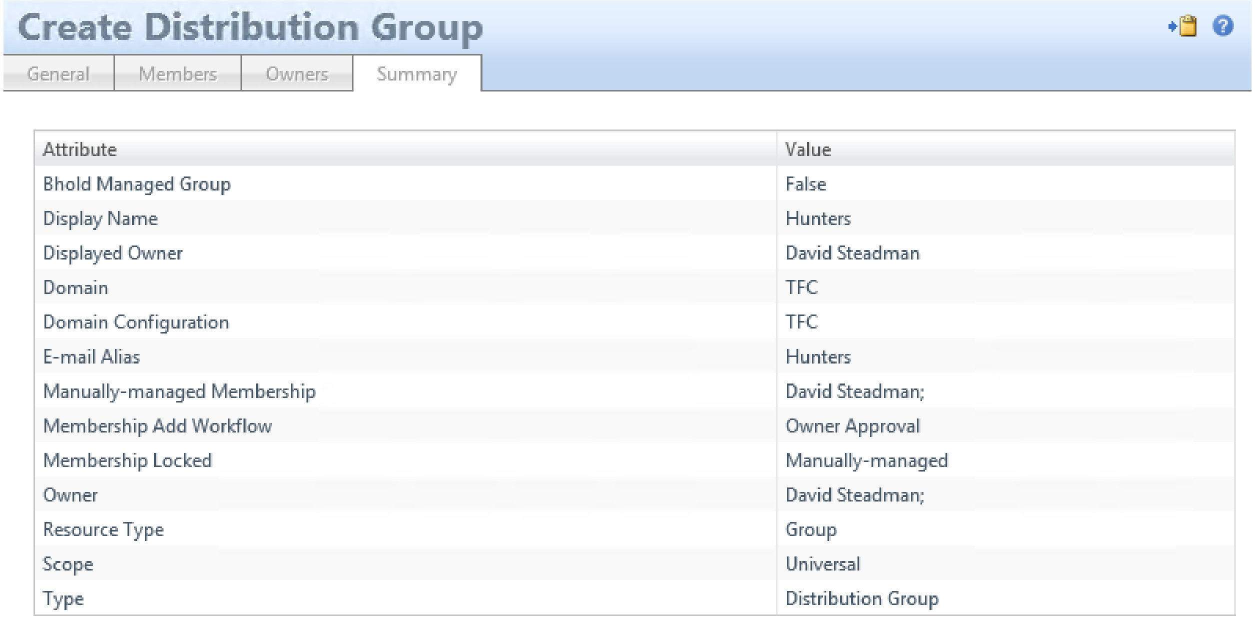
Displayed Owner * David Steadman

The group owner who will be displayed in Outlook or other systems which show only one owner for a group

Join Restriction *

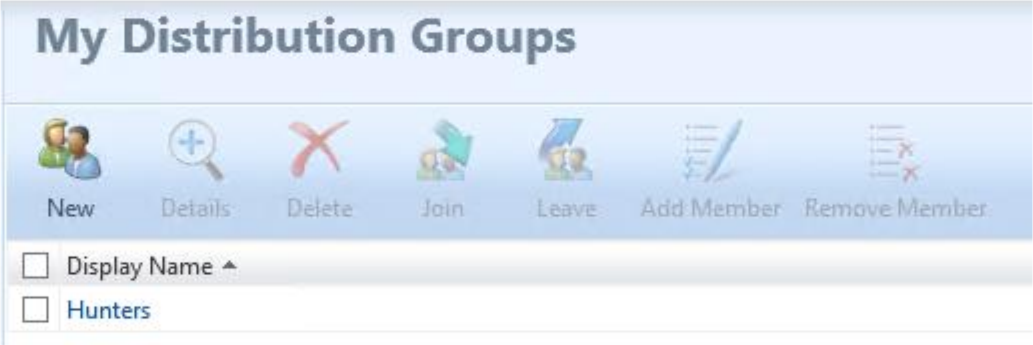
● Owner approval required
A user will become a member of the group only after the group owner has approved the join request.

○ None
Any user can become a member of the group.



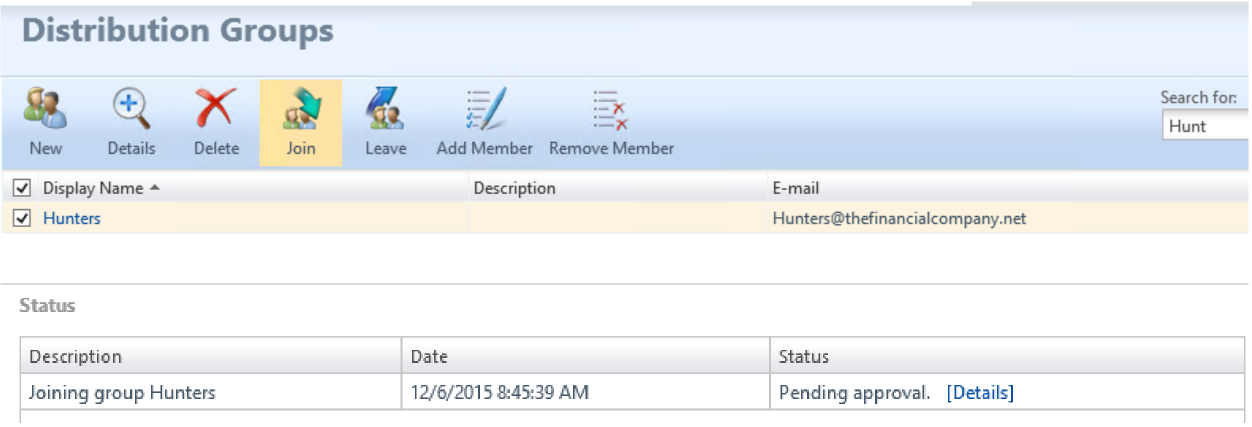
Create Distribution Group

Attribute	Value
Bhold Managed Group	False
Display Name	Hunters
Displayed Owner	David Steadman
Domain	TFC
Domain Configuration	TFC
E-mail Alias	Hunters
Manually-managed Membership	David Steadman;
Membership Add Workflow	Owner Approval
Membership Locked	Manually-managed
Owner	David Steadman;
Resource Type	Group
Scope	Universal
Type	Distribution Group



My Distribution Groups

□	Display Name ▲
□	Hunters



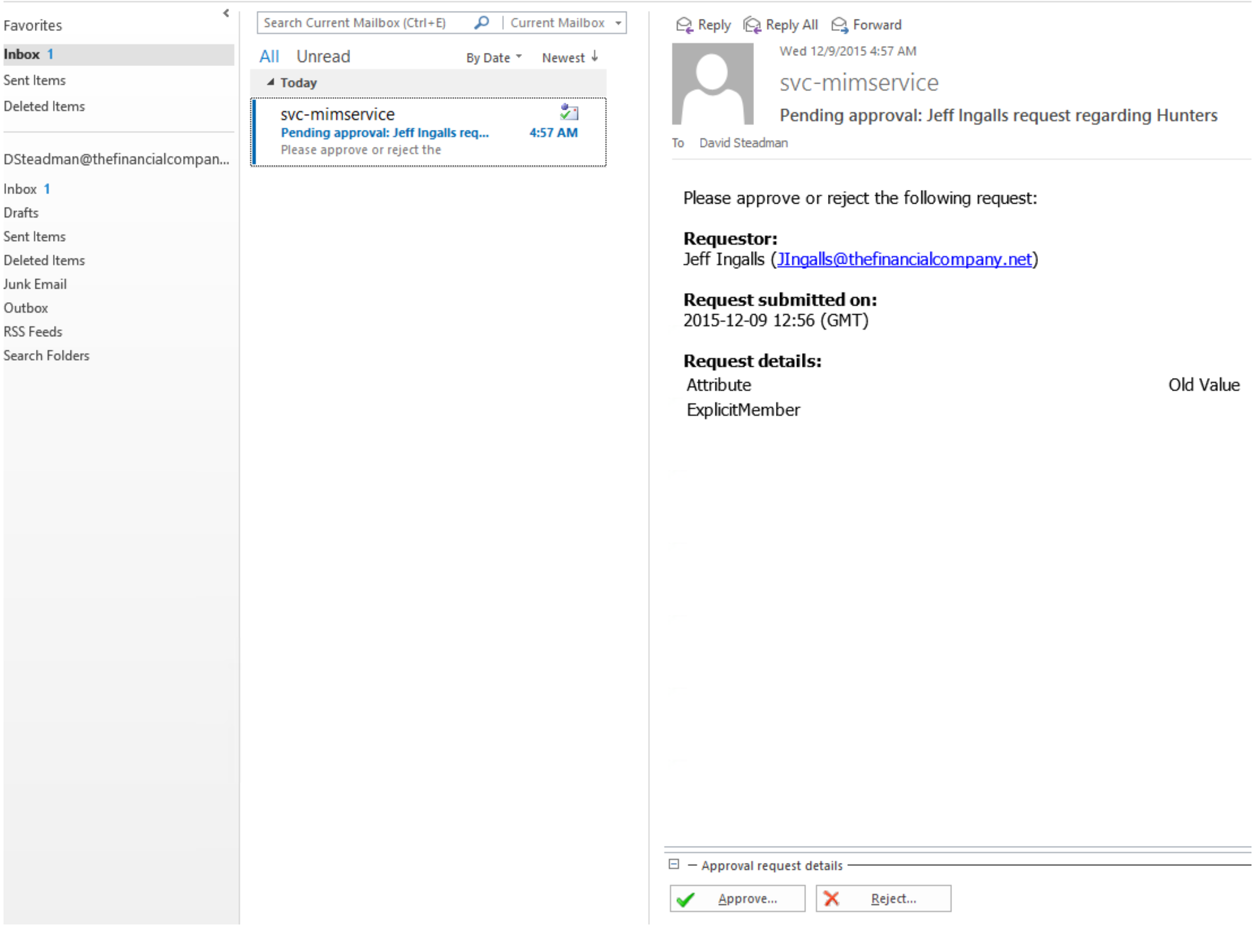
Distribution Groups

Search for: Hunt

☑	Display Name ▲	Description	E-mail
☑	Hunters		Hunters@thefinancialcompany.net

Status

Description	Date	Status
Joining group Hunters	12/6/2015 8:45:39 AM	Pending approval. [Details]



svc-mimservice
Pending approval: Jeff Ingalls req... 4:57 AM
Please approve or reject the

Wed 12/9/2015 4:57 AM

svc-mimservice

Pending approval: Jeff Ingalls request regarding Hunters

To David Steadman

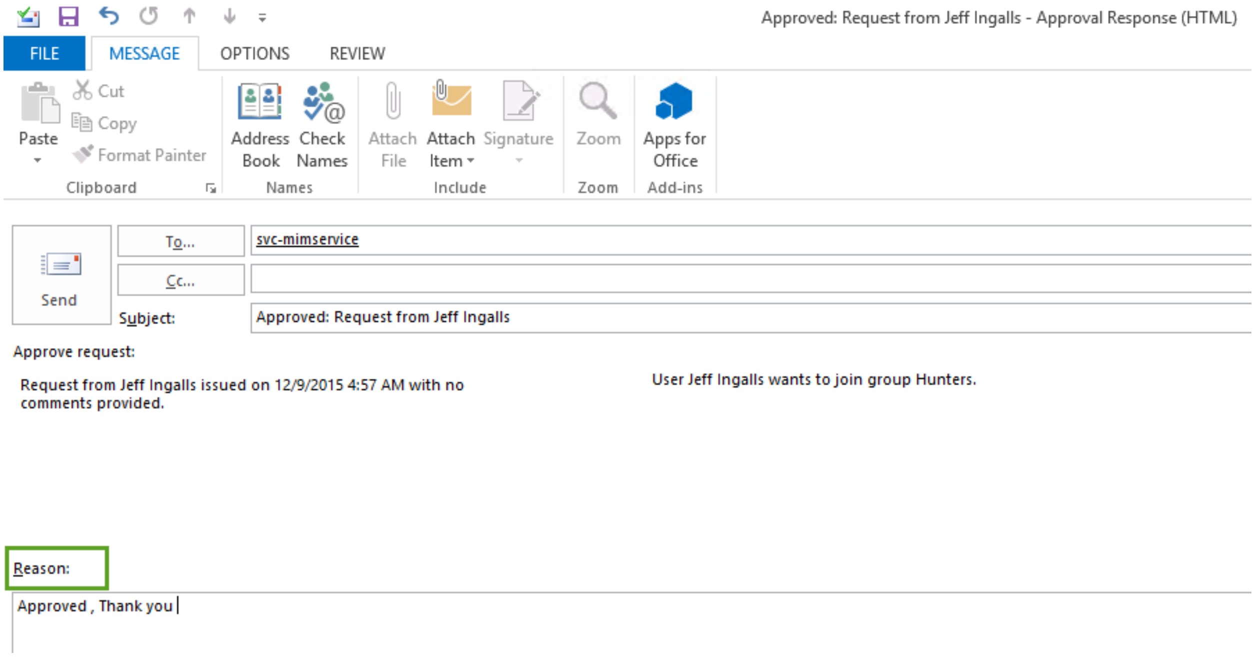
Please approve or reject the following request:

Requestor:
Jeff Ingalls (JIngalls@thefinancialcompany.net)

Request submitted on:
2015-12-09 12:56 (GMT)

Request details:

Attribute	Old Value
ExplicitMember	



Approved: Request from Jeff Ingalls - Approval Response (HTML)

To... svc-mimservice

Cc...

Subject: Approved: Request from Jeff Ingalls

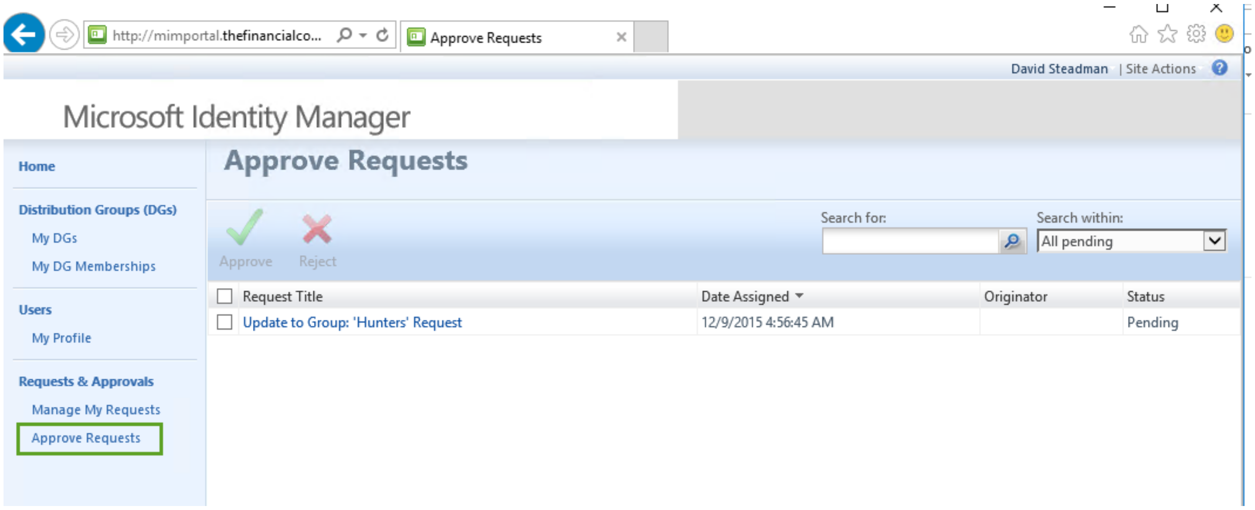
Approve request:

Request from Jeff Ingalls issued on 12/9/2015 4:57 AM with no comments provided.

User Jeff Ingalls wants to join group Hunters.

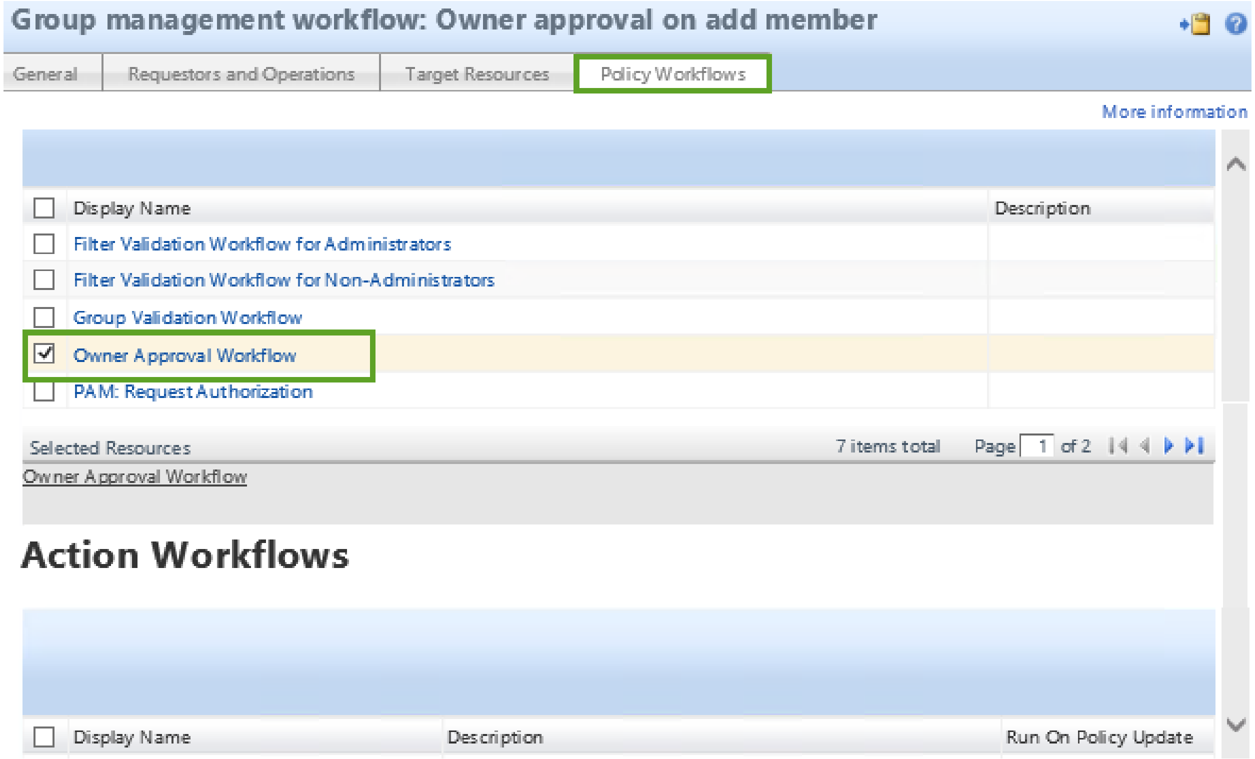
Reason:

Approved , Thank you



Approve Requests

□	Request Title	Date Assigned	Originator	Status
□	Update to Group: 'Hunters' Request	12/9/2015 4:56:45 AM		Pending



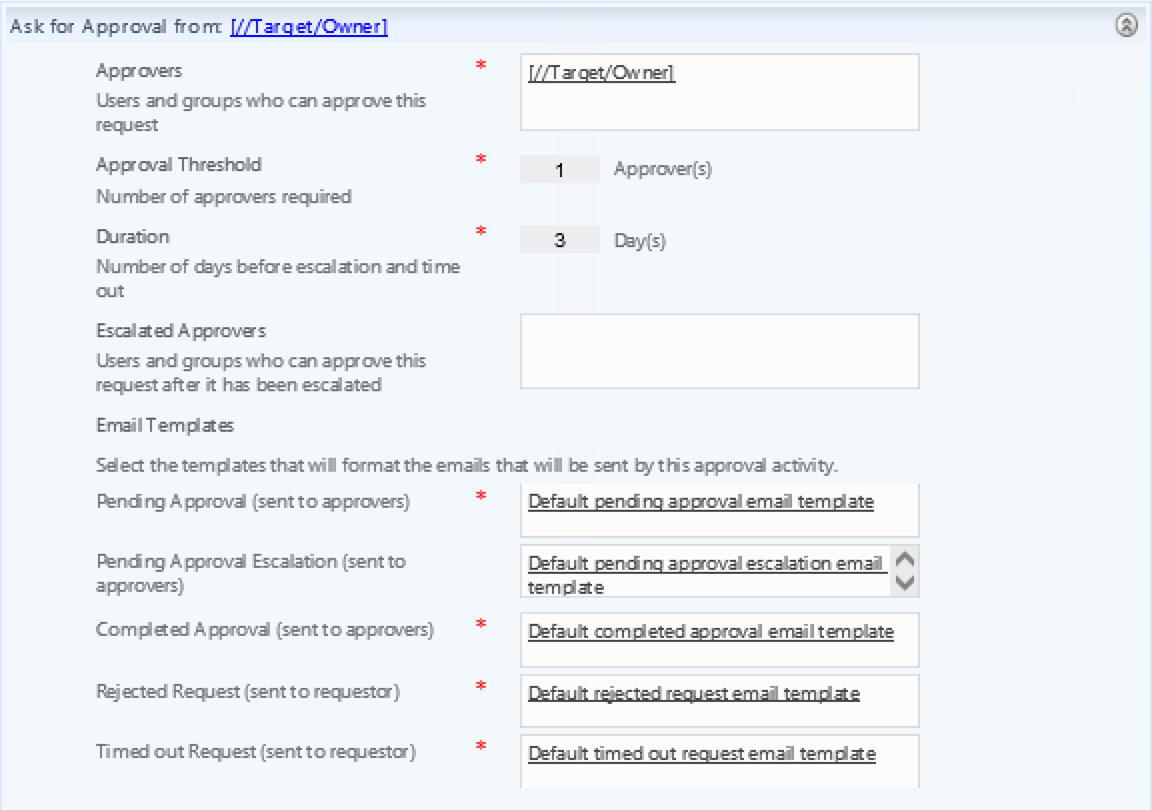
Group management workflow: Owner approval on add member

□	Display Name	Description
□	Filter Validation Workflow for Administrators	
□	Filter Validation Workflow for Non-Administrators	
□	Group Validation Workflow	
☑	Owner Approval Workflow	
□	PAM: Request Authorization	

Owner Approval Workflow

Action Workflows

□	Display Name	Description	Run On Policy Update



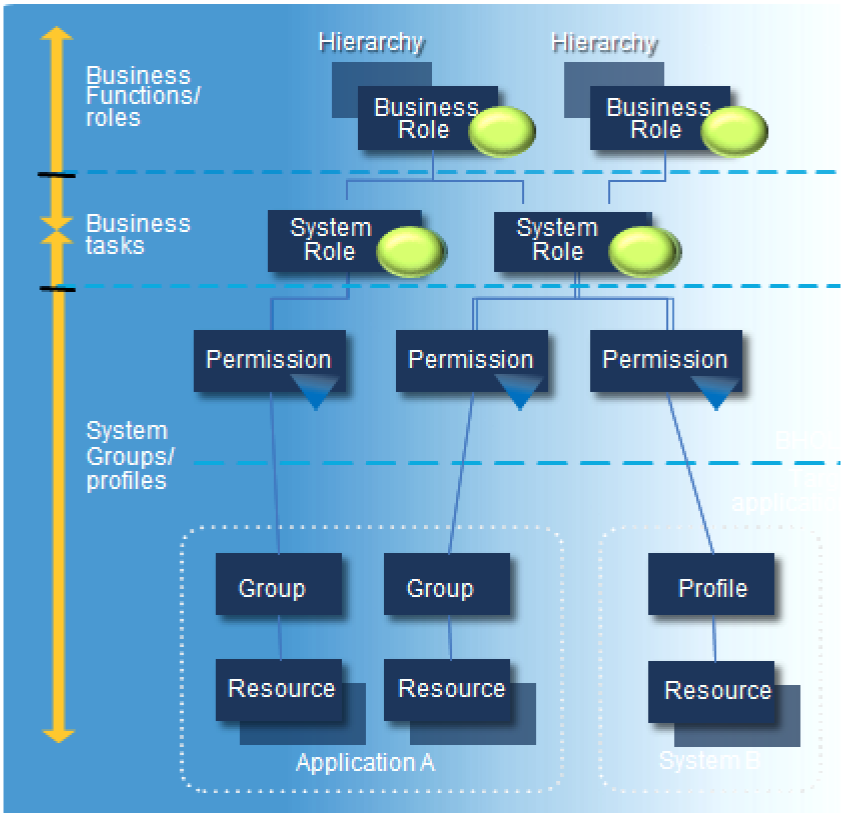
Ask for Approval from: [//Target/Owner]

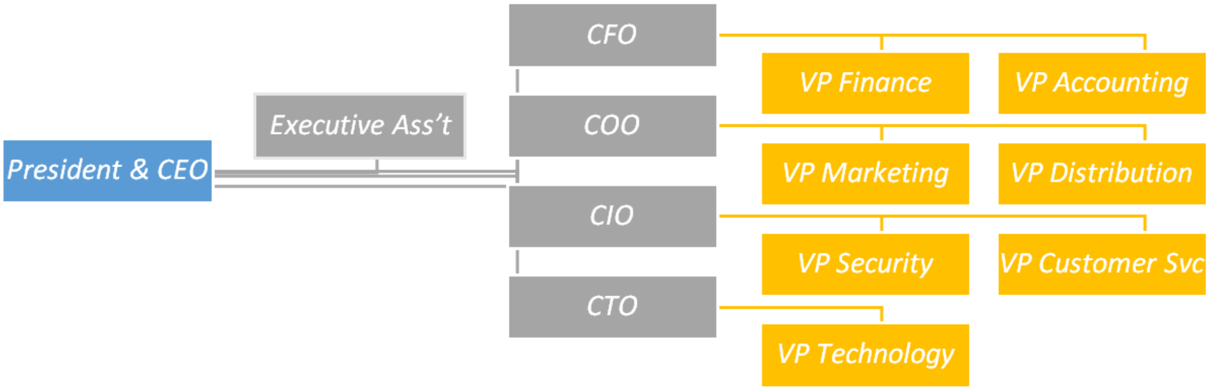
Approvers Users and groups who can approve this request	*	[//Target/Owner]	
Approval Threshold Number of approvers required	*	1	Approver(s)
Duration Number of days before escalation and time out	*	3	Day(s)
Escalated Approvers Users and groups who can approve this request after it has been escalated			

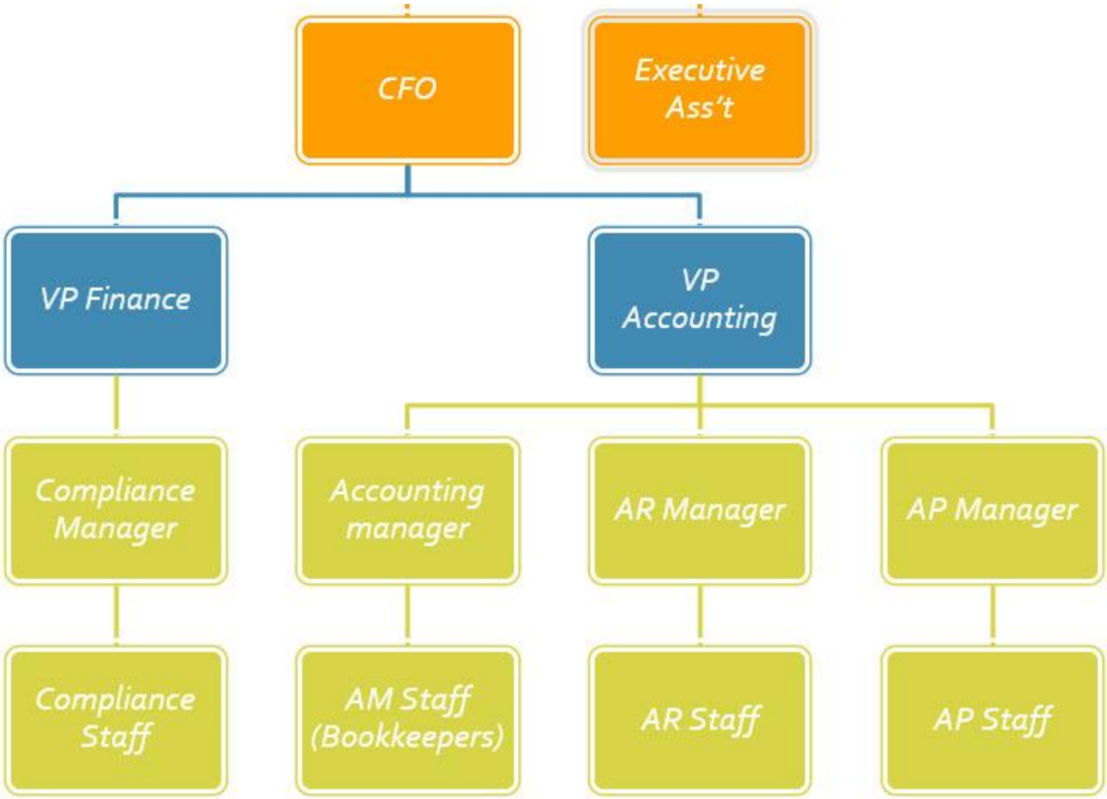
Email Templates

Select the templates that will format the emails that will be sent by this approval activity.

Pending Approval (sent to approvers)	*	Default pending approval email template
Pending Approval Escalation (sent to approvers)		Default pending approval escalation 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


Hierarchy
Hierarchy
Business Functions/ roles
Business Role
Business Role
Business tasks
System Role
System Role
Permission
Permission
Permission
System Groups/ profiles
BHOL
Targ
applicatio
Group
Group
Profile
Resource
Resource
Resource
Application A
System B


CFO
VP Finance
VP Accounting
Executive Ass't
COO
President & CEO
VP Marketing
VP Distribution
CIO
VP Security
VP Customer Svc
CTO
VP Technology



CFO

Executive Ass't

VP Finance

VP Accounting

Compliance Manager

Accounting manager

AR Manager

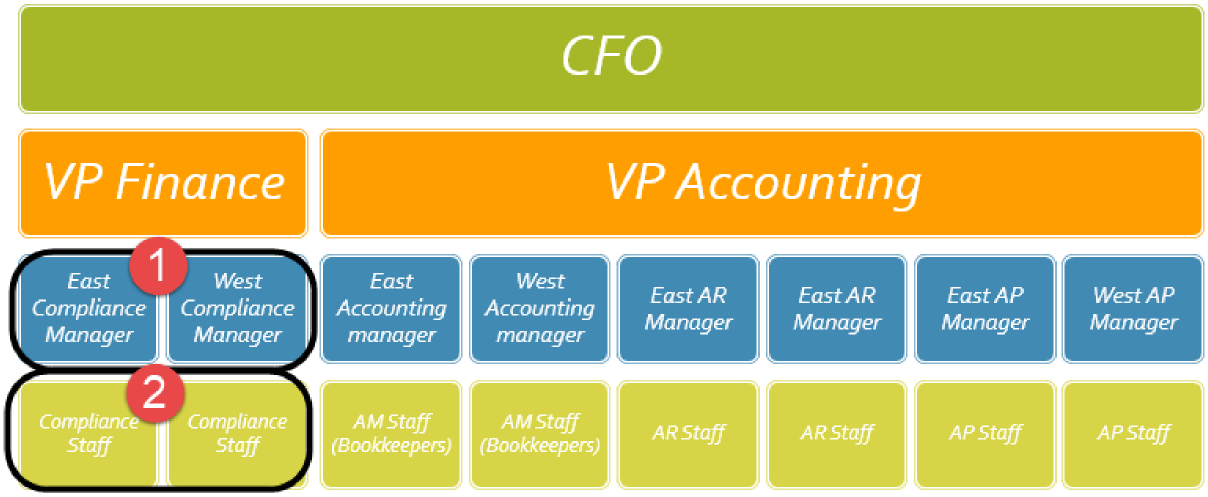
AP Manager

Compliance Staff

AM Staff (Bookkeepers)

AR Staff

AP Staff



CFO

VP Finance

VP Accounting

1

East Compliance Manager

West Compliance Manager

East Accounting manager

West Accounting manager

East AR Manager

East AR Manager

East AP Manager

West AP Manager

2

Compliance Staff

Compliance Staff

AM Staff (Bookkeepers)

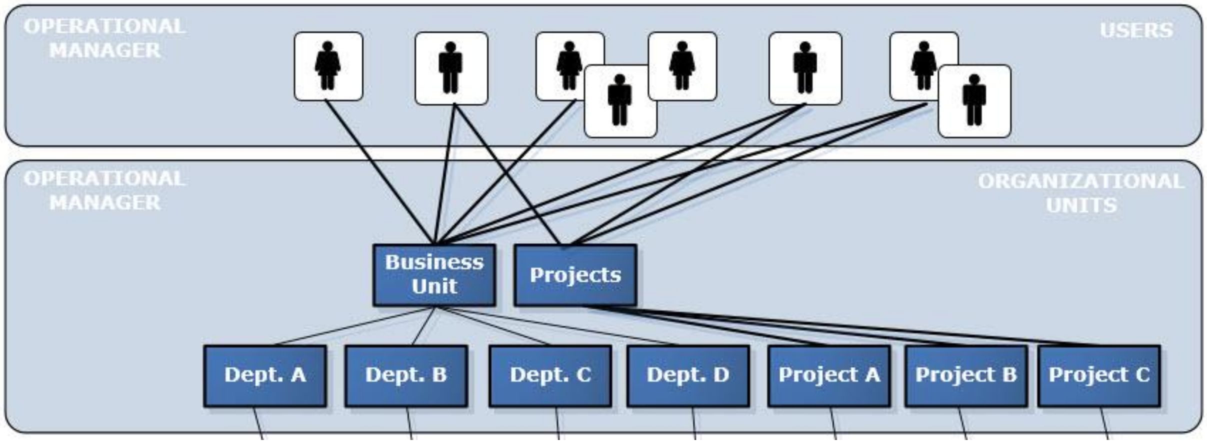
AM Staff (Bookkeepers)

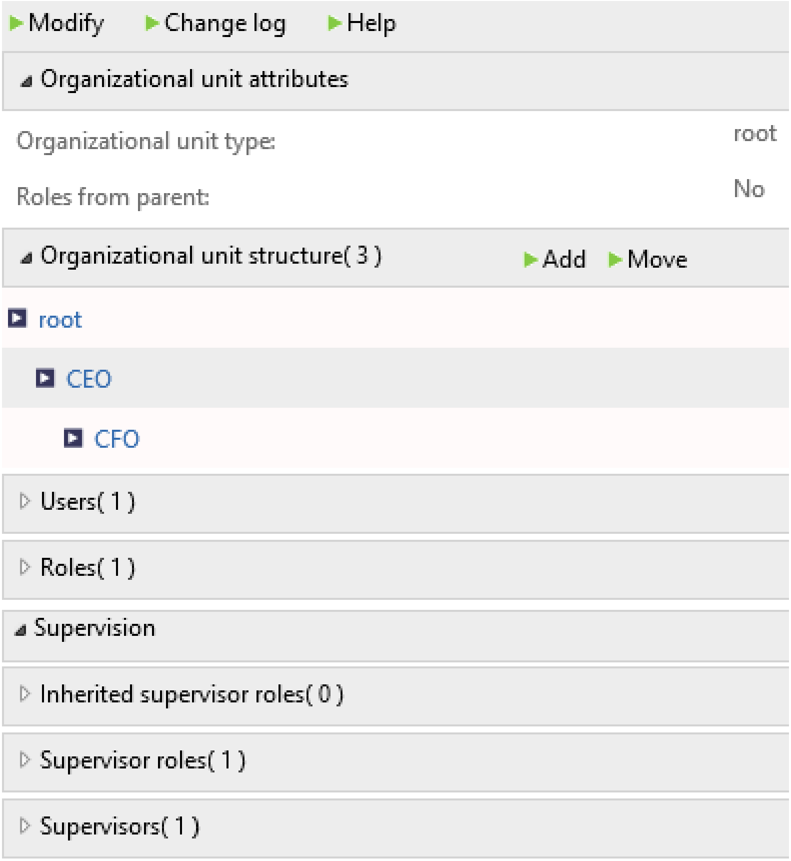
AR Staff

AR Staff

AP Staff

AP Staff





◢ Organizational unit attributes

Organizational unit type: root

Roles from parent: No

◢ Organizational unit structure(3)

- root
  - CEO
    - CFO

▷ Users(1)

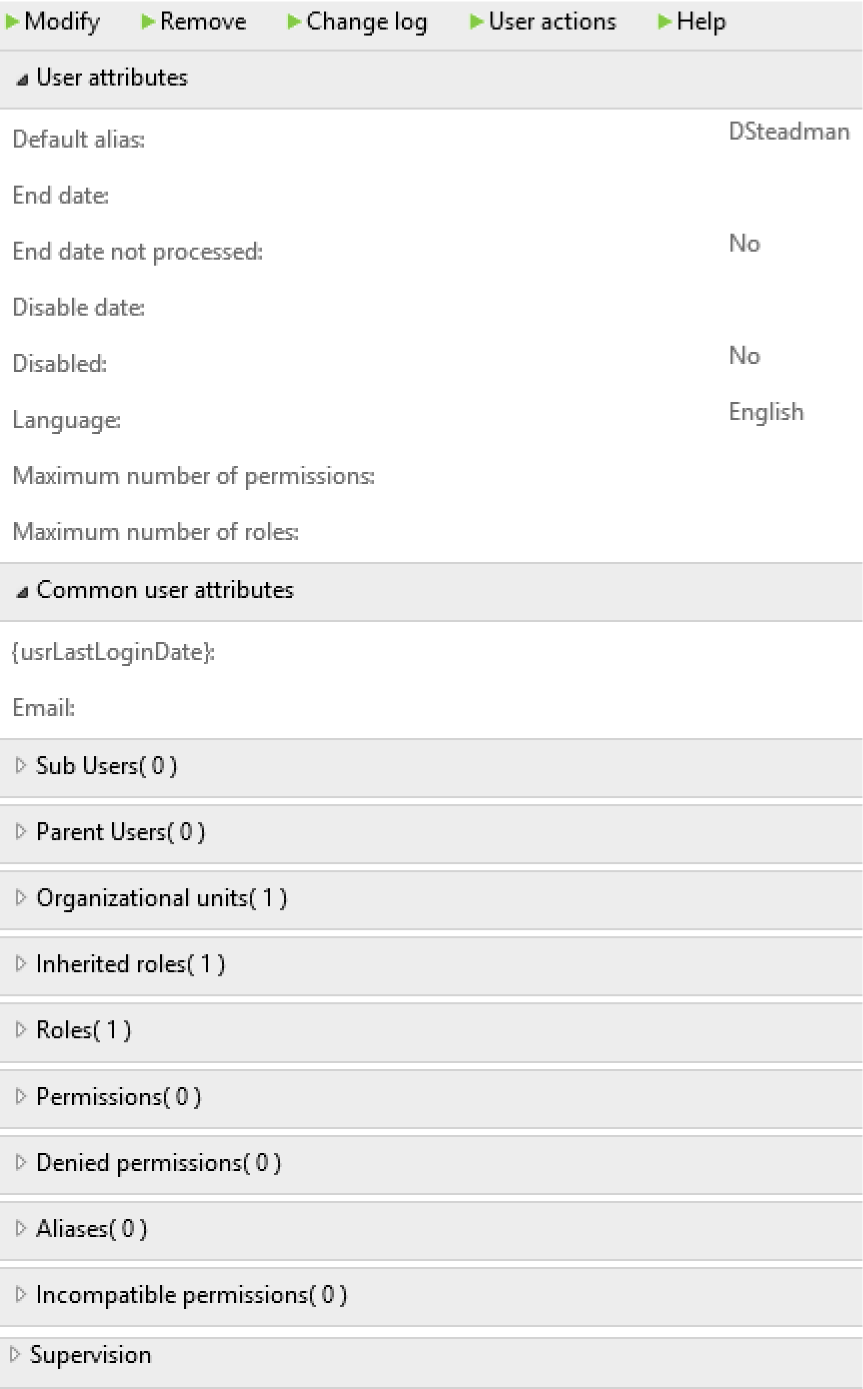
▷ Roles(1)

◢ Supervision

▷ Inherited supervisor roles(0)

▷ Supervisor roles(1)

▷ Supervisors(1)



◢ User attributes

Default alias: DSteadman

End date:

End date not processed: No

Disable date:

Disabled: No

Language: English

Maximum number of permissions:

Maximum number of roles:

◢ Common user attributes

{usrLastLoginDate}:

Email:

▷ Sub Users(0)

▷ Parent Users(0)

▷ Organizational units(1)

▷ Inherited roles(1)

▷ Roles(1)

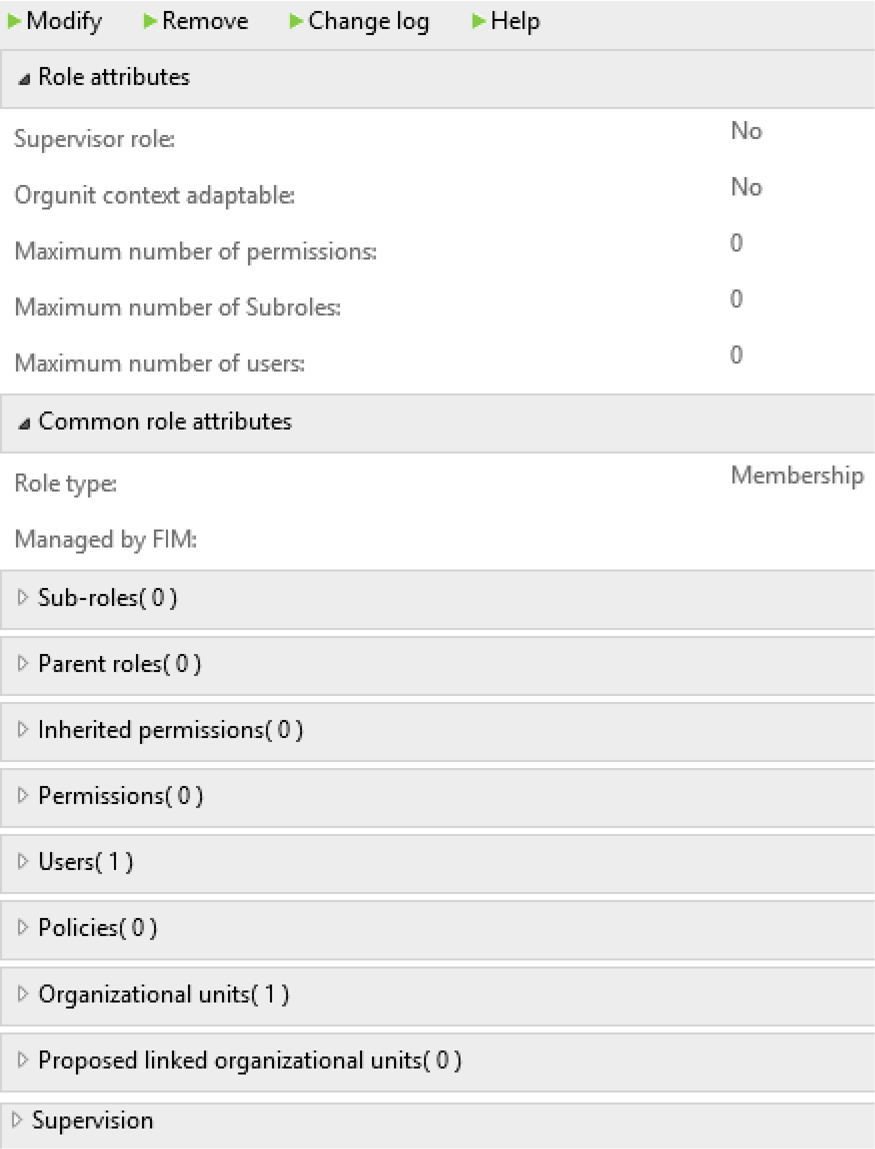
▷ Permissions(0)

▷ Denied permissions(0)

▷ Aliases(0)

▷ Incompatible permissions(0)

▷ Supervision



Role attributes

Supervisor role:	No
Orgunit context adaptable:	No
Maximum number of permissions:	0
Maximum number of Subroles:	0
Maximum number of users:	0

Common role attributes

Role type:	Membership
Managed by FIM:	

Sub-roles(0)

Parent roles(0)

Inherited permissions(0)

Permissions(0)

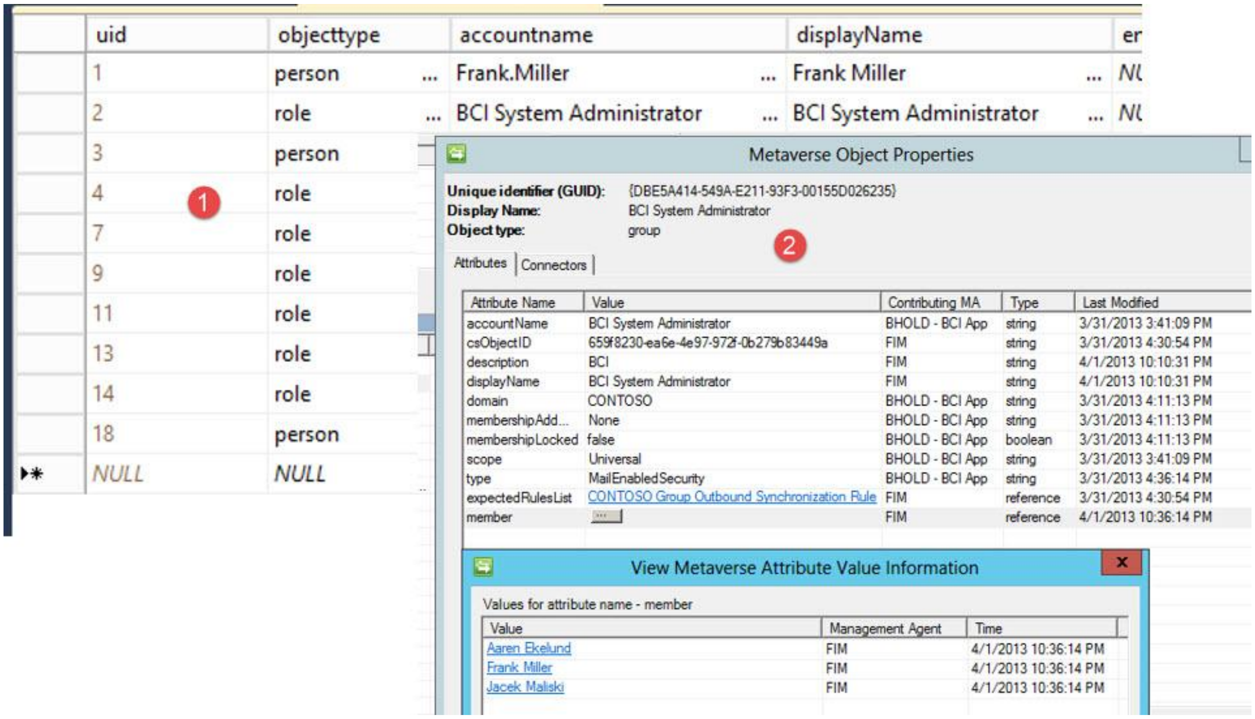
Users(1)

Policies(0)

Organizational units(1)

Proposed linked organizational units(0)

Supervision



	uid	objecttype	accountname	displayName	er
	1	person ...	Frank.Miller ...	Frank Miller ...	NU
	2	role ...	BCI System Administrator ...	BCI System Administrator ...	NU
	3	person			
	4	role			
	7	role			
	9	role			
	11	role			
	13	role			
	14	role			
	18	person			
▸✱	NULL	NULL			

Metaverse Object Properties

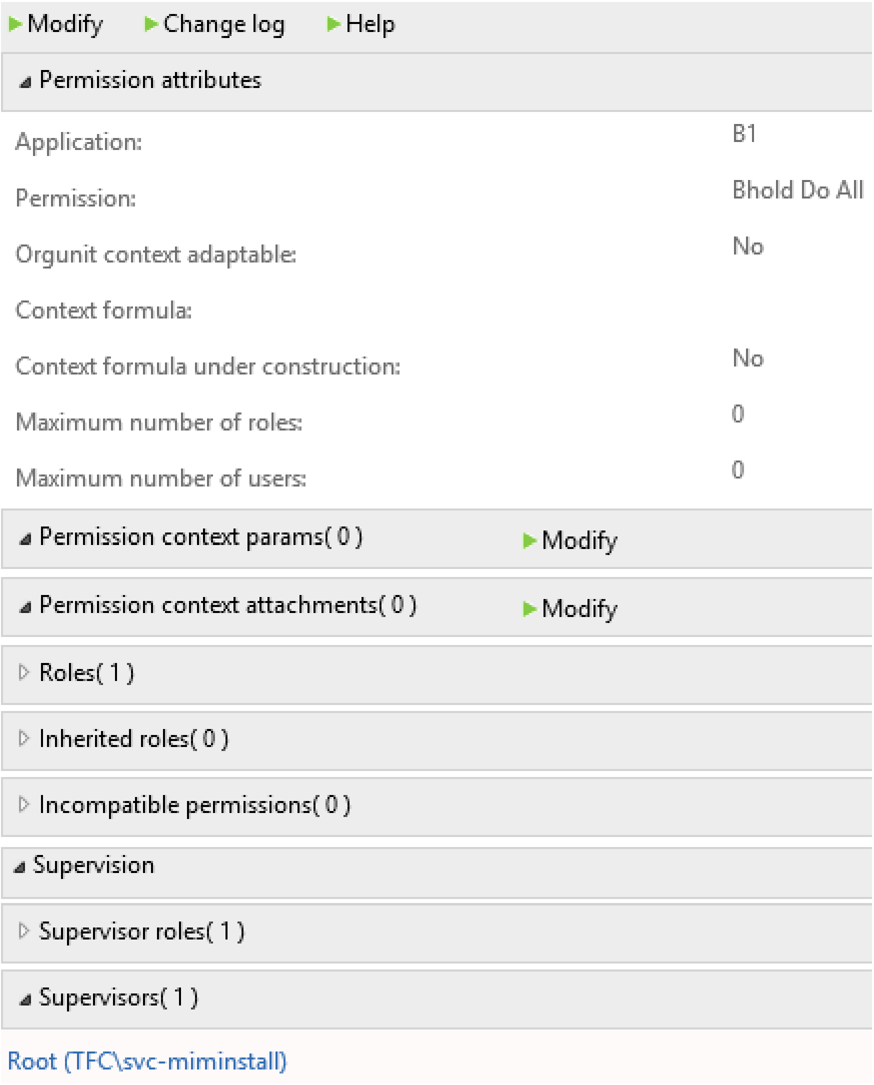
Unique identifier (GUID): {DBE5A414-549A-E211-93F3-00155D026235}
Display Name: BCI System Administrator
Object type: group

Attribute Name	Value	Contributing MA	Type	Last Modified
accountName	BCI System Administrator	BHOLD - BCI App	string	3/31/2013 3:41:09 PM
csObjectID	659f8230-ea6e-4e97-972f-0b279b83449a	FIM	string	3/31/2013 4:30:54 PM
description	BCI	FIM	string	4/1/2013 10:10:31 PM
displayName	BCI System Administrator	FIM	string	4/1/2013 10:10:31 PM
domain	CONTOSO	BHOLD - BCI App	string	3/31/2013 4:11:13 PM
membershipAdd...	None	BHOLD - BCI App	string	3/31/2013 4:11:13 PM
membershipLocked	false	BHOLD - BCI App	boolean	3/31/2013 4:11:13 PM
scope	Universal	BHOLD - BCI App	string	3/31/2013 3:41:09 PM
type	MailEnabledSecurity	BHOLD - BCI App	string	3/31/2013 4:36:14 PM
expectedRulesList	CONTOSO Group Outbound Synchronization Rule	FIM	reference	3/31/2013 4:30:54 PM
member	...	FIM	reference	4/1/2013 10:36:14 PM

View Metaverse Attribute Value Information

Values for attribute name - member

Value	Management Agent	Time
Aaren Ekelund	FIM	4/1/2013 10:36:14 PM
Frank Miller	FIM	4/1/2013 10:36:14 PM
Jacek Maliski	FIM	4/1/2013 10:36:14 PM



▶ Modify ▶ Change log ▶ Help

◢ Permission attributes

Application:	B1
Permission:	Bhold Do All
Orgunit context adaptable:	No
Context formula:	
Context formula under construction:	No
Maximum number of roles:	0
Maximum number of users:	0

◢ Permission context params(0) ▶ Modify

◢ Permission context attachments(0) ▶ Modify

▷ Roles(1)

▷ Inherited roles(0)

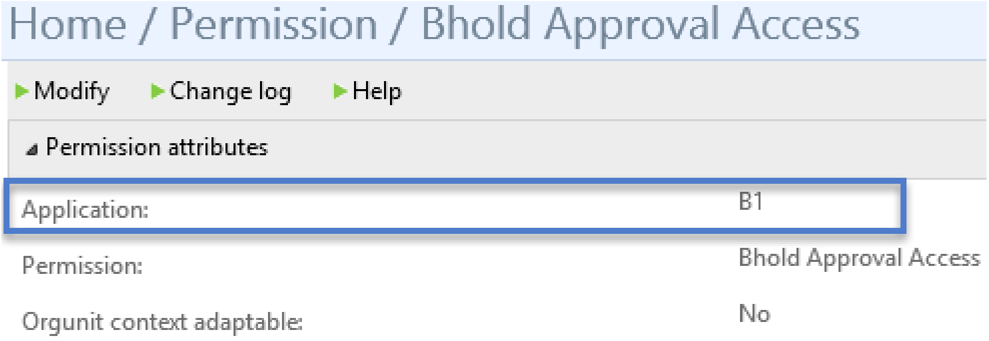
▷ Incompatible permissions(0)

◢ Supervision

▷ Supervisor roles(1)

◢ Supervisors(1)

Root (TFC\svc-miminstall)

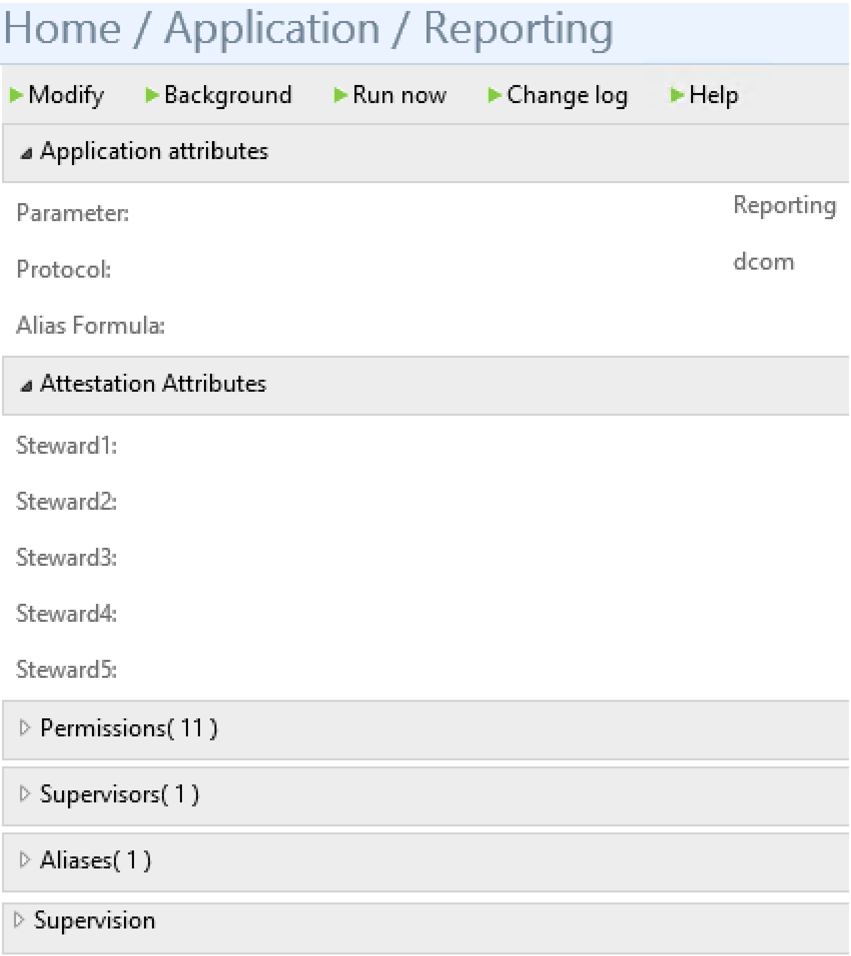


Home / Permission / Bhold Approval Access

▶ Modify ▶ Change log ▶ Help

◢ Permission attributes

Application:	B1
Permission:	Bhold Approval Access
Orgunit context adaptable:	No



Home / Application / Reporting

◢ Application attributes

Parameter: Reporting

Protocol: dcom

Alias Formula:

◢ Attestation Attributes

Steward1:

Steward2:

Steward3:

Steward4:

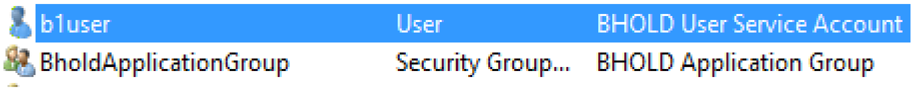
Steward5:

▷ Permissions(11)

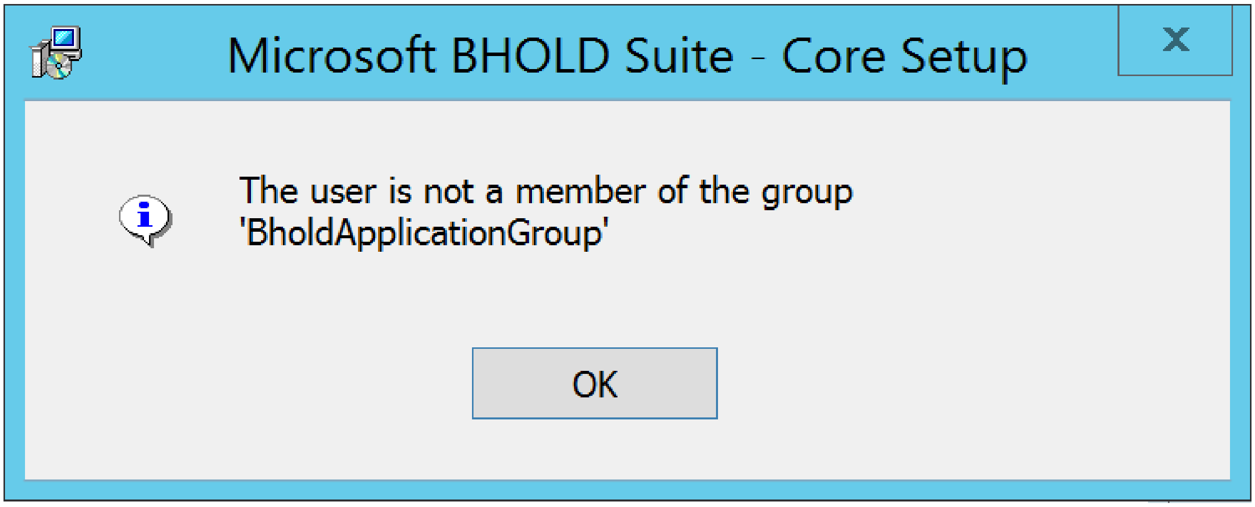
▷ Supervisors(1)

▷ Aliases(1)

▷ Supervision

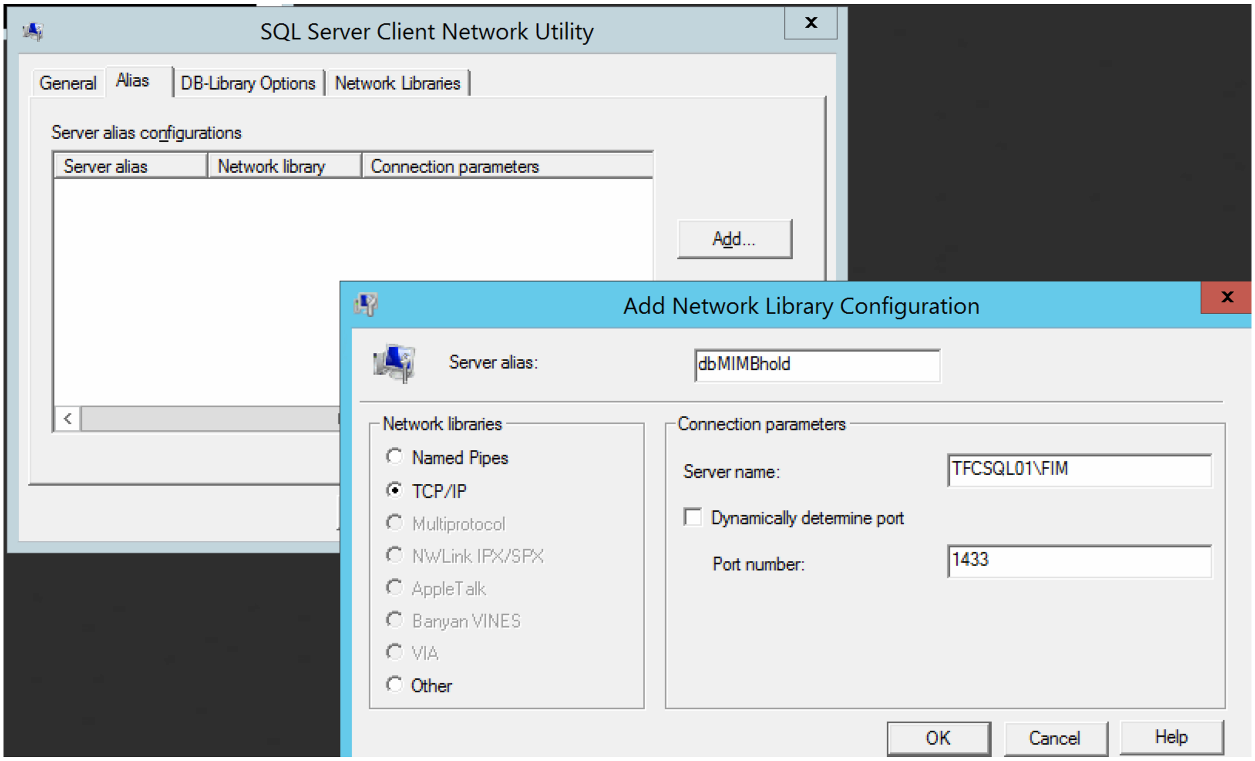


b1user	User	BHOLD User Service Account
BholdApplicationGroup	Security Group...	BHOLD Application Group



Microsoft BHOLD Suite - Core Setup

The user is not a member of the group 'BholdApplicationGroup'


SQL Server Client Network Utility
General
Alias
DB-Library Options
Network Libraries
Add...
Add Network Library Configuration
OK
Cancel
Help

Server alias configurations

Server alias	Network library	Connection parameters

Server alias: dbMIMBhold

Network libraries

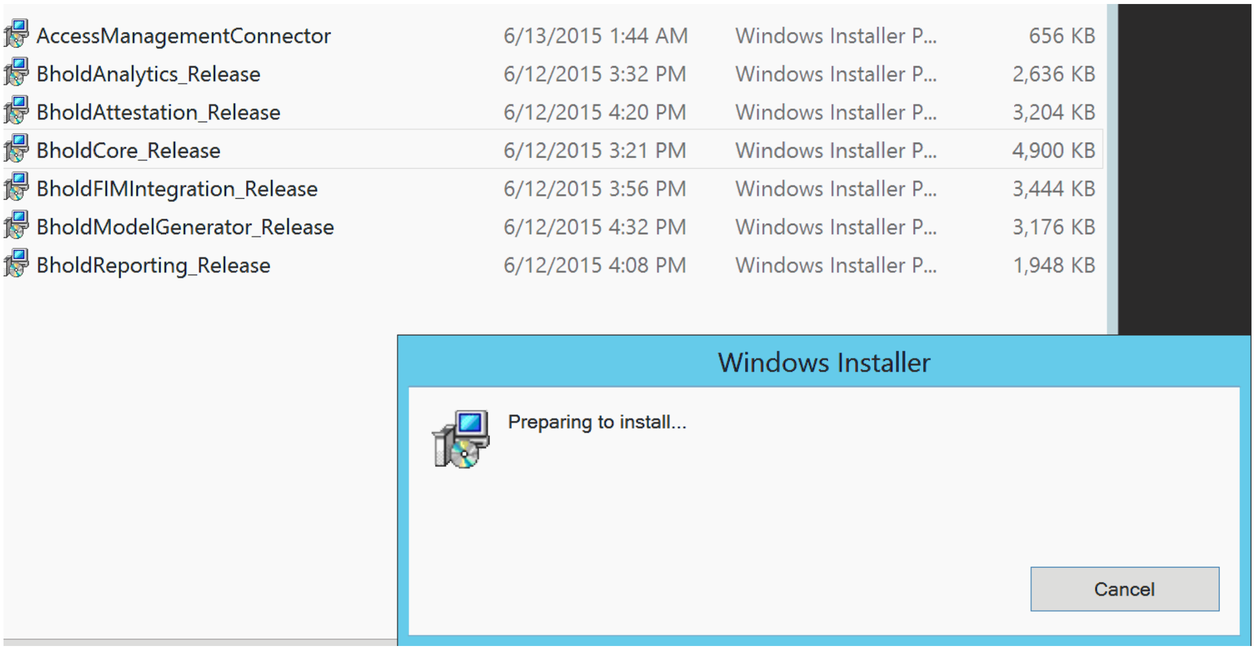
○ Named Pipes
● TCP/IP
○ Multiprotocol
○ NWLink IPX/SPX
○ AppleTalk
○ Banyan VINES
○ VIA
○ Other

Connection parameters

Server name: TFCSQL01\FIM

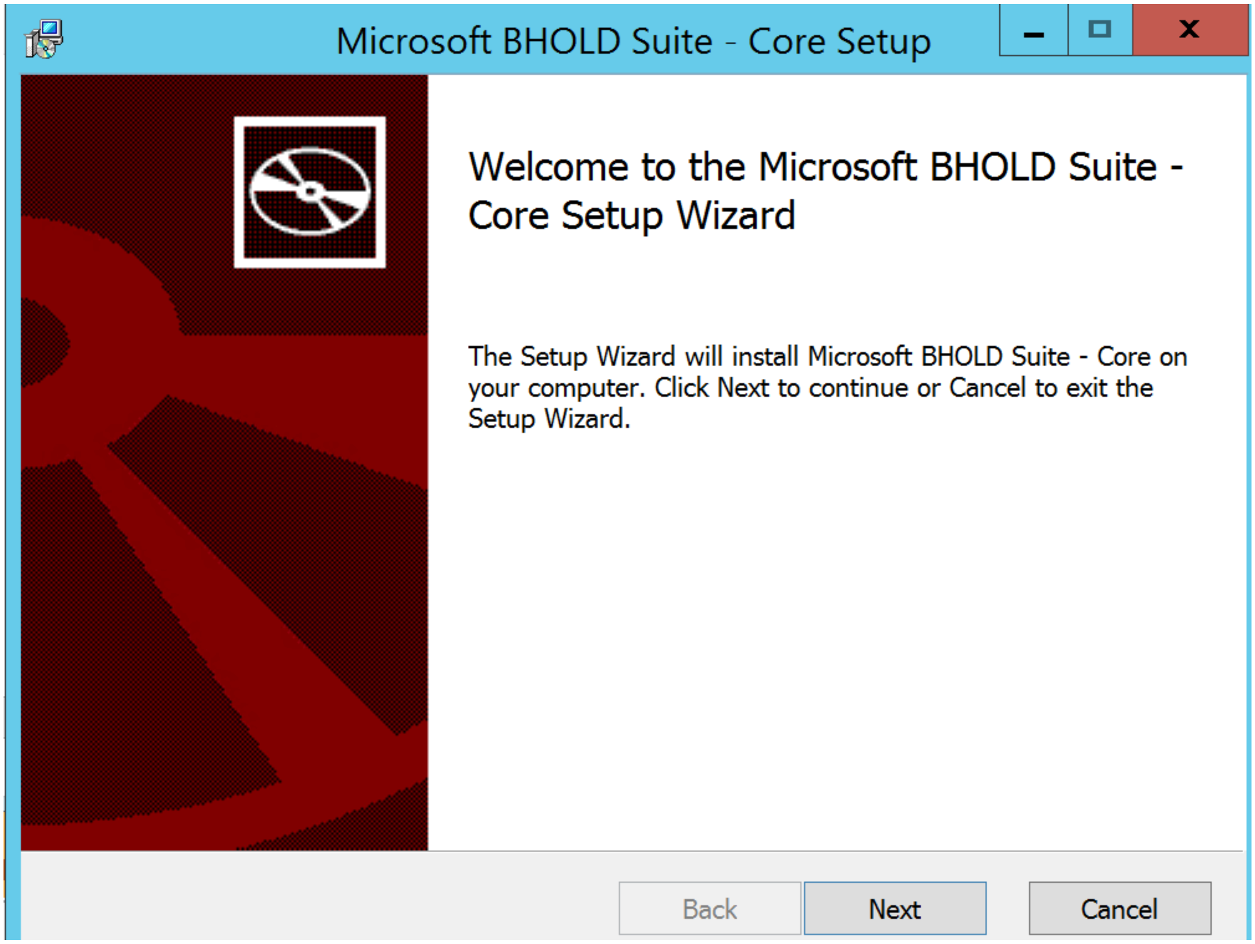
□ Dynamically determine port

Port number: 1433



AccessManagementConnector	6/13/2015 1:44 AM	Windows Installer P...	656 KB
BholdAnalytics_Release	6/12/2015 3:32 PM	Windows Installer P...	2,636 KB
BholdAttestation_Release	6/12/2015 4:20 PM	Windows Installer P...	3,204 KB
BholdCore_Release	6/12/2015 3:21 PM	Windows Installer P...	4,900 KB
BholdFIMIntegration_Release	6/12/2015 3:56 PM	Windows Installer P...	3,444 KB
BholdModelGenerator_Release	6/12/2015 4:32 PM	Windows Installer P...	3,176 KB
BholdReporting_Release	6/12/2015 4:08 PM	Windows Installer P...	1,948 KB

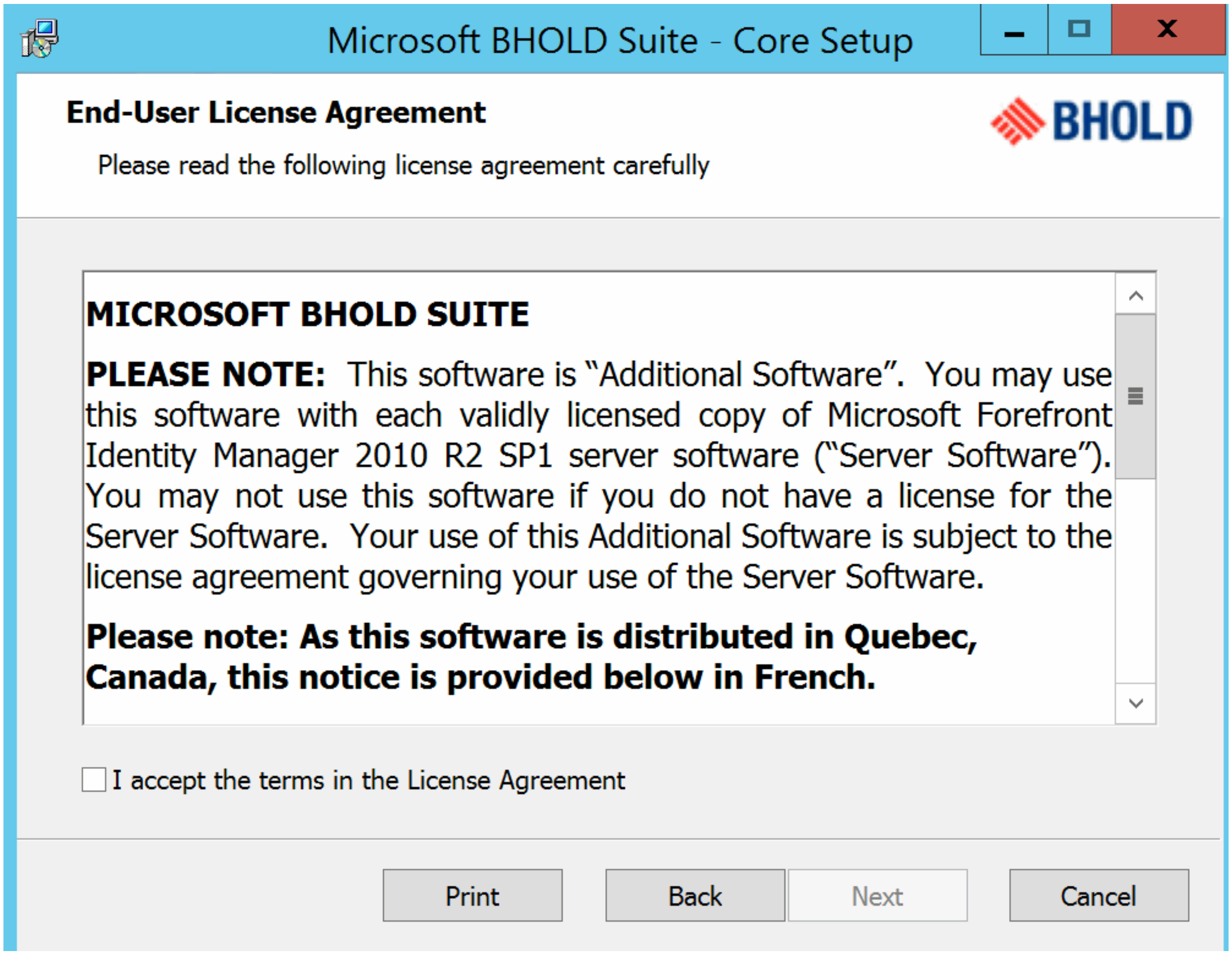
Preparing to install...



Microsoft BHOLD Suite - Core Setup

Welcome to the Microsoft BHOLD Suite - Core Setup Wizard

The Setup Wizard will install Microsoft BHOLD Suite - Core on your computer. Click Next to continue or Cancel to exit the Setup Wizard.



End-User License Agreement

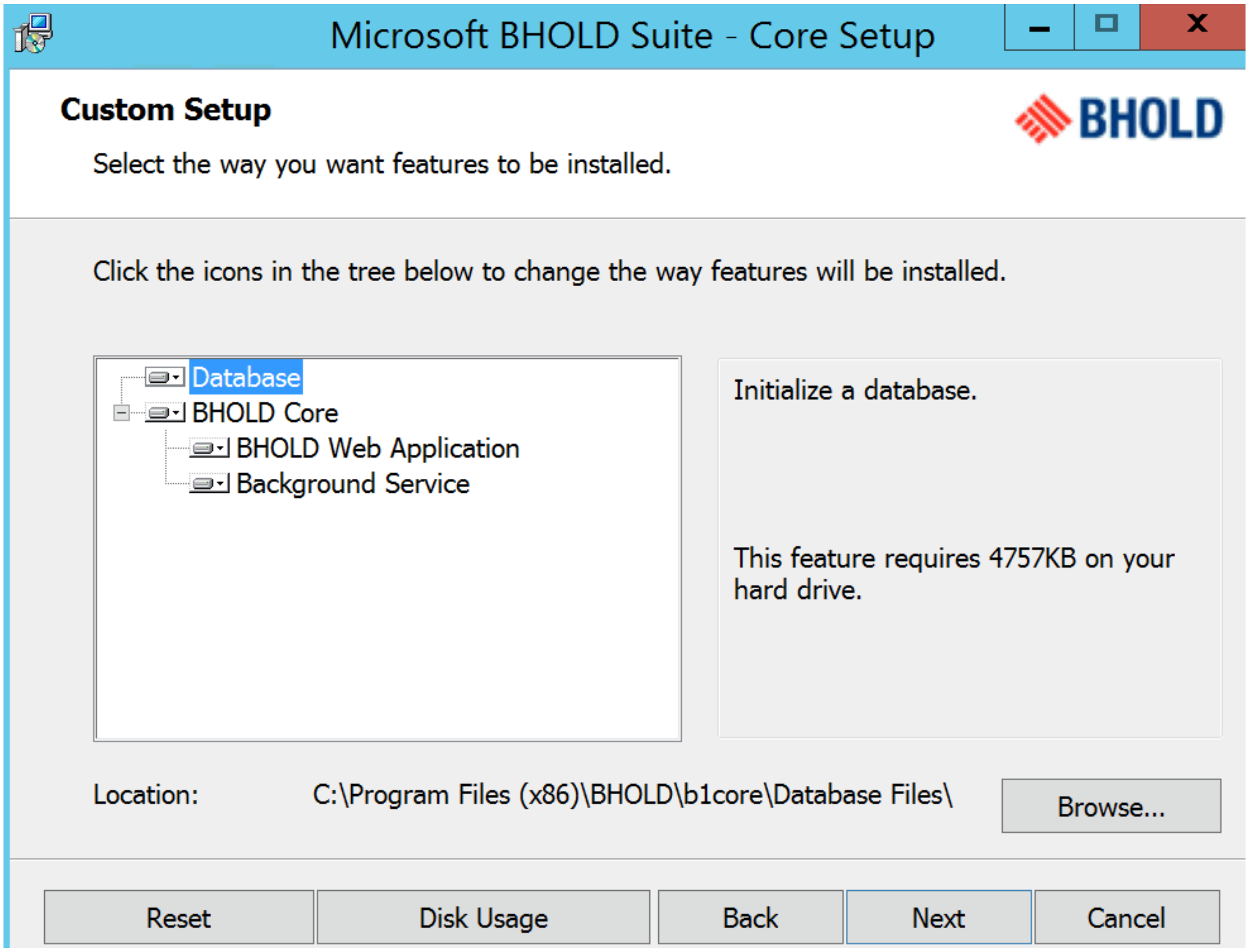
Please read the following license agreement carefully

MICROSOFT BHOLD SUITE

PLEASE NOTE: This software is "Additional Software". You may use this software with each validly licensed copy of Microsoft Forefront Identity Manager 2010 R2 SP1 server software ("Server Software"). You may not use this software if you do not have a license for the Server Software. Your use of this Additional Software is subject to the license agreement governing your use of the Server Software.

Please note: As this software is distributed in Quebec, Canada, this notice is provided below in French.

□ I accept the terms in the License Agreement



Microsoft BHOLD Suite - Core Setup

Custom Setup

Select the way you want features to be installed.

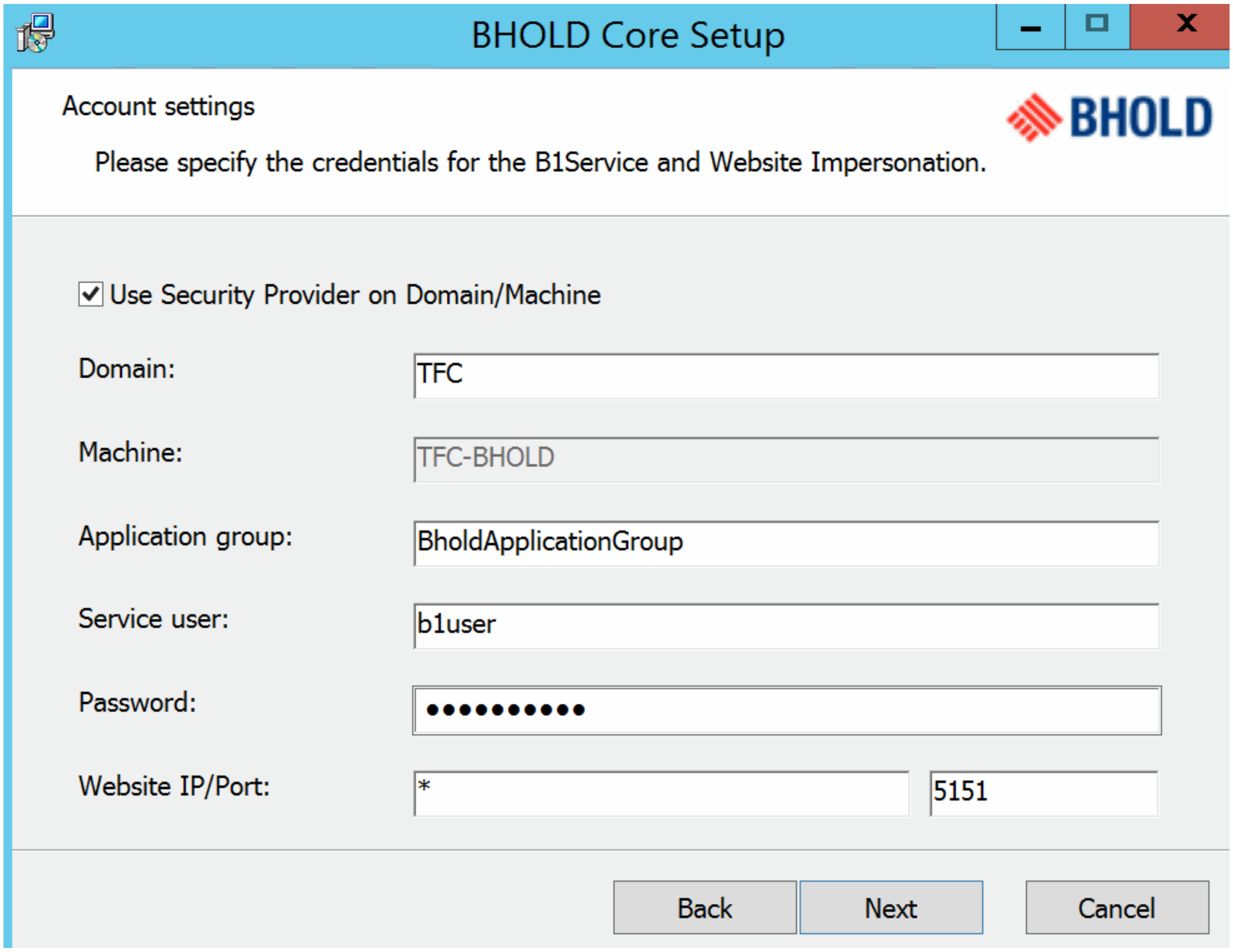
Click the icons in the tree below to change the way features will be installed.

- Database
- BHOLD Core
  - BHOLD Web Application
  - Background Service

Initialize a database.

This feature requires 4757KB on your hard drive.

Location: C:\Program Files (x86)\BHOLD\b1core\Database Files\



Account settings

Please specify the credentials for the B1Service and Website Impersonation.

☑ Use Security Provider on Domain/Machine

Domain: TFC

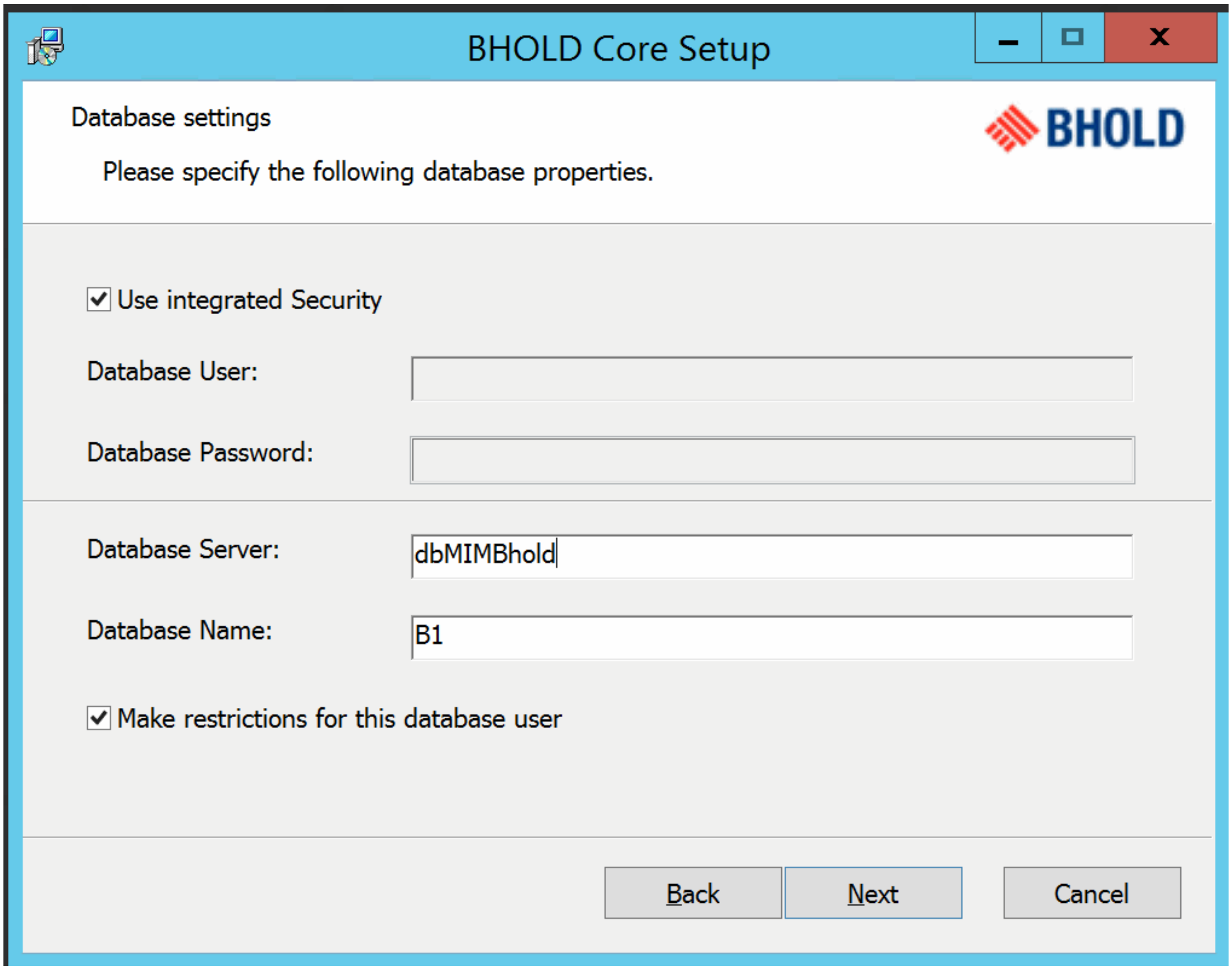
Machine: TFC-BHOLD

Application group: BholdApplicationGroup

Service user: b1user

Password: ●●●●●●●●●●

Website IP/Port: * 5151



Database settings

Please specify the following database properties.

☑ Use integrated Security

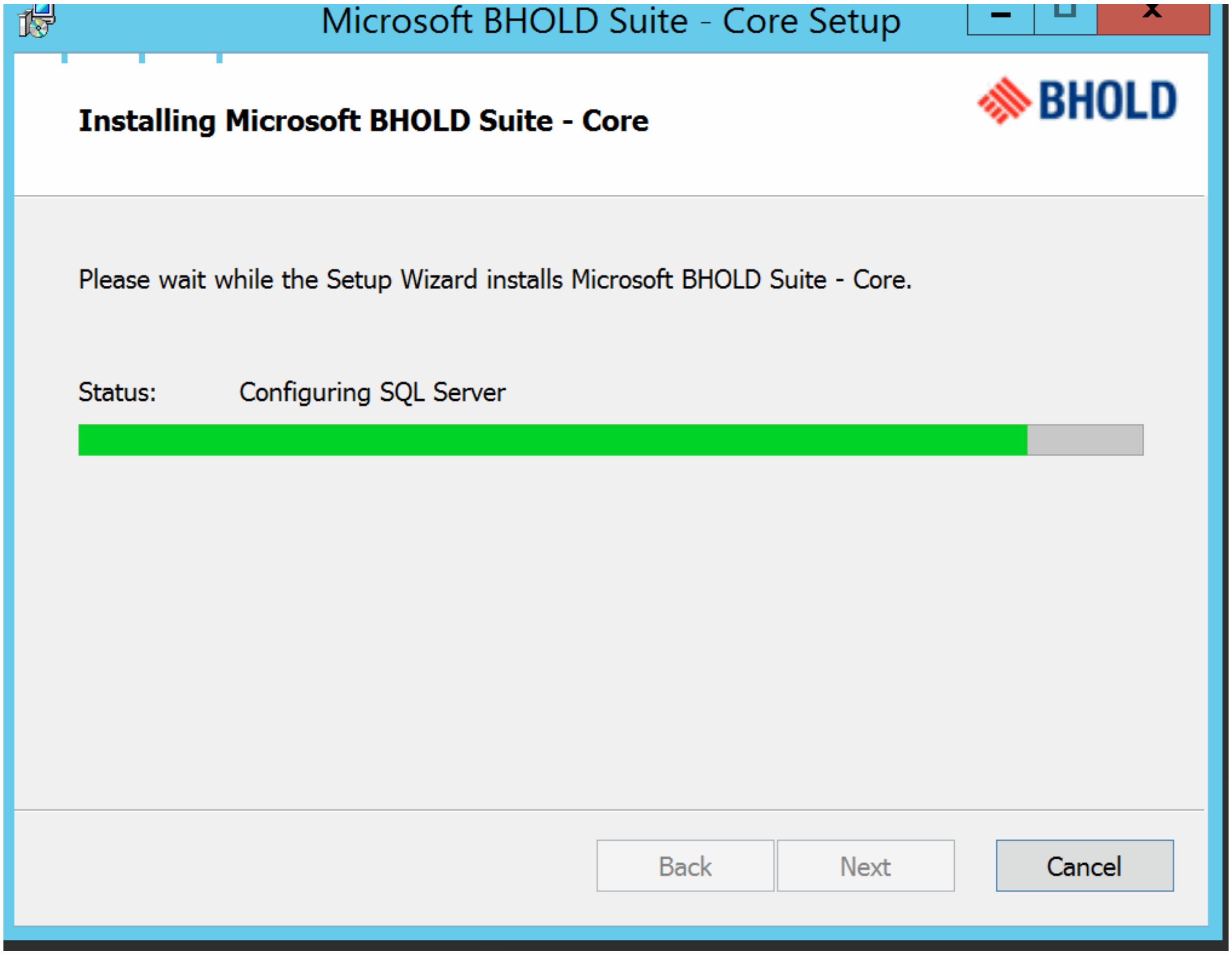
Database User:

Database Password:

Database Server: dbMIMBhold

Database Name: B1

☑ Make restrictions for this database user

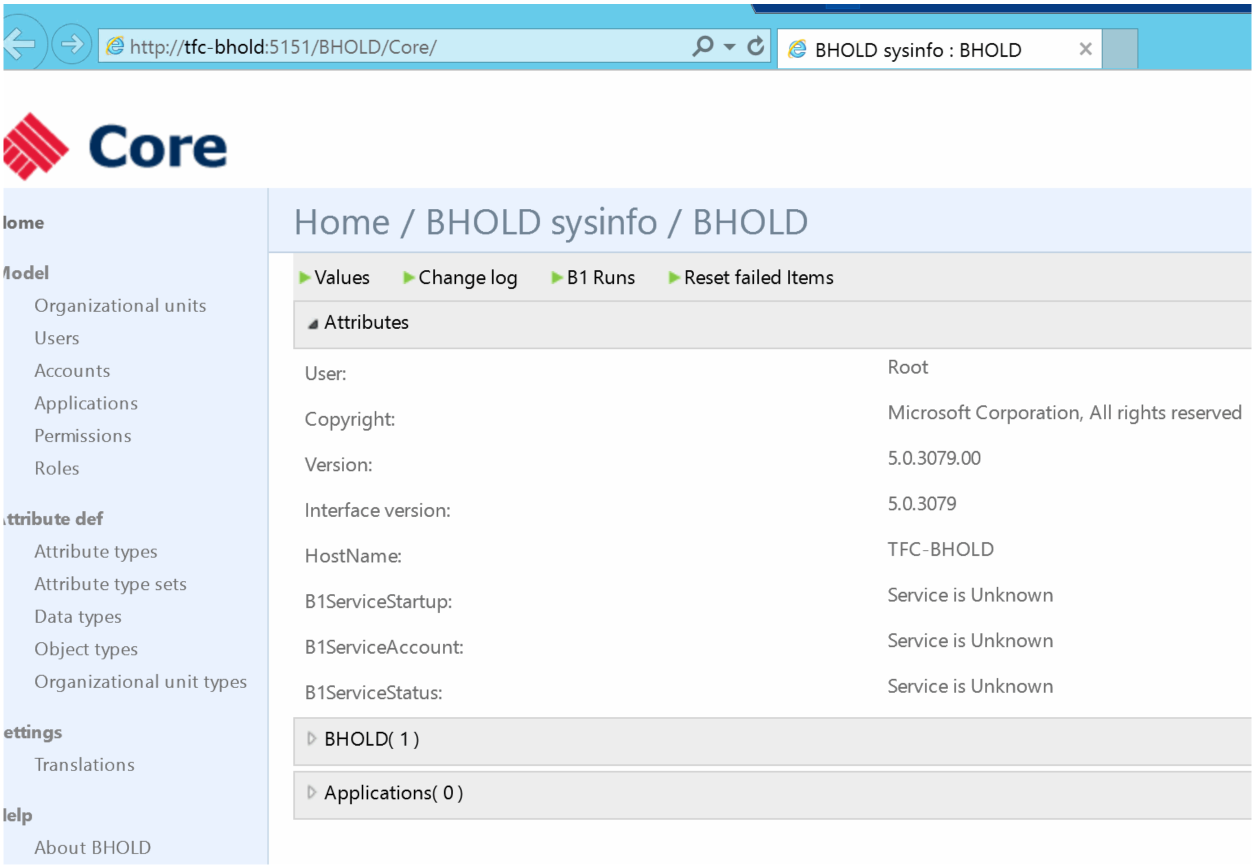


Microsoft BHOLD Suite - Core Setup

Installing Microsoft BHOLD Suite - Core

Please wait while the Setup Wizard installs Microsoft BHOLD Suite - Core.

Status: Configuring SQL Server



Home / BHOLD sysinfo / BHOLD

User: Root

Copyright: Microsoft Corporation, All rights reserved

Version: 5.0.3079.00

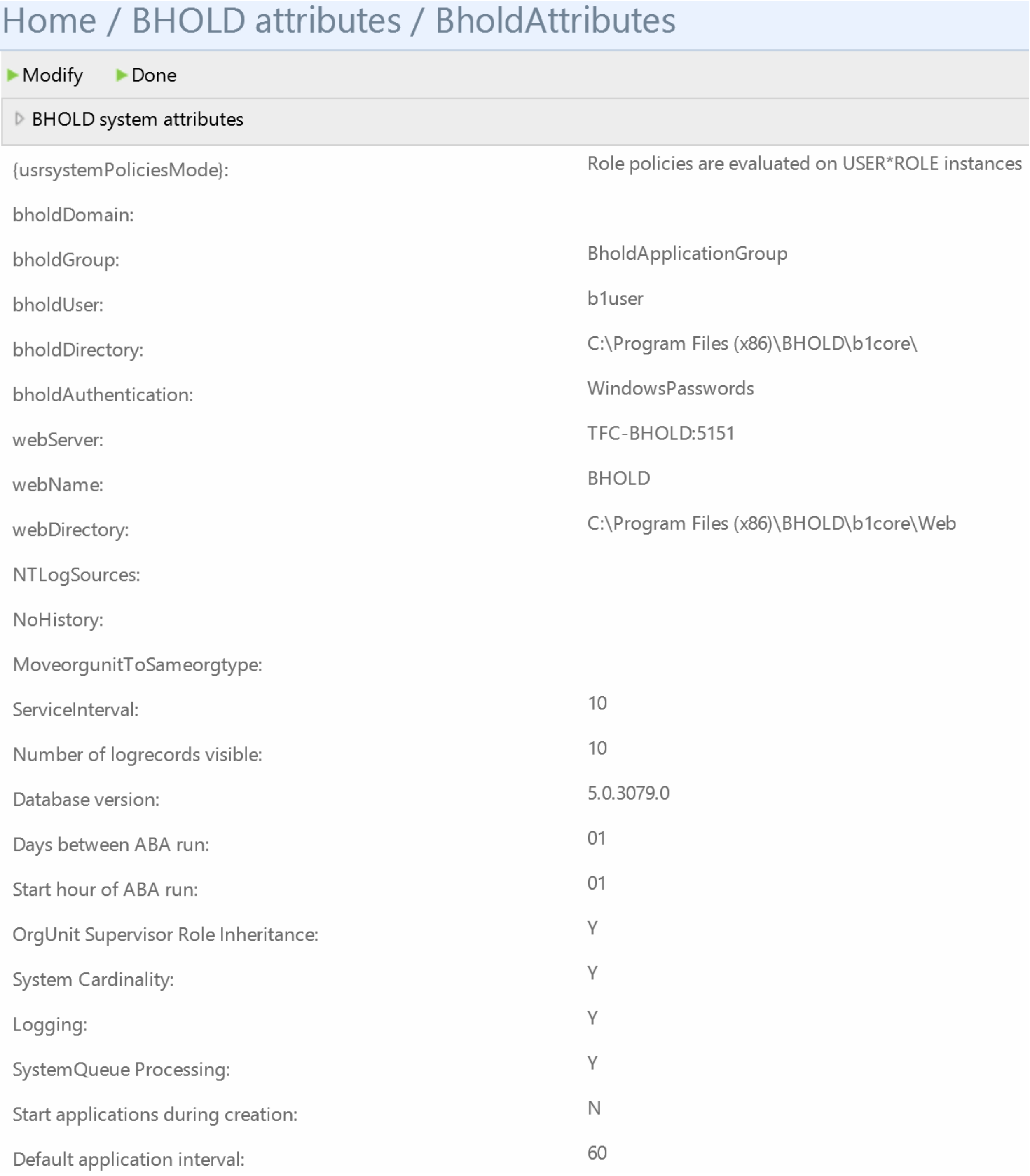
Interface version: 5.0.3079

HostName: TFC-BHOLD

B1ServiceStartup: Service is Unknown

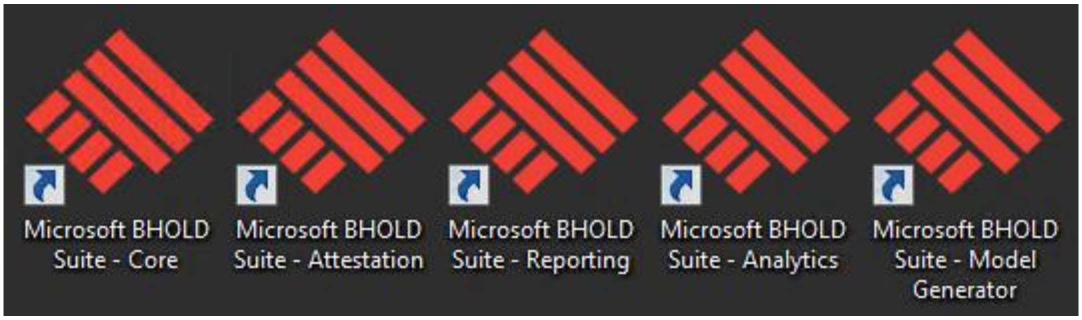
B1ServiceAccount: Service is Unknown

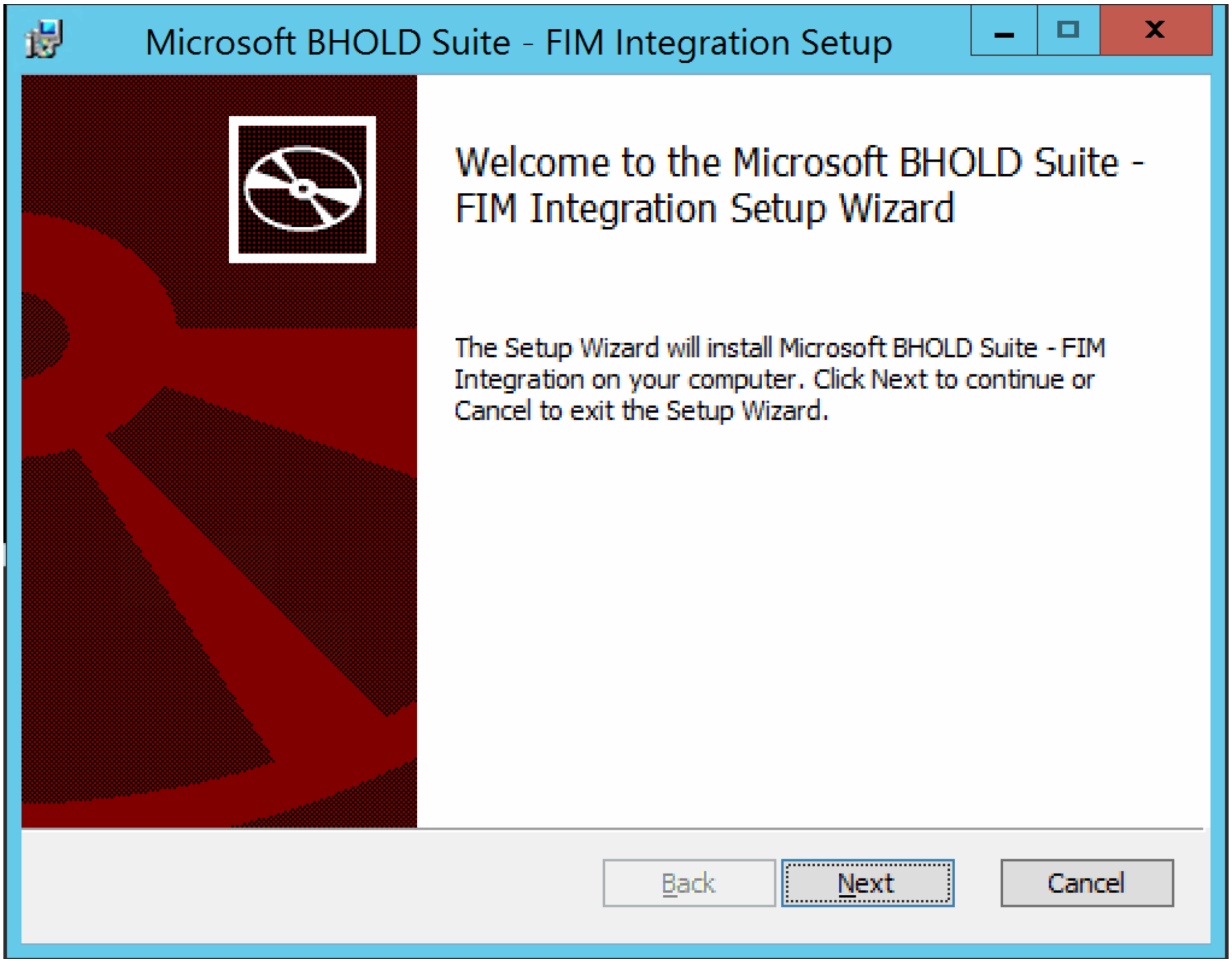
B1ServiceStatus: Service is Unknown



Home / BHOLD attributes / BholdAttributes

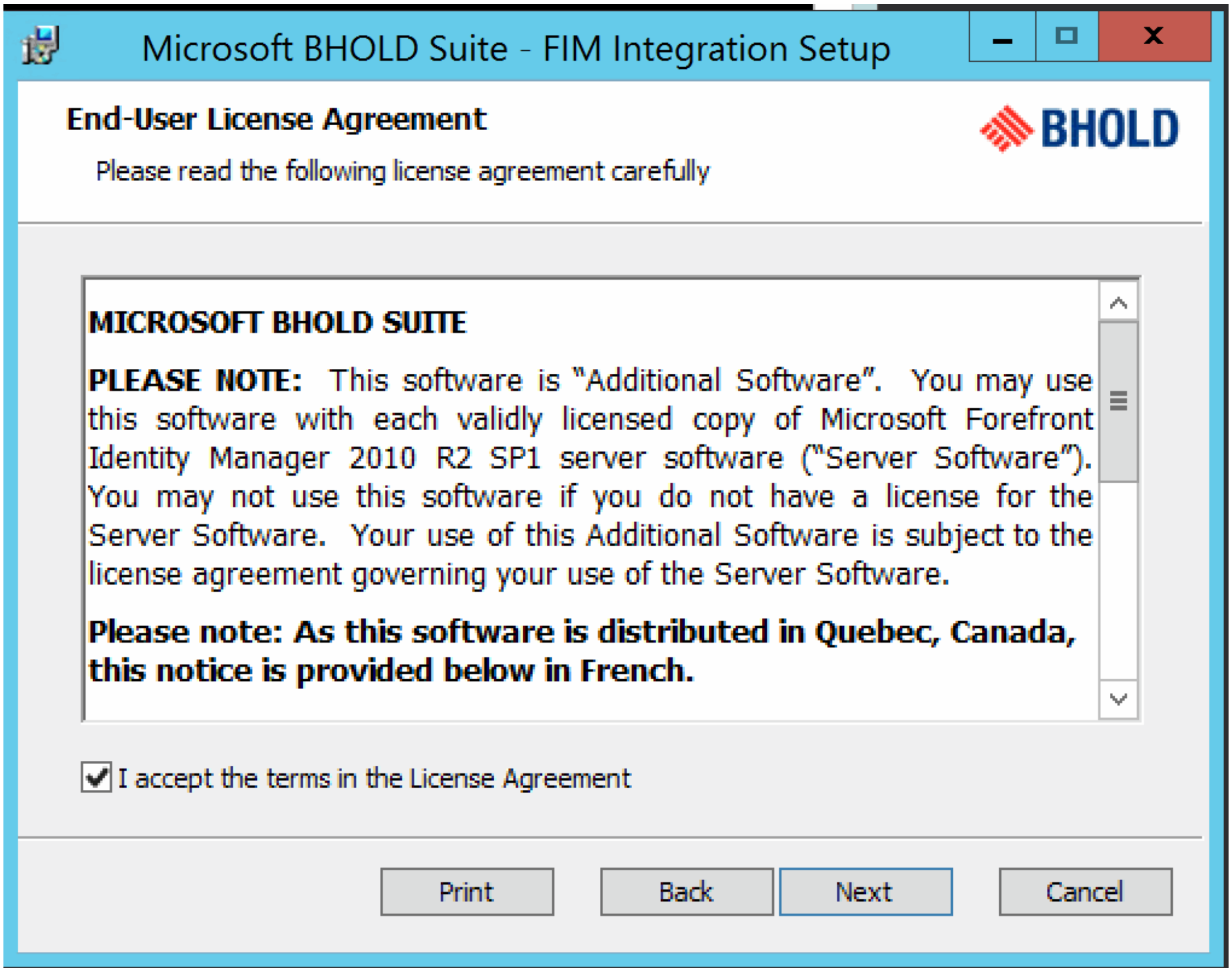
{usrsystemPoliciesMode}:	Role policies are evaluated on USER*ROLE instances
bholdDomain:	
bholdGroup:	BholdApplicationGroup
bholdUser:	b1user
bholdDirectory:	C:\Program Files (x86)\BHOLD\b1core\
bholdAuthentication:	WindowsPasswords
webServer:	TFC-BHOLD:5151
webName:	BHOLD
webDirectory:	C:\Program Files (x86)\BHOLD\b1core\Web
NTLogSources:	
NoHistory:	
MoveorgunitToSameorgtype:	
ServiceInterval:	10
Number of logrecords visible:	10
Database version:	5.0.3079.0
Days between ABA run:	01
Start hour of ABA run:	01
OrgUnit Supervisor Role Inheritance:	Y
System Cardinality:	Y
Logging:	Y
SystemQueue Processing:	Y
Start applications during creation:	N
Default application interval:	60


Microsoft BHOLD Suite - Core
Microsoft BHOLD Suite - Attestation
Microsoft BHOLD Suite - Reporting
Microsoft BHOLD Suite - Analytics
Microsoft BHOLD Suite - Model Generator


Microsoft BHOLD Suite - FIM Integration Setup

Welcome to the Microsoft BHOLD Suite - FIM Integration Setup Wizard

The Setup Wizard will install Microsoft BHOLD Suite - FIM Integration on your computer. Click Next to continue or Cancel to exit the Setup Wizard.



End-User License Agreement

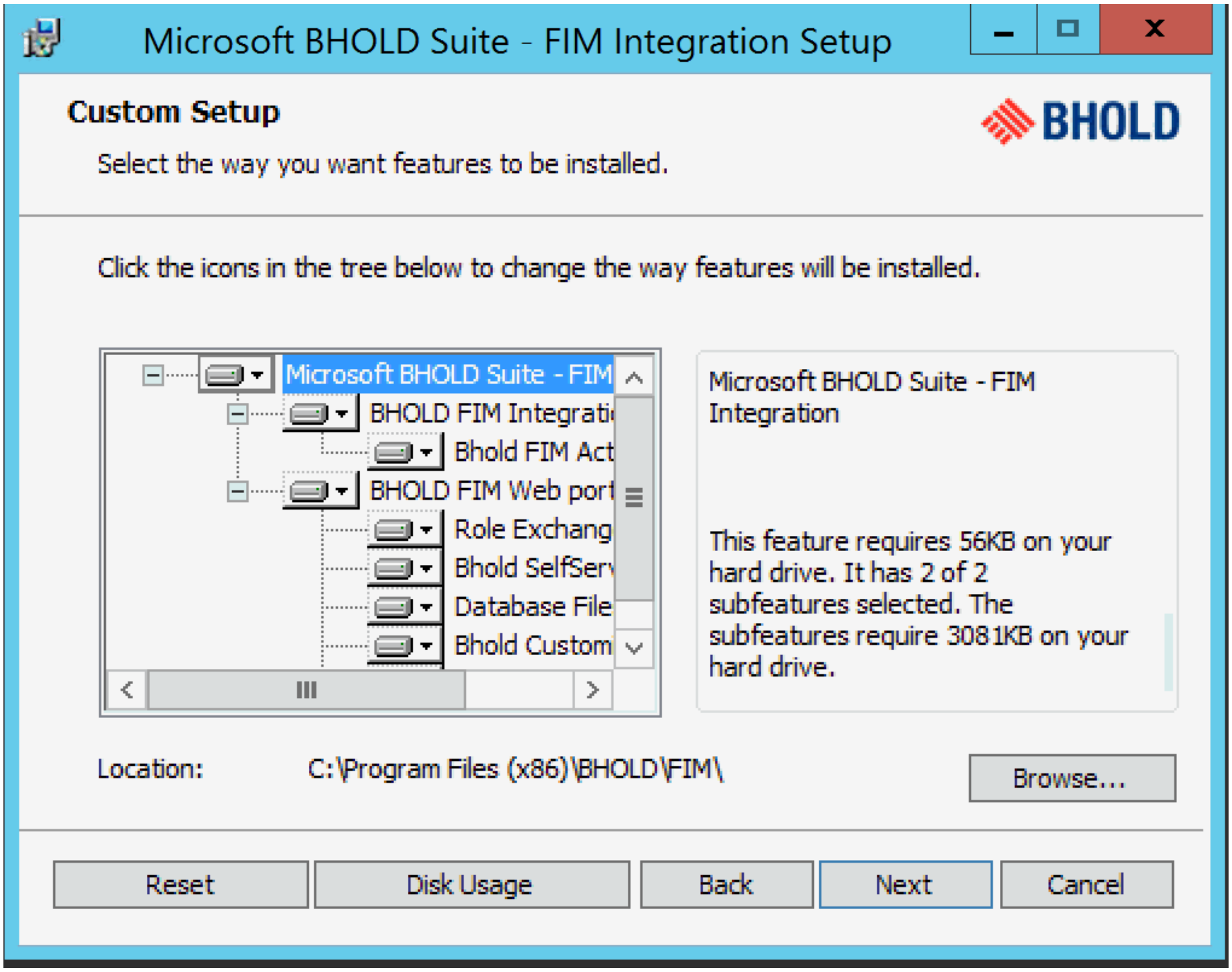
Please read the following license agreement carefully

MICROSOFT BHOLD SUITE

PLEASE NOTE: This software is "Additional Software". You may use this software with each validly licensed copy of Microsoft Forefront Identity Manager 2010 R2 SP1 server software ("Server Software"). You may not use this software if you do not have a license for the Server Software. Your use of this Additional Software is subject to the license agreement governing your use of the Server Software.

Please note: As this software is distributed in Quebec, Canada, this notice is provided below in French.

☑ I accept the terms in the License Agreement



Microsoft BHOLD Suite - FIM Integration Setup

Custom Setup

Select the way you want features to be installed.

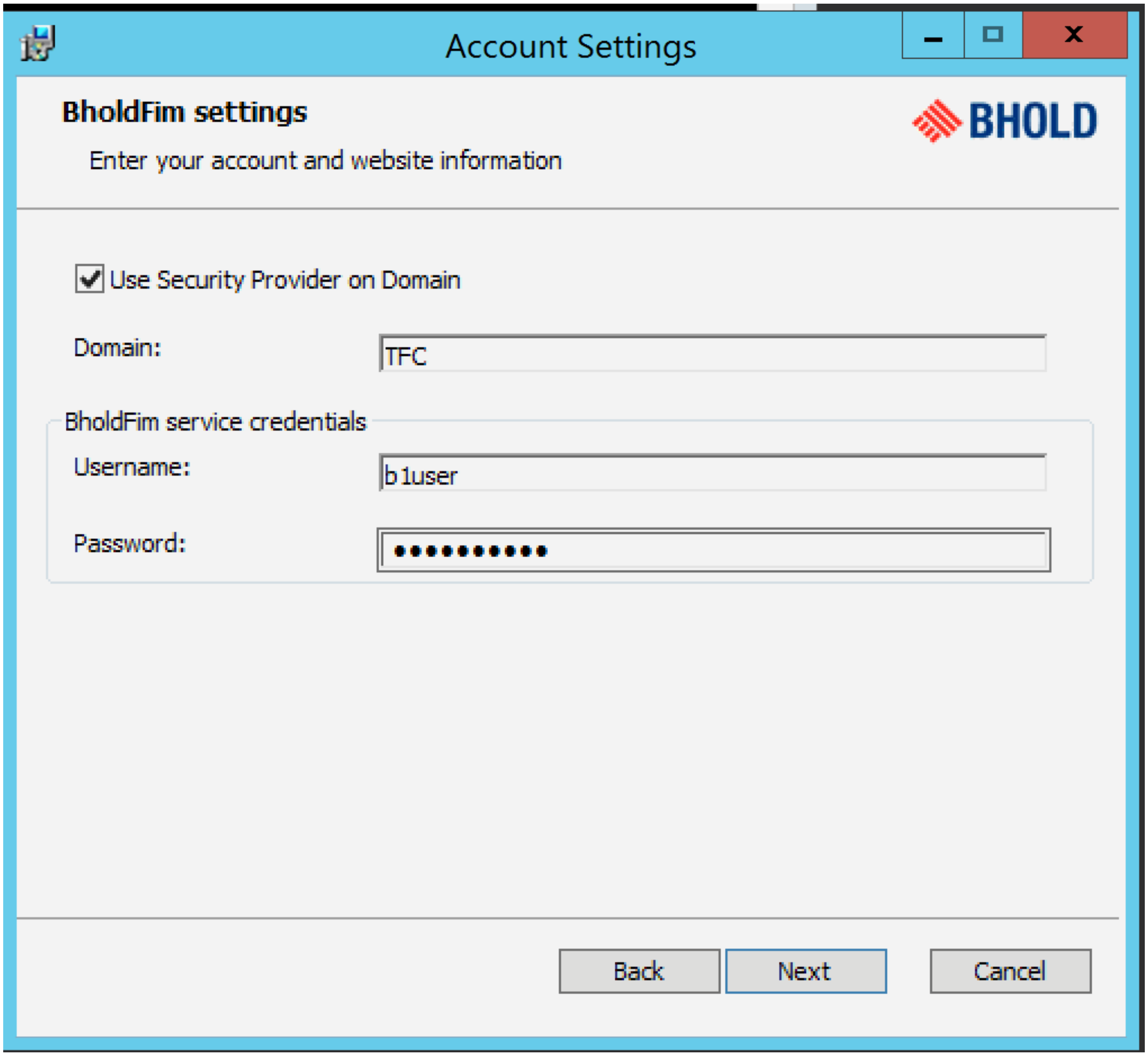
Click the icons in the tree below to change the way features will be installed.

- Microsoft BHOLD Suite - FIM
  - BHOLD FIM Integrati
    - Bhold FIM Act
  - BHOLD FIM Web port
    - Role Exchang
    - Bhold SelfServ
    - Database File
    - Bhold Custom

Microsoft BHOLD Suite - FIM Integration

This feature requires 56KB on your hard drive. It has 2 of 2 subfeatures selected. The subfeatures require 3081KB on your hard drive.

Location: C:\Program Files (x86)\BHOLD\FIM\



Account Settings

BholdFim settings

Enter your account and website information

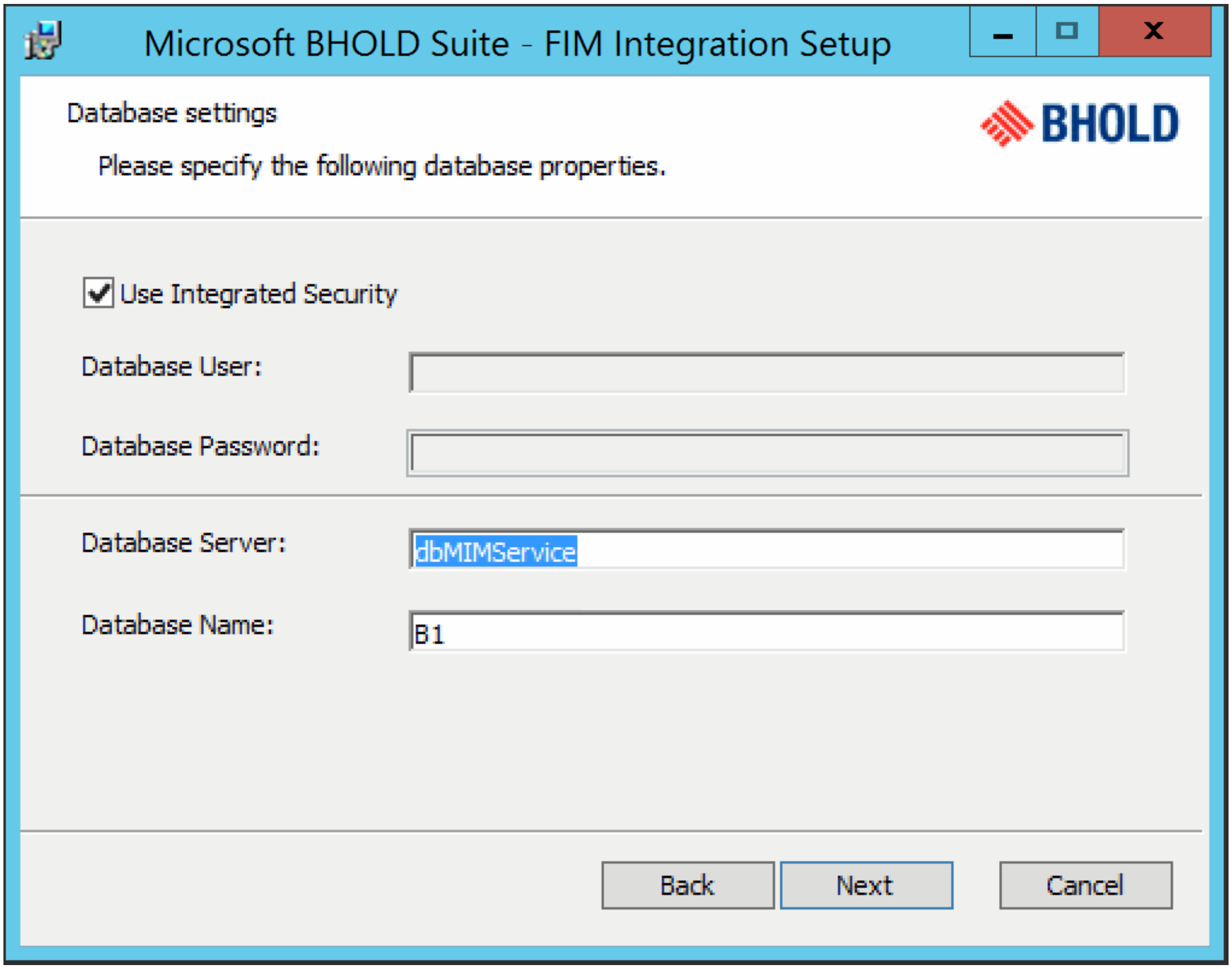
☑ Use Security Provider on Domain

Domain: TFC

BholdFim service credentials

Username: b1user

Password: ●●●●●●●●●●●



Microsoft BHOLD Suite - FIM Integration Setup

Database settings

Please specify the following database properties.

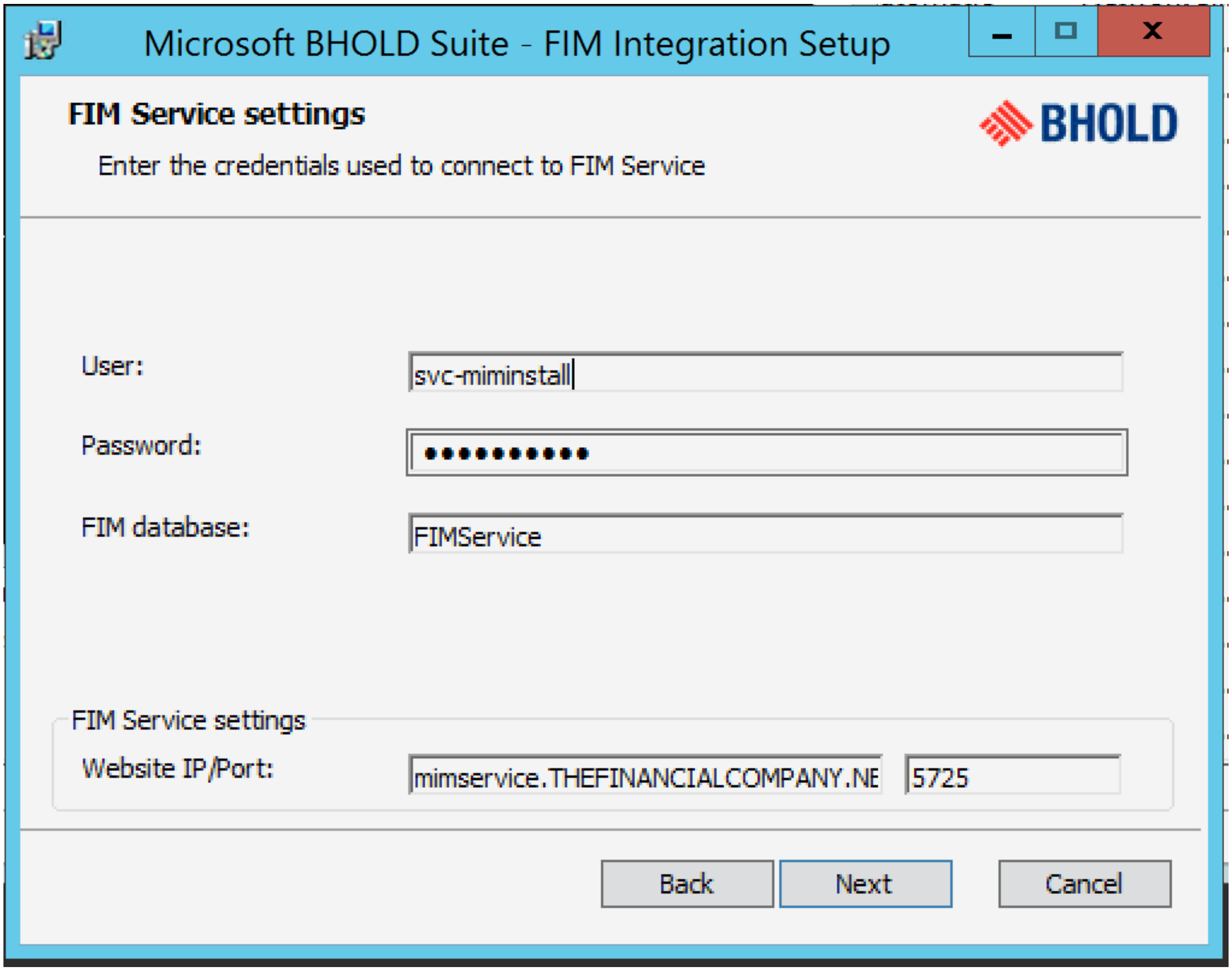
☑ Use Integrated Security

Database User:

Database Password:

Database Server: dbMIMService

Database Name: B1



FIM Service settings

Enter the credentials used to connect to FIM Service

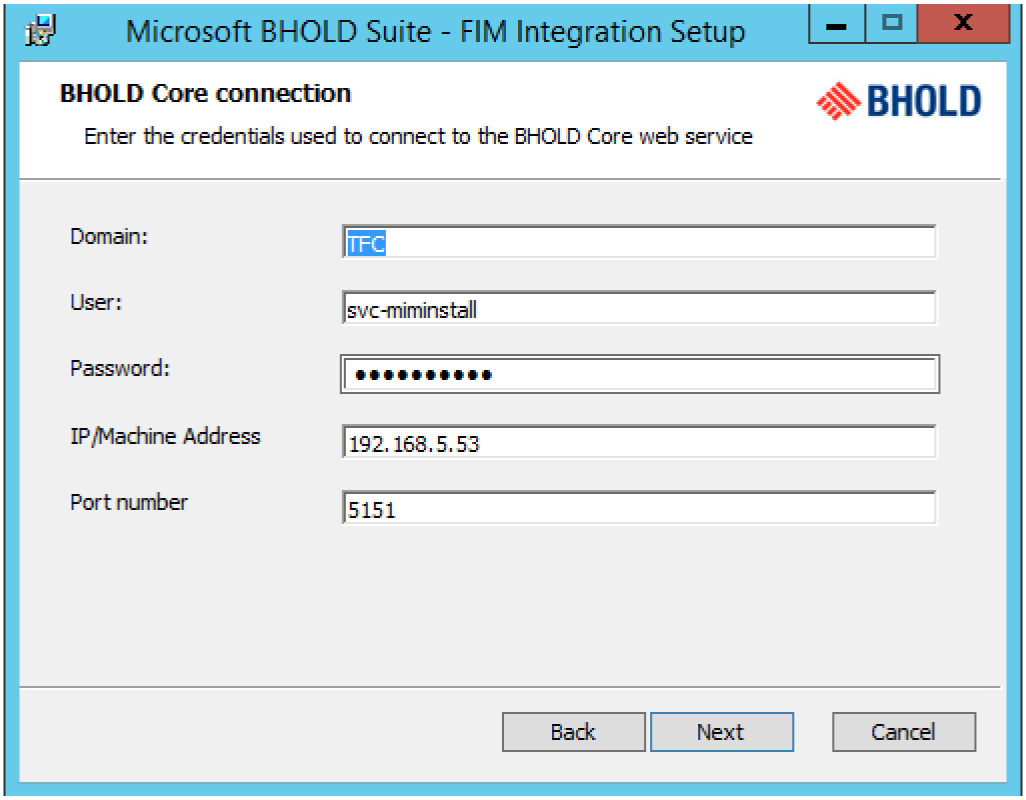
User: svc-miminstall

Password: ●●●●●●●●●●●

FIM database: FIMService

FIM Service settings

Website IP/Port: mimservice.THEFINANCIALCOMPANY.NE 5725



Microsoft BHOLD Suite - FIM Integration Setup

BHOLD Core connection

Enter the credentials used to connect to the BHOLD Core web service

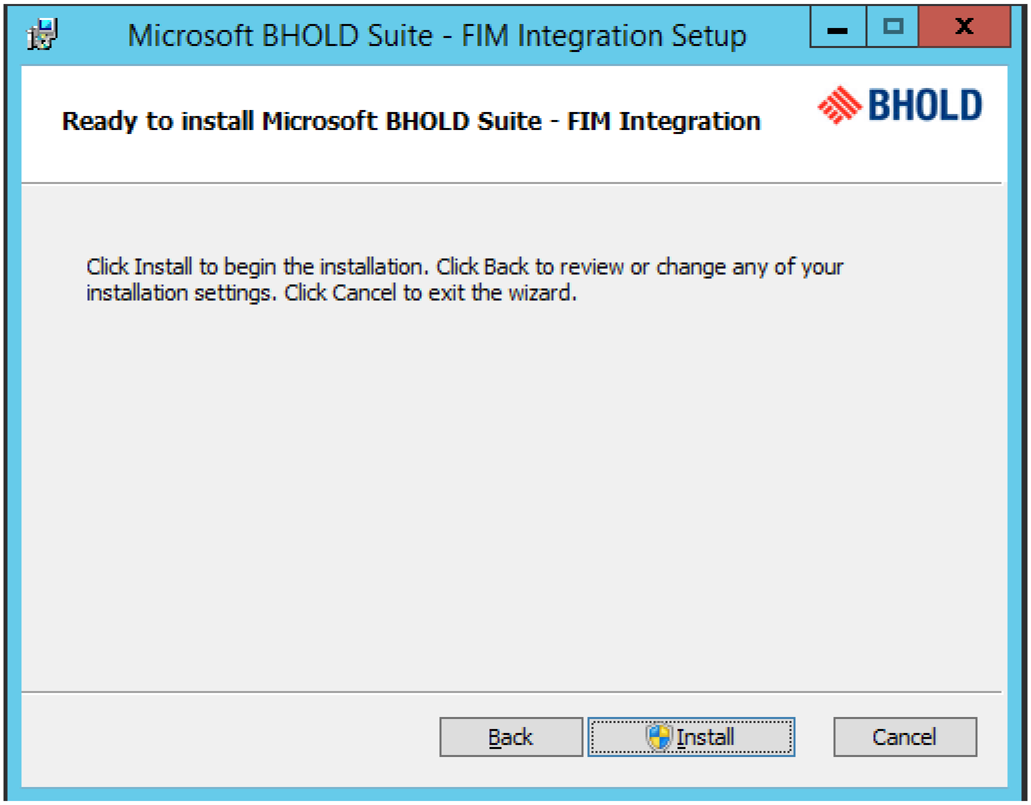
Domain: TFC

User: svc-miminstall

Password: ●●●●●●●●●●●

IP/Machine Address 192.168.5.53

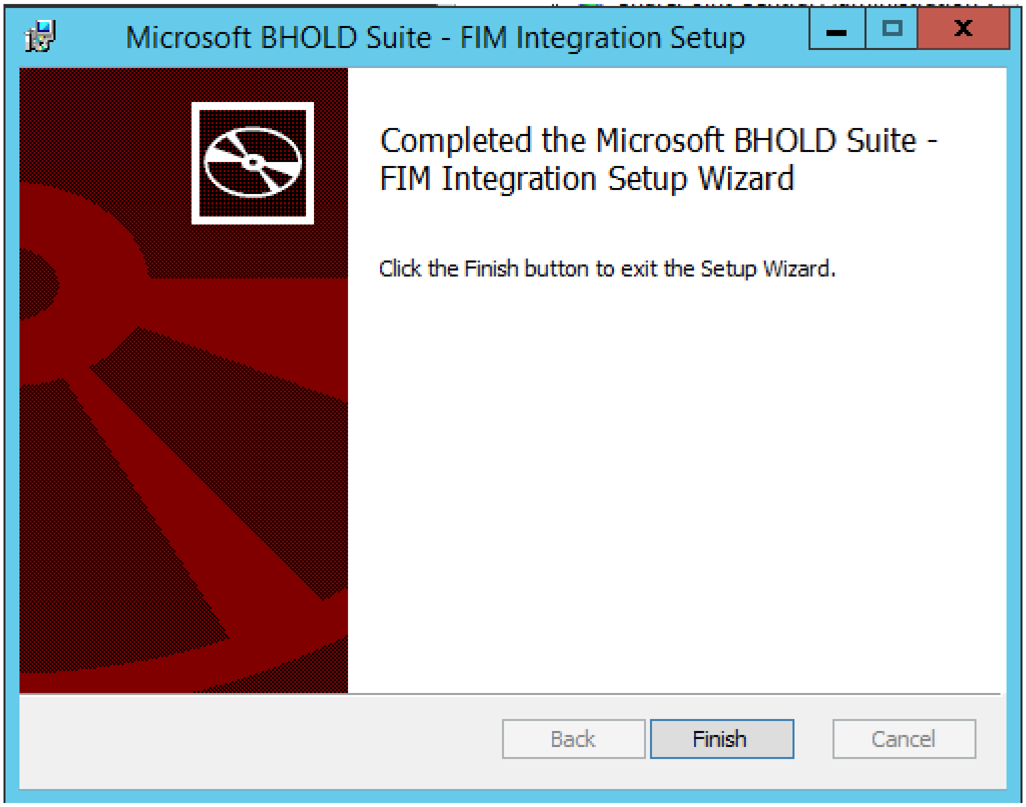
Port number 5151



Microsoft BHOLD Suite - FIM Integration Setup

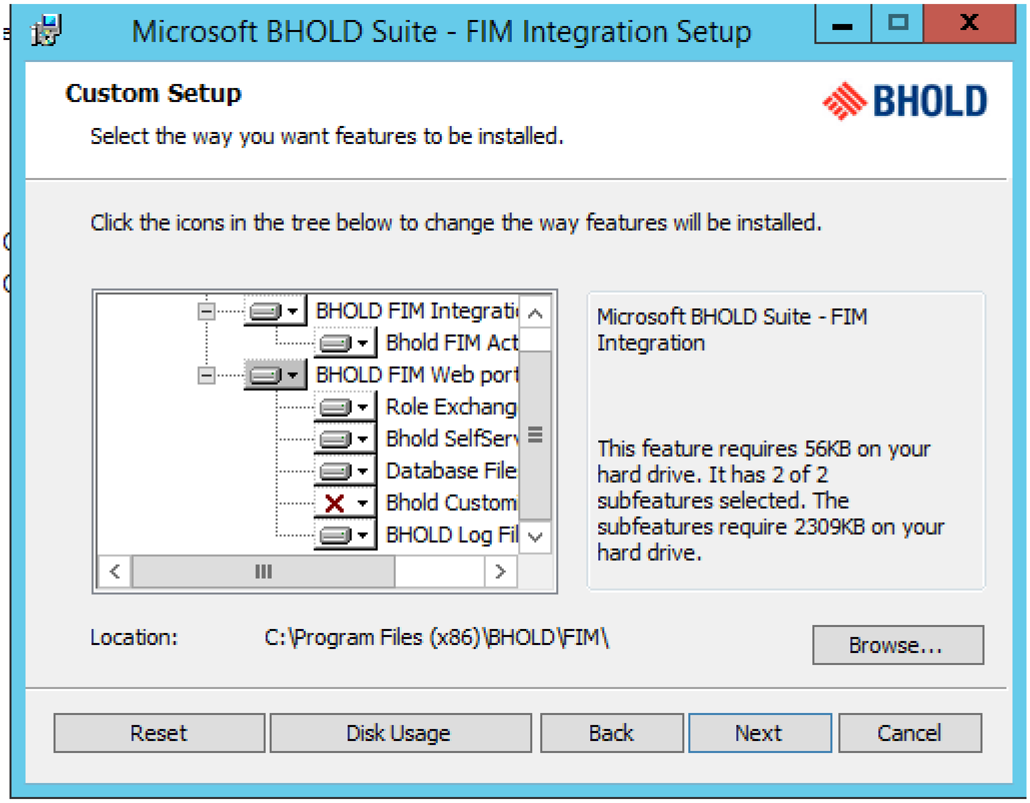
Ready to install Microsoft BHOLD Suite - FIM Integration

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.



Completed the Microsoft BHOLD Suite - FIM Integration Setup Wizard

Click the Finish button to exit the Setup Wizard.



Custom Setup

Select the way you want features to be installed.

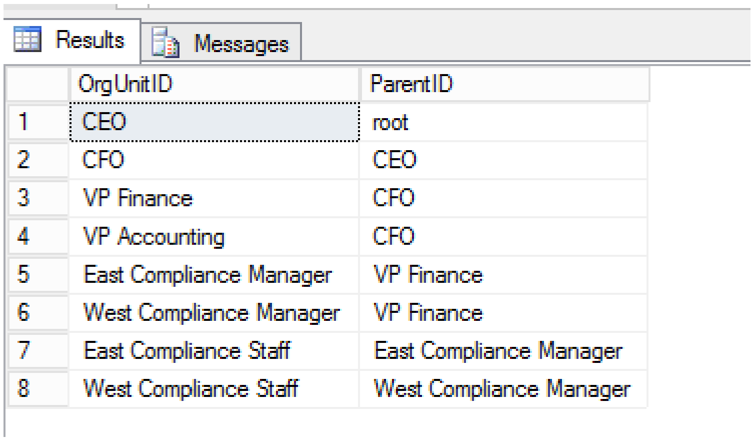
Click the icons in the tree below to change the way features will be installed.

- BHOLD FIM Integrati
  - Bhold FIM Act
- BHOLD FIM Web port
  - Role Exchang
  - Bhold SelfServ
  - Database File
  - ☒ Bhold Custom
  - BHOLD Log Fil

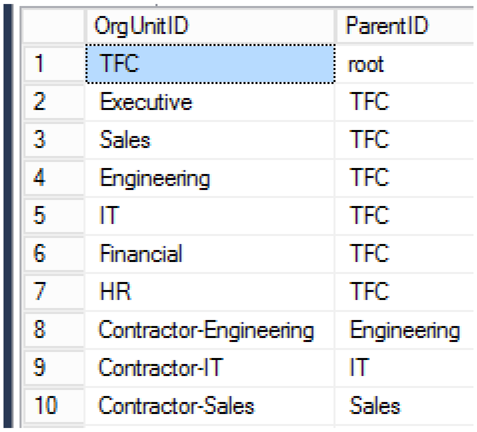
Microsoft BHOLD Suite - FIM Integration

This feature requires 56KB on your hard drive. It has 2 of 2 subfeatures selected. The subfeatures require 2309KB on your hard drive.

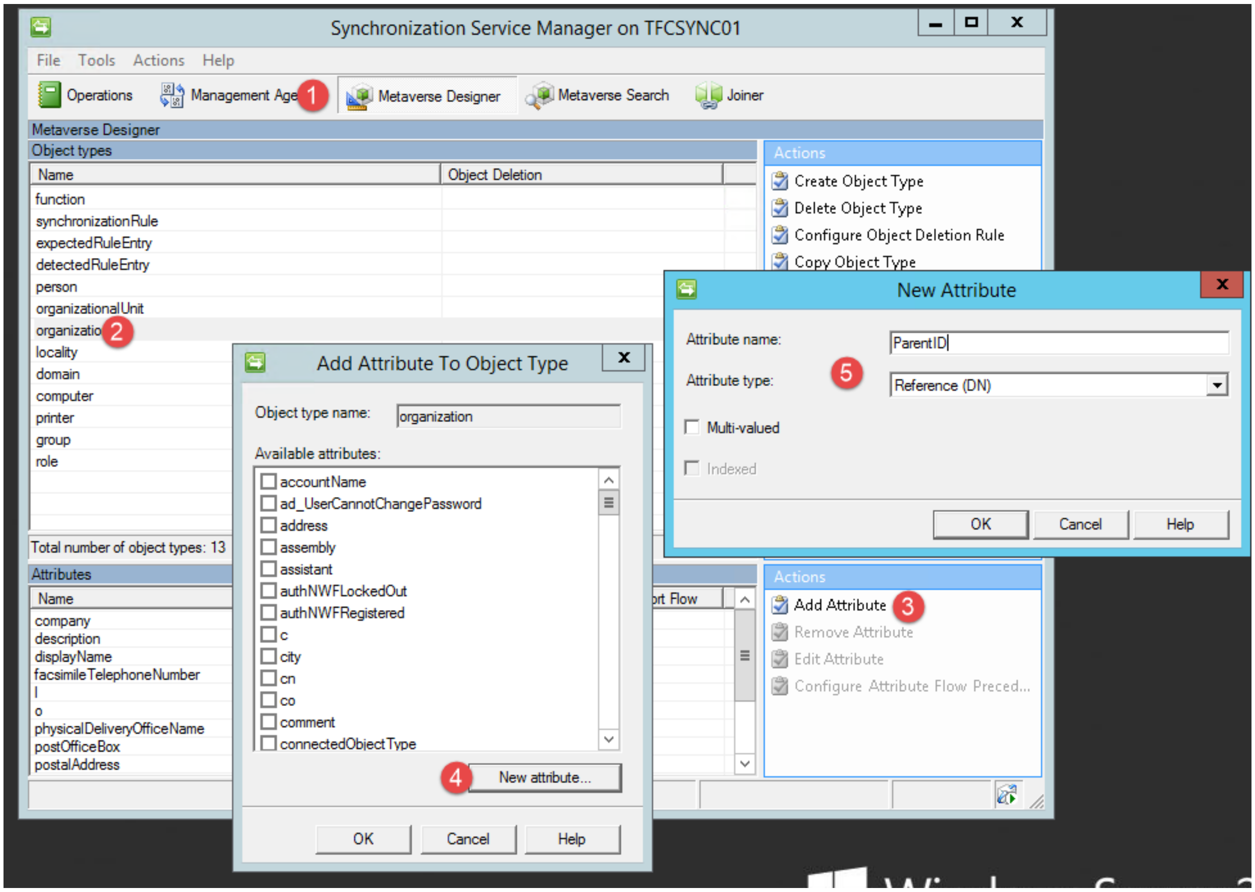
Location: C:\Program Files (x86)\BHOLD\FIM\



	OrgUnitID	ParentID
1	CEO	root
2	CFO	CEO
3	VP Finance	CFO
4	VP Accounting	CFO
5	East Compliance Manager	VP Finance
6	West Compliance Manager	VP Finance
7	East Compliance Staff	East Compliance Manager
8	West Compliance Staff	West Compliance Manager



	OrgUnitID	ParentID
1	TFC	root
2	Executive	TFC
3	Sales	TFC
4	Engineering	TFC
5	IT	TFC
6	Financial	TFC
7	HR	TFC
8	Contractor-Engineering	Engineering
9	Contractor-IT	IT
10	Contractor-Sales	Sales


Synchronization Service Manager on TFCSYNC01

Add Attribute To Object Type

Object type name: organization

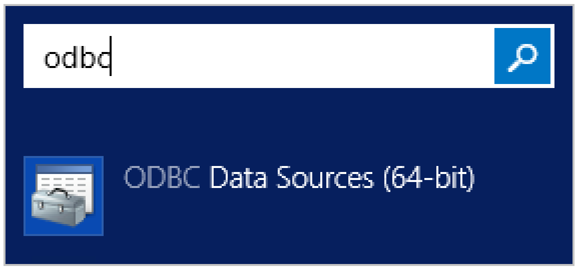
New Attribute

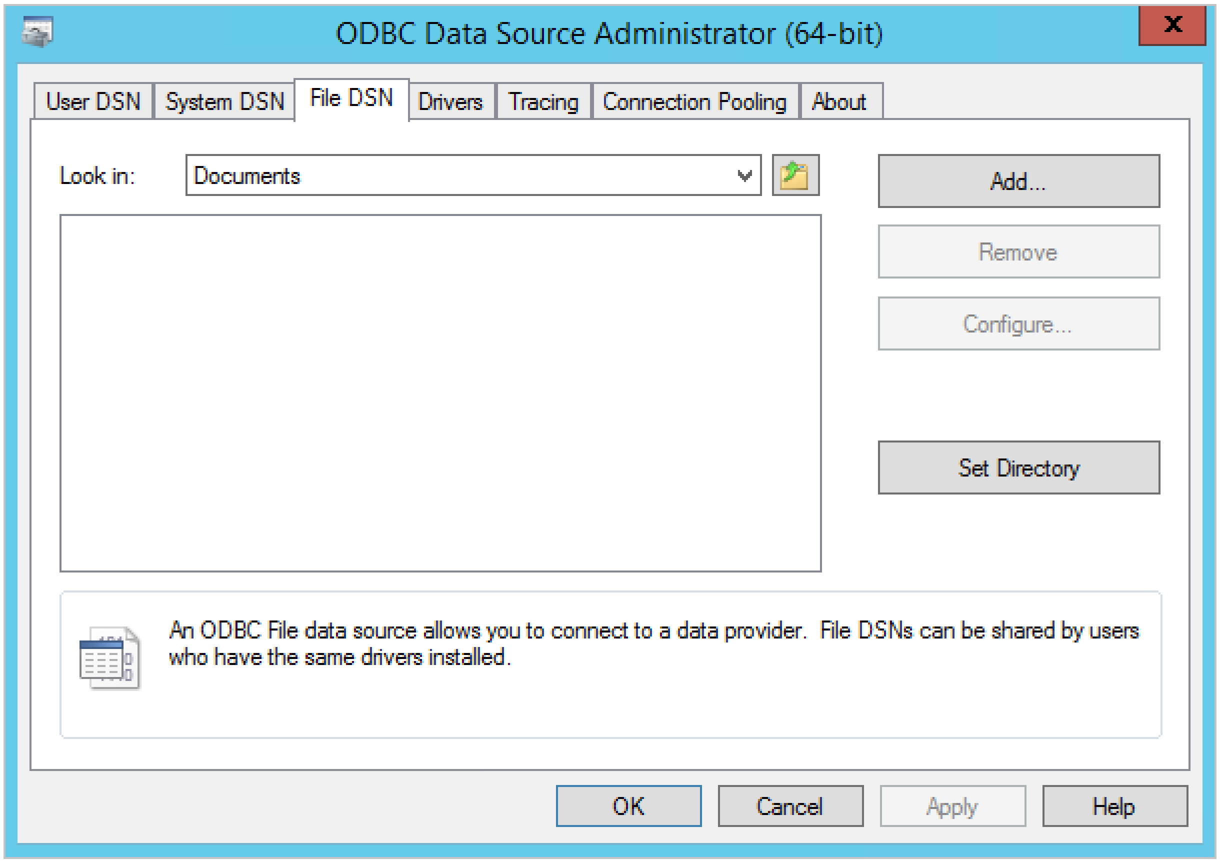
Attribute name: ParentID

Attribute type: Reference (DN)

□ Multi-valued

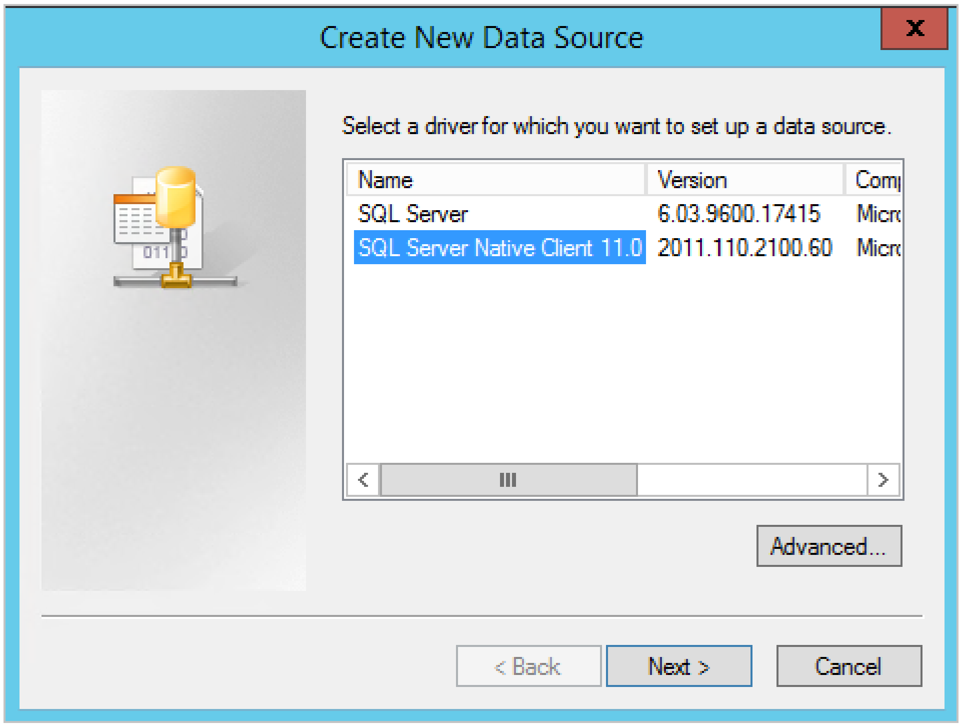
□ Indexed


odbc



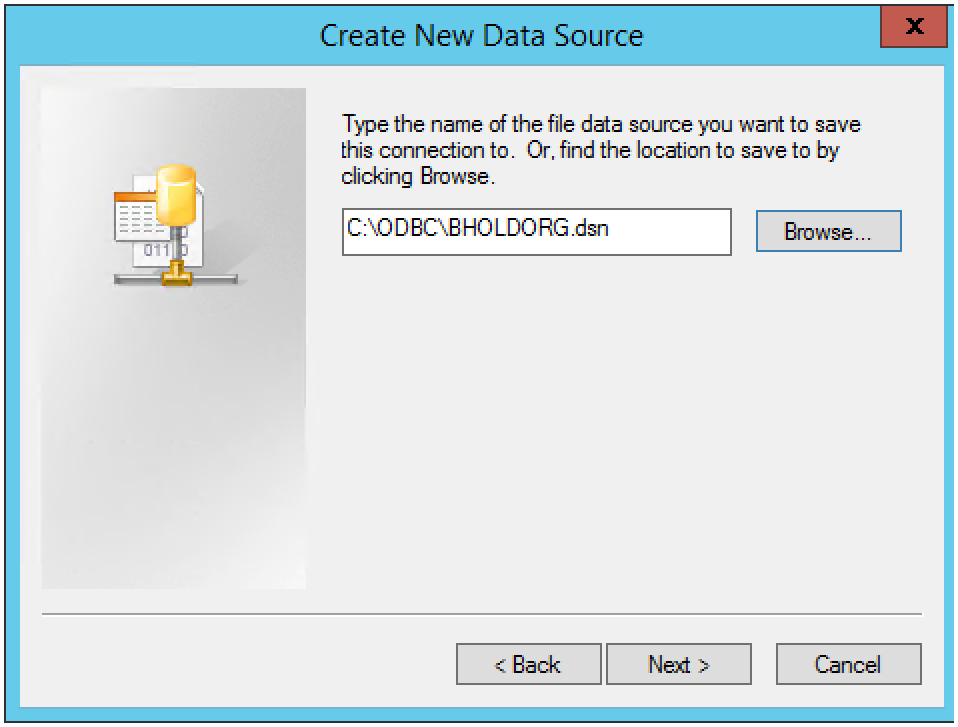
Look in: Documents

An ODBC File data source allows you to connect to a data provider. File DSNs can be shared by users who have the same drivers installed.



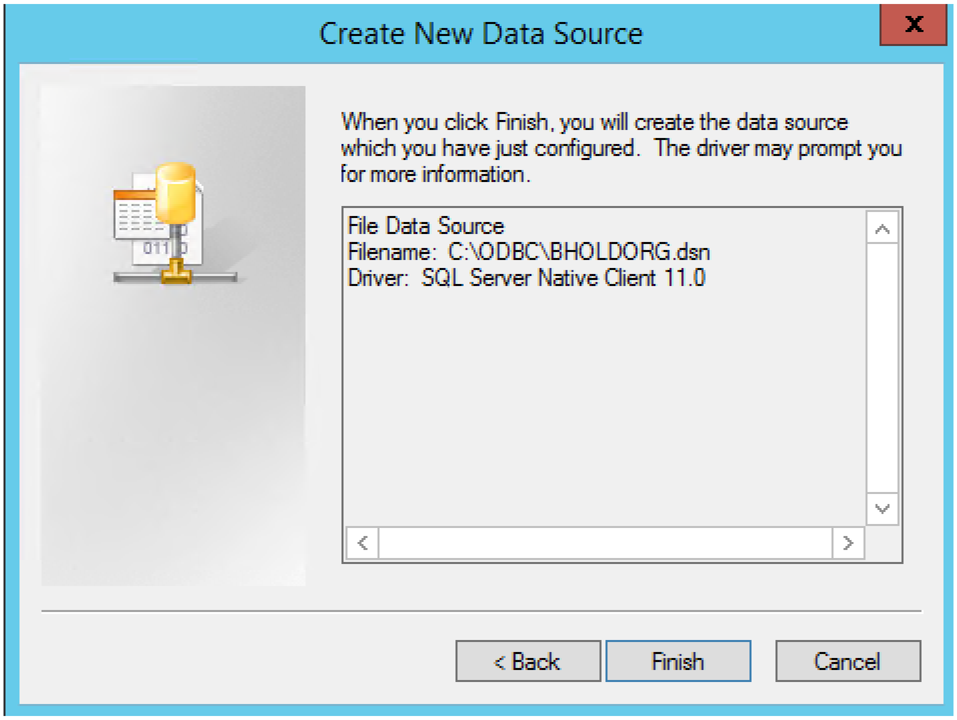
Select a driver for which you want to set up a data source.

Name	Version	Com
SQL Server	6.03.9600.17415	Micr
SQL Server Native Client 11.0	2011.110.2100.60	Micr



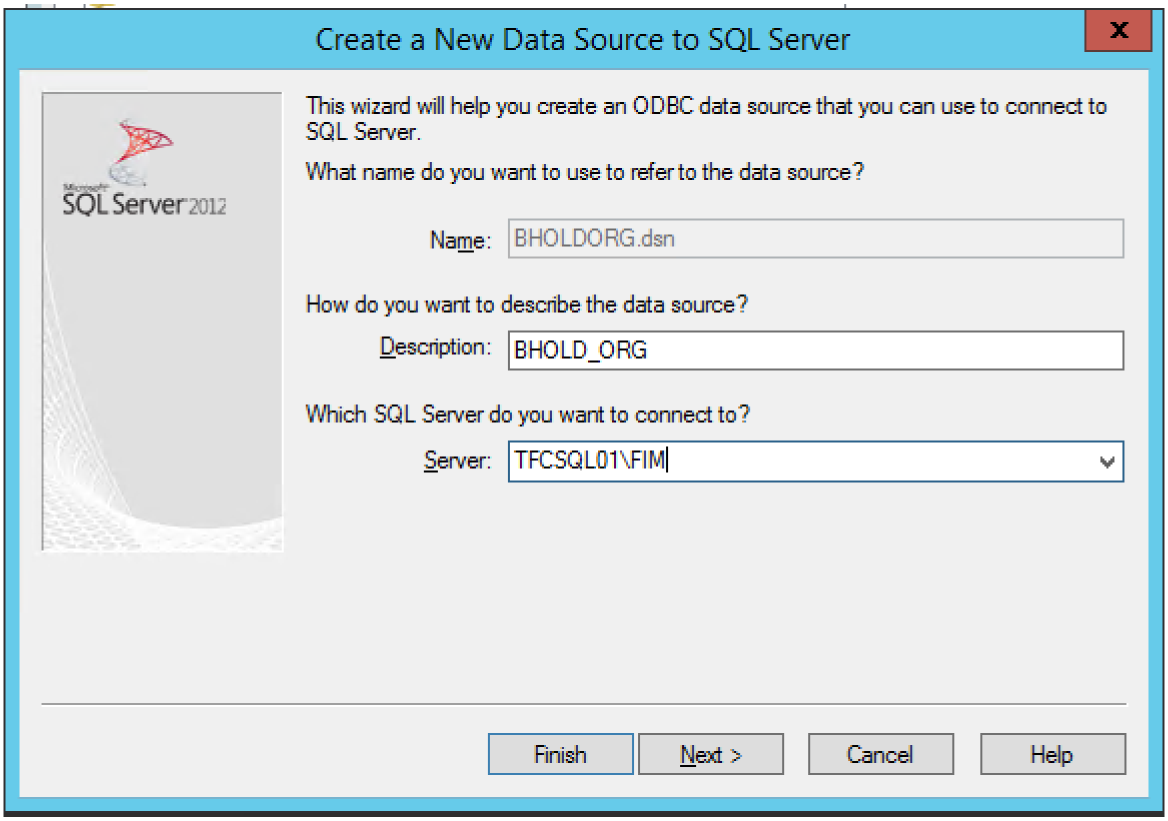
Type the name of the file data source you want to save this connection to. Or, find the location to save to by clicking Browse.

C:\ODBC\BHOLDORG.dsn



When you click Finish, you will create the data source which you have just configured. The driver may prompt you for more information.

File Data Source
Filename: C:\ODBC\BHOLDORG.dsn
Driver: SQL Server Native Client 11.0



Create a New Data Source to SQL Server

This wizard will help you create an ODBC data source that you can use to connect to SQL Server.

What name do you want to use to refer to the data source?

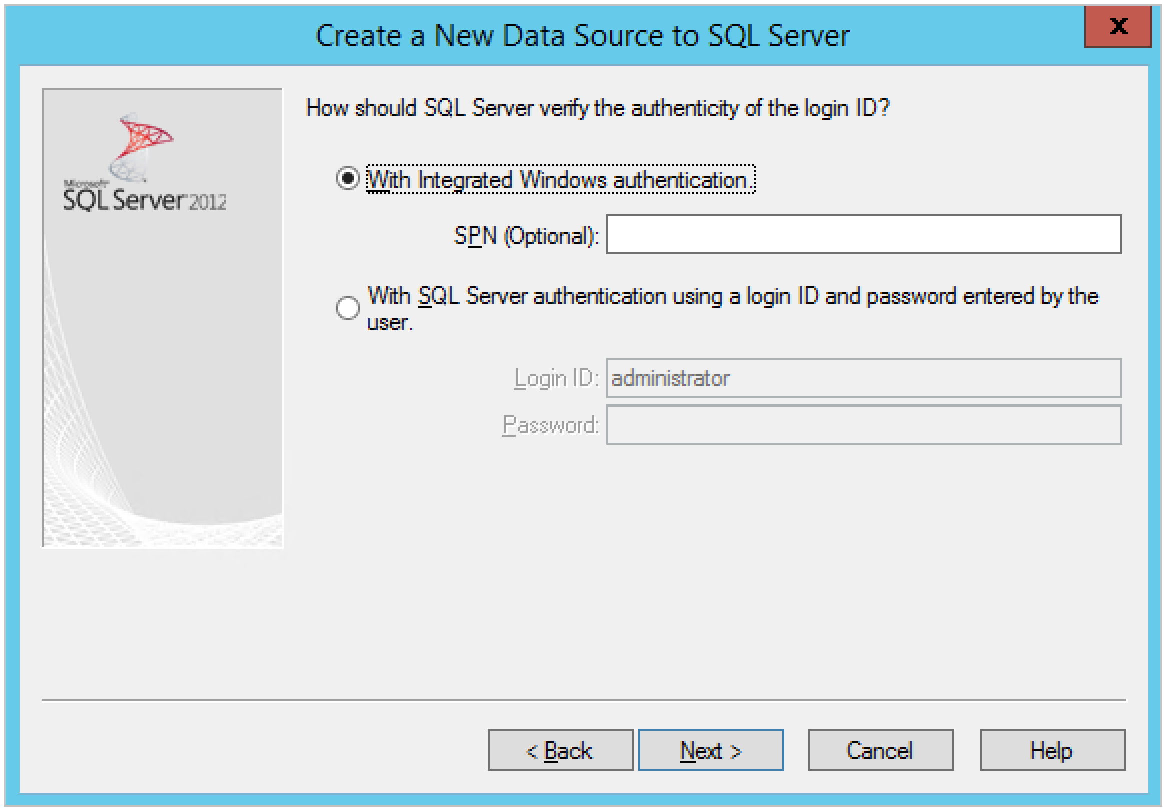
Name: BHOLDORG.dsn

How do you want to describe the data source?

Description: BHOLD_ORG

Which SQL Server do you want to connect to?

Server: TFCSQL01\FIM



Create a New Data Source to SQL Server

How should SQL Server verify the authenticity of the login ID?

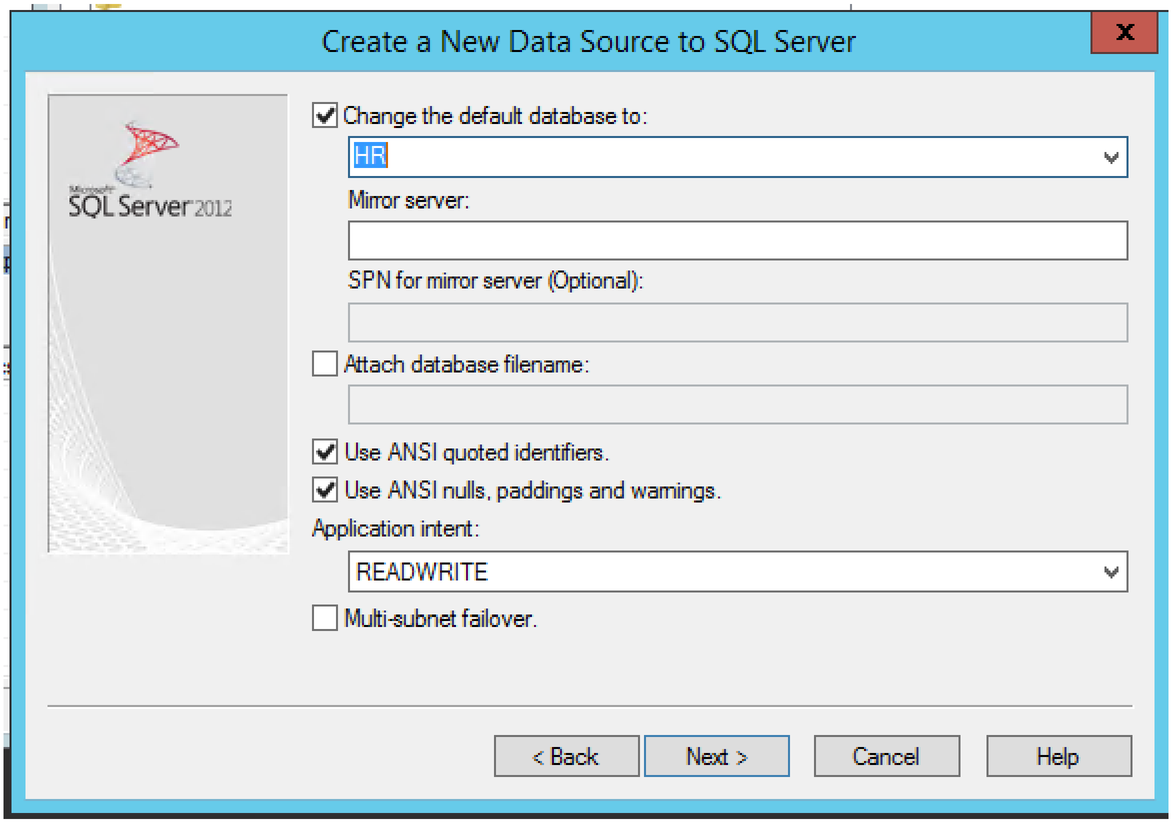
● With Integrated Windows authentication.

SPN (Optional):

○ With SQL Server authentication using a login ID and password entered by the user.

Login ID: administrator

Password:



Create a New Data Source to SQL Server

☑ Change the default database to:

HR

Mirror server:

SPN for mirror server (Optional):

☐ Attach database filename:

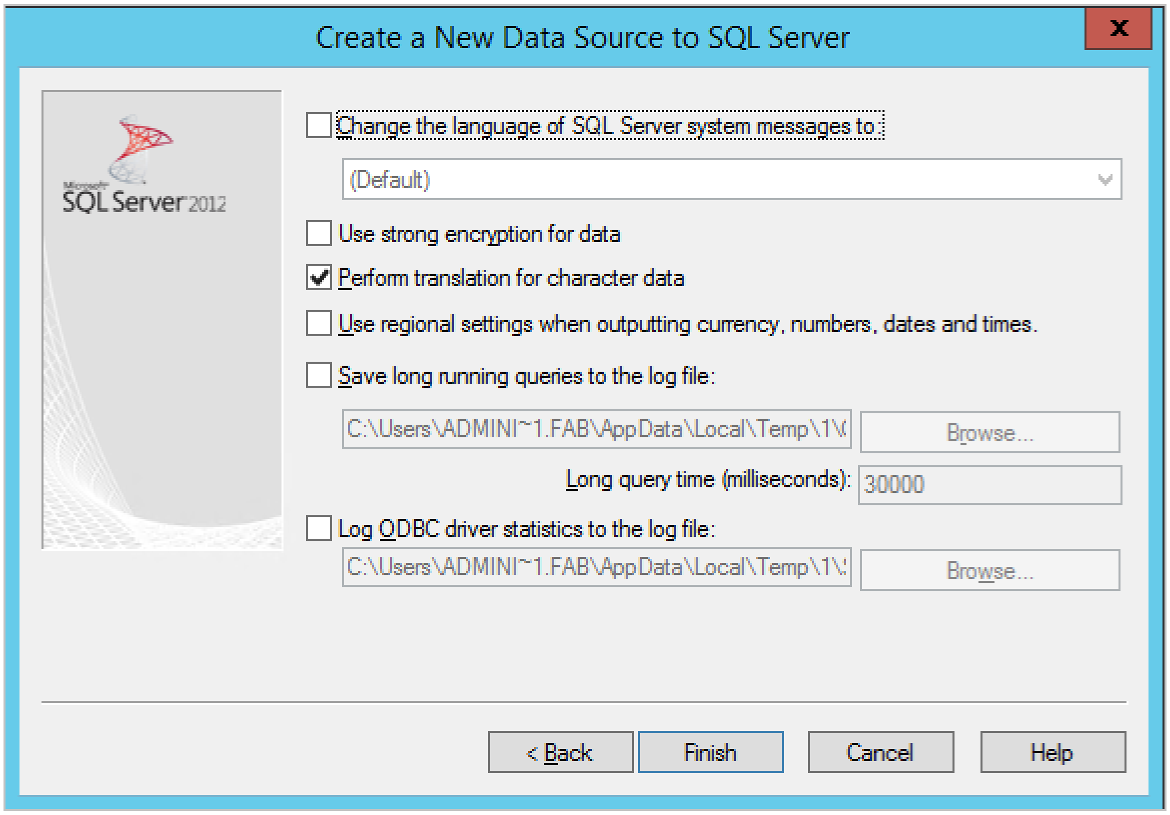
☑ Use ANSI quoted identifiers.

☑ Use ANSI nulls, paddings and warnings.

Application intent:

READWRITE

☐ Multi-subnet failover.



Create a New Data Source to SQL Server

☐ Change the language of SQL Server system messages to:

(Default)

☐ Use strong encryption for data

☑ Perform translation for character data

☐ Use regional settings when outputting currency, numbers, dates and times.

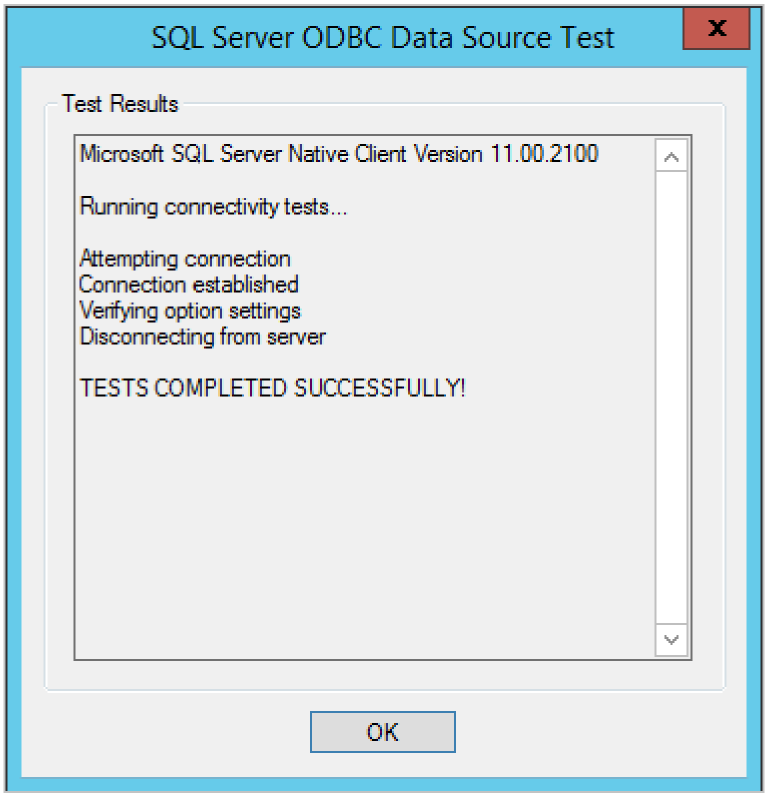
☐ Save long running queries to the log file:

C:\Users\ADMINI~1.FAB\AppData\Local\Temp\1\(

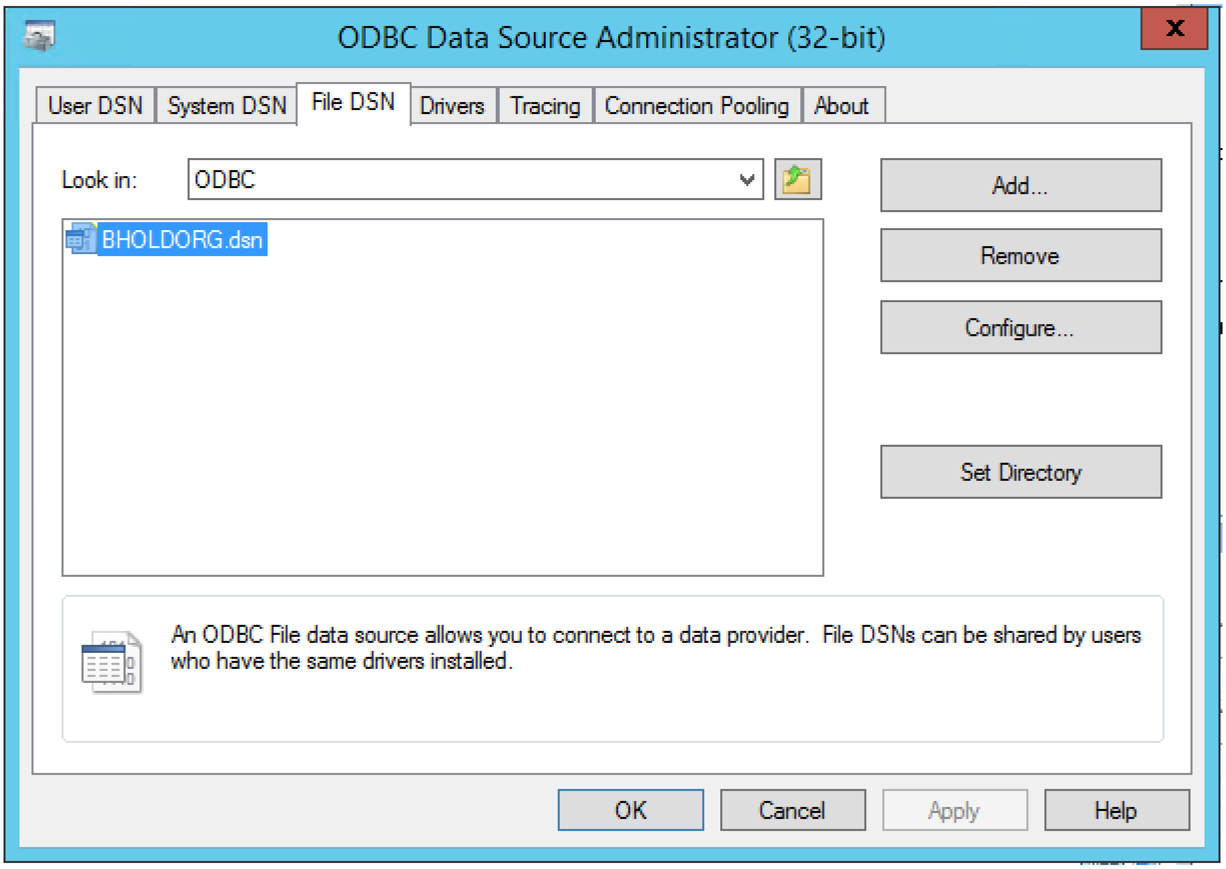
Long query time (milliseconds): 30000

☐ Log ODBC driver statistics to the log file:

C:\Users\ADMINI~1.FAB\AppData\Local\Temp\1\:



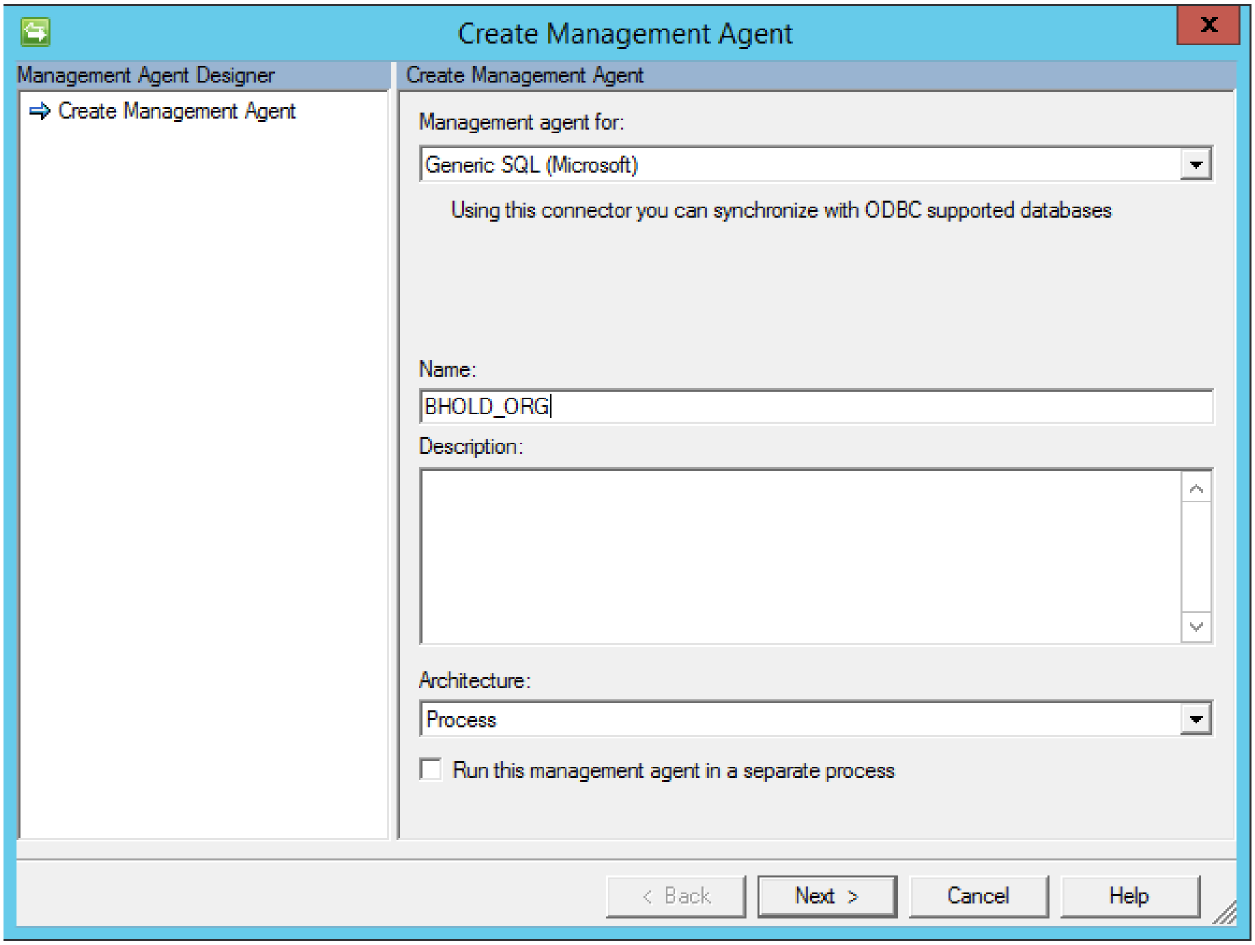
```
Microsoft SQL Server Native Client Version 11.00.2100

Running connectivity tests...

Attempting connection
Connection established
Verifying option settings
Disconnecting from server

TESTS COMPLETED SUCCESSFULLY!
```



Look in: ODBC

BHOLDORG.dsn

An ODBC File data source allows you to connect to a data provider. File DSNs can be shared by users who have the same drivers installed.



Management agent for: Generic SQL (Microsoft)

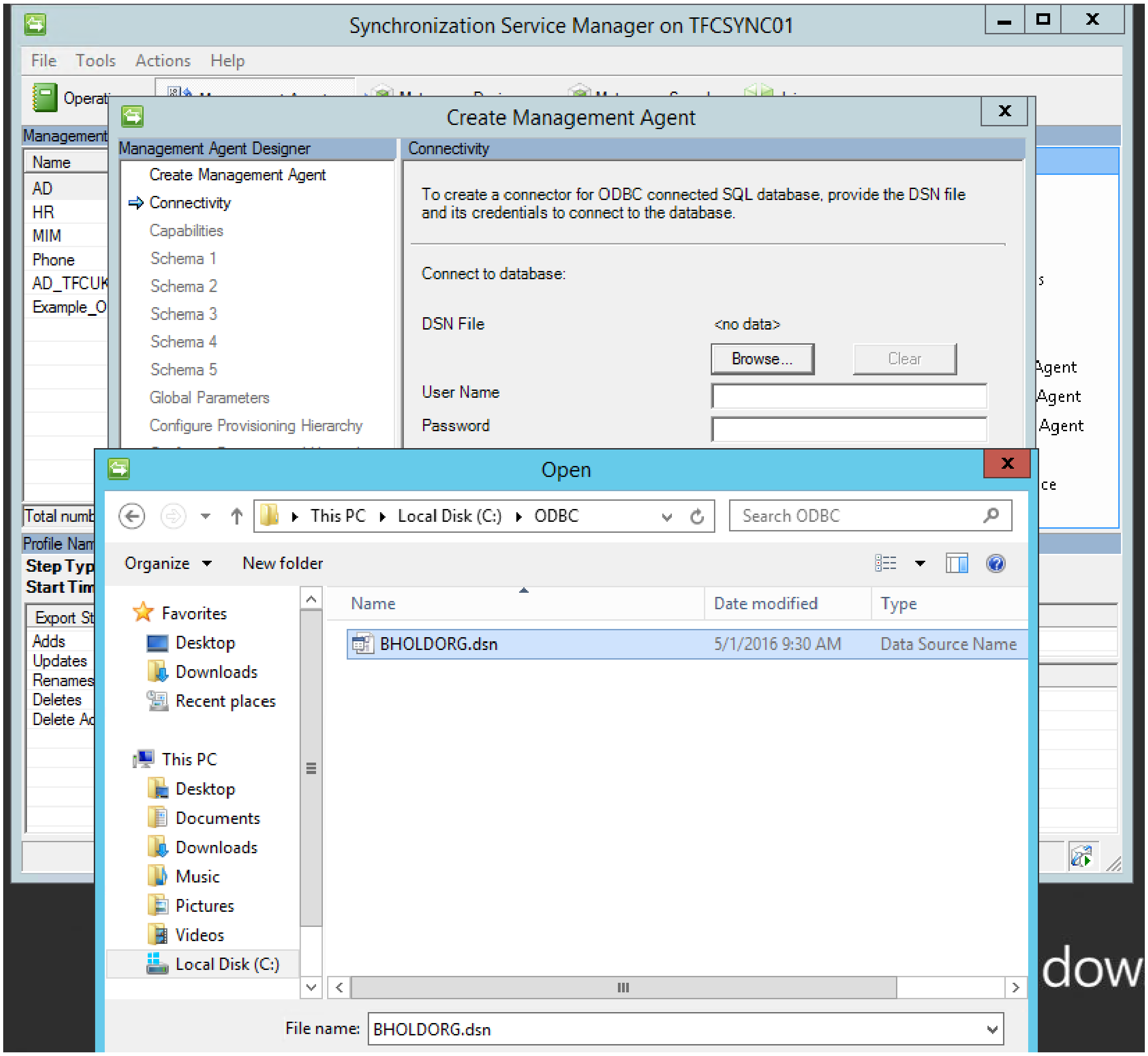
Using this connector you can synchronize with ODBC supported databases

Name: BHOLD_ORG

Description:

Architecture: Process

□ Run this management agent in a separate process



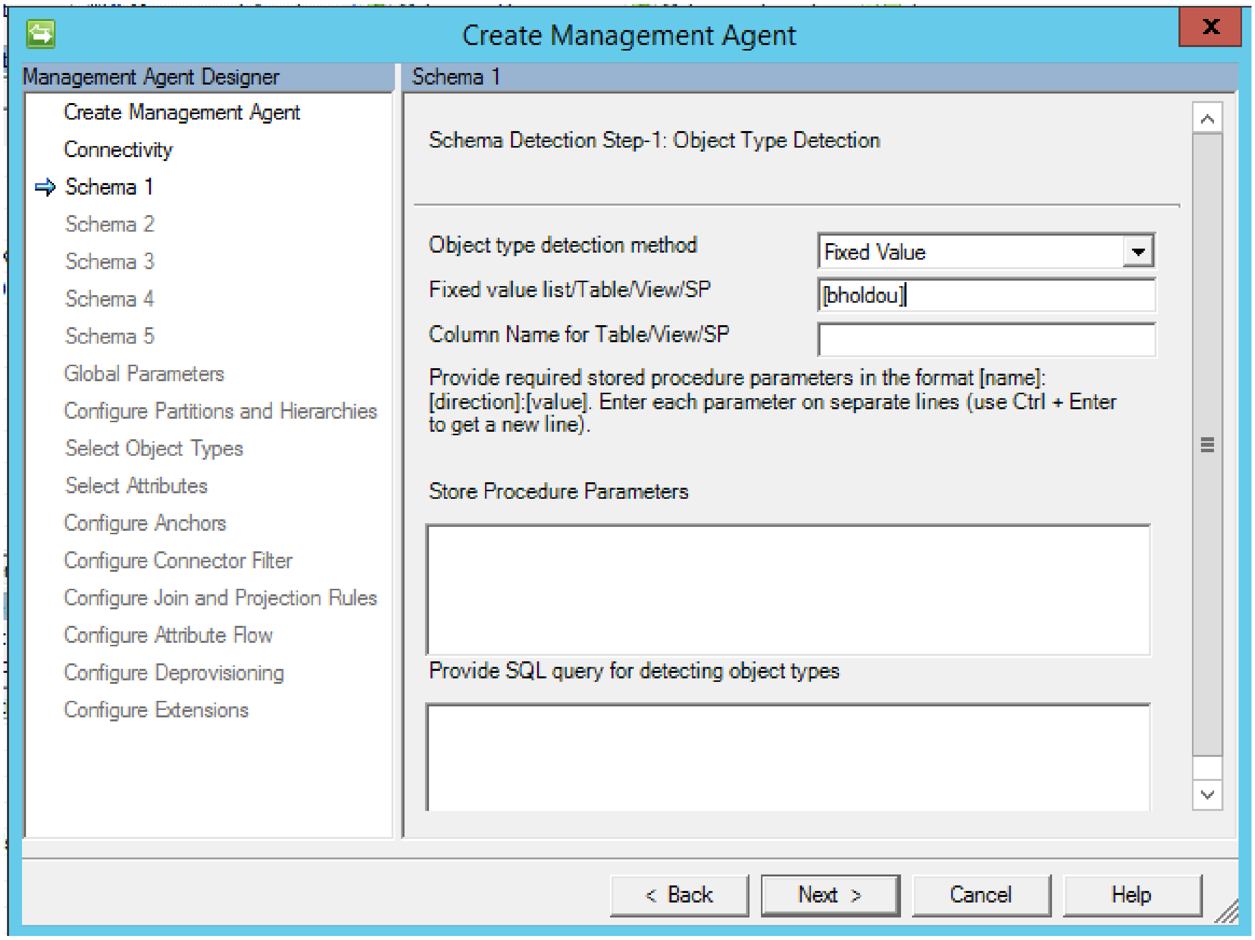
To create a connector for ODBC connected SQL database, provide the DSN file and its credentials to connect to the database.

Connect to database:

DSN File <no data>

Name	Date modified	Type
BHOLDORG.dsn	5/1/2016 9:30 AM	Data Source Name

File name: BHOLDORG.dsn



Create Management Agent

Management Agent Designer

Schema 1

Schema Detection Step-1: Object Type Detection

Object type detection method: Fixed Value

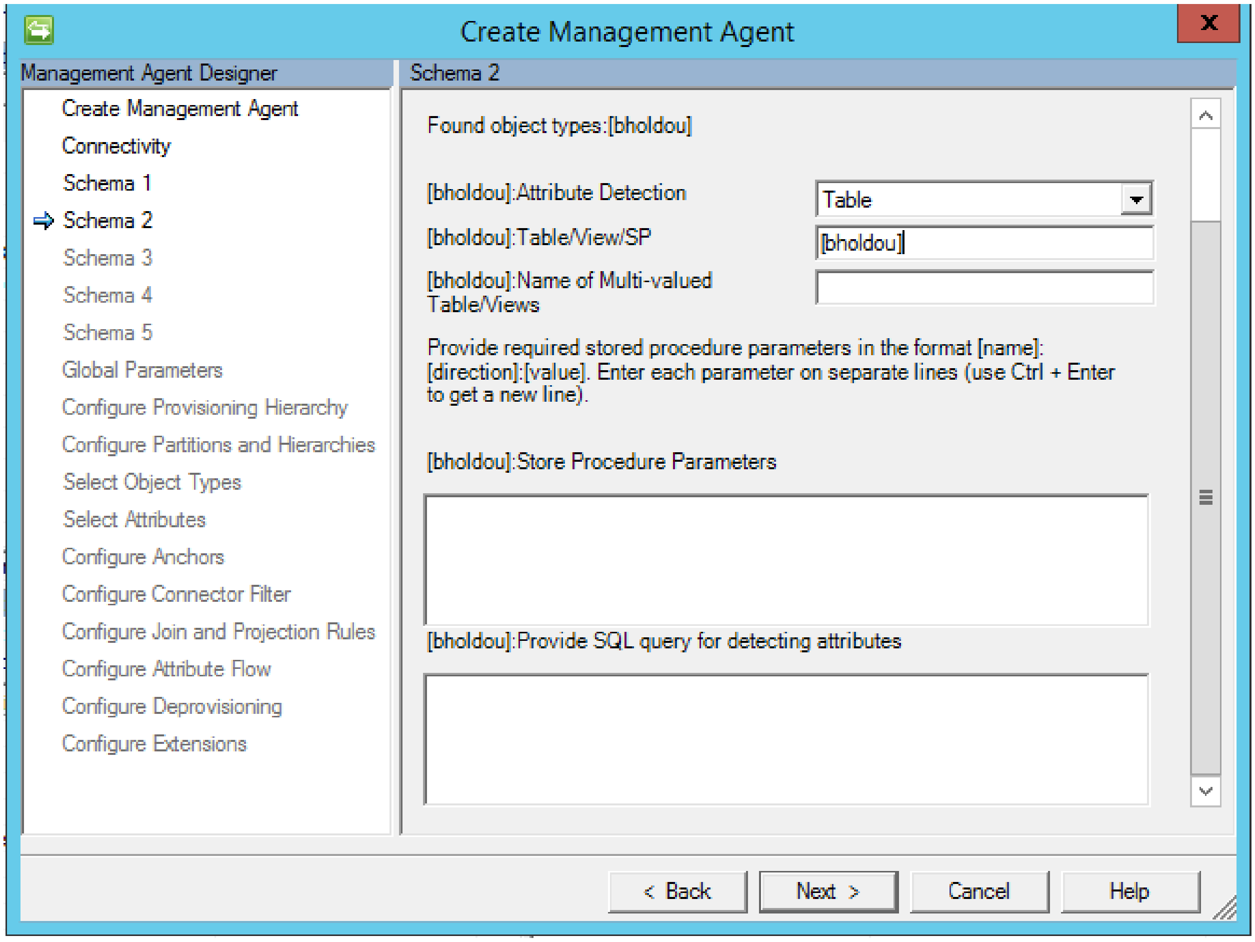
Fixed value list/Table/View/SP: [bholdou]

Column Name for Table/View/SP:

Provide required stored procedure parameters in the format [name]:[direction]:[value]. Enter each parameter on separate lines (use Ctrl + Enter to get a new line).

Store Procedure Parameters

Provide SQL query for detecting object types



Found object types:[bholdou]

[bholdou]:Attribute Detection: Table

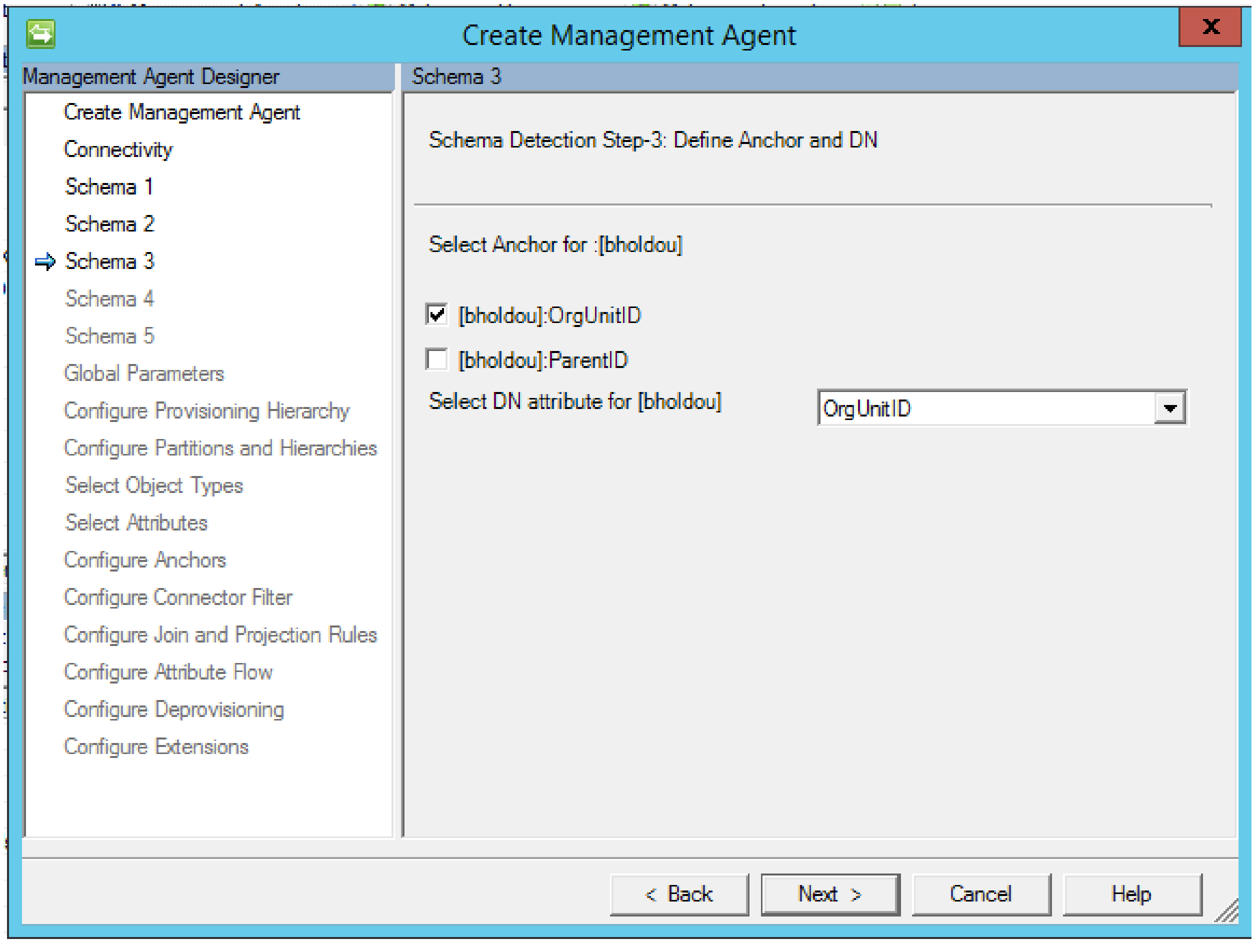
[bholdou]:Table/View/SP: [bholdou]

[bholdou]:Name of Multi-valued Table/Views:

Provide required stored procedure parameters in the format [name]:[direction]:[value]. Enter each parameter on separate lines (use Ctrl + Enter to get a new line).

[bholdou]:Store Procedure Parameters

[bholdou]:Provide SQL query for detecting attributes



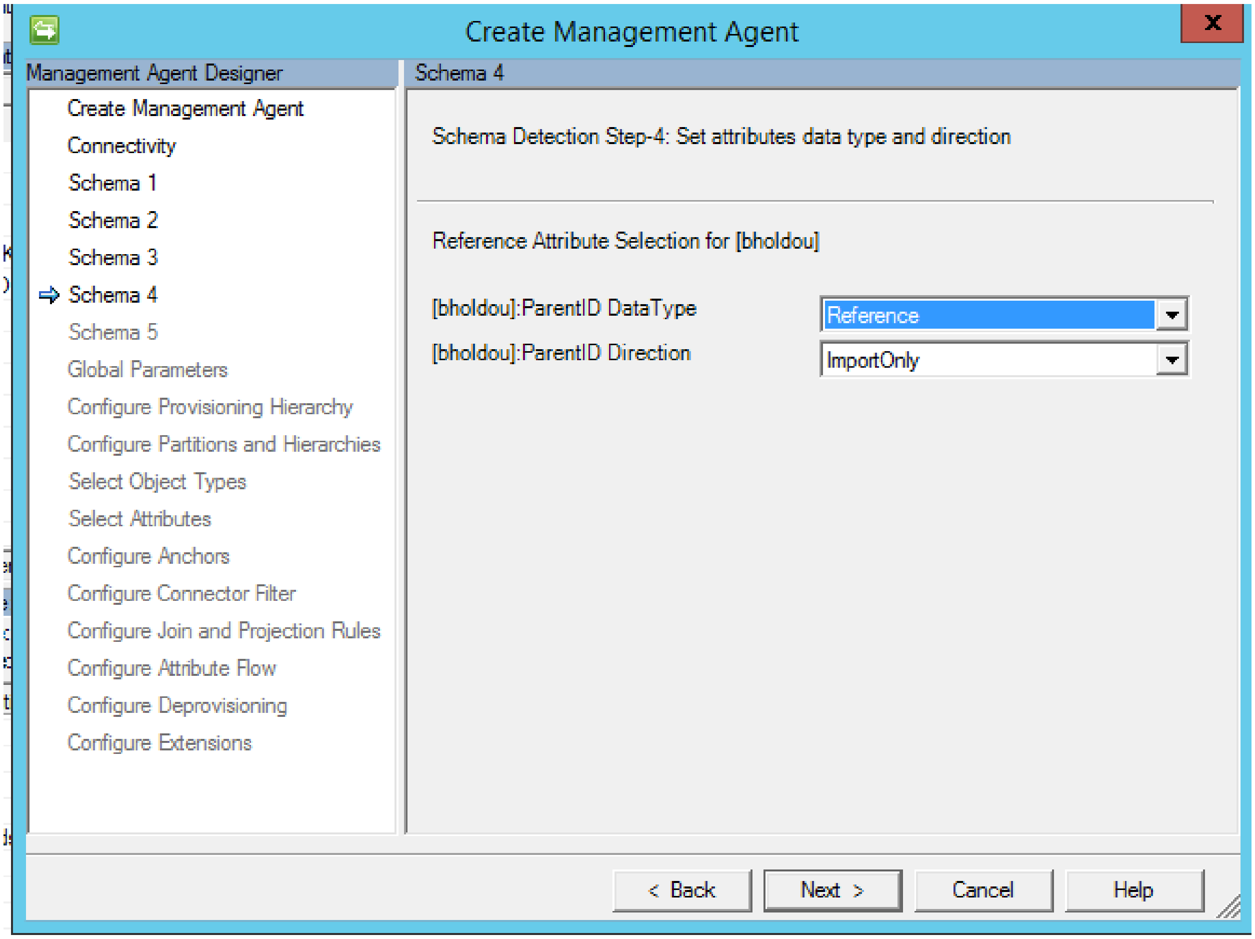
Schema Detection Step-3: Define Anchor and DN

Select Anchor for :[bholdou]

☑ [bholdou]:OrgUnitID

☐ [bholdou]:ParentID

Select DN attribute for [bholdou] OrgUnitID



Create Management Agent

Management Agent Designer

- Create Management Agent
- Connectivity
- Schema 1
- Schema 2
- Schema 3
- ⇨ Schema 4
- Schema 5
- Global Parameters
- Configure Provisioning Hierarchy
- Configure Partitions and Hierarchies
- Select Object Types
- Select Attributes
- Configure Anchors
- Configure Connector Filter
- Configure Join and Projection Rules
- Configure Attribute Flow
- Configure Deprovisioning
- Configure Extensions

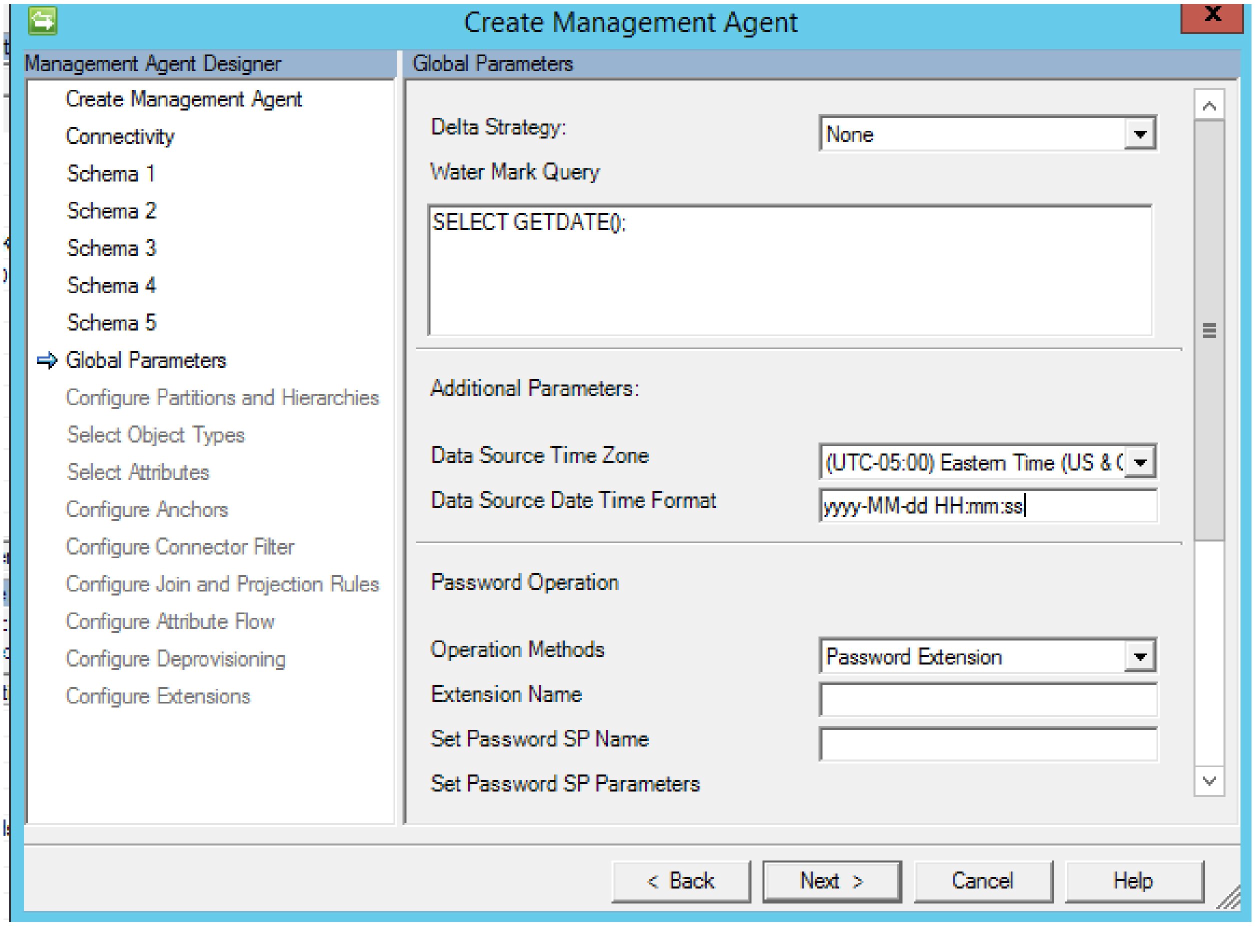
Schema 4

Schema Detection Step-4: Set attributes data type and direction

Reference Attribute Selection for [bholdou]

[bholdou]:ParentID DataType: Reference

[bholdou]:ParentID Direction: ImportOnly



Create Management Agent

Management Agent Designer

- Create Management Agent
- Connectivity
- Schema 1
- Schema 2
- Schema 3
- Schema 4
- Schema 5
- ⇨ Global Parameters
- Configure Partitions and Hierarchies
- Select Object Types
- Select Attributes
- Configure Anchors
- Configure Connector Filter
- Configure Join and Projection Rules
- Configure Attribute Flow
- Configure Deprovisioning
- Configure Extensions

Global Parameters

Delta Strategy: None

Water Mark Query

```
SELECT GETDATE();
```

Additional Parameters:

Data Source Time Zone: (UTC-05:00) Eastern Time (US & C

Data Source Date Time Format: yyyy-MM-dd HH:mm:ss

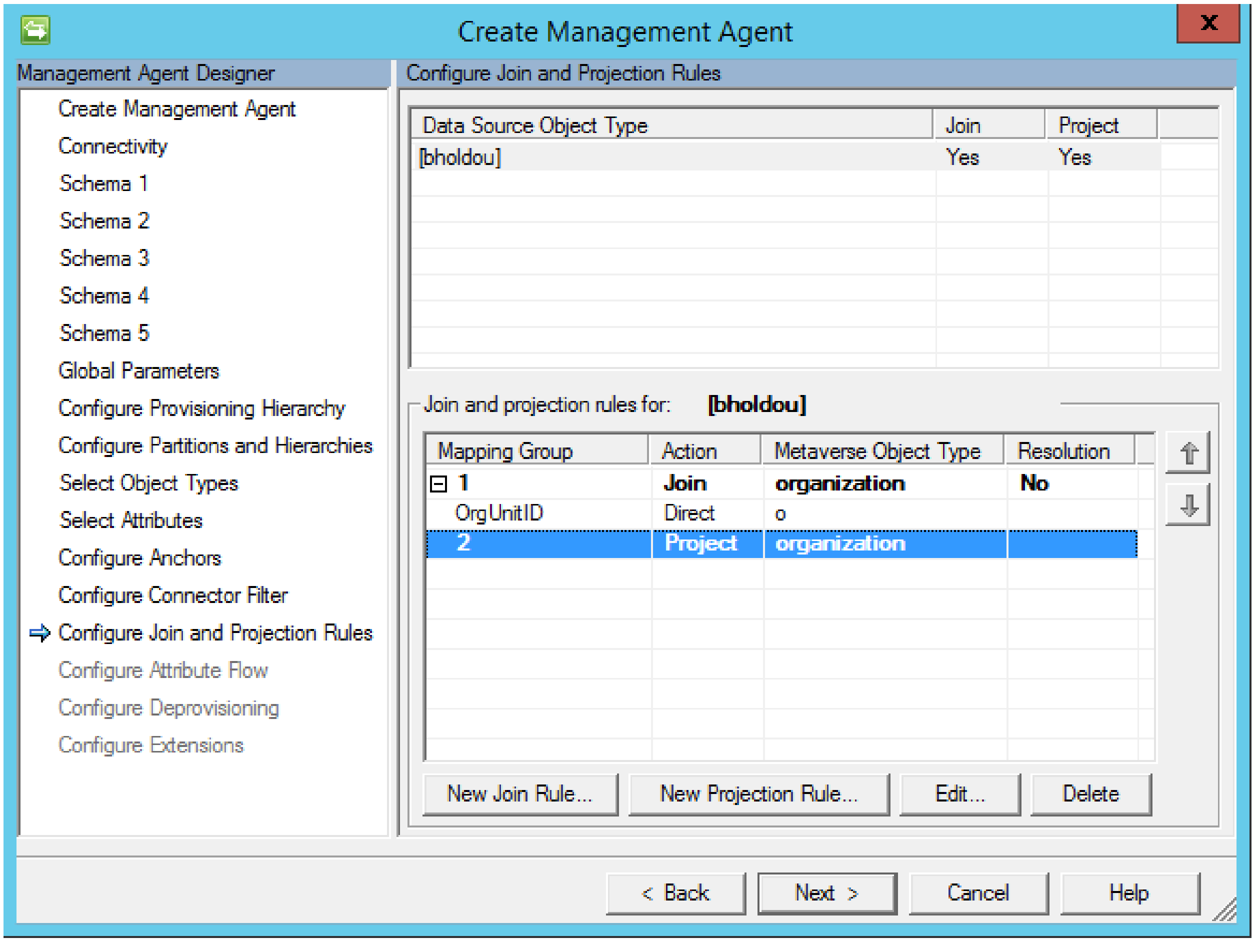
Password Operation

Operation Methods: Password Extension

Extension Name:

Set Password SP Name:

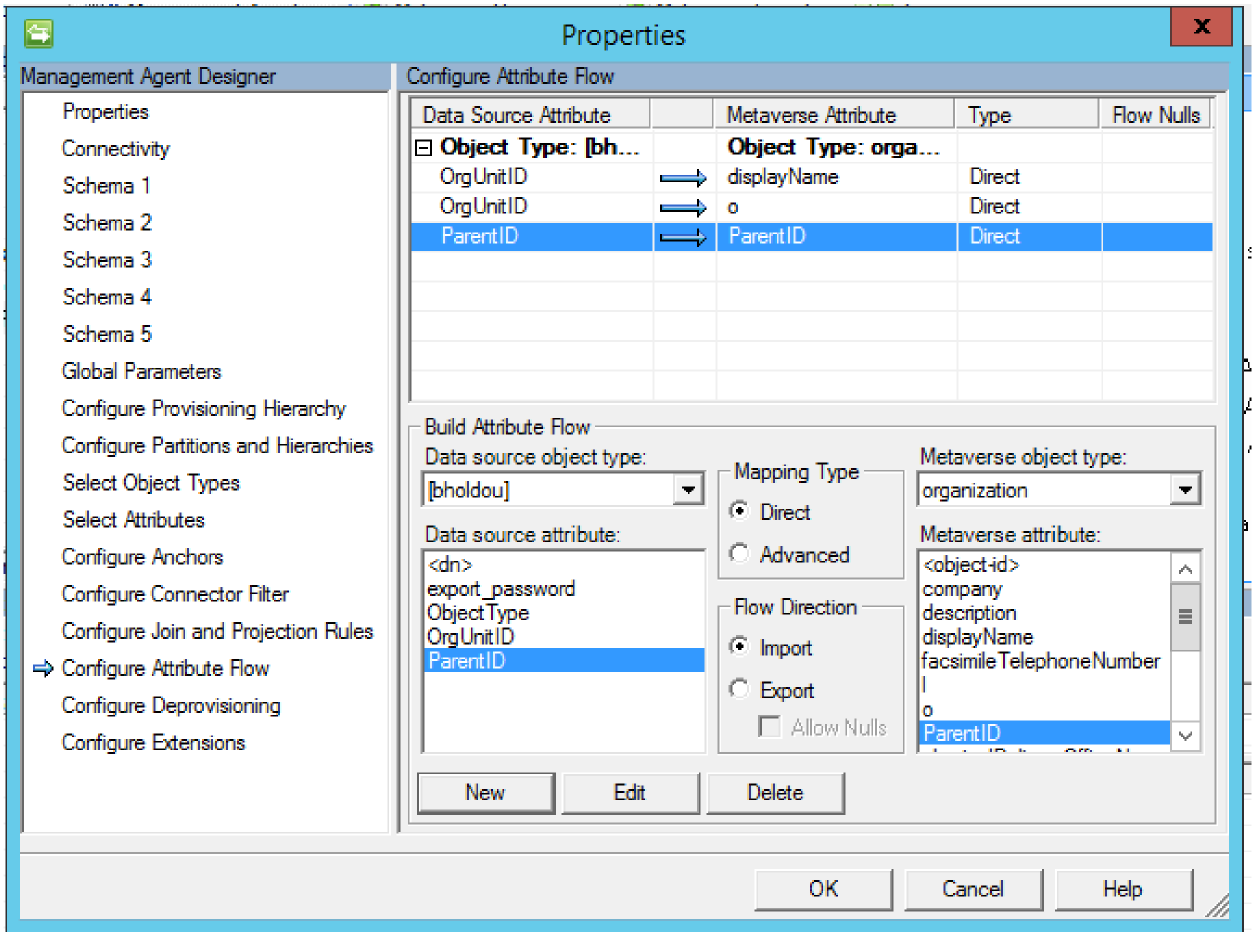
Set Password SP Parameters



Data Source Object Type	Join	Project
[bholdou]	Yes	Yes

Join and projection rules for: **[bholdou]**

Mapping Group	Action	Metaverse Object Type	Resolution
⊟ **1**	**Join**	**organization**	**No**
OrgUnitID	Direct	o	
2	Project	organization	



Data Source Attribute		Metaverse Attribute	Type	Flow Nulls
Object Type: [bh...		**Object Type: orga...**		
OrgUnitID	⟹	displayName	Direct	
OrgUnitID	⟹	o	Direct	
ParentID	⟹	ParentID	Direct	

Data source object type: [bholdou]

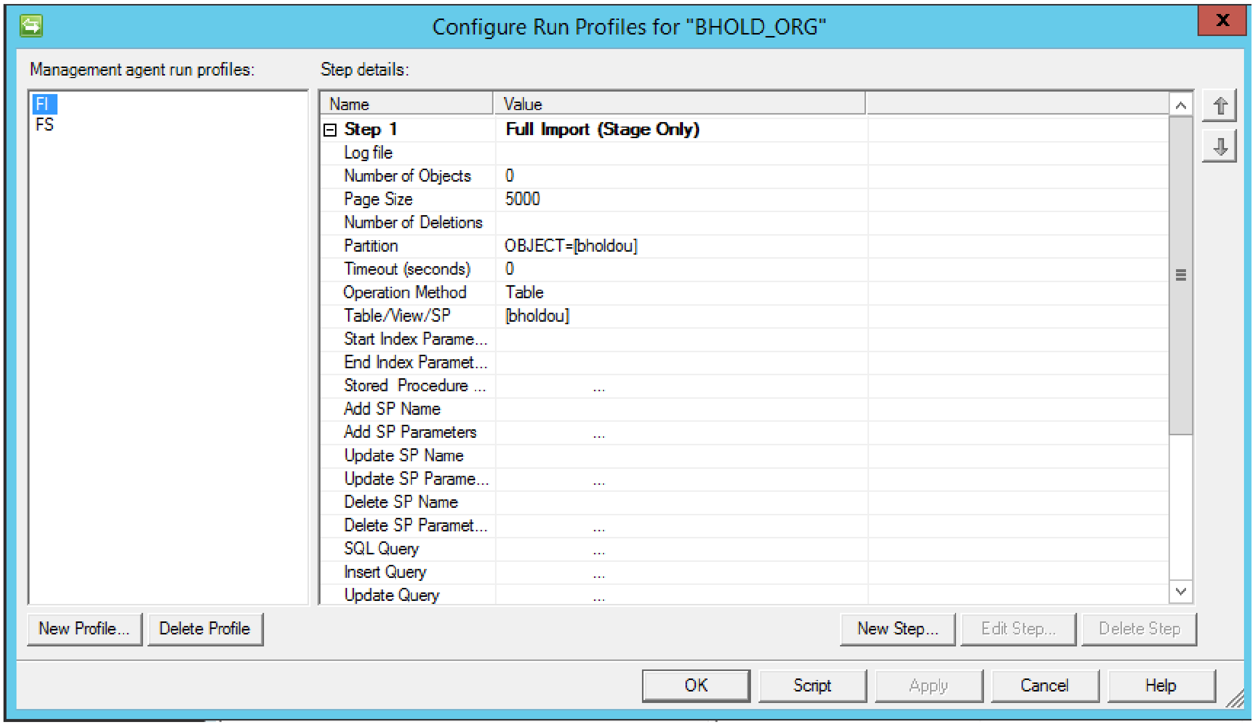
Data source attribute:
<dn>
export_password
ObjectType
OrgUnitID
ParentID

Mapping Type
● Direct
○ Advanced

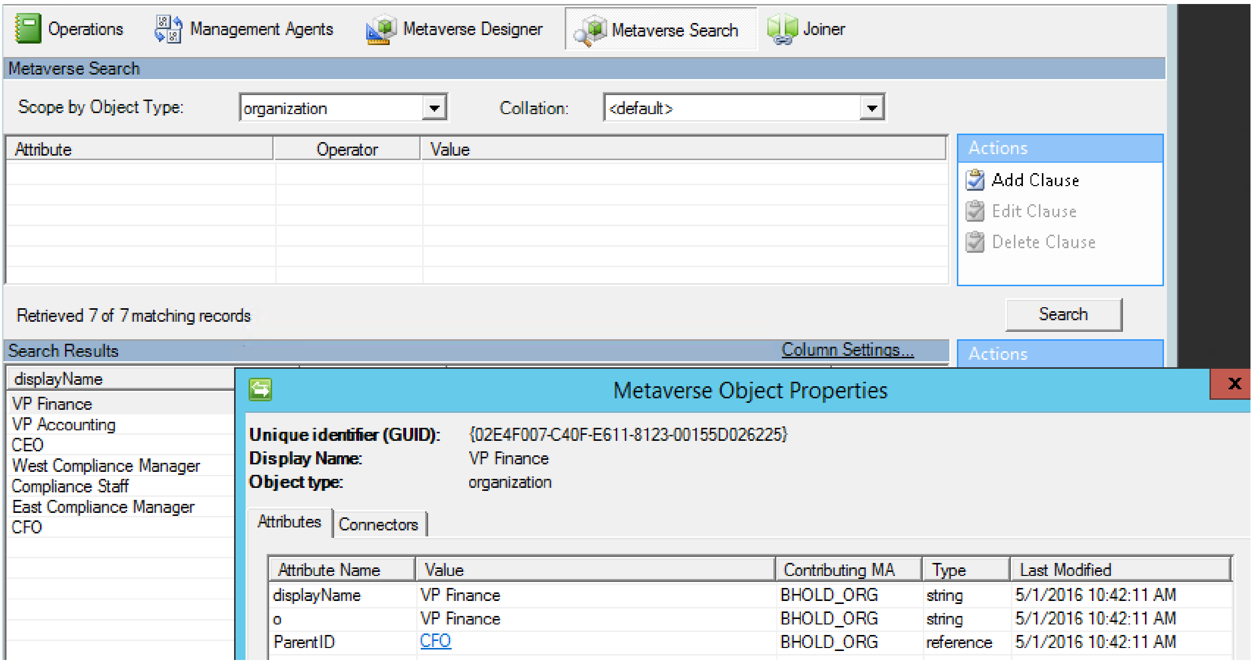
Flow Direction
● Import
○ Export
□ Allow Nulls

Metaverse object type: organization

Metaverse attribute:
<object-id>
company
description
displayName
facsimileTelephoneNumber
l
o
ParentID



Name	Value
Step 1	**Full Import (Stage Only)**
Log file	
Number of Objects	0
Page Size	5000
Number of Deletions	
Partition	OBJECT=[bholdou]
Timeout (seconds)	0
Operation Method	Table
Table/View/SP	[bholdou]
Start Index Parame...	
End Index Paramet...	
Stored Procedure ...	...
Add SP Name	
Add SP Parameters	...
Update SP Name	
Update SP Parame...	...
Delete SP Name	
Delete SP Paramet...	...
SQL Query	...
Insert Query	...
Update Query	...



Scope by Object Type: organization

Collation: <default>

Attribute	Operator	Value

Retrieved 7 of 7 matching records

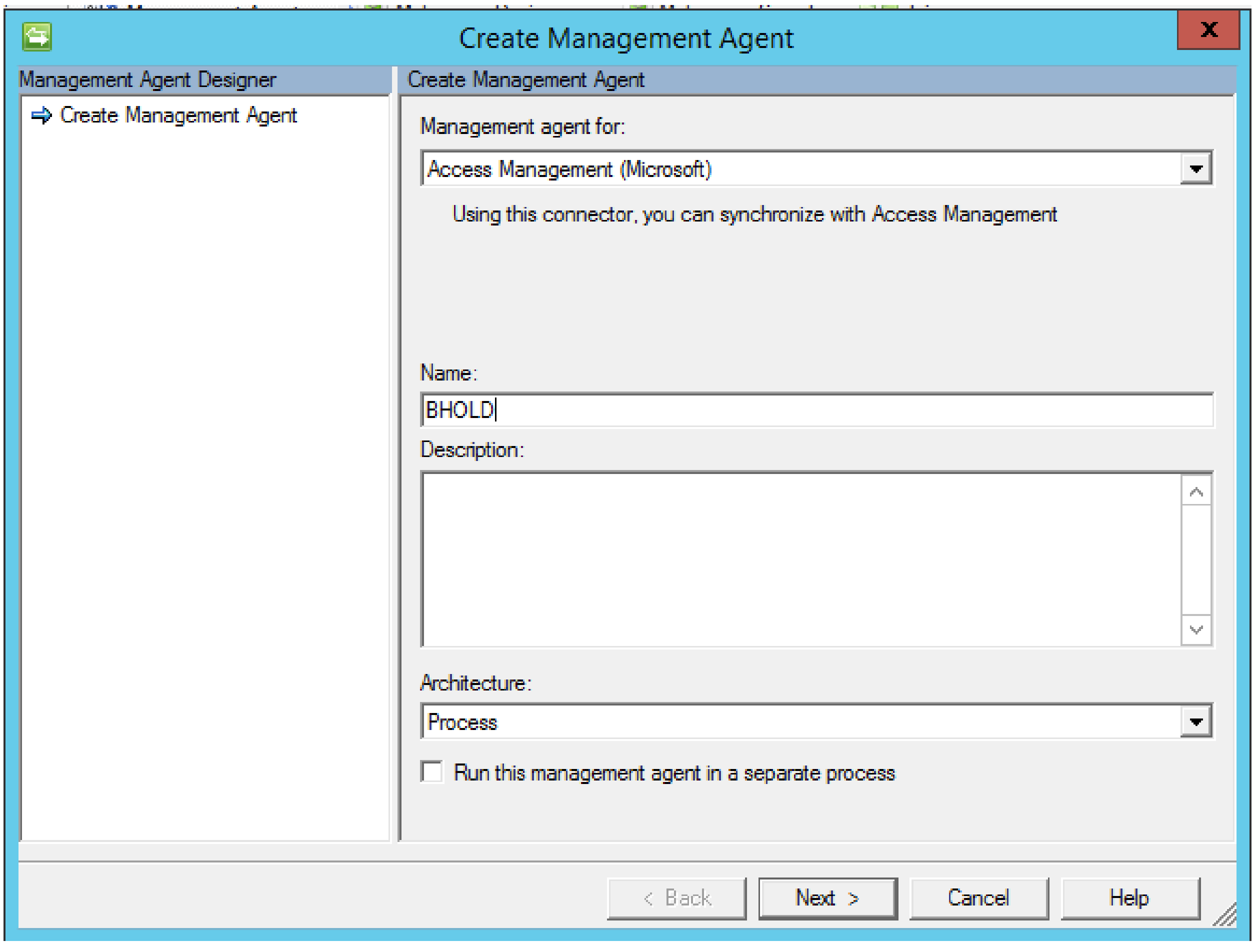
displayName
VP Finance
VP Accounting
CEO
West Compliance Manager
Compliance Staff
East Compliance Manager
CFO

Unique identifier (GUID): {02E4F007-C40F-E611-8123-00155D026225}

Display Name: VP Finance

Object type: organization

Attribute Name	Value	Contributing MA	Type	Last Modified
displayName	VP Finance	BHOLD_ORG	string	5/1/2016 10:42:11 AM
o	VP Finance	BHOLD_ORG	string	5/1/2016 10:42:11 AM
ParentID	CFO	BHOLD_ORG	reference	5/1/2016 10:42:11 AM



Management agent for: Access Management (Microsoft)

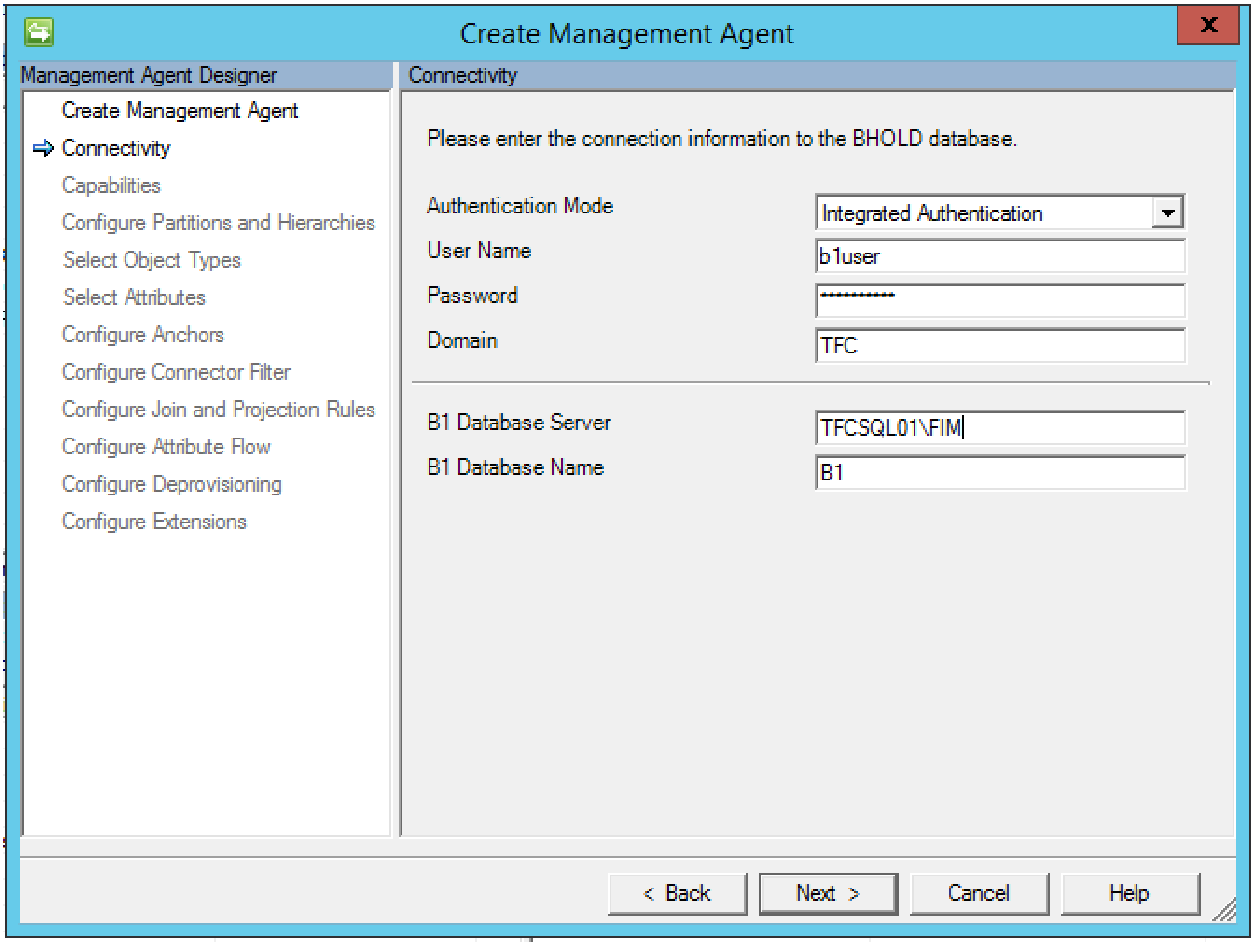
Using this connector, you can synchronize with Access Management

Name: BHOLD

Description:

Architecture: Process

□ Run this management agent in a separate process



Please enter the connection information to the BHOLD database.

Authentication Mode: Integrated Authentication

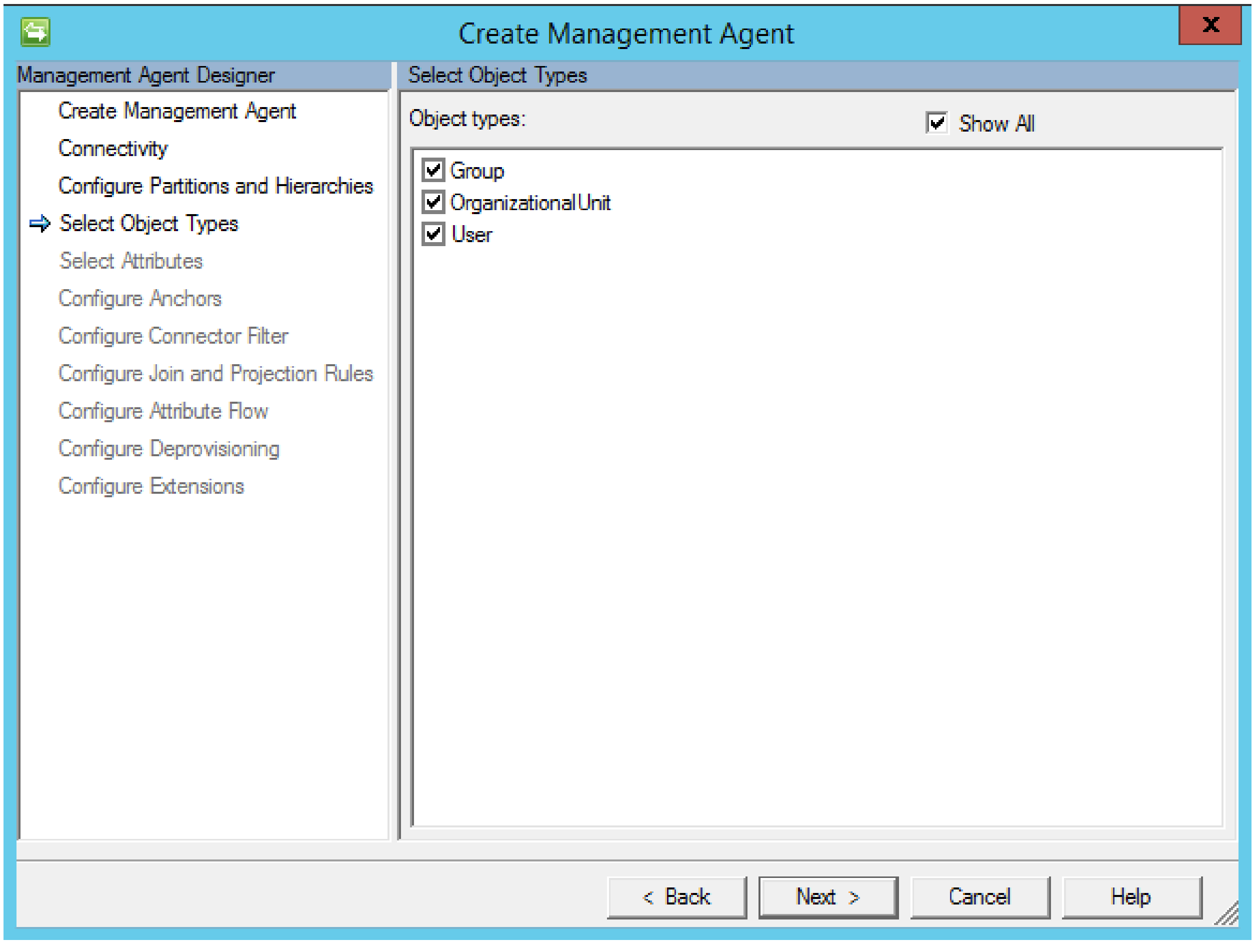
User Name: b1user

Password: ***********

Domain: TFC

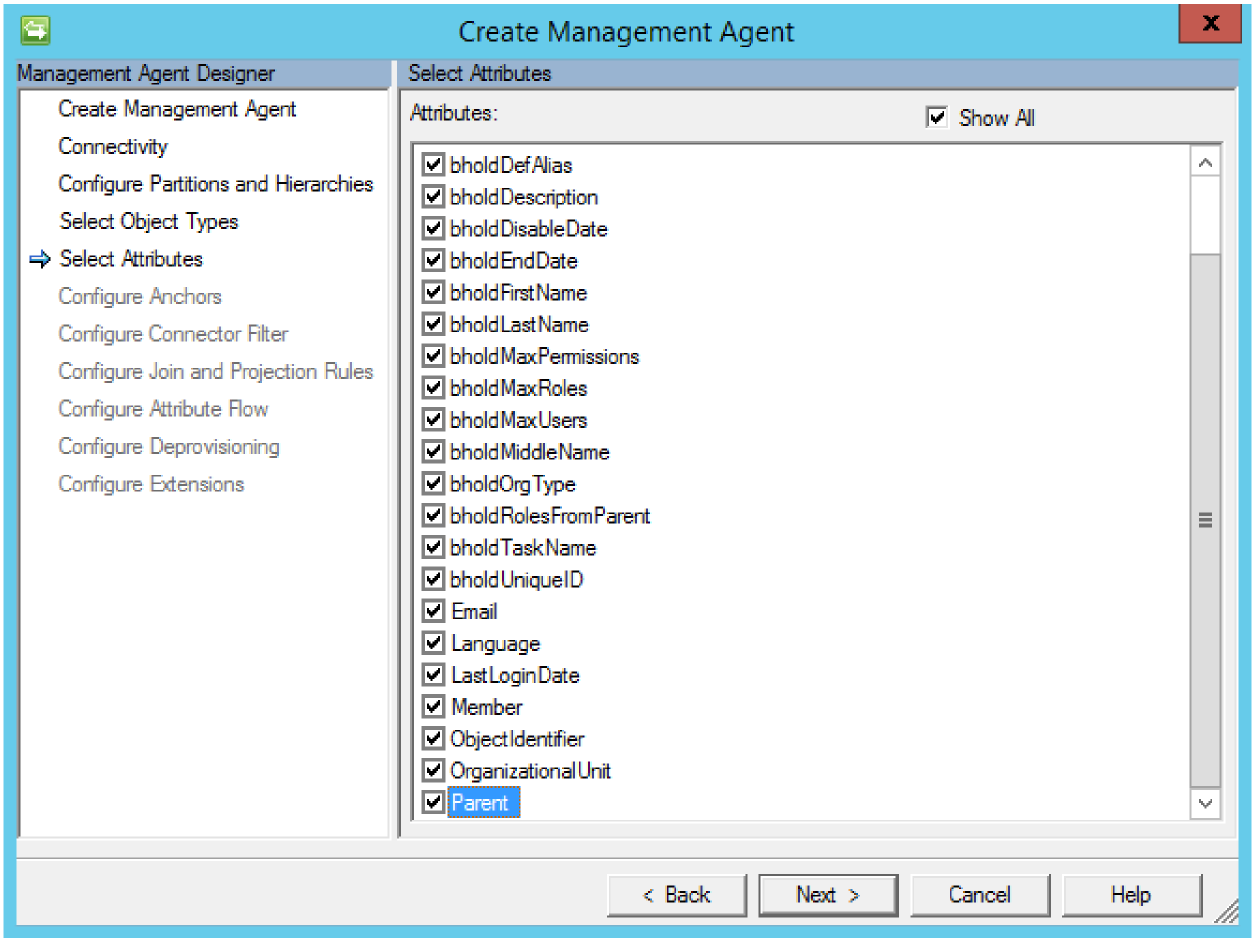
B1 Database Server: TFCSQL01\FIM

B1 Database Name: B1



Object types: ☑ Show All

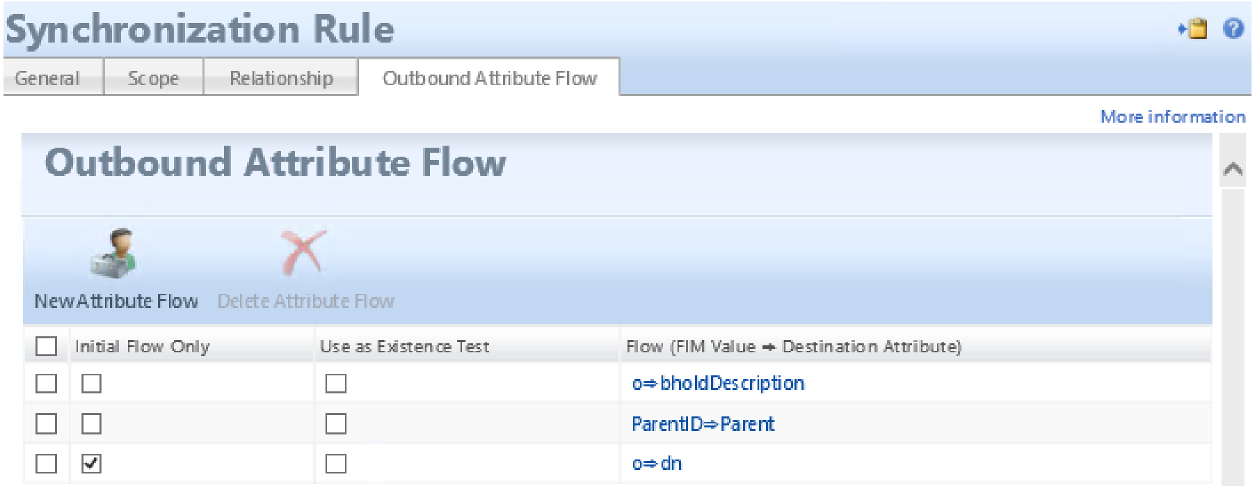
☑ Group
☑ OrganizationalUnit
☑ User



Select Attributes

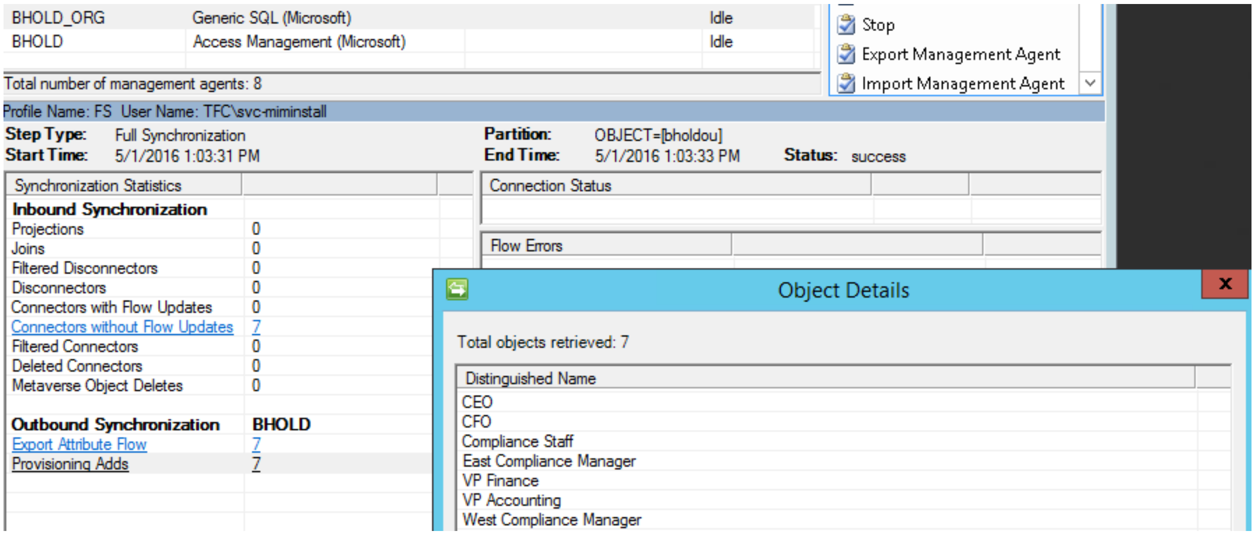
Attributes: ☑ Show All

- ☑ bholdDefAlias
- ☑ bholdDescription
- ☑ bholdDisableDate
- ☑ bholdEndDate
- ☑ bholdFirstName
- ☑ bholdLastName
- ☑ bholdMaxPermissions
- ☑ bholdMaxRoles
- ☑ bholdMaxUsers
- ☑ bholdMiddleName
- ☑ bholdOrgType
- ☑ bholdRolesFromParent
- ☑ bholdTaskName
- ☑ bholdUniqueID
- ☑ Email
- ☑ Language
- ☑ LastLoginDate
- ☑ Member
- ☑ ObjectIdentifier
- ☑ OrganizationalUnit
- ☑ Parent



Outbound Attribute Flow

□	Initial Flow Only	Use as Existence Test	Flow (FIM Value ➔ Destination Attribute)
□	□	□	o⇒bholdDescription
□	□	□	ParentID⇒Parent
□	☑	□	o⇒dn



BHOLD_ORG	Generic SQL (Microsoft)	Idle
BHOLD	Access Management (Microsoft)	Idle

Total number of management agents: 8

Profile Name: FS User Name: TFC\svc-miminstall

Step Type: Full Synchronization **Partition:** OBJECT=[bholdou]
Start Time: 5/1/2016 1:03:31 PM **End Time:** 5/1/2016 1:03:33 PM **Status:** success

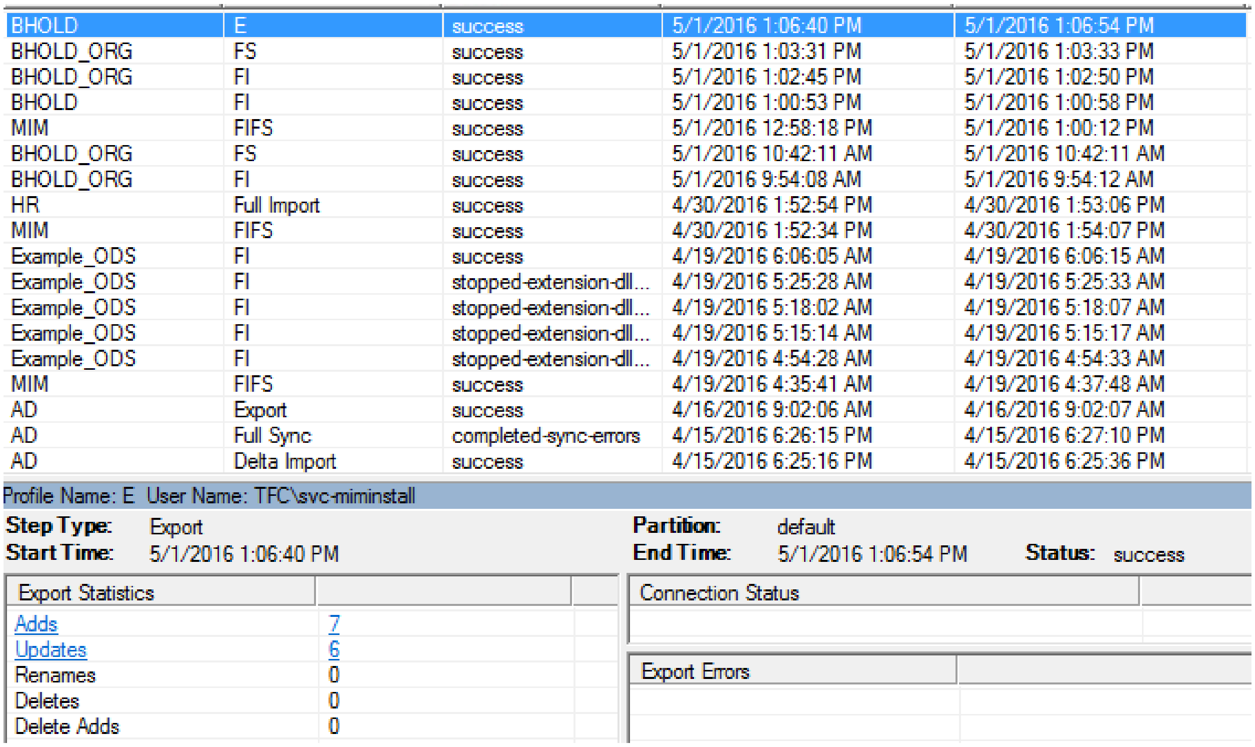
Synchronization Statistics	
Inbound Synchronization	
Projections	0
Joins	0
Filtered Disconnectors	0
Disconnectors	0
Connectors with Flow Updates	0
Connectors without Flow Updates	7
Filtered Connectors	0
Deleted Connectors	0
Metaverse Object Deletes	0
Outbound Synchronization	**BHOLD**
Export Attribute Flow	7
Provisioning Adds	7

Connection Status

Flow Errors

Total objects retrieved: 7

Distinguished Name
CEO
CFO
Compliance Staff
East Compliance Manager
VP Finance
VP Accounting
West Compliance Manager



BHOLD	E	success	5/1/2016 1:06:40 PM	5/1/2016 1:06:54 PM
BHOLD_ORG	FS	success	5/1/2016 1:03:31 PM	5/1/2016 1:03:33 PM
BHOLD_ORG	FI	success	5/1/2016 1:02:45 PM	5/1/2016 1:02:50 PM
BHOLD	FI	success	5/1/2016 1:00:53 PM	5/1/2016 1:00:58 PM
MIM	FIFS	success	5/1/2016 12:58:18 PM	5/1/2016 1:00:12 PM
BHOLD_ORG	FS	success	5/1/2016 10:42:11 AM	5/1/2016 10:42:11 AM
BHOLD_ORG	FI	success	5/1/2016 9:54:08 AM	5/1/2016 9:54:12 AM
HR	Full Import	success	4/30/2016 1:52:54 PM	4/30/2016 1:53:06 PM
MIM	FIFS	success	4/30/2016 1:52:34 PM	4/30/2016 1:54:07 PM
Example_ODS	FI	success	4/19/2016 6:06:05 AM	4/19/2016 6:06:15 AM
Example_ODS	FI	stopped-extension-dll...	4/19/2016 5:25:28 AM	4/19/2016 5:25:33 AM
Example_ODS	FI	stopped-extension-dll...	4/19/2016 5:18:02 AM	4/19/2016 5:18:07 AM
Example_ODS	FI	stopped-extension-dll...	4/19/2016 5:15:14 AM	4/19/2016 5:15:17 AM
Example_ODS	FI	stopped-extension-dll...	4/19/2016 4:54:28 AM	4/19/2016 4:54:33 AM
MIM	FIFS	success	4/19/2016 4:35:41 AM	4/19/2016 4:37:48 AM
AD	Export	success	4/16/2016 9:02:06 AM	4/16/2016 9:02:07 AM
AD	Full Sync	completed-sync-errors	4/15/2016 6:26:15 PM	4/15/2016 6:27:10 PM
AD	Delta Import	success	4/15/2016 6:25:16 PM	4/15/2016 6:25:36 PM

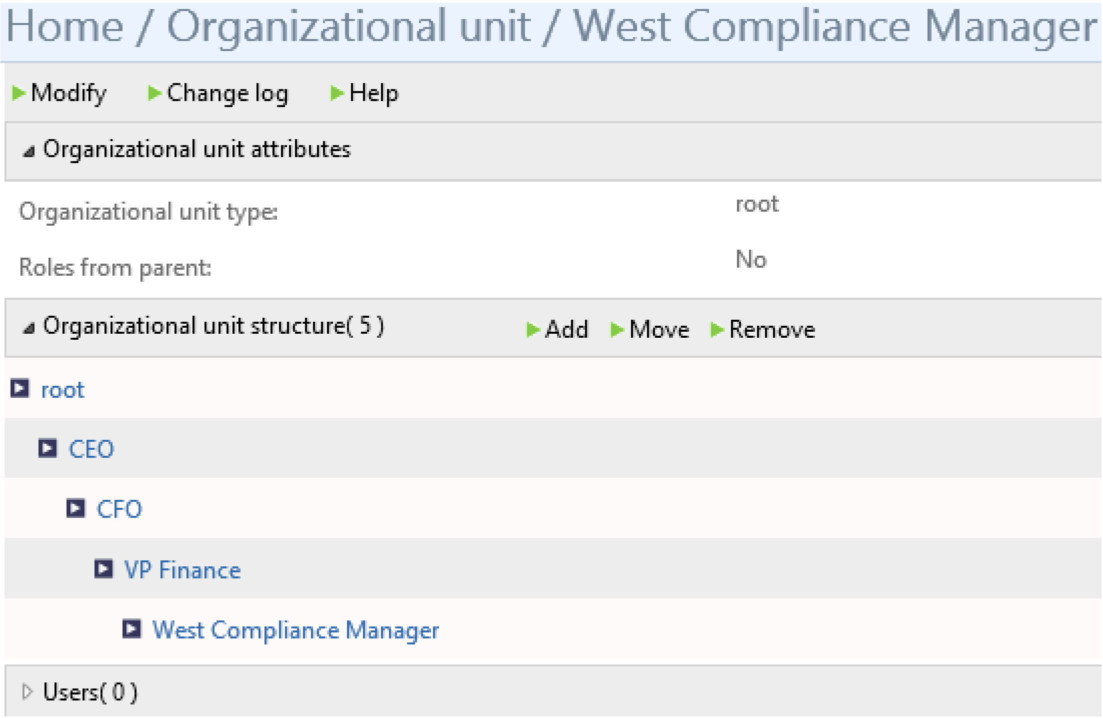
Profile Name: E User Name: TFC\svc-miminstall

Step Type: Export **Partition:** default
Start Time: 5/1/2016 1:06:40 PM **End Time:** 5/1/2016 1:06:54 PM **Status:** success

Export Statistics	
Adds	7
Updates	6
Renames	0
Deletes	0
Delete Adds	0

Connection Status

Export Errors



Home / Organizational unit / West Compliance Manager

▶ Modify ▶ Change log ▶ Help

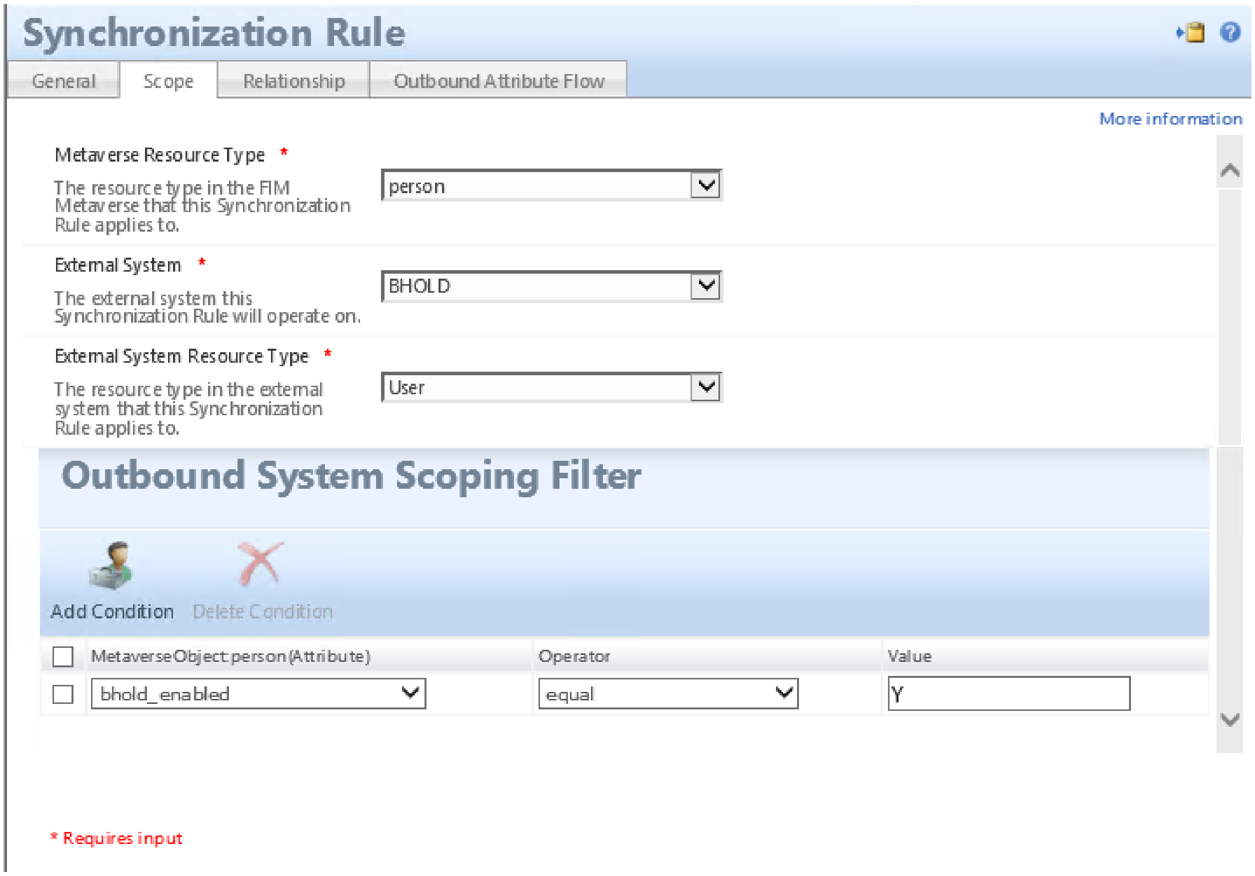
◢ Organizational unit attributes

Organizational unit type:	root
Roles from parent:	No

◢ Organizational unit structure(5) ▶ Add ▶ Move ▶ Remove

- root
  - CEO
    - CFO
      - VP Finance
        - West Compliance Manager

▷ Users(0)



Synchronization Rule

Metaverse Resource Type * : person
The resource type in the FIM Metaverse that this Synchronization Rule applies to.

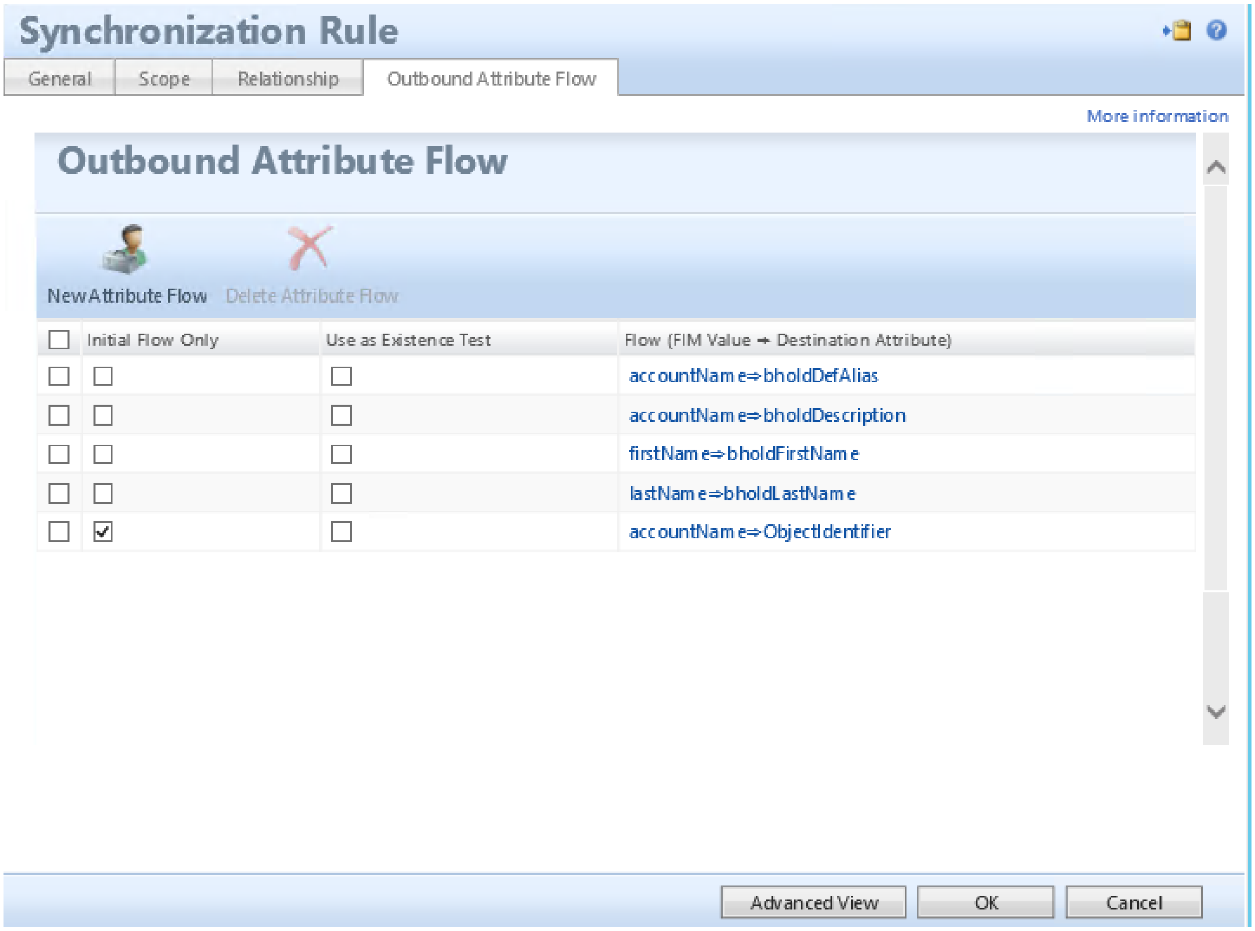
External System * : BHOLD
The external system this Synchronization Rule will operate on.

External System Resource Type * : User
The resource type in the external system that this Synchronization Rule applies to.

Outbound System Scoping Filter

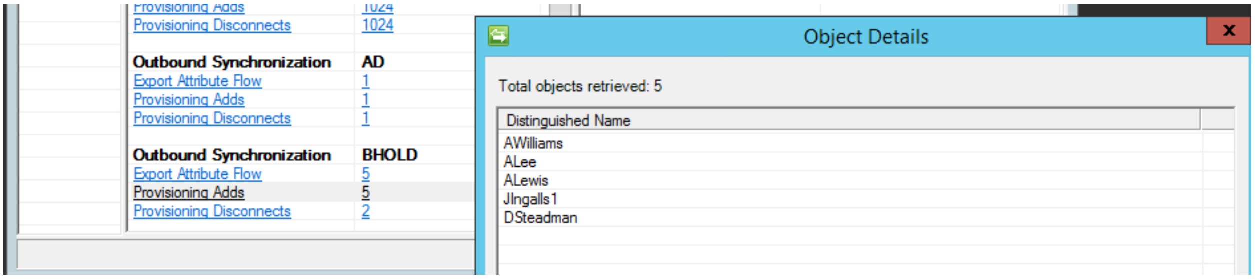
□	MetaverseObject:person(Attribute)	Operator	Value
□	bhold_enabled	equal	Y

* Requires input



Outbound Attribute Flow

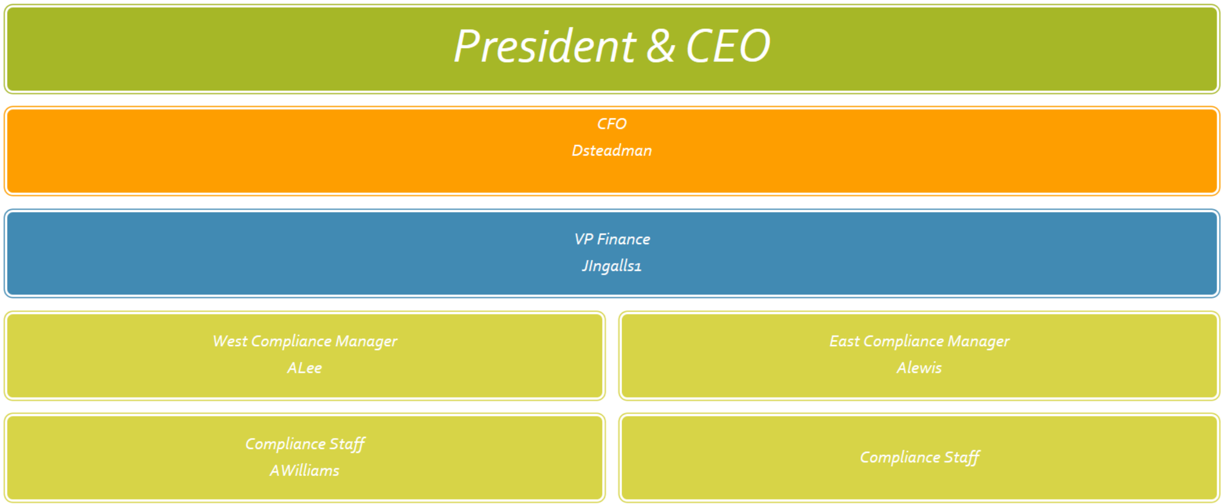
□	Initial Flow Only	Use as Existence Test	Flow (FIM Value ➡ Destination Attribute)
□	□	□	accountName⇒bholdDefAlias
□	□	□	accountName⇒bholdDescription
□	□	□	firstName⇒bholdFirstName
□	□	□	lastName⇒bholdLastName
□	☑	□	accountName⇒ObjectIdentifier

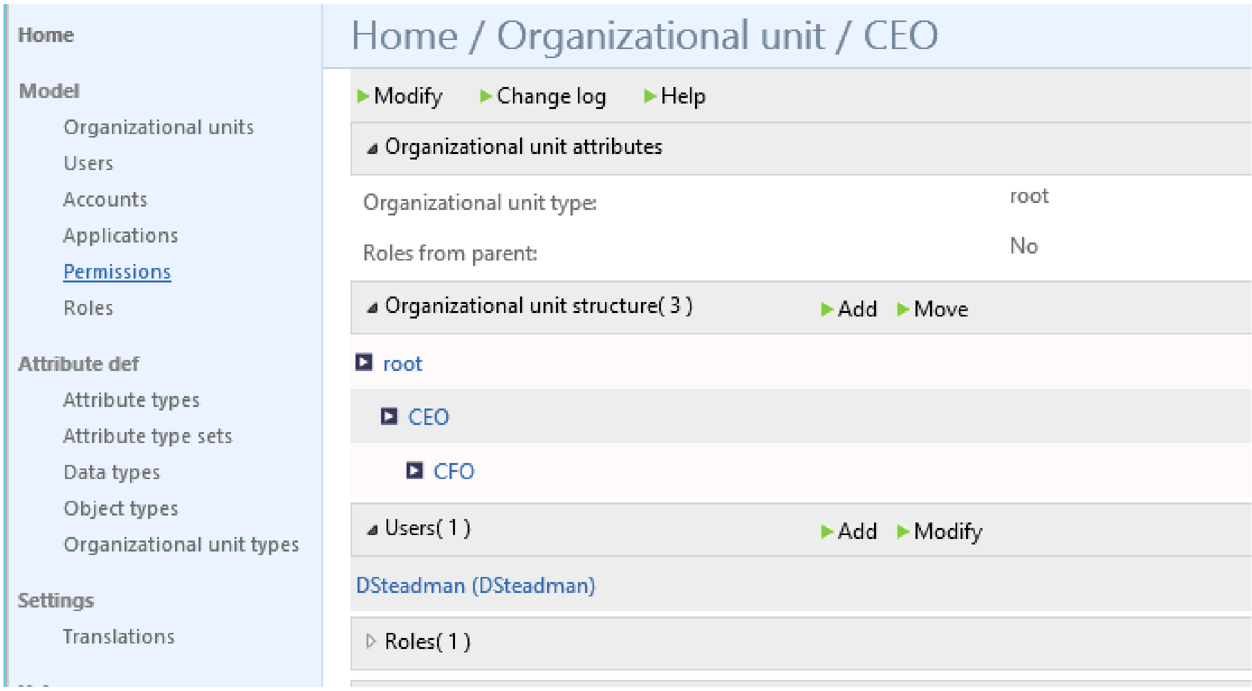


Provisioning Adds	1024
Provisioning Disconnects	1024
Outbound Synchronization	**AD**
Export Attribute Flow	1
Provisioning Adds	1
Provisioning Disconnects	1
Outbound Synchronization	**BHOLD**
Export Attribute Flow	5
Provisioning Adds	5
Provisioning Disconnects	2

Total objects retrieved: 5

Distinguished Name
AWilliams
ALee
ALewis
JIngalls1
DSteadman





Home / Organizational unit / CEO

Organizational unit attributes

Organizational unit type:	root
Roles from parent:	No

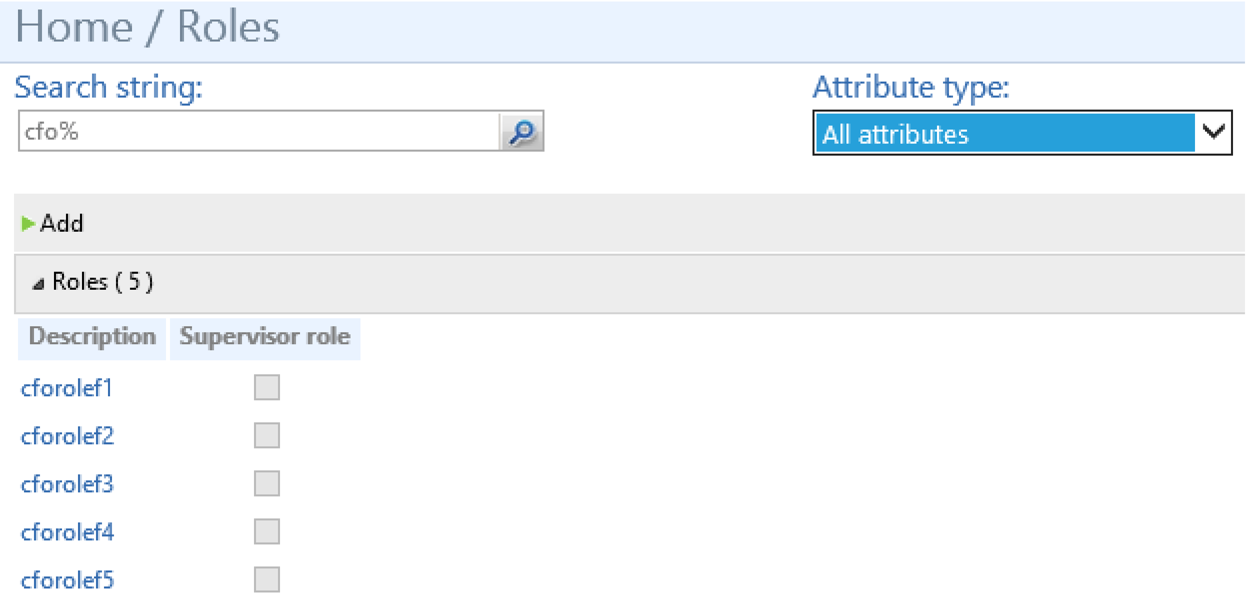
Organizational unit structure(3)

- root
  - CEO
    - CFO

Users(1)

DSteadman (DSteadman)

Roles(1)



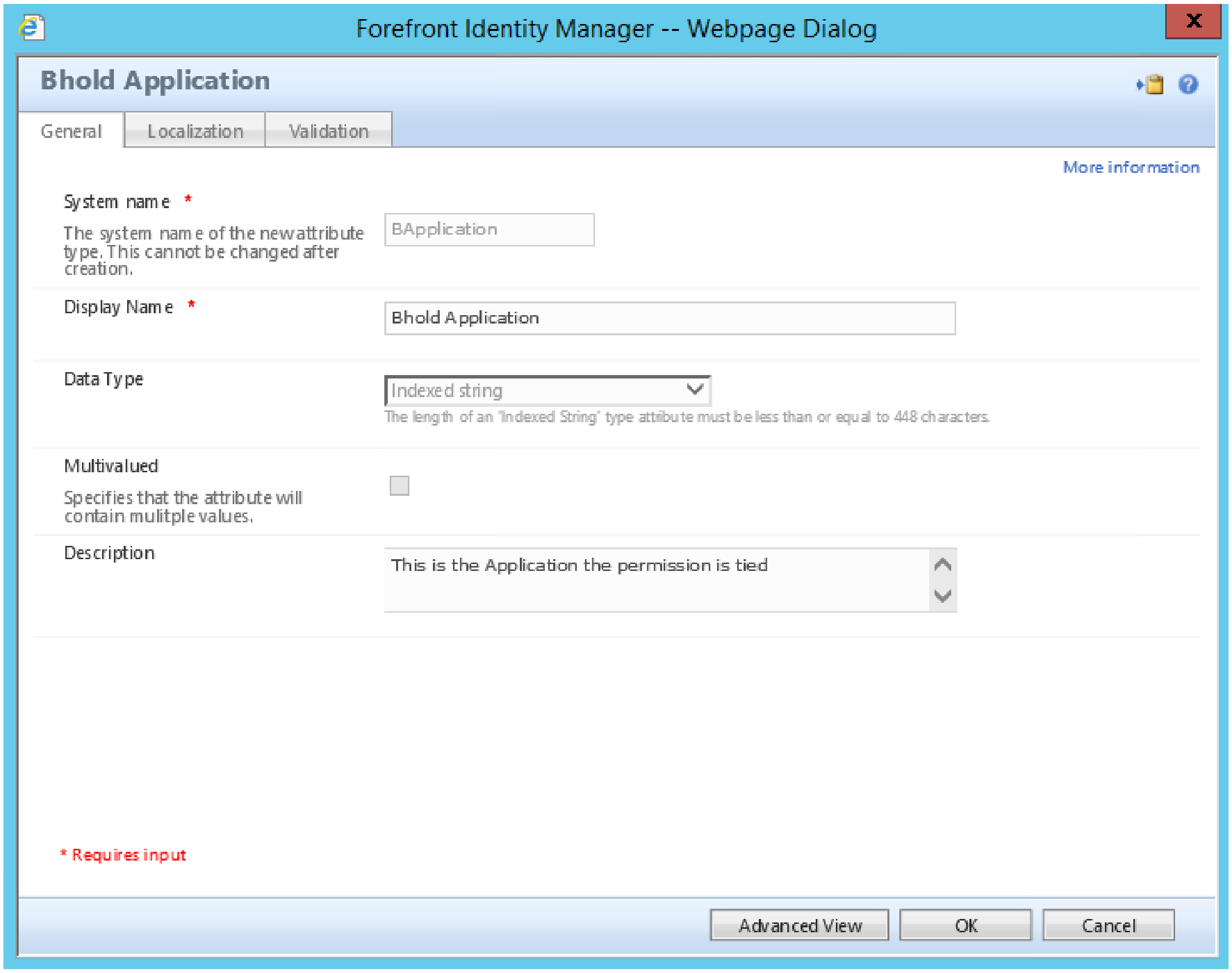
Home / Roles

Search string: cfo%

Attribute type: All attributes

Roles (5)

Description	Supervisor role
cforolef1	□
cforolef2	□
cforolef3	□
cforolef4	□
cforolef5	□



Forefront Identity Manager -- Webpage Dialog

Bhold Application

System name * BApplication

The system name of the new attribute type. This cannot be changed after creation.

Display Name * Bhold Application

Data Type Indexed string

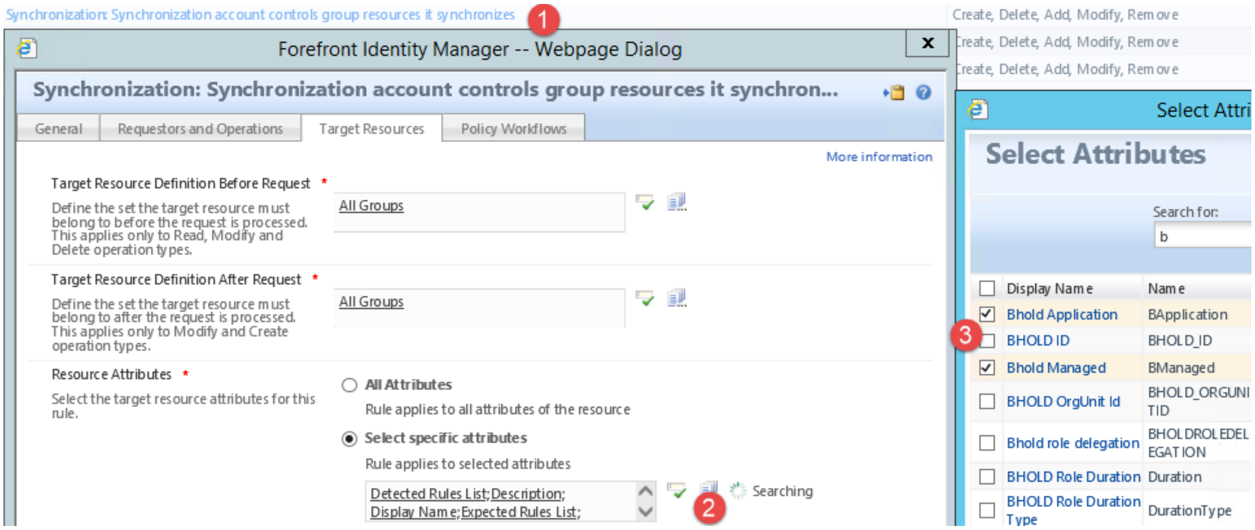
The length of an 'Indexed String' type attribute must be less than or equal to 448 characters.

Multivalued □

Specifies that the attribute will contain mulitple values.

Description This is the Application the permission is tied

* Requires input



Synchronization: Synchronization account controls group resources it synchronizes

Create, Delete, Add, Modify, Remove
Create, Delete, Add, Modify, Remove
Create, Delete, Add, Modify, Remove

Forefront Identity Manager -- Webpage Dialog

Synchronization: Synchronization account controls group resources it synchron...

General | Requestors and Operations | Target Resources | Policy Workflows

More information

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 Groups

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 Groups

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

Detected Rules List;Description;
Display Name;Expected Rules List;

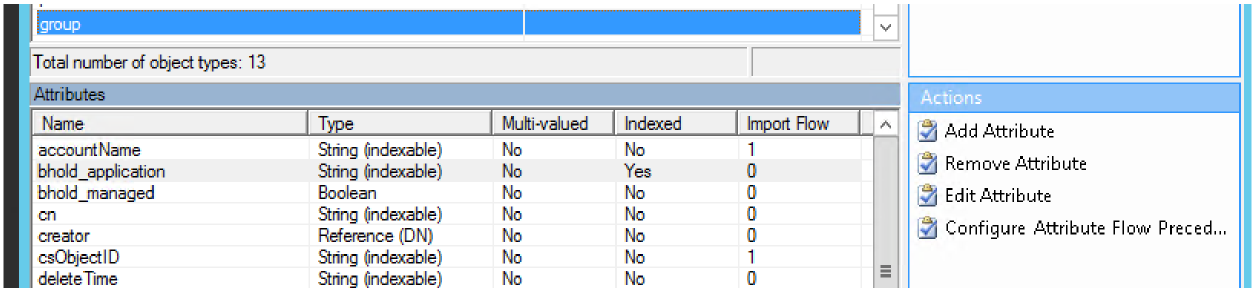
Searching

Select Attri

Select Attributes

Search for:
b

□	Display Name	Name
☑	Bhold Application	BApplication
□	BHOLD ID	BHOLD_ID
☑	Bhold Managed	BManaged
□	BHOLD OrgUnit Id	BHOLD_ORGUNITID
□	Bhold role delegation	BHOLDROLEDELEGATION
□	BHOLD Role Duration	Duration
□	BHOLD Role Duration Type	DurationType



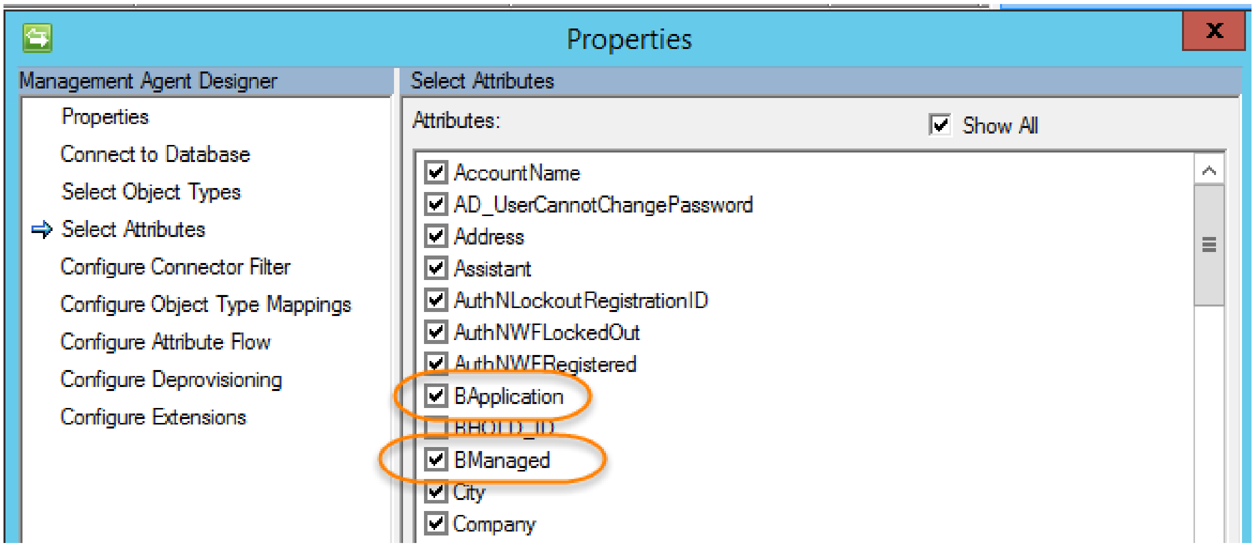
group

Total number of object types: 13

Attributes

Name	Type	Multi-valued	Indexed	Import Flow
accountName	String (indexable)	No	No	1
bhold_application	String (indexable)	No	Yes	0
bhold_managed	Boolean	No	No	0
cn	String (indexable)	No	No	0
creator	Reference (DN)	No	No	0
csObjectID	String (indexable)	No	No	1
deleteTime	String (indexable)	No	No	0

Actions
- Add Attribute
- Remove Attribute
- Edit Attribute
- Configure Attribute Flow Preced...



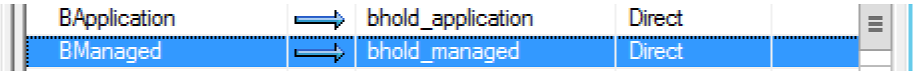
Properties

Management Agent Designer
- Properties
- Connect to Database
- Select Object Types
- Select Attributes
- Configure Connector Filter
- Configure Object Type Mappings
- Configure Attribute Flow
- Configure Deprovisioning
- Configure Extensions

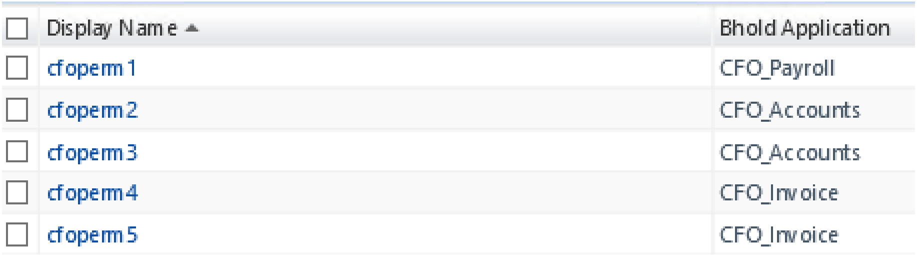
Select Attributes

Attributes: ☑ Show All

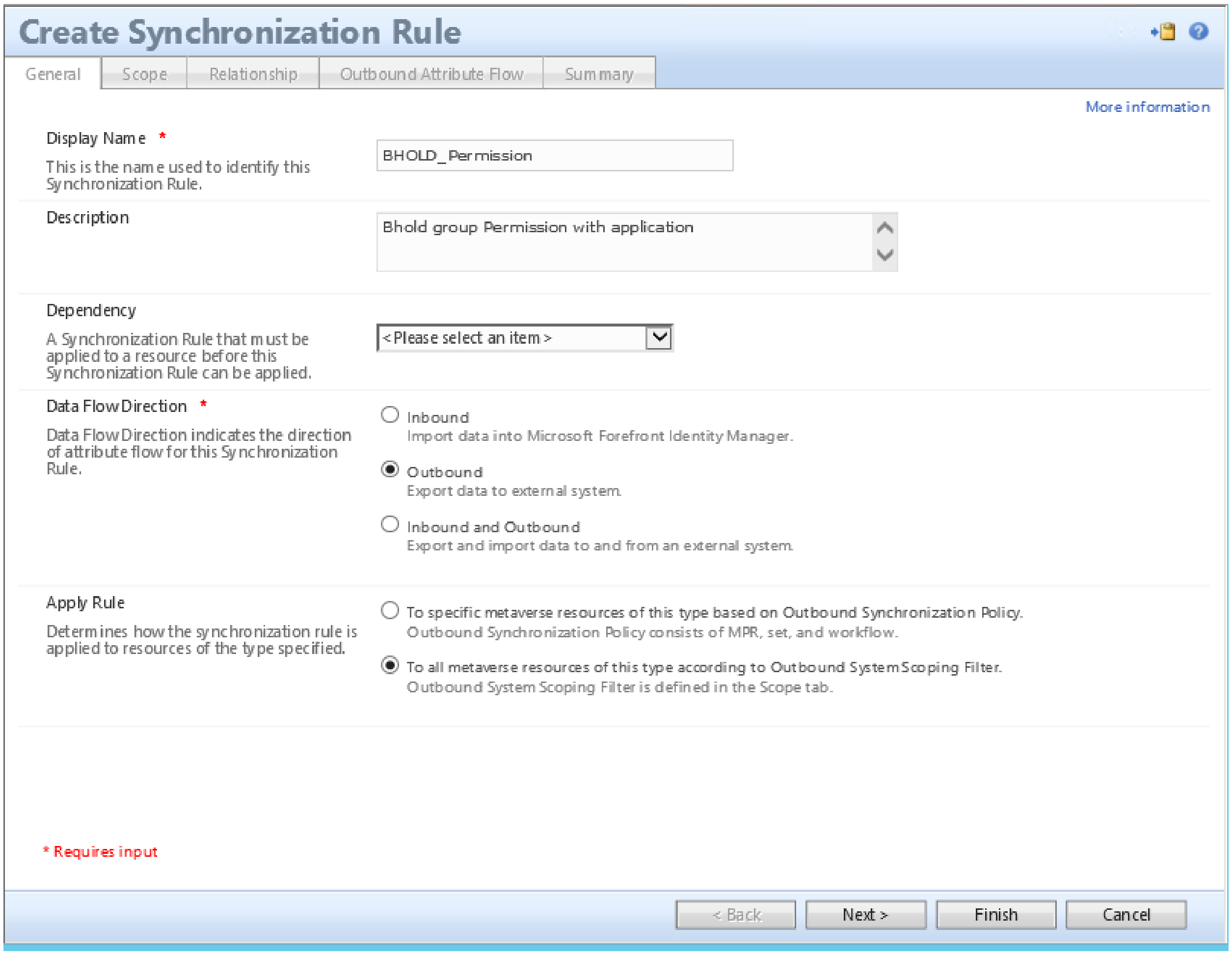
☑ AccountName
☑ AD_UserCannotChangePassword
☑ Address
☑ Assistant
☑ AuthNLockoutRegistrationID
☑ AuthNWFLockedOut
☑ AuthNWFRegistered
☑ BApplication
□ BHOLD_ID
☑ BManaged
☑ City
☑ Company



BApplication	→	bhold_application	Direct
BManaged	→	bhold_managed	Direct



□	Display Name ▲	Bhold Application
□	cfoperm1	CFO_Payroll
□	cfoperm2	CFO_Accounts
□	cfoperm3	CFO_Accounts
□	cfoperm4	CFO_Invoice
□	cfoperm5	CFO_Invoice



Create Synchronization Rule

Display Name *

This is the name used to identify this Synchronization Rule.

BHOLD_Permission

Description

Bhold group Permission with application

Dependency

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

<Please select an item>

Data Flow Direction *

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

○ 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.

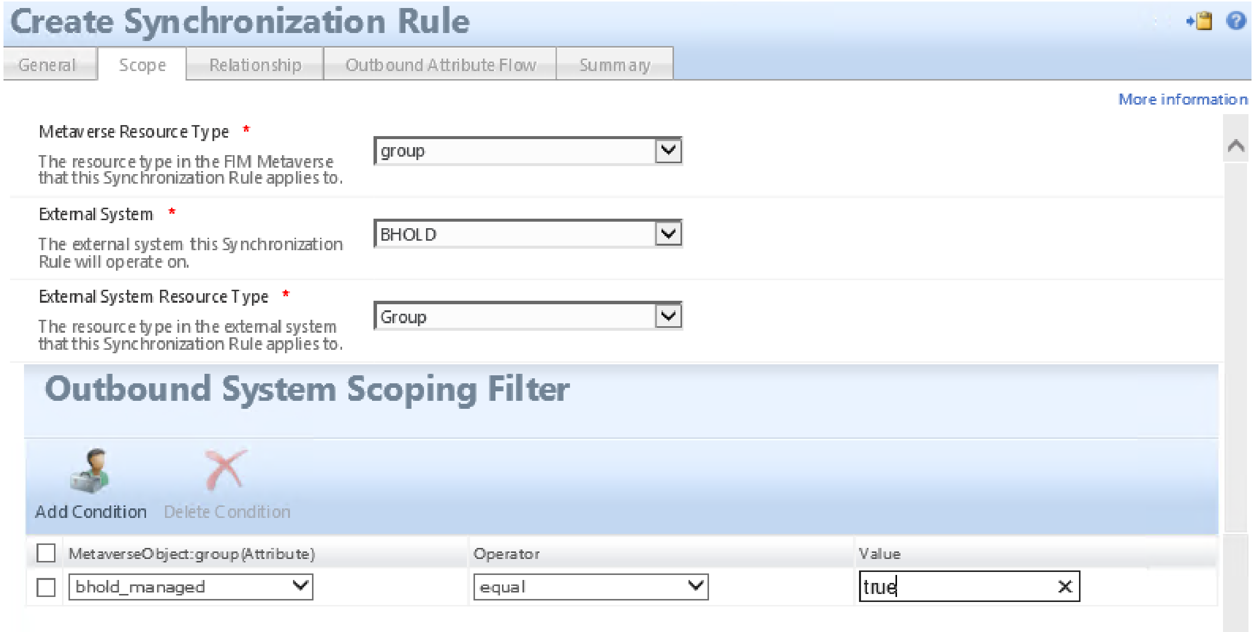
Apply Rule

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



Metaverse Resource Type *

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

group

External System *

The external system this Synchronization Rule will operate on.

BHOLD

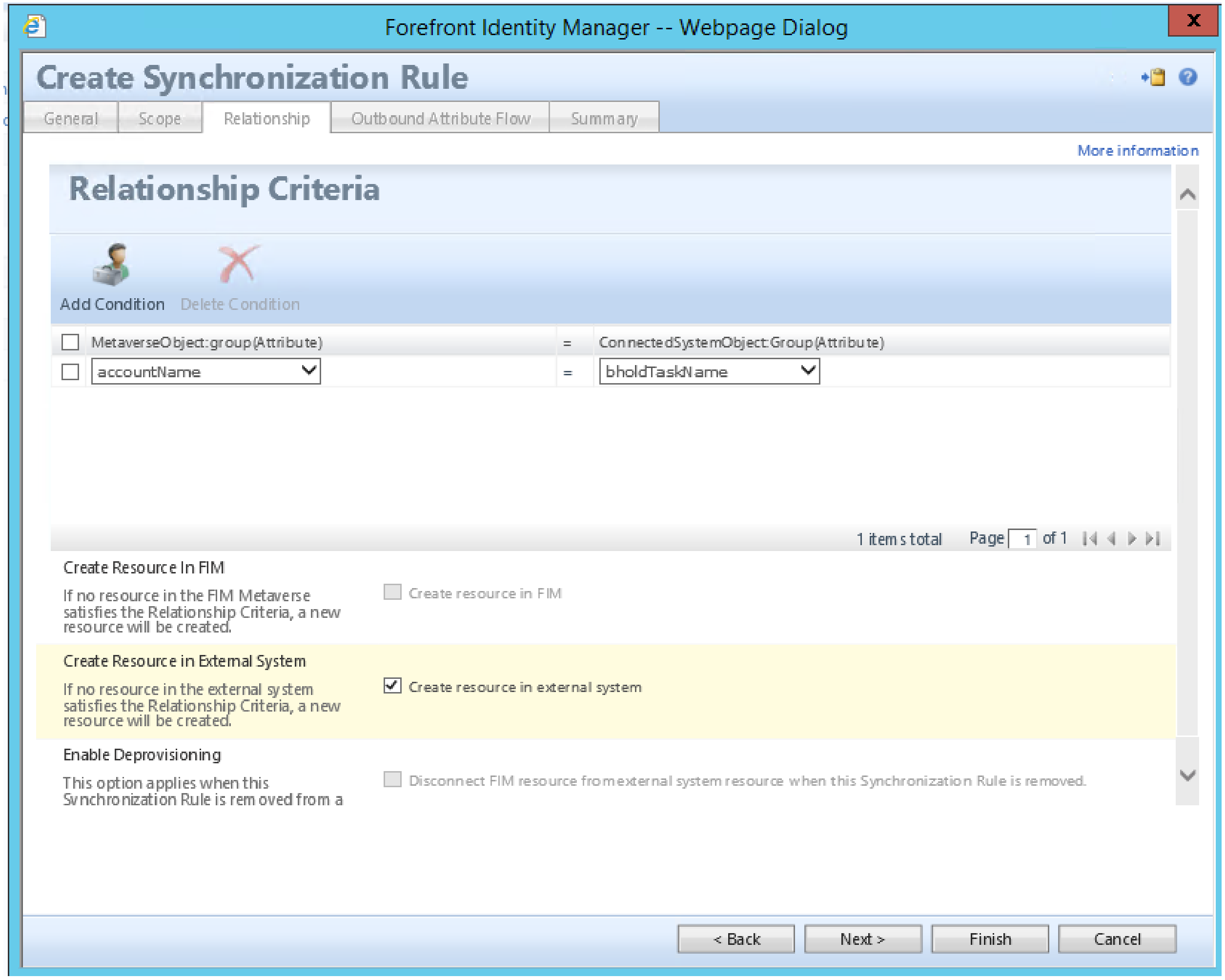
External System Resource Type *

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

Group

Outbound System Scoping Filter

□	MetaverseObject:group(Attribute)	Operator	Value
□	bhold_managed	equal	true



Relationship Criteria

□	MetaverseObject:group(Attribute)	=	ConnectedSystemObject:Group(Attribute)
□	accountName	=	bholdTaskName

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

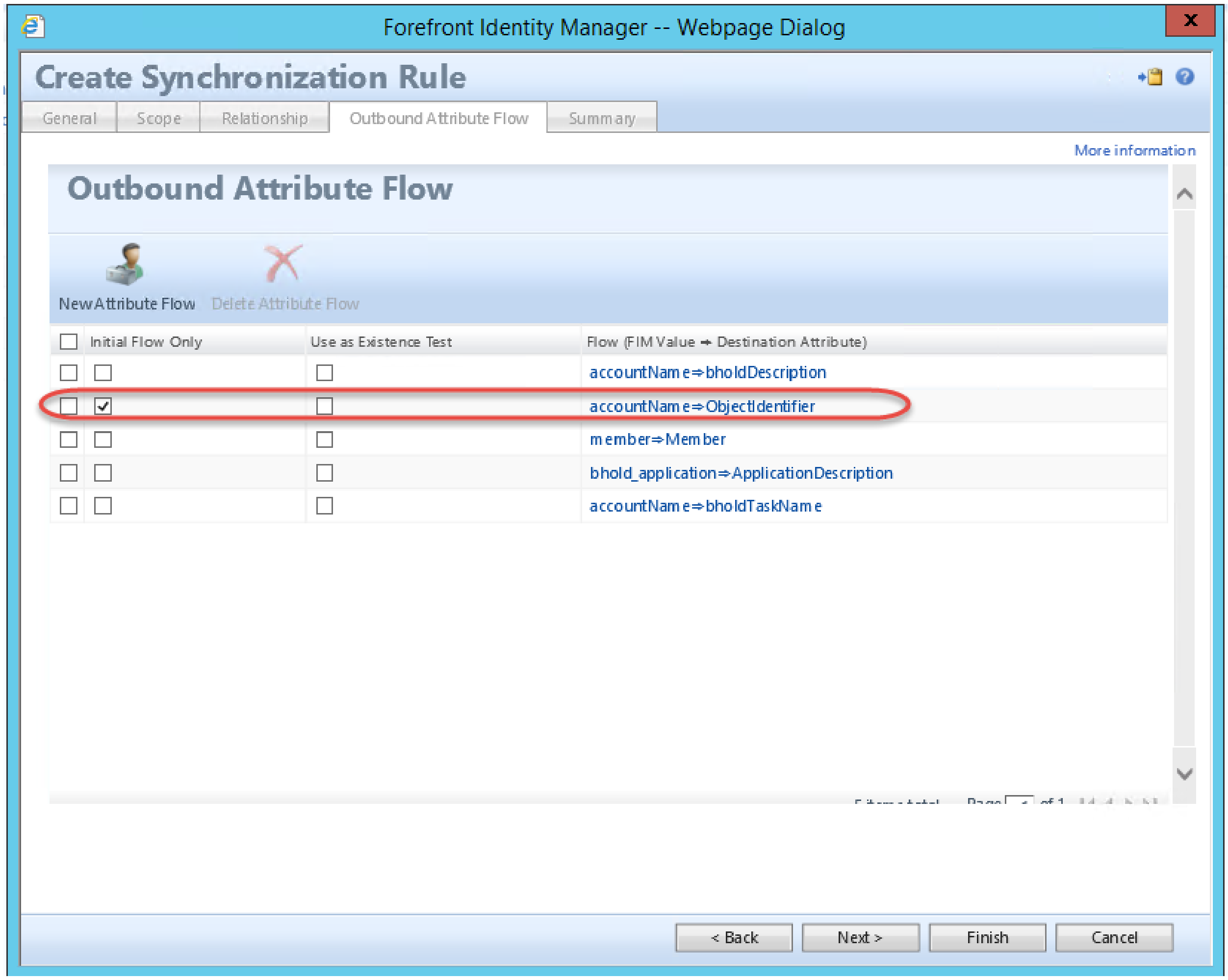
If no resource in the external system satisfies the Relationship Criteria, a new resource will be created.

☑ Create resource in external system

Enable Deprovisioning

This option applies when this Synchronization Rule is removed from a

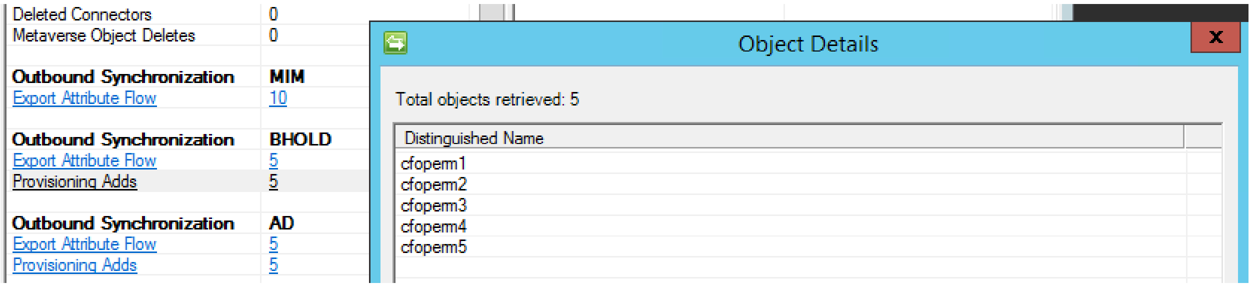
□ Disconnect FIM resource from external system resource when this Synchronization Rule is removed.



Create Synchronization Rule

Outbound Attribute Flow

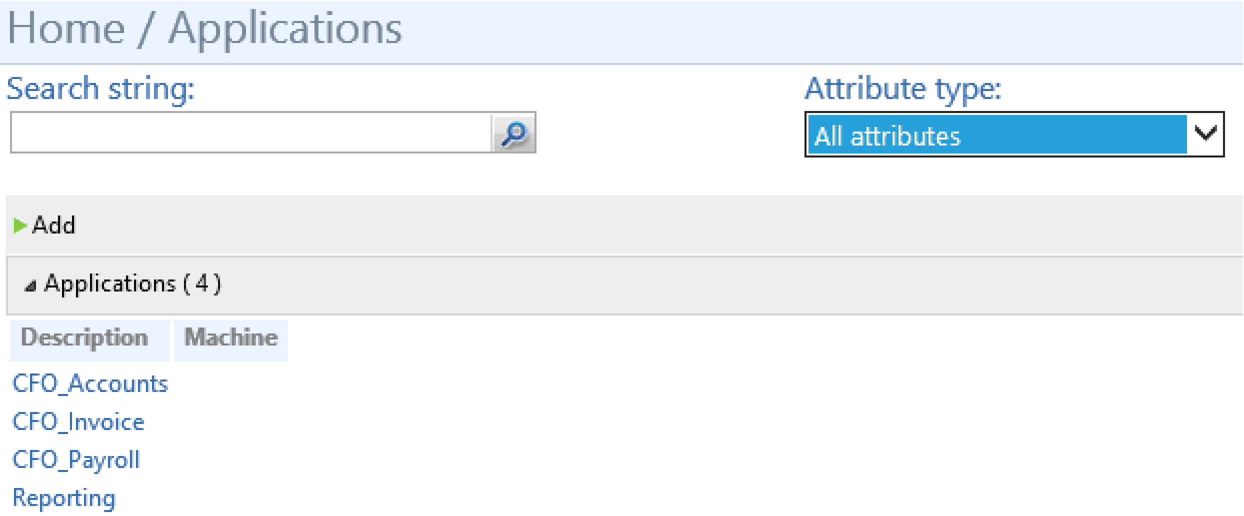
□	Initial Flow Only	Use as Existence Test	Flow (FIM Value → Destination Attribute)
□	□	□	accountName⇒bholdDescription
□	☑	□	accountName⇒ObjectIdentifier
□	□	□	member⇒Member
□	□	□	bhold_application⇒ApplicationDescription
□	□	□	accountName⇒bholdTaskName



Deleted Connectors	0
Metaverse Object Deletes	0
Outbound Synchronization	**MIM**
Export Attribute Flow	10
Outbound Synchronization	**BHOLD**
Export Attribute Flow	5
Provisioning Adds	5
Outbound Synchronization	**AD**
Export Attribute Flow	5
Provisioning Adds	5

Total objects retrieved: 5

Distinguished Name
cfoperm1
cfoperm2
cfoperm3
cfoperm4
cfoperm5



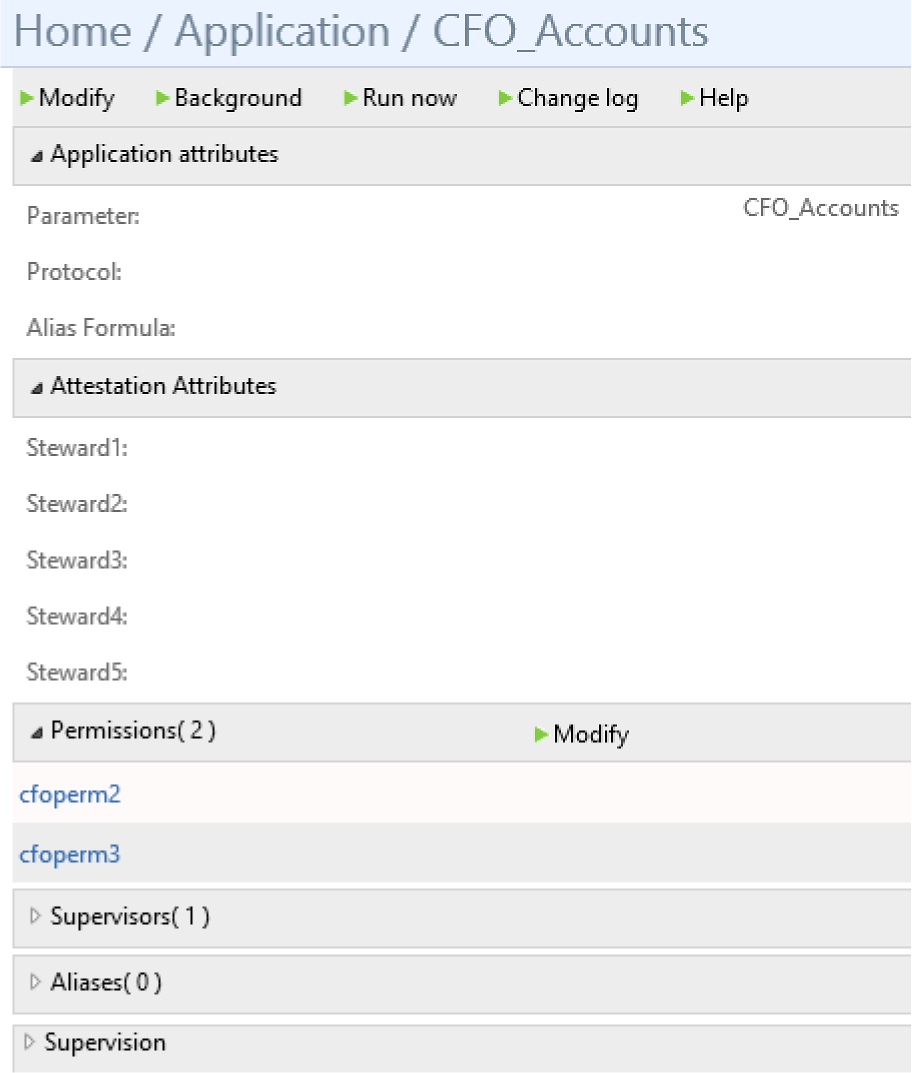
Home / Applications

Search string:

Attribute type: All attributes

◢ Applications (4)

Description	Machine
CFO_Accounts	
CFO_Invoice	
CFO_Payroll	
Reporting	



Home / Application / CFO_Accounts

◢ Application attributes

Parameter: CFO_Accounts

Protocol:

Alias Formula:

◢ Attestation Attributes

Steward1:

Steward2:

Steward3:

Steward4:

Steward5:

◢ Permissions(2) ▶ Modify

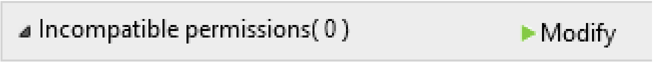
cfoperm2

cfoperm3

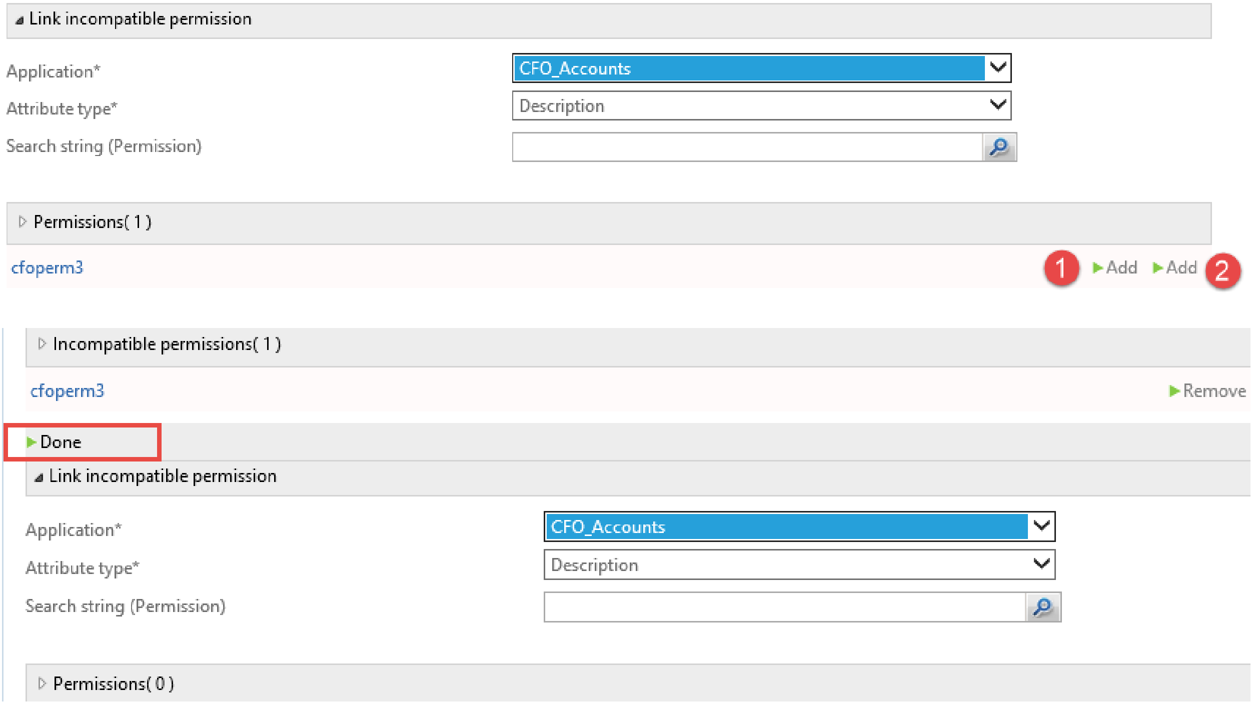
▷ Supervisors(1)

▷ Aliases(0)

▷ Supervision



◢ Incompatible permissions(0) ▶ Modify



◢ Link incompatible permission

Application* CFO_Accounts

Attribute type* Description

Search string (Permission)

▷ Permissions(1)

cfoperm3 1 ▶Add ▶Add 2

▷ Incompatible permissions(1)

cfoperm3 ▶Remove

▶Done

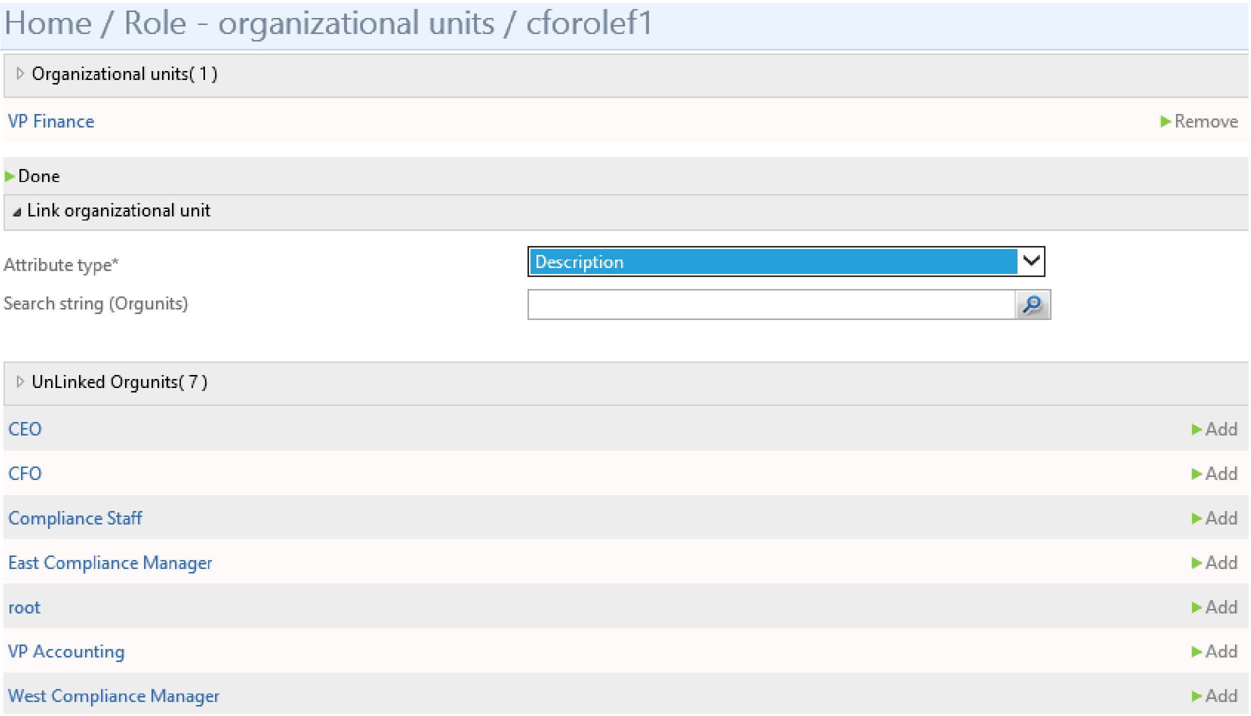
◢ Link incompatible permission

Application* CFO_Accounts

Attribute type* Description

Search string (Permission)

▷ Permissions(0)



Home / Role - organizational units / cforolef1

▷ Organizational units(1)

VP Finance ▶Remove

▶Done

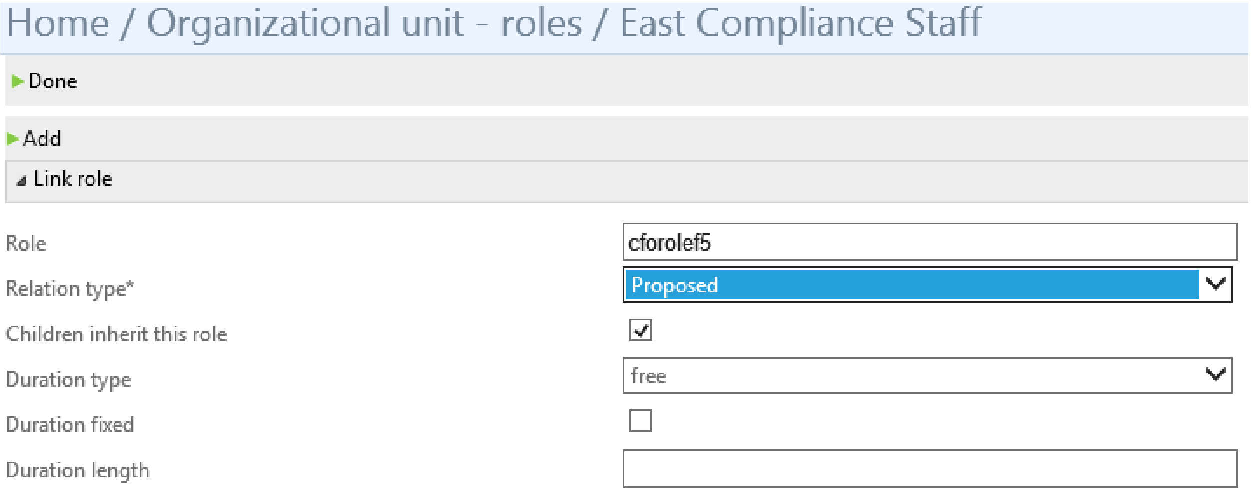
◢ Link organizational unit

Attribute type* Description

Search string (Orgunits)

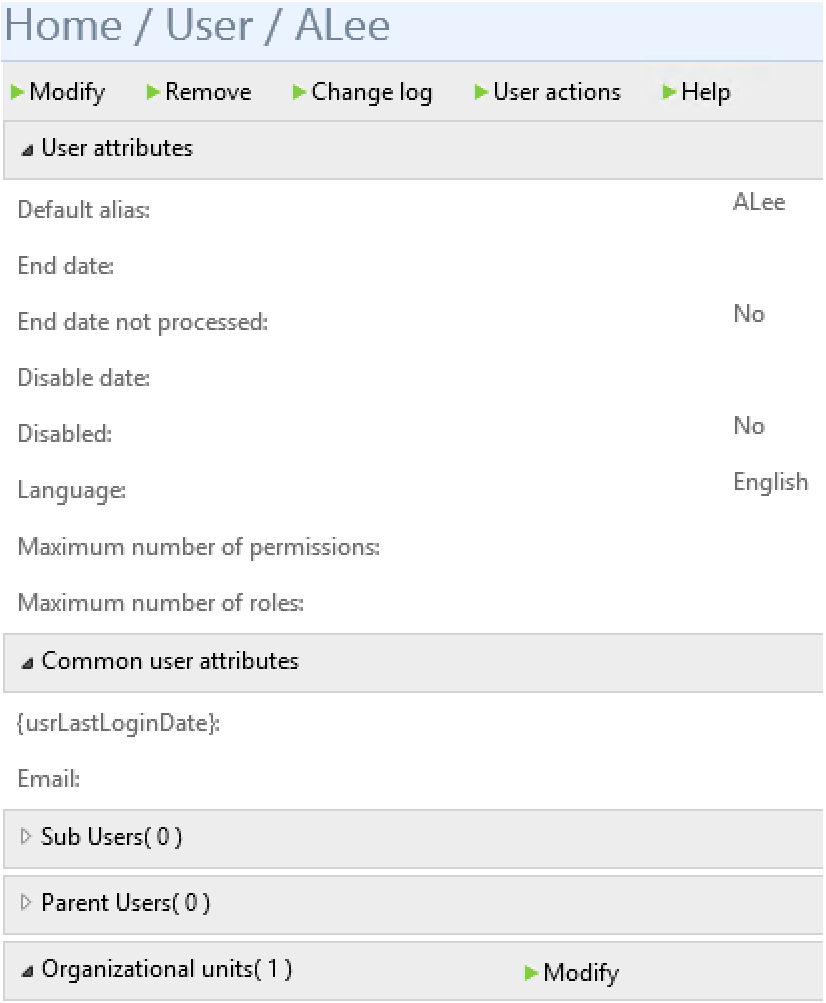
▷ UnLinked Orgunits(7)

CEO	▶Add
CFO	▶Add
Compliance Staff	▶Add
East Compliance Manager	▶Add
root	▶Add
VP Accounting	▶Add
West Compliance Manager	▶Add



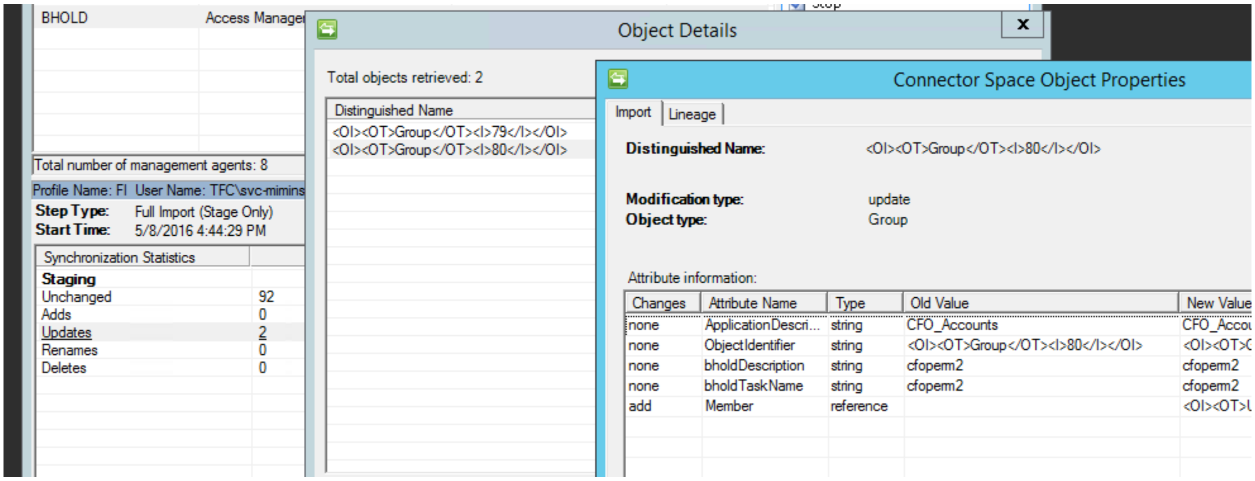
Home / Organizational unit - roles / East Compliance Staff

Role	cforolef5
Relation type*	Proposed
Children inherit this role	☑
Duration type	free
Duration fixed	□
Duration length	



Home / User / ALee

Default alias:	ALee
End date:	
End date not processed:	No
Disable date:	
Disabled:	No
Language:	English
Maximum number of permissions:	
Maximum number of roles:	
{usrLastLoginDate}:	
Email:	



BHOLD Access Manager

Total number of management agents: 8

Profile Name: FI User Name: TFC\svc-mimins

Step Type: Full Import (Stage Only)
Start Time: 5/8/2016 4:44:29 PM

Synchronization Statistics	
Staging	
Unchanged	92
Adds	0
Updates	2
Renames	0
Deletes	0

Object Details

Total objects retrieved: 2

Distinguished Name
<OI><OT>Group</OT><I>79</I></OI>
<OI><OT>Group</OT><I>80</I></OI>

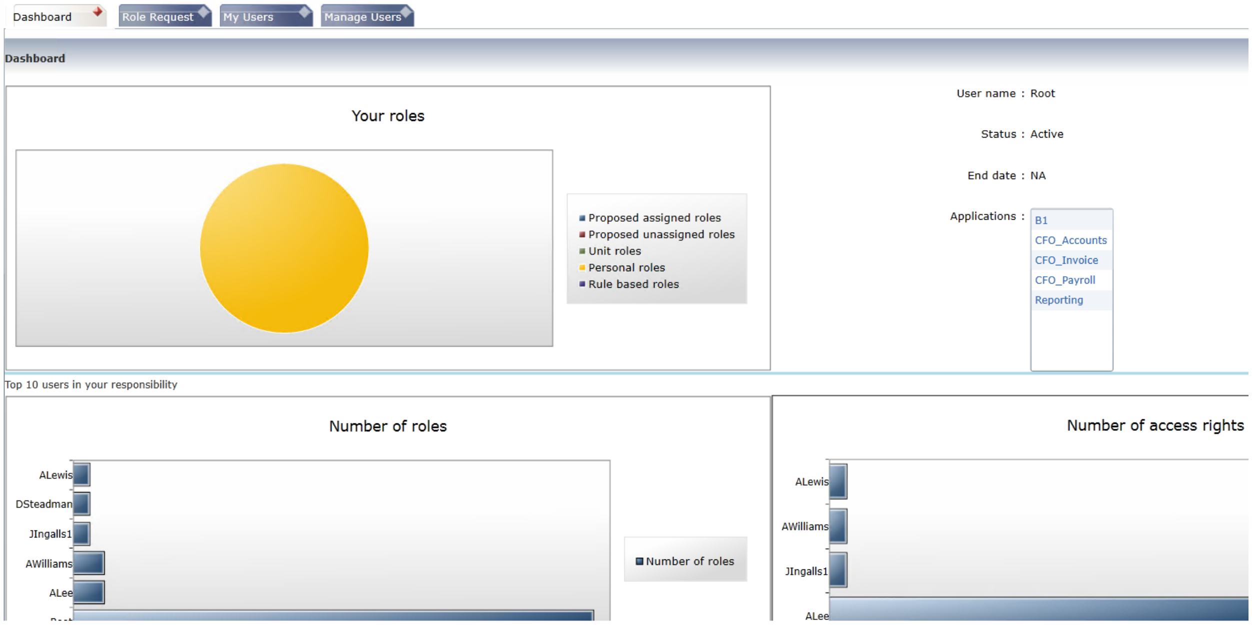
Connector Space Object Properties

Distinguished Name: <OI><OT>Group</OT><I>80</I></OI>

Modification type: update
Object type: Group

Attribute information:

Changes	Attribute Name	Type	Old Value	New Value
none	ApplicationDescri...	string	CFO_Accounts	CFO_Accou
none	ObjectIdentifier	string	<OI><OT>Group</OT><I>80</I></OI>	<OI><OT>(
none	bholdDescription	string	cfoperm2	cfoperm2
none	bholdTaskName	string	cfoperm2	cfoperm2
add	Member	reference		<OI><OT>l



Dashboard

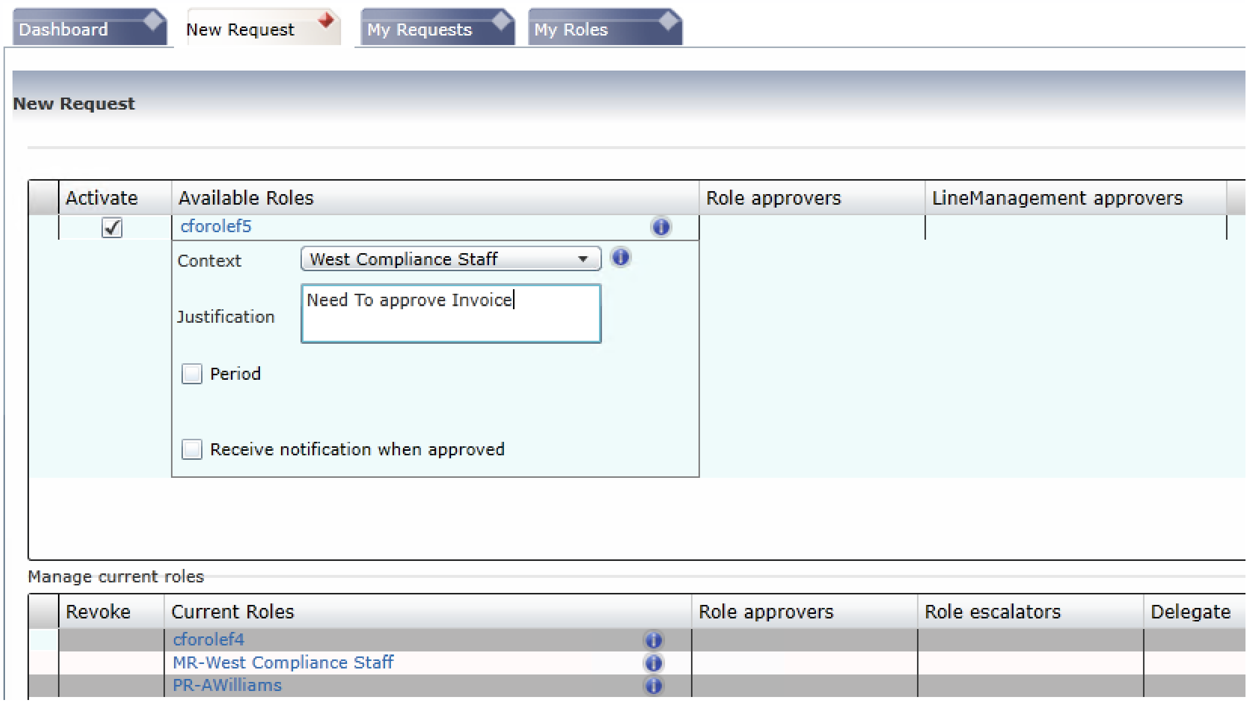
User name : Root

Status : Active

End date : NA

Applications : B1
CFO_Accounts
CFO_Invoice
CFO_Payroll
Reporting

Top 10 users in your responsibility



New Request

	Activate	Available Roles	Role approvers	LineManagement approvers
	☑	cforolef5		

Context: West Compliance Staff

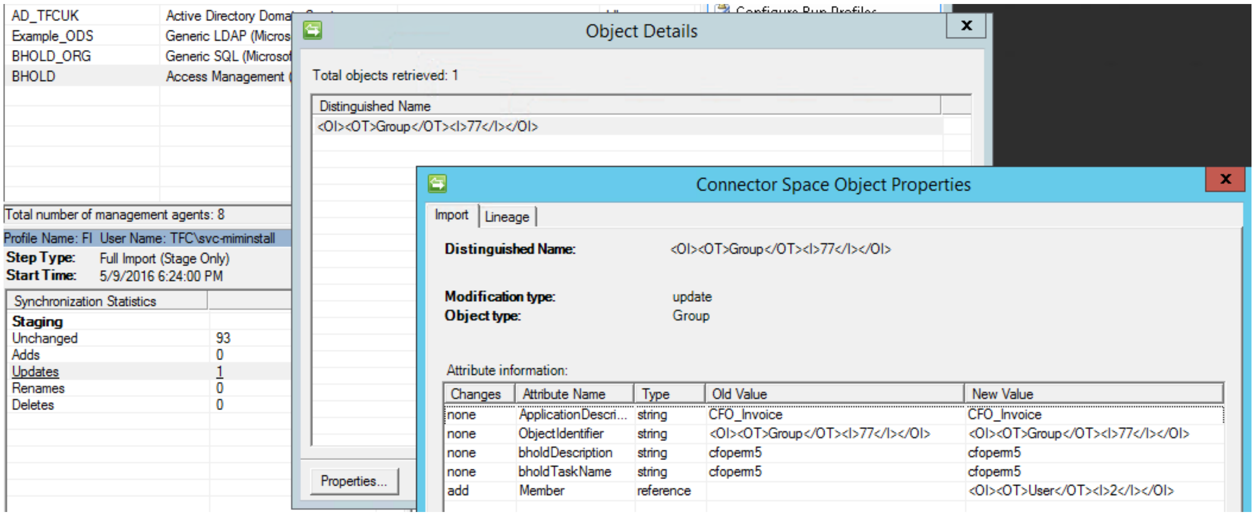
Justification: Need To approve Invoice

□ Period

□ Receive notification when approved

Manage current roles

	Revoke	Current Roles	Role approvers	Role escalators	Delegate
		cforolef4			
		MR-West Compliance Staff			
		PR-AWilliams			



AD_TFCUK	Active Directory Doma
Example_ODS	Generic LDAP (Micros
BHOLD_ORG	Generic SQL (Microsof
BHOLD	Access Management (

Total number of management agents: 8

Profile Name: FI User Name: TFC\svc-miminstall

Step Type: Full Import (Stage Only)
Start Time: 5/9/2016 6:24:00 PM

Synchronization Statistics	
Staging	
Unchanged	93
Adds	0
Updates	1
Renames	0
Deletes	0

Object Details

Total objects retrieved: 1

Distinguished Name
<OI><OT>Group</OT><I>77</I></OI>

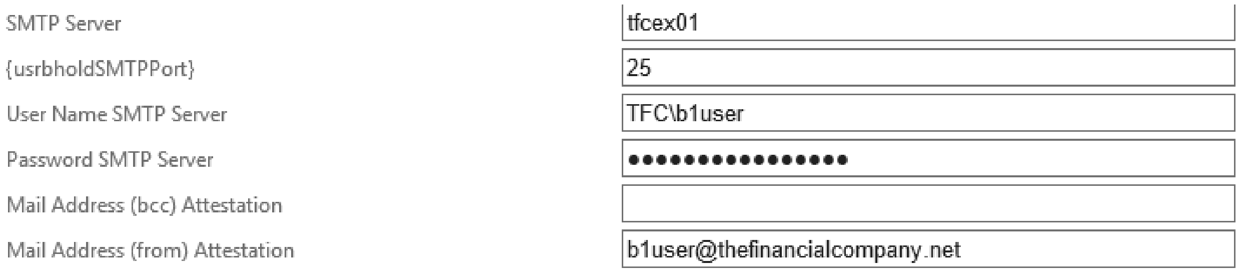
Connector Space Object Properties

Distinguished Name: <OI><OT>Group</OT><I>77</I></OI>

Modification type: update
Object type: Group

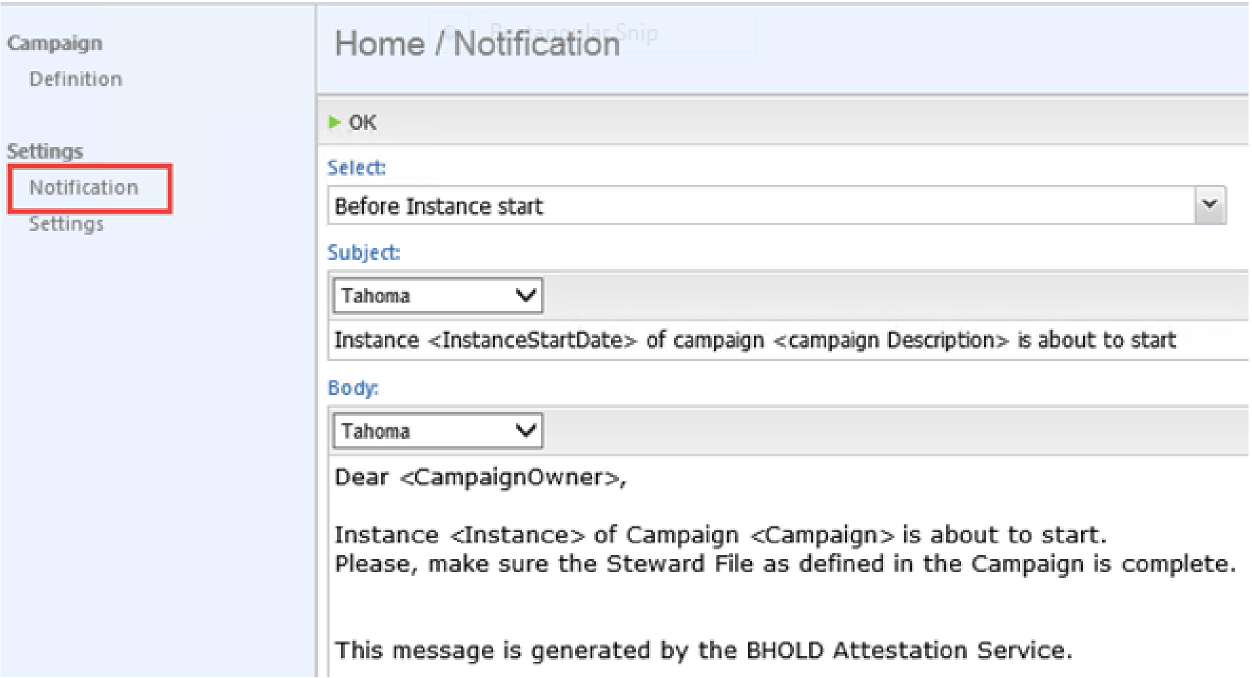
Attribute information:

Changes	Attribute Name	Type	Old Value	New Value
none	ApplicationDescri...	string	CFO_Invoice	CFO_Invoice
none	ObjectIdentifier	string	<OI><OT>Group</OT><I>77</I></OI>	<OI><OT>Group</OT><I>77</I></OI>
none	bholdDescription	string	cfoperm5	cfoperm5
none	bholdTaskName	string	cfoperm5	cfoperm5
add	Member	reference		<OI><OT>User</OT><I>2</I></OI>



SMTP Server	tfcex01
{usrbholdSMTPPort}	25
User Name SMTP Server	TFC\b1user
Password SMTP Server	●●●●●●●●●●●●●●●●
Mail Address (bcc) Attestation	
Mail Address (from) Attestation	b1user@thefinancialcompany.net

Attestation



Home / Notification

Select: Before Instance start

Subject: Tahoma

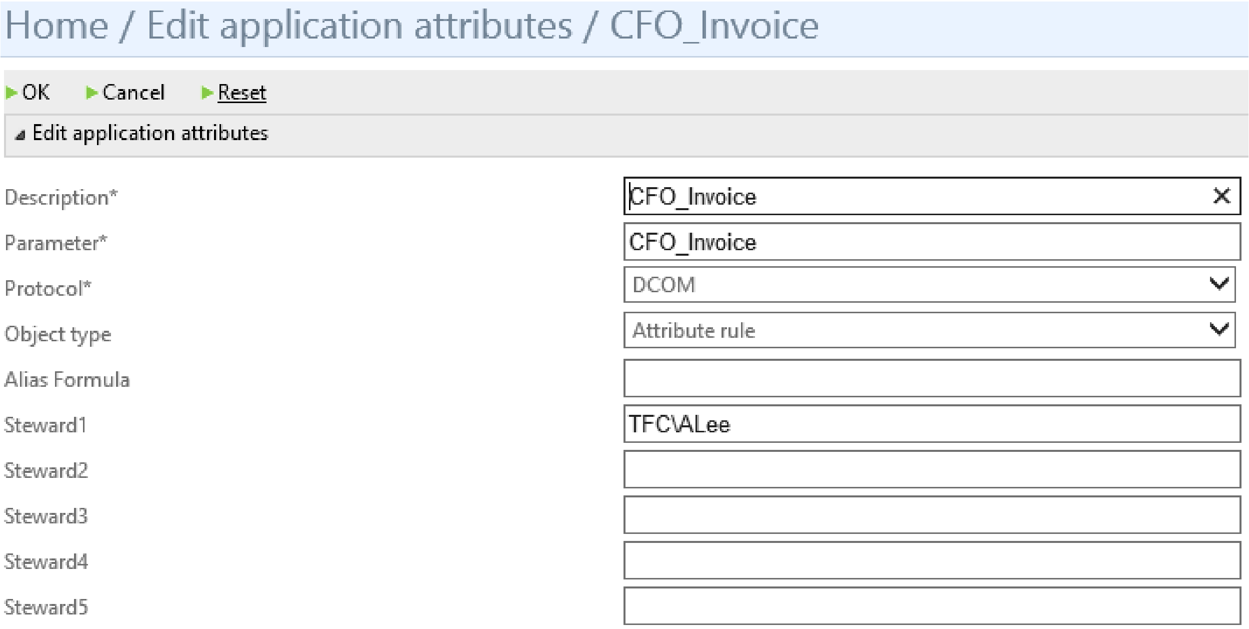
Instance <InstanceStartDate> of campaign <campaign Description> is about to start

Body: Tahoma

Dear <CampaignOwner>,

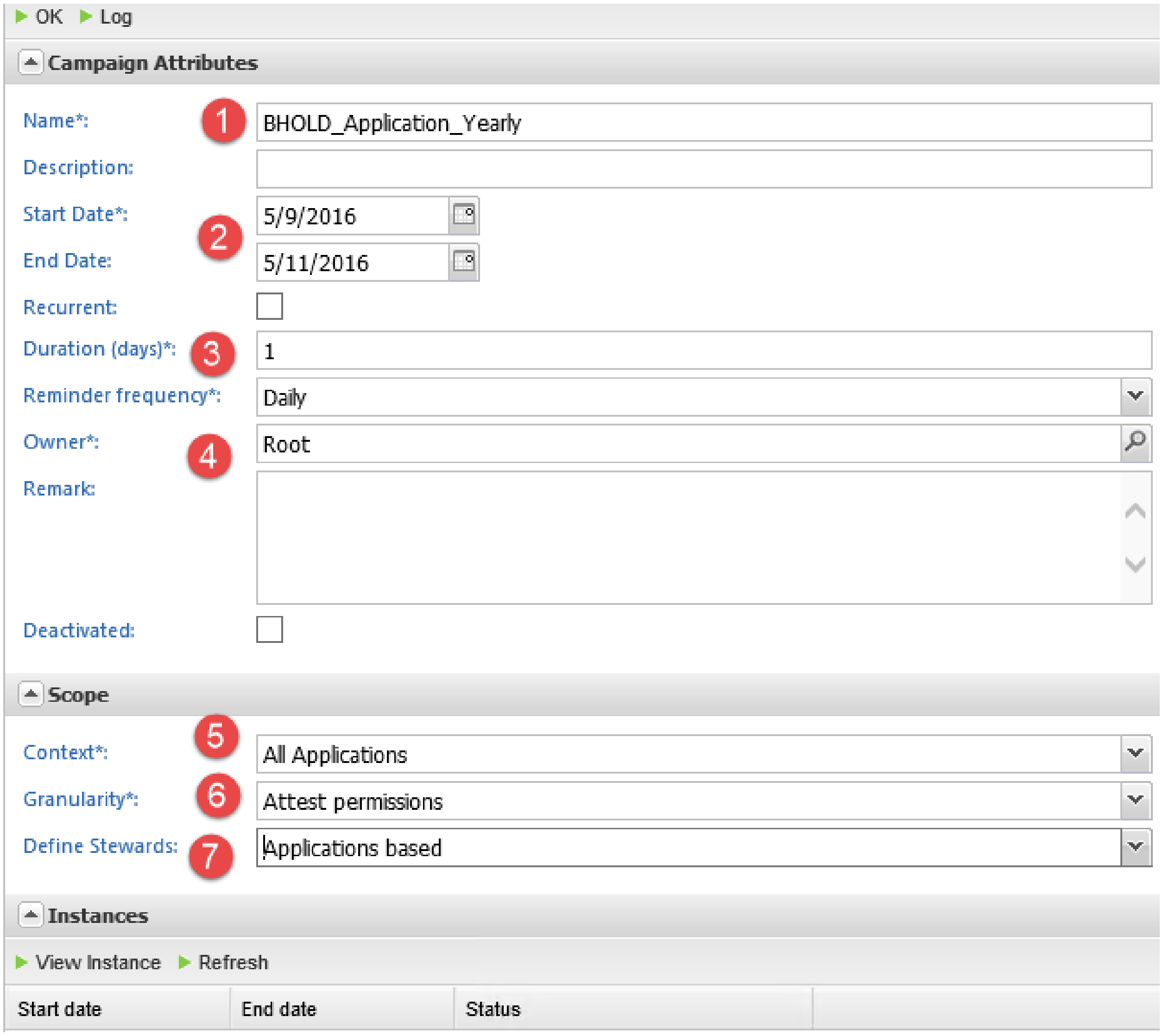
Instance <Instance> of Campaign <Campaign> is about to start.
Please, make sure the Steward File as defined in the Campaign is complete.

This message is generated by the BHOLD Attestation Service.



Home / Edit application attributes / CFO_Invoice

Description*	CFO_Invoice
Parameter*	CFO_Invoice
Protocol*	DCOM
Object type	Attribute rule
Alias Formula	
Steward1	TFC\ALee
Steward2	
Steward3	
Steward4	
Steward5	



Campaign Attributes

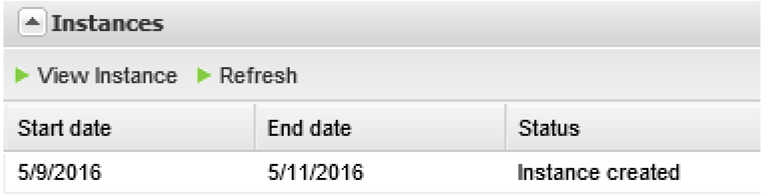
Name*:	BHOLD_Application_Yearly
Description:	
Start Date*:	5/9/2016
End Date:	5/11/2016
Recurrent:	□
Duration (days)*:	1
Reminder frequency*:	Daily
Owner*:	Root
Remark:	
Deactivated:	□

Scope

Context*:	All Applications
Granularity*:	Attest permissions
Define Stewards:	Applications based

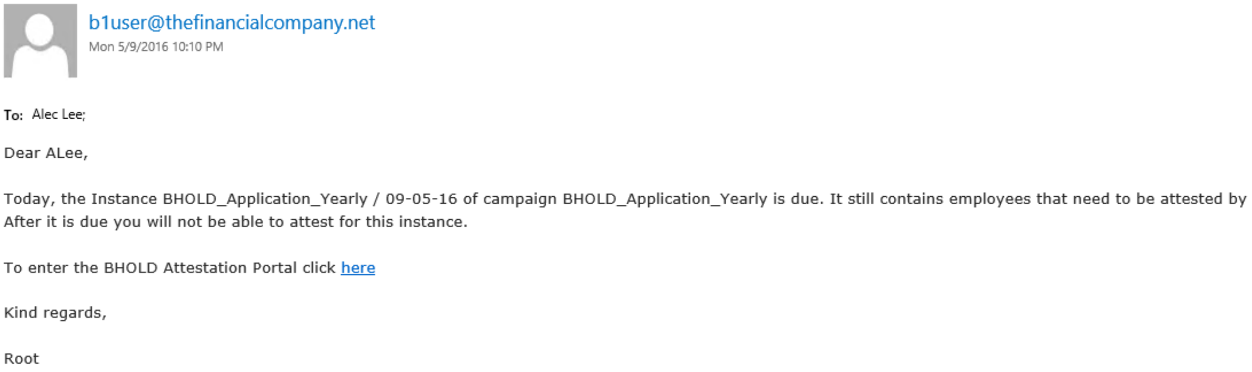
Instances

Start date	End date	Status



Instances

Start date	End date	Status
5/9/2016	5/11/2016	Instance created



b1user@thefinancialcompany.net
Mon 5/9/2016 10:10 PM

To: Alec Lee;

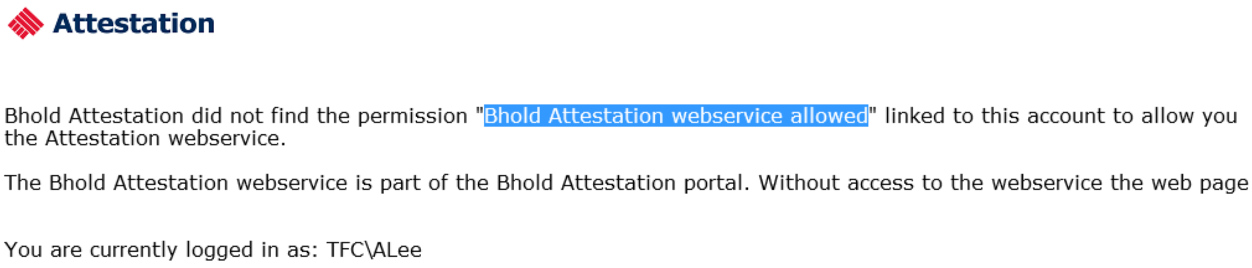
Dear ALee,

Today, the Instance BHOLD_Application_Yearly / 09-05-16 of campaign BHOLD_Application_Yearly is due. It still contains employees that need to be attested by
After it is due you will not be able to attest for this instance.

To enter the BHOLD Attestation Portal click here

Kind regards,

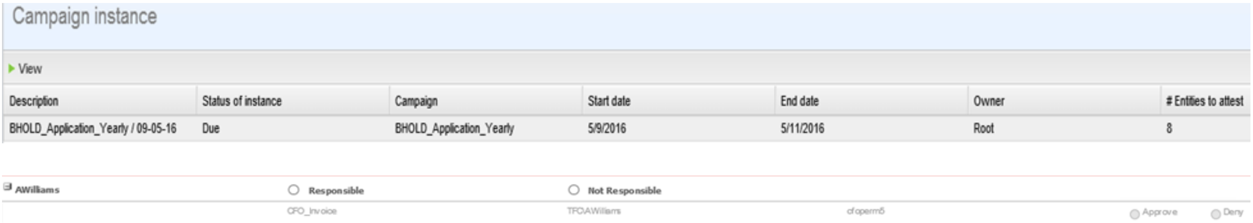
Root



Bhold Attestation did not find the permission "Bhold Attestation webservice allowed" linked to this account to allow you the Attestation webservice.

The Bhold Attestation webservice is part of the Bhold Attestation portal. Without access to the webservice the web page

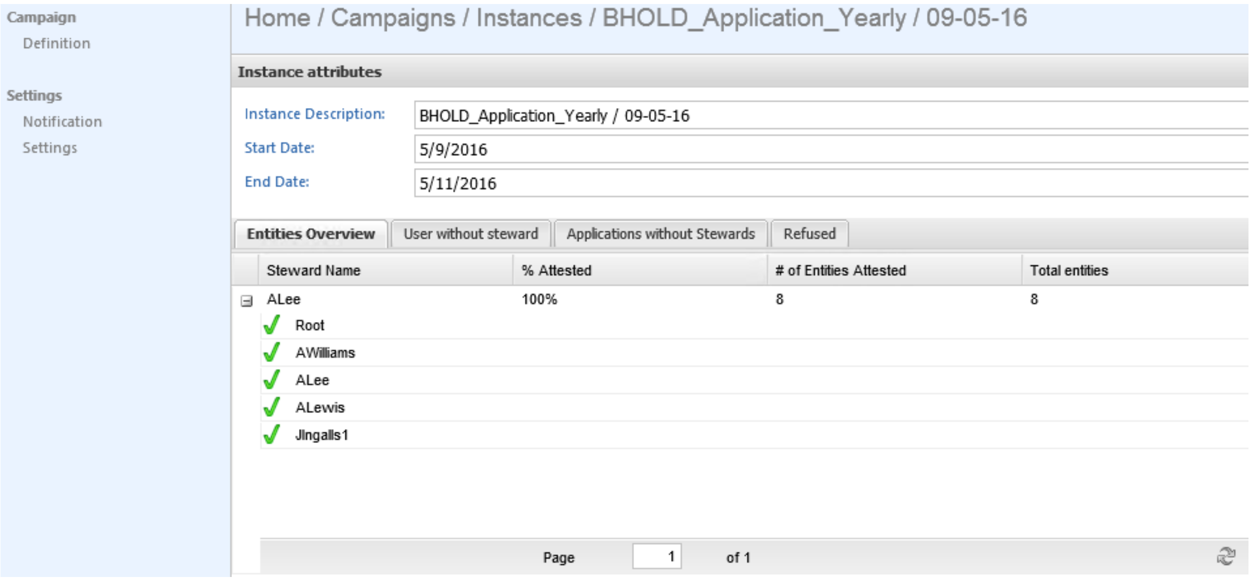
You are currently logged in as: TFC\ALee



Campaign instance

Description	Status of instance	Campaign	Start date	End date	Owner	# Entities to attest
BHOLD_Application_Yearly / 09-05-16	Due	BHOLD_Application_Yearly	5/9/2016	5/11/2016	Root	8

AWilliams	○ Responsible	○ Not Responsible			
	CFO_Invoice	TFC\AWilliams	cfoperm5	○ Approve	○ Deny

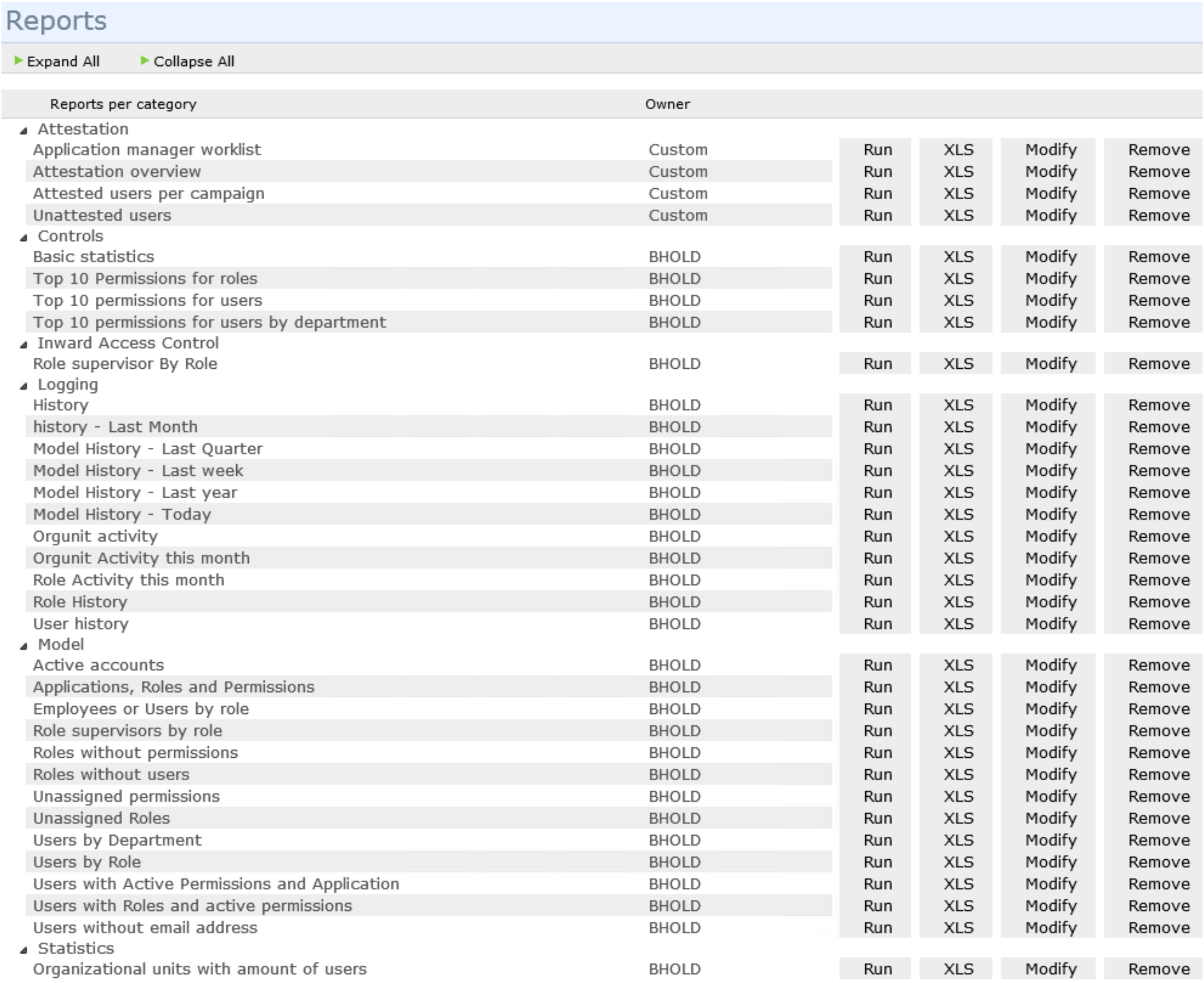


Home / Campaigns / Instances / BHOLD_Application_Yearly / 09-05-16

Instance attributes

Instance Description: BHOLD_Application_Yearly / 09-05-16
Start Date: 5/9/2016
End Date: 5/11/2016

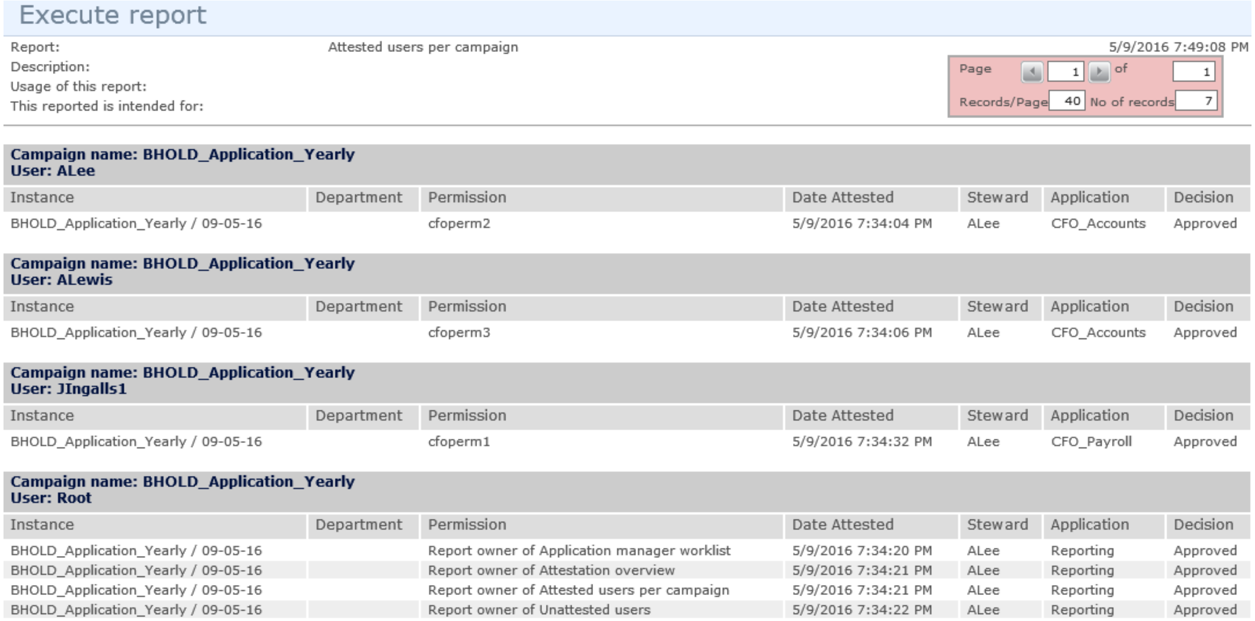
Steward Name	% Attested	# of Entities Attested	Total entities
ALee	100%	8	8
✓ Root			
✓ AWilliams			
✓ ALee			
✓ ALewis			
✓ JIngalls1			



Reports

▸ Expand All ▸ Collapse All

Reports per category	Owner				
◢ Attestation					
Application manager worklist	Custom	Run	XLS	Modify	Remove
Attestation overview	Custom	Run	XLS	Modify	Remove
Attested users per campaign	Custom	Run	XLS	Modify	Remove
Unattested users	Custom	Run	XLS	Modify	Remove
◢ Controls					
Basic statistics	BHOLD	Run	XLS	Modify	Remove
Top 10 Permissions for roles	BHOLD	Run	XLS	Modify	Remove
Top 10 permissions for users	BHOLD	Run	XLS	Modify	Remove
Top 10 permissions for users by department	BHOLD	Run	XLS	Modify	Remove
◢ Inward Access Control					
Role supervisor By Role	BHOLD	Run	XLS	Modify	Remove
◢ Logging					
History	BHOLD	Run	XLS	Modify	Remove
history - Last Month	BHOLD	Run	XLS	Modify	Remove
Model History - Last Quarter	BHOLD	Run	XLS	Modify	Remove
Model History - Last week	BHOLD	Run	XLS	Modify	Remove
Model History - Last year	BHOLD	Run	XLS	Modify	Remove
Model History - Today	BHOLD	Run	XLS	Modify	Remove
Orgunit activity	BHOLD	Run	XLS	Modify	Remove
Orgunit Activity this month	BHOLD	Run	XLS	Modify	Remove
Role Activity this month	BHOLD	Run	XLS	Modify	Remove
Role History	BHOLD	Run	XLS	Modify	Remove
User history	BHOLD	Run	XLS	Modify	Remove
◢ Model					
Active accounts	BHOLD	Run	XLS	Modify	Remove
Applications, Roles and Permissions	BHOLD	Run	XLS	Modify	Remove
Employees or Users by role	BHOLD	Run	XLS	Modify	Remove
Role supervisors by role	BHOLD	Run	XLS	Modify	Remove
Roles without permissions	BHOLD	Run	XLS	Modify	Remove
Roles without users	BHOLD	Run	XLS	Modify	Remove
Unassigned permissions	BHOLD	Run	XLS	Modify	Remove
Unassigned Roles	BHOLD	Run	XLS	Modify	Remove
Users by Department	BHOLD	Run	XLS	Modify	Remove
Users by Role	BHOLD	Run	XLS	Modify	Remove
Users with Active Permissions and Application	BHOLD	Run	XLS	Modify	Remove
Users with Roles and active permissions	BHOLD	Run	XLS	Modify	Remove
Users without email address	BHOLD	Run	XLS	Modify	Remove
◢ Statistics					
Organizational units with amount of users	BHOLD	Run	XLS	Modify	Remove



Execute report

Report:	Attested users per campaign	5/9/2016 7:49:08 PM
Description:		Page ◀ 1 ▶ of 1
Usage of this report:		
This reported is intended for:		Records/Page 40 No of records 7

Campaign name: BHOLD_Application_Yearly
User: ALee

Instance	Department	Permission	Date Attested	Steward	Application	Decision
BHOLD_Application_Yearly / 09-05-16		cfoperm2	5/9/2016 7:34:04 PM	ALee	CFO_Accounts	Approved

Campaign name: BHOLD_Application_Yearly
User: ALewis

Instance	Department	Permission	Date Attested	Steward	Application	Decision
BHOLD_Application_Yearly / 09-05-16		cfoperm3	5/9/2016 7:34:06 PM	ALee	CFO_Accounts	Approved

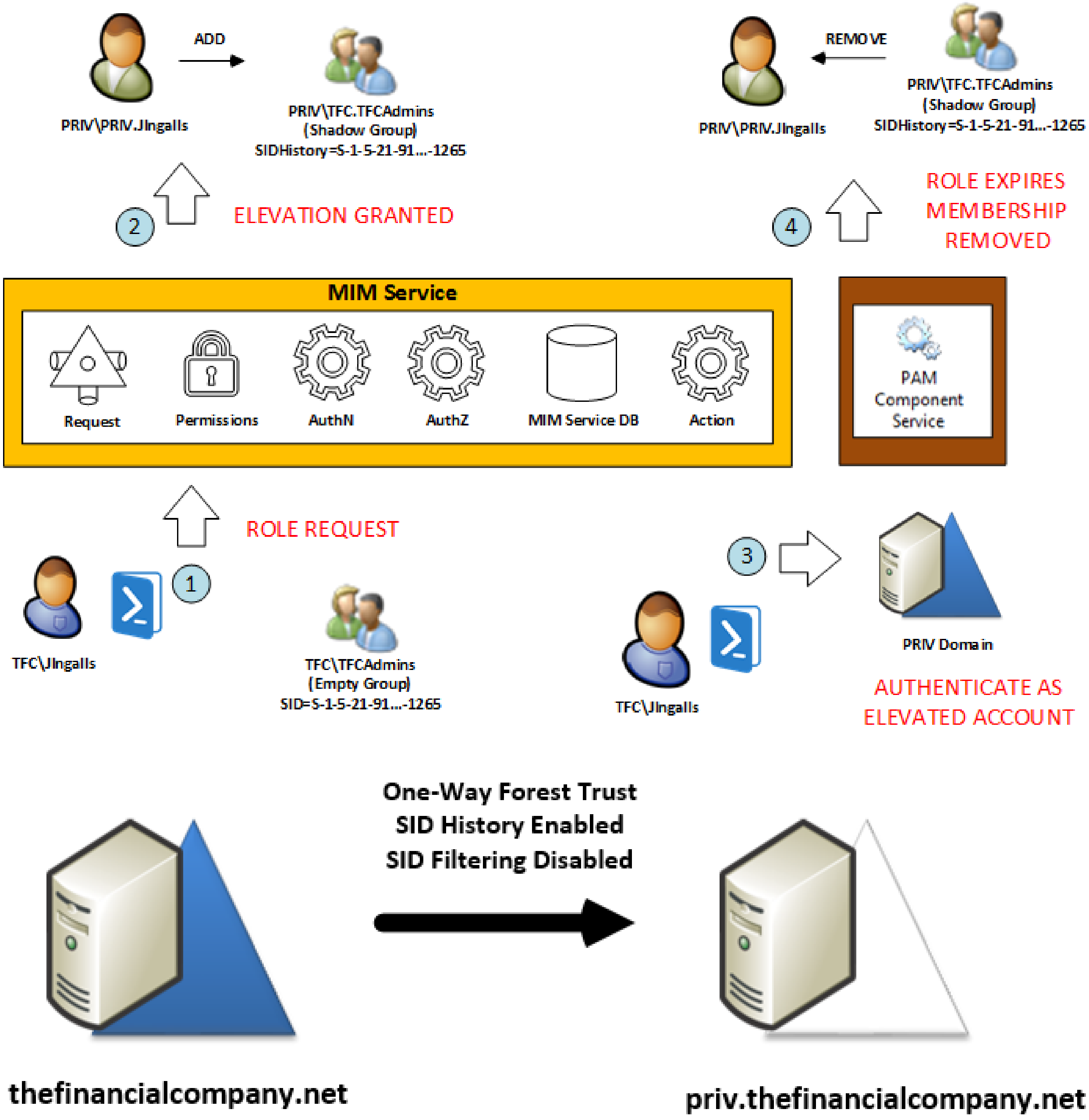
Campaign name: BHOLD_Application_Yearly
User: JIngalls1

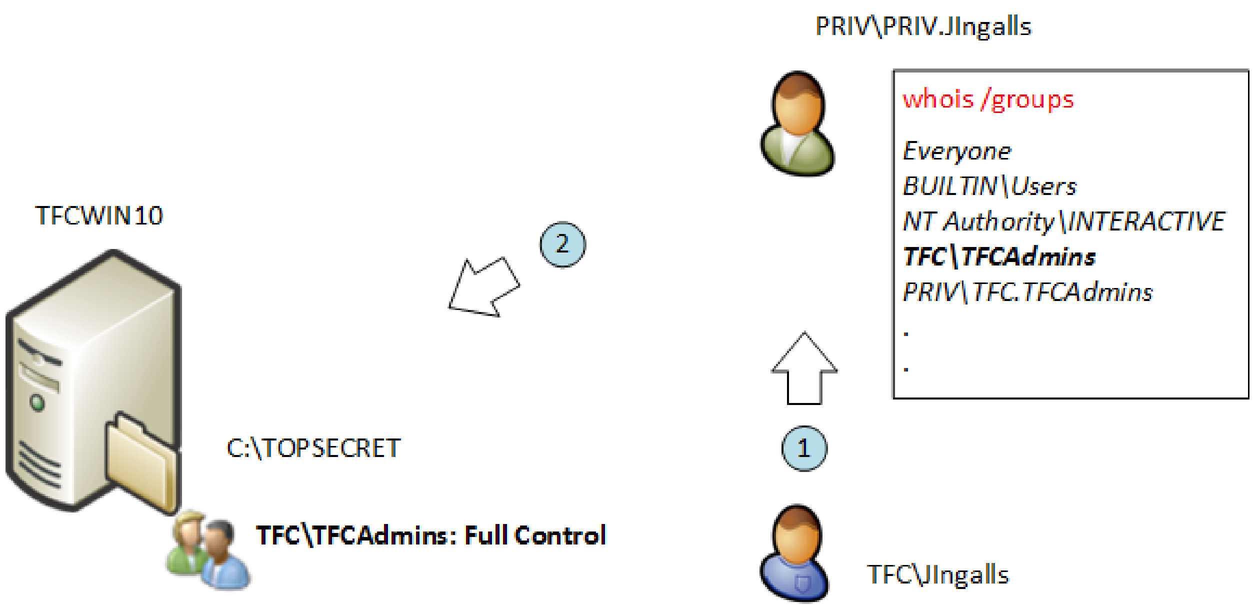
Instance	Department	Permission	Date Attested	Steward	Application	Decision
BHOLD_Application_Yearly / 09-05-16		cfoperm1	5/9/2016 7:34:32 PM	ALee	CFO_Payroll	Approved

Campaign name: BHOLD_Application_Yearly
User: Root

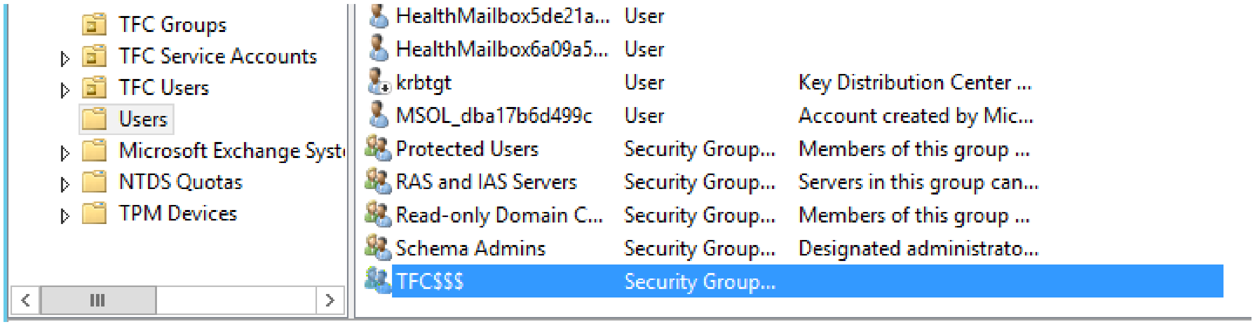
Instance	Department	Permission	Date Attested	Steward	Application	Decision
BHOLD_Application_Yearly / 09-05-16		Report owner of Application manager worklist	5/9/2016 7:34:20 PM	ALee	Reporting	Approved
BHOLD_Application_Yearly / 09-05-16		Report owner of Attestation overview	5/9/2016 7:34:21 PM	ALee	Reporting	Approved
BHOLD_Application_Yearly / 09-05-16		Report owner of Attested users per campaign	5/9/2016 7:34:21 PM	ALee	Reporting	Approved
BHOLD_Application_Yearly / 09-05-16		Report owner of Unattested users	5/9/2016 7:34:22 PM	ALee	Reporting	Approved

Chapter 8: Reducing Threats with PAM

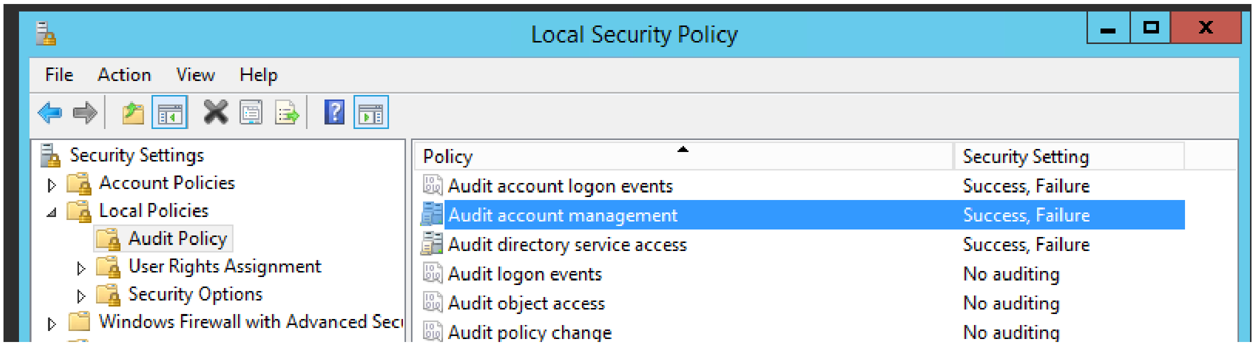




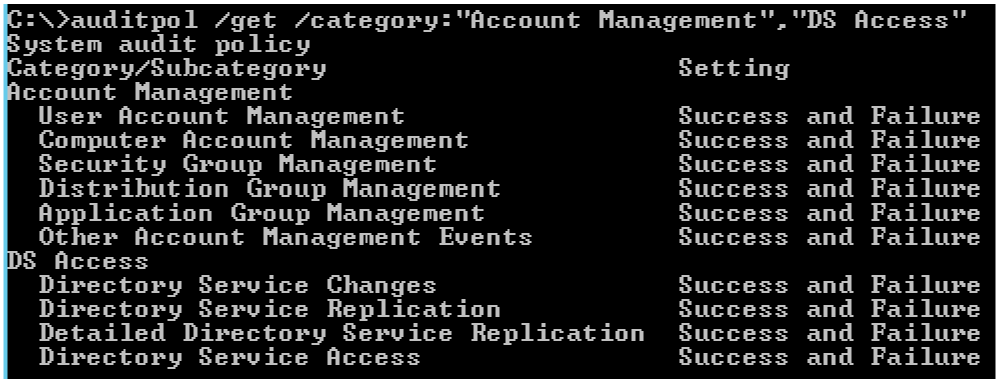
```
whois /groups

Everyone
BUILTIN\Users
NT Authority\INTERACTIVE
TFC\TFCAdmins
PRIV\TFC.TFCAdmins
.
.
```



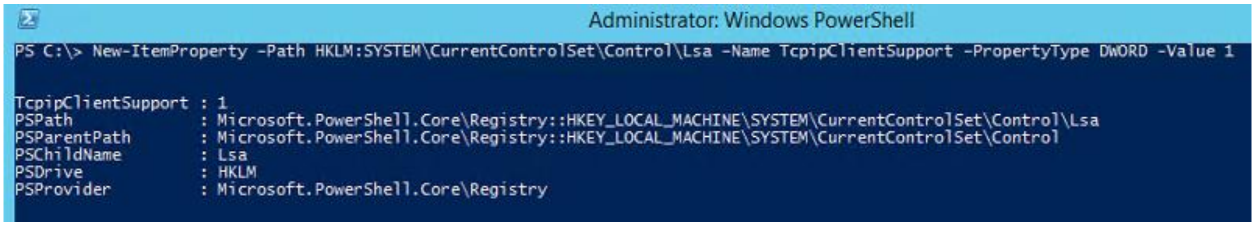
HealthMailbox5de21a...	User	
HealthMailbox6a09a5...	User	
krbtgt	User	Key Distribution Center ...
MSOL_dba17b6d499c	User	Account created by Mic...
Protected Users	Security Group...	Members of this group ...
RAS and IAS Servers	Security Group...	Servers in this group can...
Read-only Domain C...	Security Group...	Members of this group ...
Schema Admins	Security Group...	Designated administrato...
TFC$$$	Security Group...	



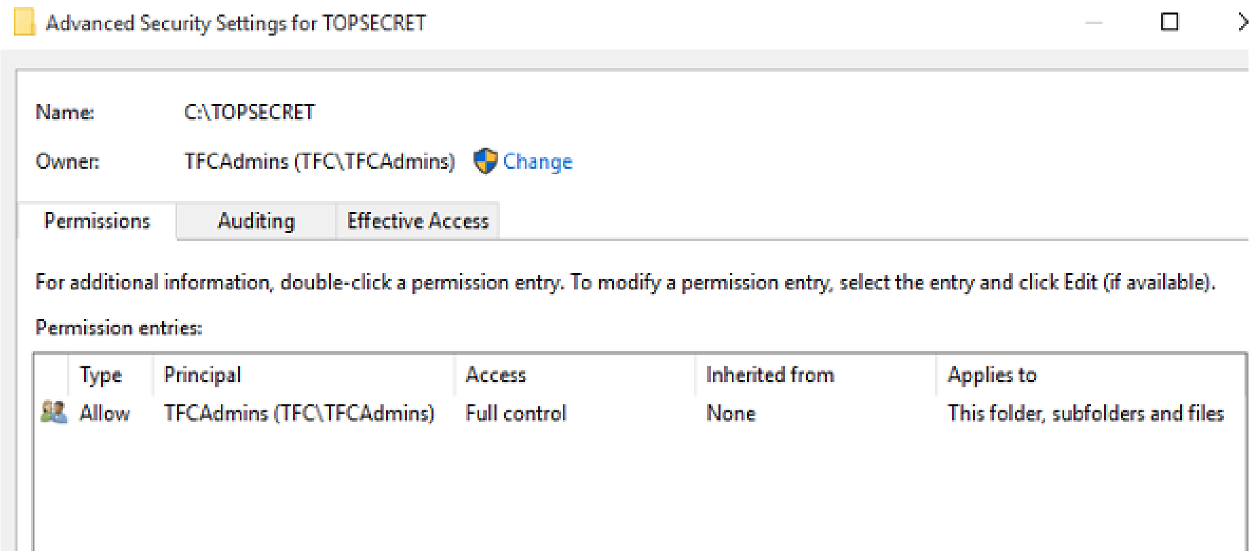
Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	No auditing
Audit object access	No auditing
Audit policy change	No auditing



```
C:\>auditpol /get /category:"Account Management","DS Access"
System audit policy
Category/Subcategory                      Setting
Account Management
  User Account Management                 Success and Failure
  Computer Account Management             Success and Failure
  Security Group Management               Success and Failure
  Distribution Group Management           Success and Failure
  Application Group Management            Success and Failure
  Other Account Management Events         Success and Failure
DS Access
  Directory Service Changes               Success and Failure
  Directory Service Replication           Success and Failure
  Detailed Directory Service Replication  Success and Failure
  Directory Service Access                Success and Failure
```



```
PS C:\> New-ItemProperty -Path HKLM:SYSTEM\CurrentControlSet\Control\Lsa -Name TcpipClientSupport -PropertyType DWORD -Value 1


TcpipClientSupport : 1
PSPath             : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
PSParentPath       : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control
PSChildName        : Lsa
PSDrive            : HKLM
PSProvider         : Microsoft.PowerShell.Core\Registry
```



Advanced Security Settings for TOPSECRET

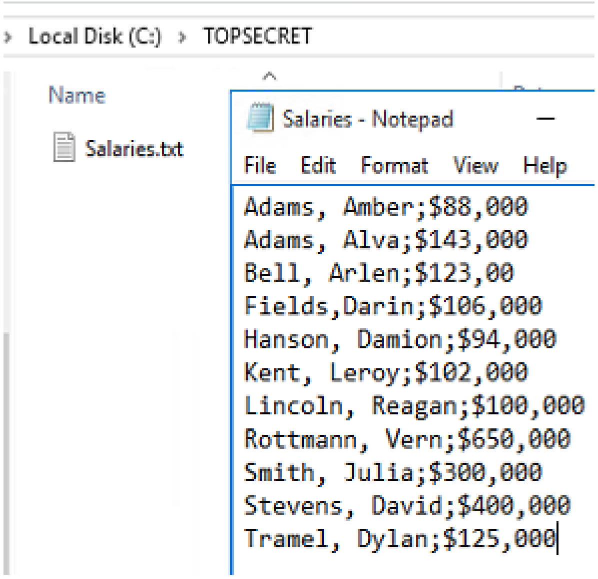
Name: C:\TOPSECRET

Owner: TFCAdmins (TFC\TFCAdmins) Change

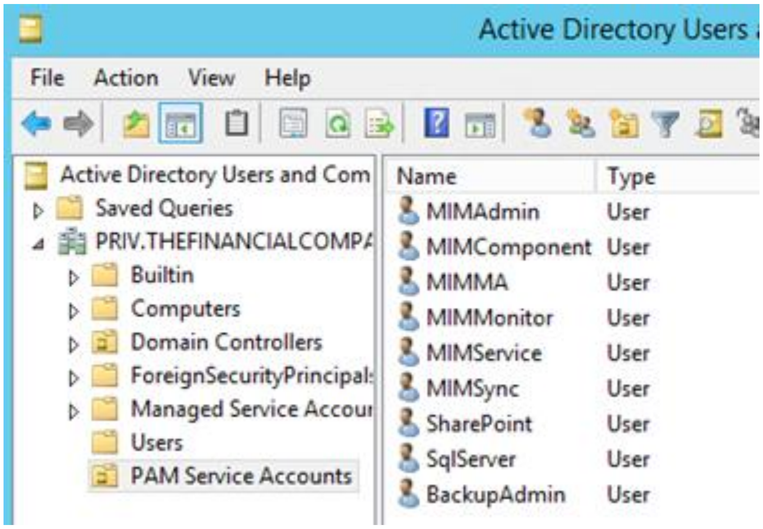
For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

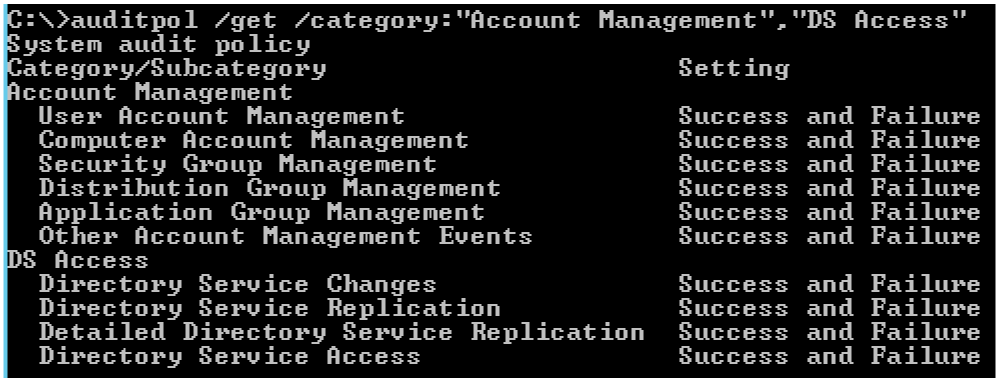
Type	Principal	Access	Inherited from	Applies to
Allow	TFCAdmins (TFC\TFCAdmins)	Full control	None	This folder, subfolders and files



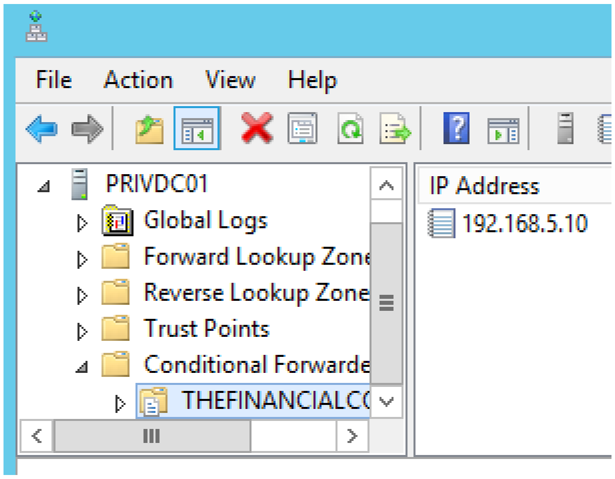
```
Adams, Amber;$88,000
Adams, Alva;$143,000
Bell, Arlen;$123,00
Fields,Darin;$106,000
Hanson, Damion;$94,000
Kent, Leroy;$102,000
Lincoln, Reagan;$100,000
Rottmann, Vern;$650,000
Smith, Julia;$300,000
Stevens, David;$400,000
Tramel, Dylan;$125,000
```



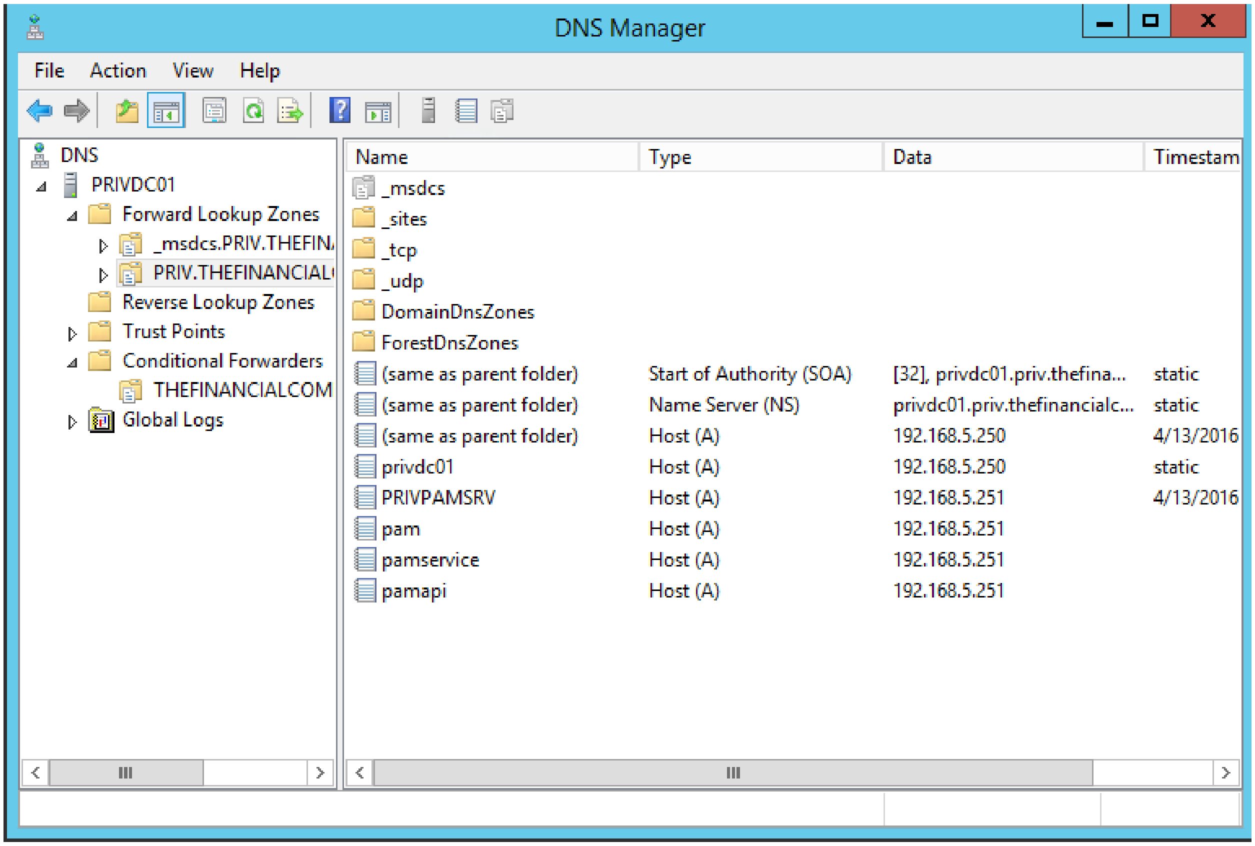
Name	Type
MIMAdmin	User
MIMComponent	User
MIMMA	User
MIMMonitor	User
MIMService	User
MIMSync	User
SharePoint	User
SqlServer	User
BackupAdmin	User



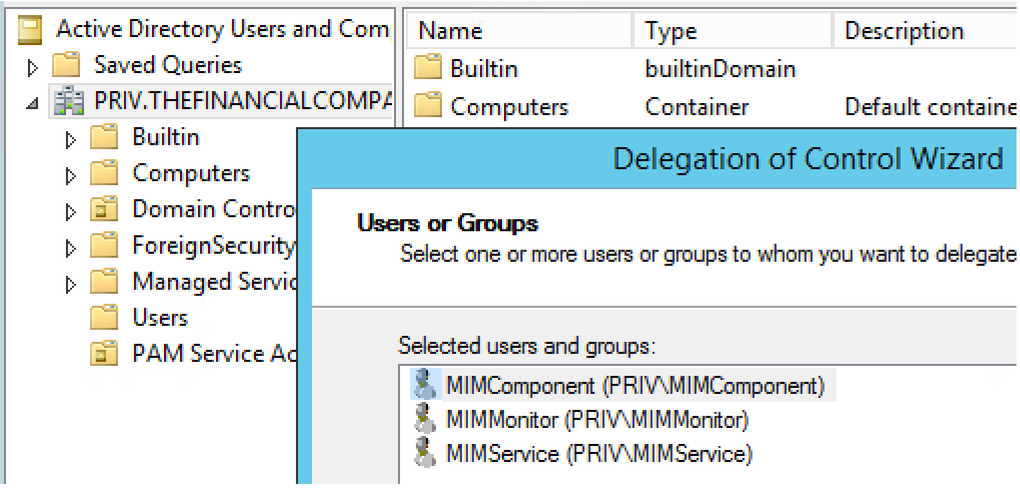
```
C:\>auditpol /get /category:"Account Management","DS Access"
System audit policy
Category/Subcategory                      Setting
Account Management
  User Account Management                 Success and Failure
  Computer Account Management             Success and Failure
  Security Group Management               Success and Failure
  Distribution Group Management           Success and Failure
  Application Group Management            Success and Failure
  Other Account Management Events         Success and Failure
DS Access
  Directory Service Changes               Success and Failure
  Directory Service Replication           Success and Failure
  Detailed Directory Service Replication  Success and Failure
  Directory Service Access                Success and Failure
```



IP Address
192.168.5.10



Name	Type	Data	Timestam
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[32], privdc01.priv.thefina...	static
(same as parent folder)	Name Server (NS)	privdc01.priv.thefinancialc...	static
(same as parent folder)	Host (A)	192.168.5.250	4/13/2016
privdc01	Host (A)	192.168.5.250	static
PRIVPAMSRV	Host (A)	192.168.5.251	4/13/2016
pam	Host (A)	192.168.5.251	
pamservice	Host (A)	192.168.5.251	
pamapi	Host (A)	192.168.5.251	



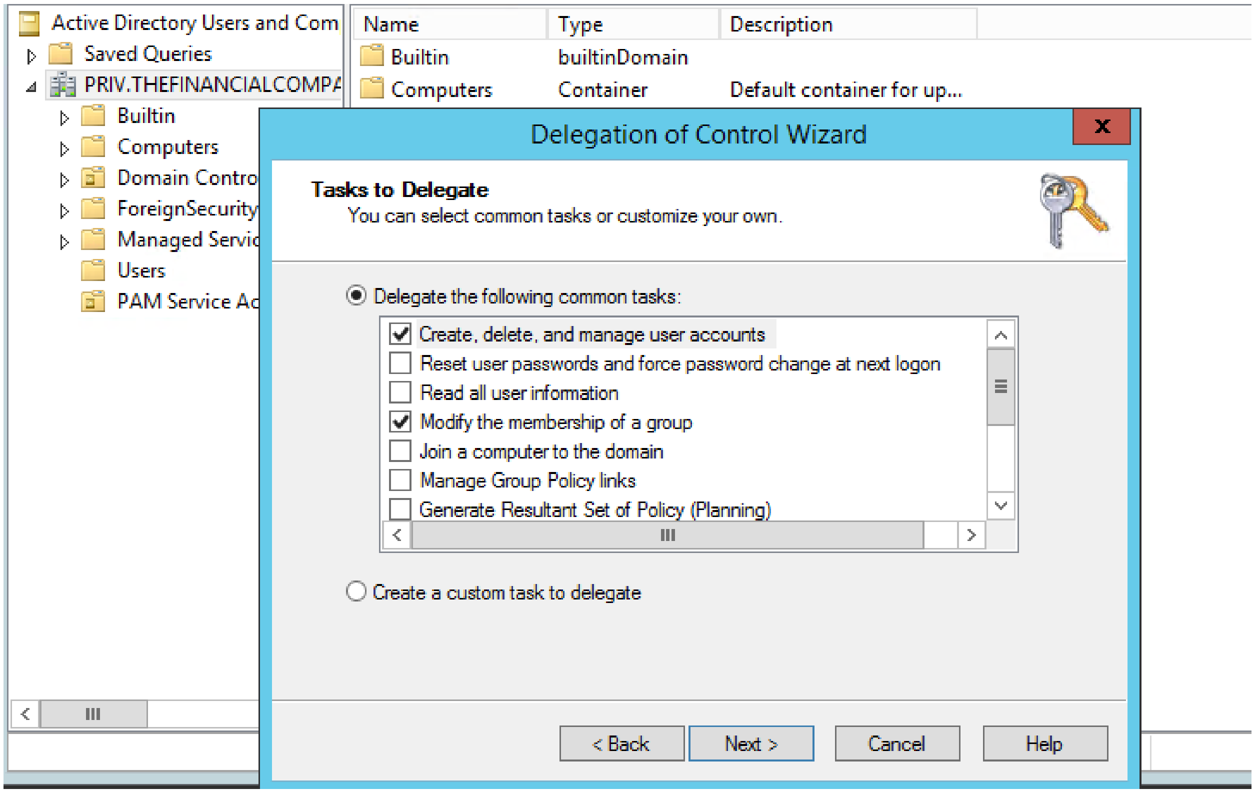
Delegation of Control Wizard

Users or Groups

Select one or more users or groups to whom you want to delegate

Selected users and groups:

- MIMComponent (PRIV\MIMComponent)
- MIMMonitor (PRIV\MIMMonitor)
- MIMService (PRIV\MIMService)



Delegation of Control Wizard

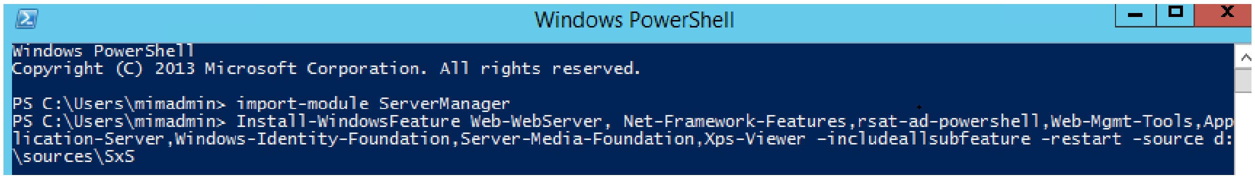
Tasks to Delegate

You can select common tasks or customize your own.

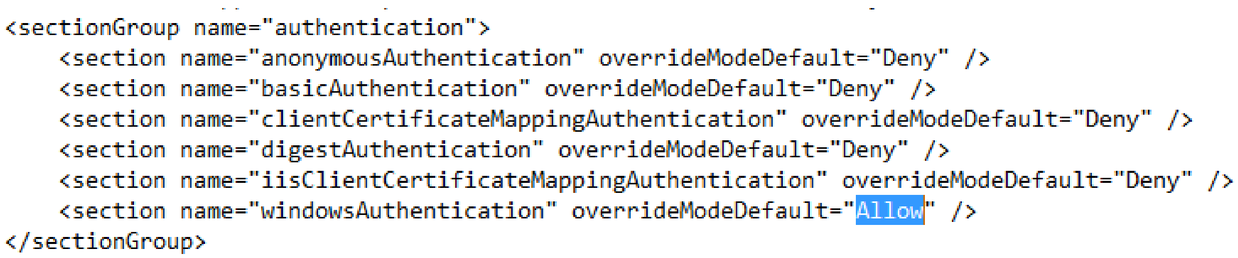
● Delegate the following common tasks:

- ☑ Create, delete, and manage user accounts
- ☐ Reset user passwords and force password change at next logon
- ☐ Read all user information
- ☑ Modify the membership of a group
- ☐ Join a computer to the domain
- ☐ Manage Group Policy links
- ☐ Generate Resultant Set of Policy (Planning)

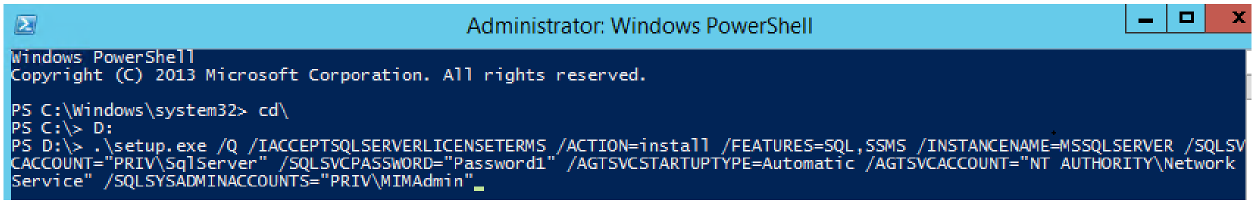
○ Create a custom task to delegate



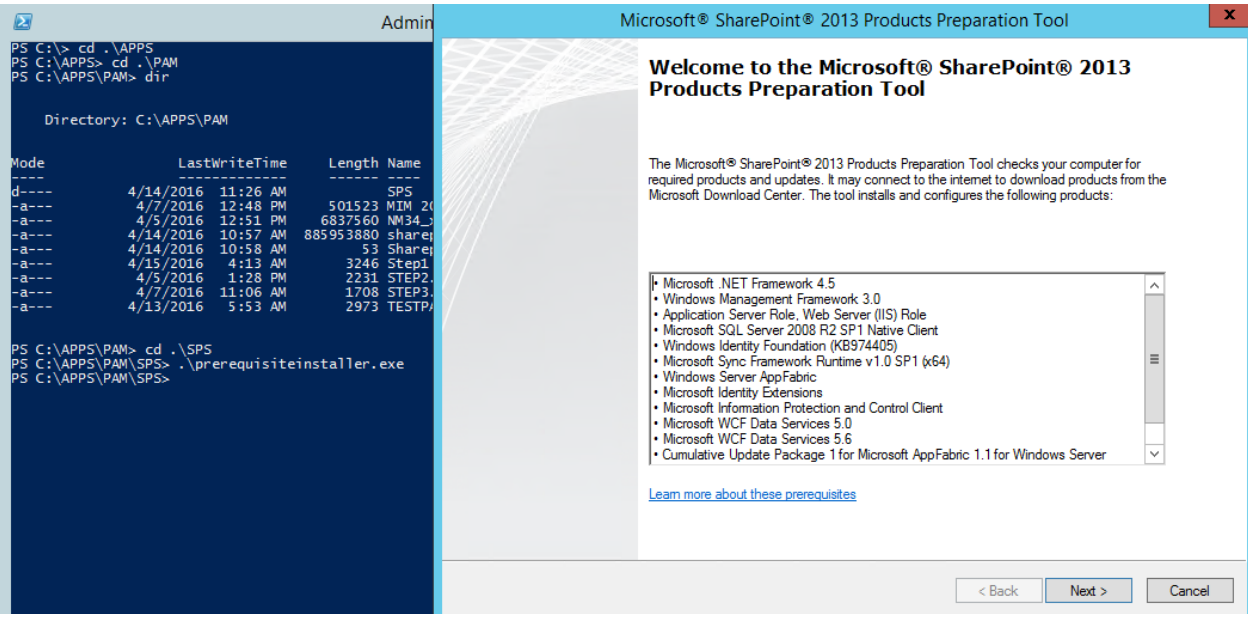
```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\mimadmin> import-module ServerManager
PS C:\Users\mimadmin> Install-WindowsFeature Web-WebServer, Net-Framework-Features,rsat-ad-powershell,Web-Mgmt-Tools,App
lication-Server,Windows-Identity-Foundation,Server-Media-Foundation,Xps-Viewer -includeallsubfeature -restart -source d:
\sources\SxS
```



```
<sectionGroup name="authentication">
    <section name="anonymousAuthentication" overrideModeDefault="Deny" />
    <section name="basicAuthentication" overrideModeDefault="Deny" />
    <section name="clientCertificateMappingAuthentication" overrideModeDefault="Deny" />
    <section name="digestAuthentication" overrideModeDefault="Deny" />
    <section name="iisClientCertificateMappingAuthentication" overrideModeDefault="Deny" />
    <section name="windowsAuthentication" overrideModeDefault="Allow" />
</sectionGroup>
```



```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> cd\
PS C:\> D:
PS D:\> .\setup.exe /Q /IACCEPTSQLSERVERLICENSETERMS /ACTION=install /FEATURES=SQL,SSMS /INSTANCENAME=MSSQLSERVER /SQLSV
CACCOUNT="PRIV\SqlServer" /SQLSVCPASSWORD="Password1" /AGTSVCSTARTUPTYPE=Automatic /AGTSVCACCOUNT="NT AUTHORITY\Network
Service" /SQLSYSADMINACCOUNTS="PRIV\MIMAdmin"
```



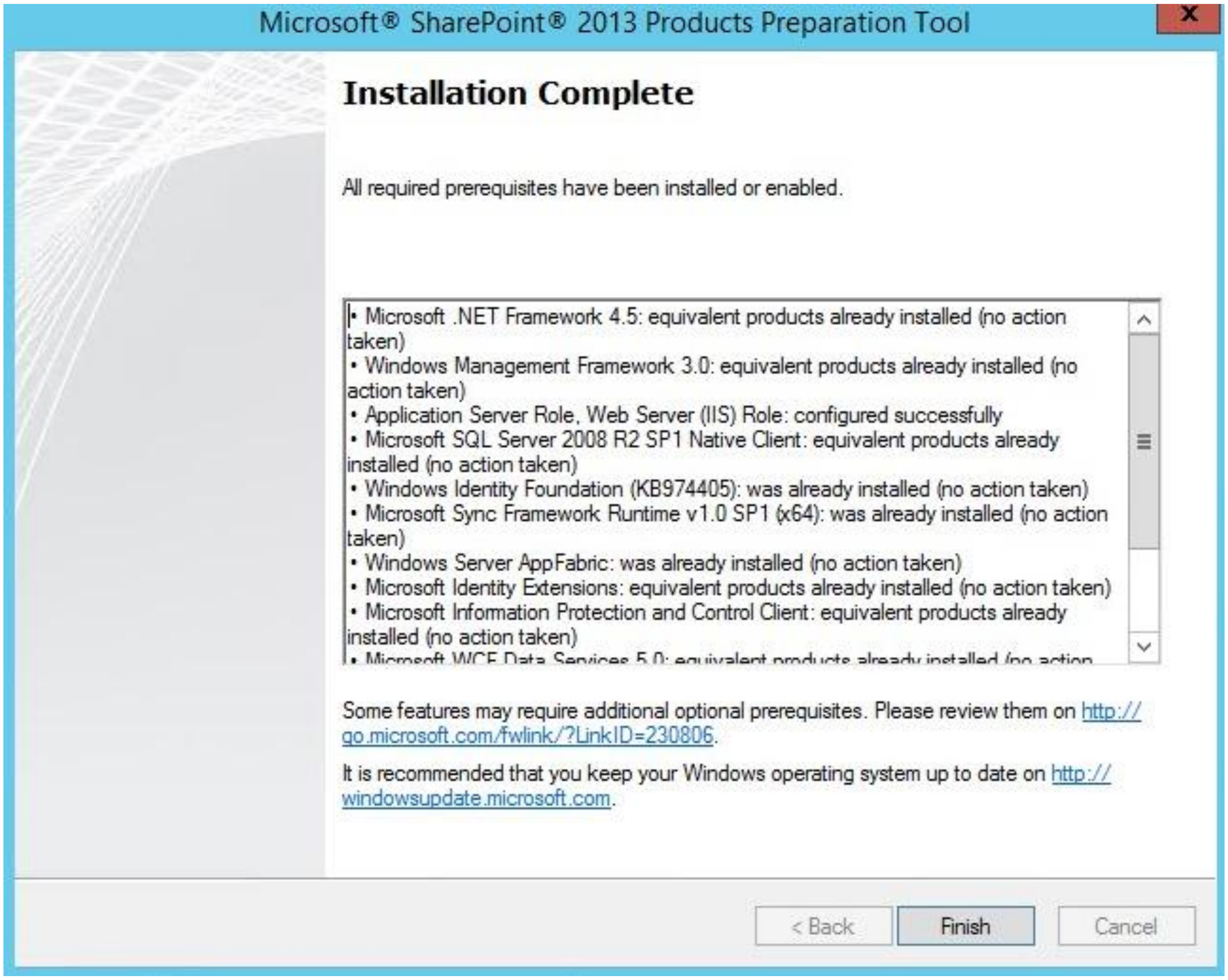
```
PS C:\> cd .\APPS
PS C:\APPS> cd .\PAM
PS C:\APPS\PAM> dir


    Directory: C:\APPS\PAM


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
d----         4/14/2016  11:26 AM            SPS
-a---          4/7/2016  12:48 PM     501523 MIM 2
-a---          4/5/2016  12:51 PM    6837560 NM34_
-a---         4/14/2016  10:57 AM  885953880 share
-a---         4/14/2016  10:58 AM         53 Share
-a---         4/15/2016   4:13 AM       3246 Step1
-a---          4/5/2016   1:28 PM       2231 STEP2.
-a---          4/7/2016  11:06 AM       1708 STEP3.
-a---         4/13/2016   5:53 AM       2973 TESTP


PS C:\APPS\PAM> cd .\SPS
PS C:\APPS\PAM\SPS> .\prerequisiteinstaller.exe
PS C:\APPS\PAM\SPS>
```

Welcome to the Microsoft® SharePoint® 2013 Products Preparation Tool

The Microsoft® SharePoint® 2013 Products Preparation Tool checks your computer for required products and updates. It may connect to the internet to download products from the Microsoft Download Center. The tool installs and configures the following products:

- Microsoft .NET Framework 4.5
- Windows Management Framework 3.0
- Application Server Role, Web Server (IIS) Role
- Microsoft SQL Server 2008 R2 SP1 Native Client
- Windows Identity Foundation (KB974405)
- Microsoft Sync Framework Runtime v1.0 SP1 (x64)
- Windows Server AppFabric
- Microsoft Identity Extensions
- Microsoft Information Protection and Control Client
- Microsoft WCF Data Services 5.0
- Microsoft WCF Data Services 5.6
- Cumulative Update Package 1 for Microsoft AppFabric 1.1 for Windows Server

Learn more about these prerequisites



Microsoft® SharePoint® 2013 Products Preparation Tool

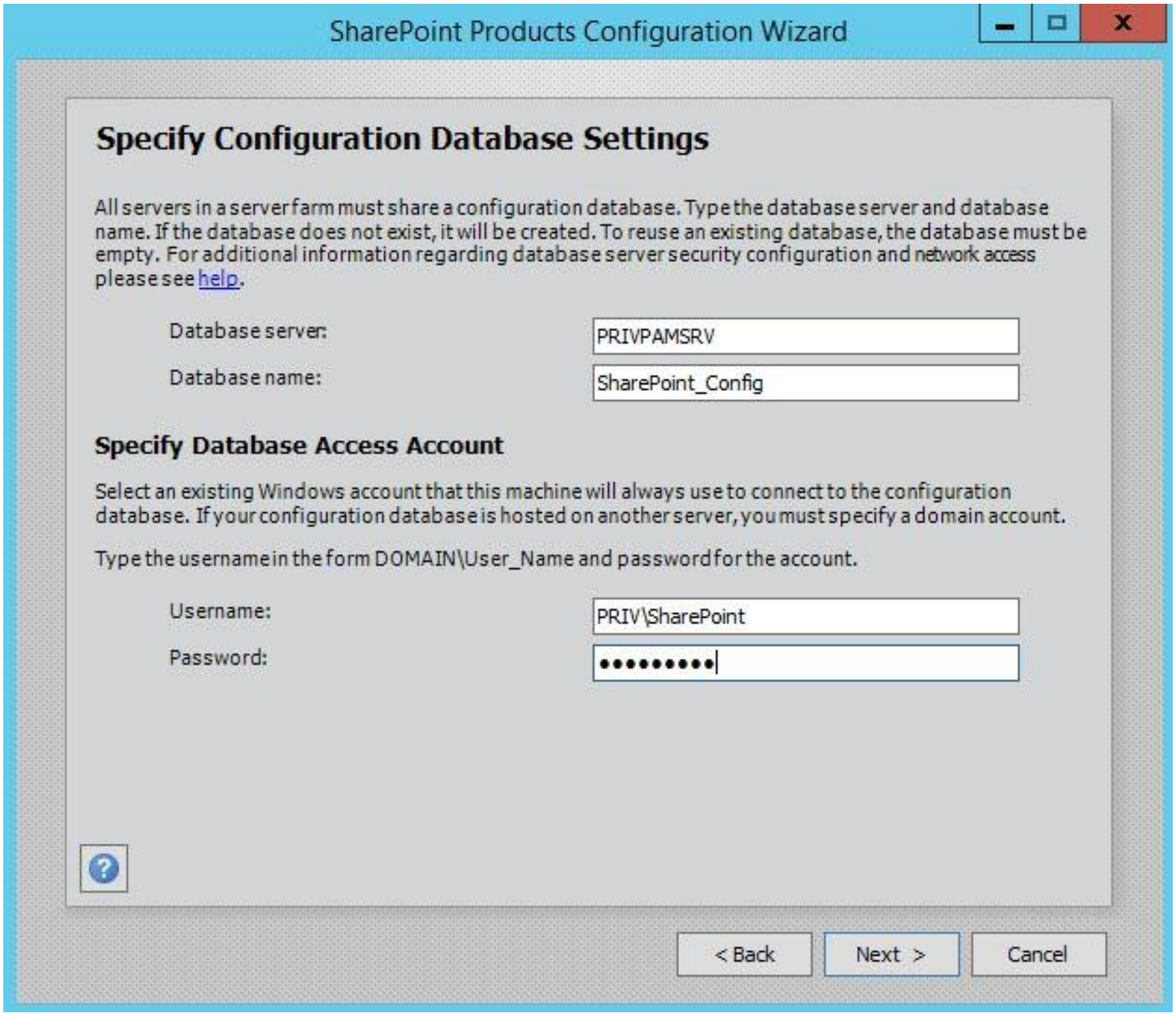
Installation Complete

All required prerequisites have been installed or enabled.

- Microsoft .NET Framework 4.5: equivalent products already installed (no action taken)
- Windows Management Framework 3.0: equivalent products already installed (no action taken)
- Application Server Role, Web Server (IIS) Role: configured successfully
- Microsoft SQL Server 2008 R2 SP1 Native Client: equivalent products already installed (no action taken)
- Windows Identity Foundation (KB974405): was already installed (no action taken)
- Microsoft Sync Framework Runtime v1.0 SP1 (x64): was already installed (no action taken)
- Windows Server AppFabric: was already installed (no action taken)
- Microsoft Identity Extensions: equivalent products already installed (no action taken)
- Microsoft Information Protection and Control Client: equivalent products already installed (no action taken)
- Microsoft WCF Data Services 5.0: equivalent products already installed (no action

Some features may require additional optional prerequisites. Please review them on http://go.microsoft.com/fwlink/?LinkID=230806.

It is recommended that you keep your Windows operating system up to date on http://windowsupdate.microsoft.com.



SharePoint Products Configuration Wizard

Specify Configuration Database Settings

All servers in a server farm must share a configuration database. Type the database server and database name. If the database does not exist, it will be created. To reuse an existing database, the database must be empty. For additional information regarding database server security configuration and network access please see help.

Database server: PRIVPAMSRV

Database name: SharePoint_Config

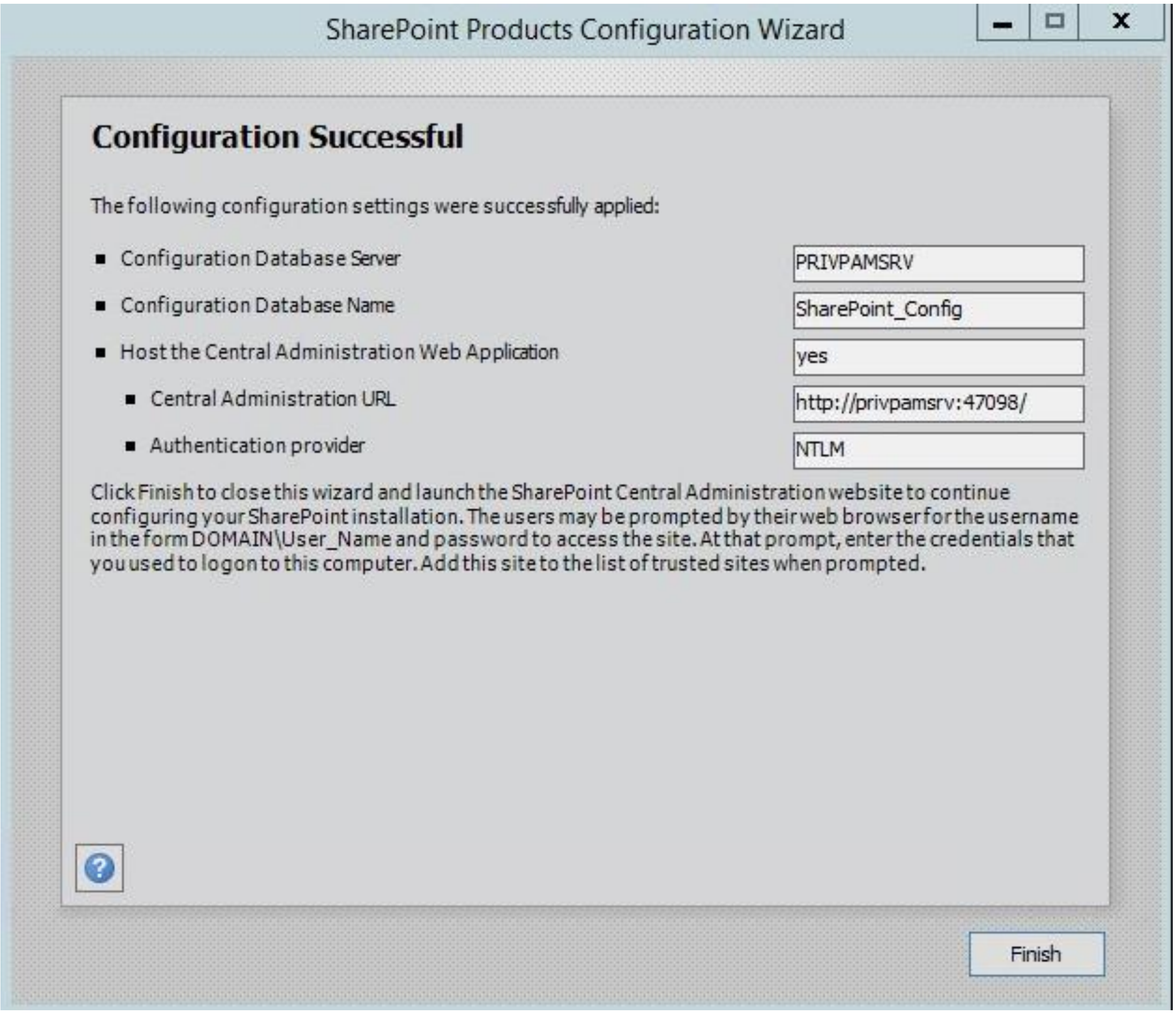
Specify Database Access Account

Select an existing Windows account that this machine will always use to connect to the configuration database. If your configuration database is hosted on another server, you must specify a domain account.

Type the username in the form DOMAIN\User_Name and password for the account.

Username: PRIV\SharePoint

Password: ●●●●●●●●●●

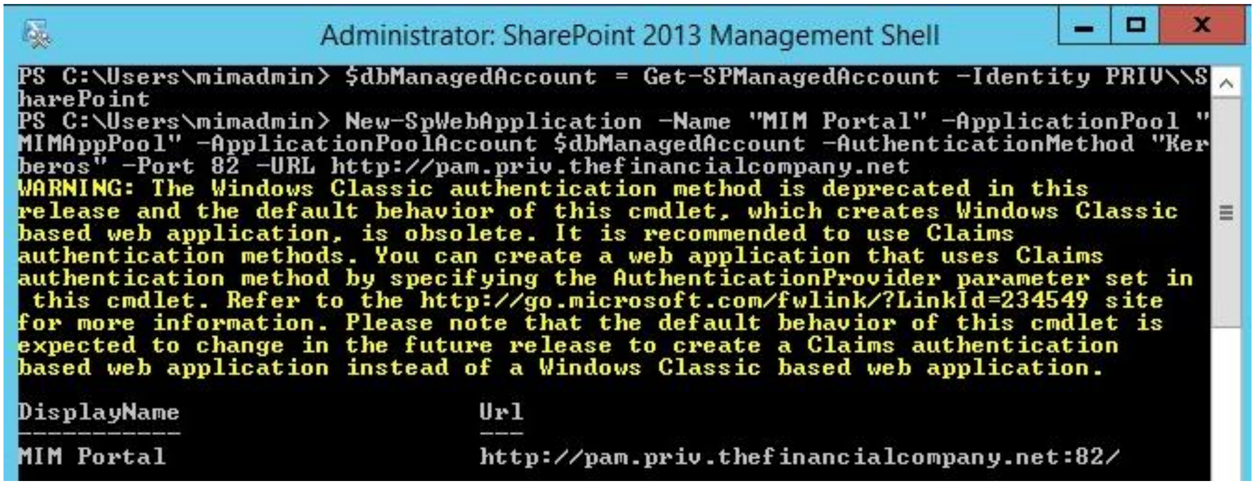


Configuration Successful

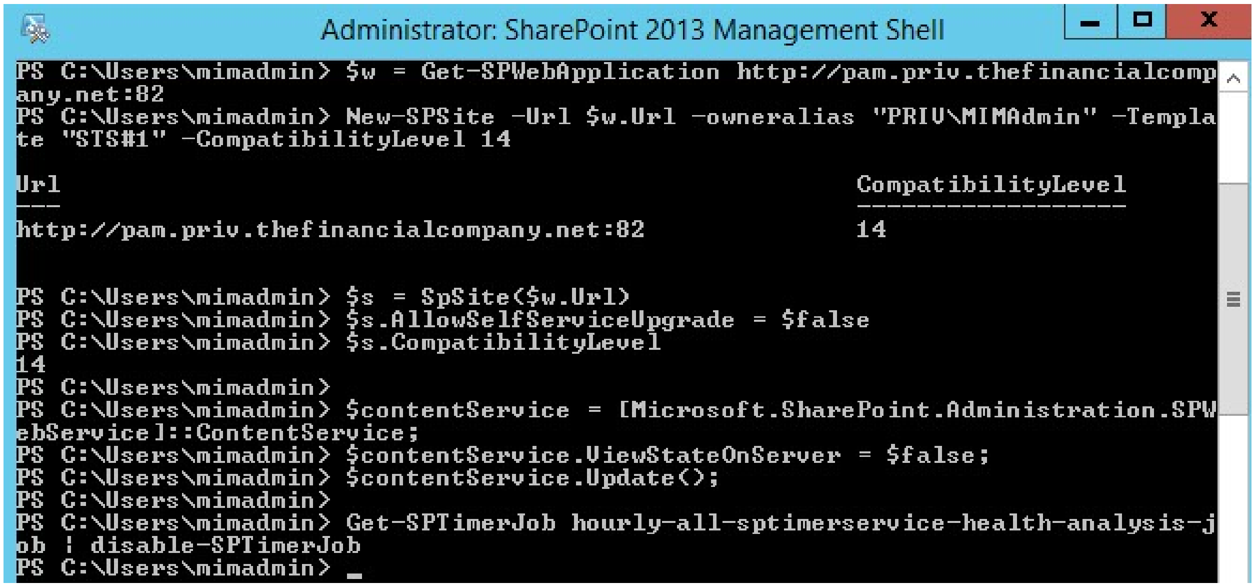
The following configuration settings were successfully applied:

Configuration Database Server	PRIVPAMSRV
Configuration Database Name	SharePoint_Config
Host the Central Administration Web Application	yes
Central Administration URL	http://privpamsrv:47098/
Authentication provider	NTLM

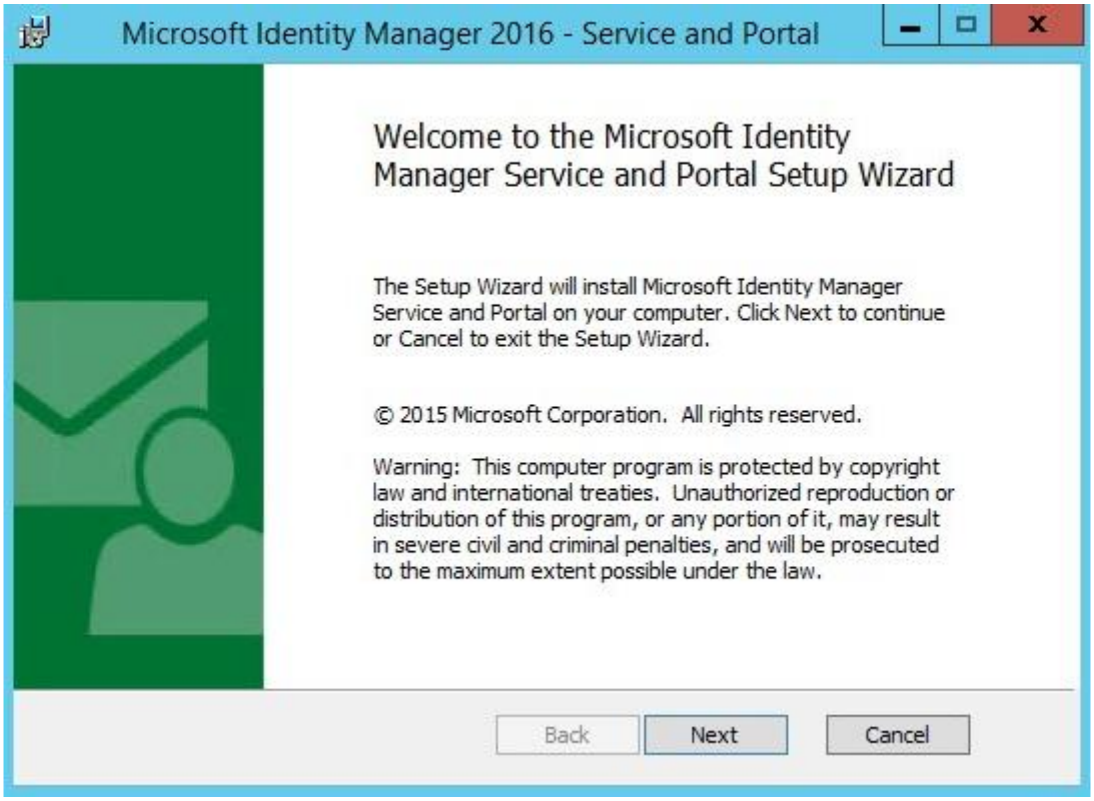
Click Finish to close this wizard and launch the SharePoint Central Administration website to continue configuring your SharePoint installation. The users may be prompted by their web browser for the username in the form DOMAIN\User_Name and password to access the site. At that prompt, enter the credentials that you used to logon to this computer. Add this site to the list of trusted sites when prompted.



```
PS C:\Users\mimadmin> $dbManagedAccount = Get-SPManagedAccount -Identity PRIV\\S
harePoint
PS C:\Users\mimadmin> New-SpWebApplication -Name "MIM Portal" -ApplicationPool "
MIMAppPool" -ApplicationPoolAccount $dbManagedAccount -AuthenticationMethod "Ker
beros" -Port 82 -URL http://pam.priv.thefinancialcompany.net
WARNING: The Windows Classic authentication method is deprecated in this
release and the default behavior of this cmdlet, which creates Windows Classic
based web application, is obsolete. It is recommended to use 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.

DisplayName                    Url
-----------                    ---
MIM Portal                     http://pam.priv.thefinancialcompany.net:82/
```



```
PS C:\Users\mimadmin> $w = Get-SPWebApplication http://pam.priv.thefinancialcomp
any.net:82
PS C:\Users\mimadmin> New-SPSite -Url $w.Url -owneralias "PRIV\MIMAdmin" -Templa
te "STS#1" -CompatibilityLevel 14

Url                                                     CompatibilityLevel
---                                                     ------------------
http://pam.priv.thefinancialcompany.net:82              14


PS C:\Users\mimadmin> $s = SpSite($w.Url)
PS C:\Users\mimadmin> $s.AllowSelfServiceUpgrade = $false
PS C:\Users\mimadmin> $s.CompatibilityLevel
14
PS C:\Users\mimadmin>
PS C:\Users\mimadmin> $contentService = [Microsoft.SharePoint.Administration.SPW
ebService]::ContentService;
PS C:\Users\mimadmin> $contentService.ViewStateOnServer = $false;
PS C:\Users\mimadmin> $contentService.Update();
PS C:\Users\mimadmin>
PS C:\Users\mimadmin> Get-SPTimerJob hourly-all-sptimerservice-health-analysis-j
ob | disable-SPTimerJob
PS C:\Users\mimadmin> _
```

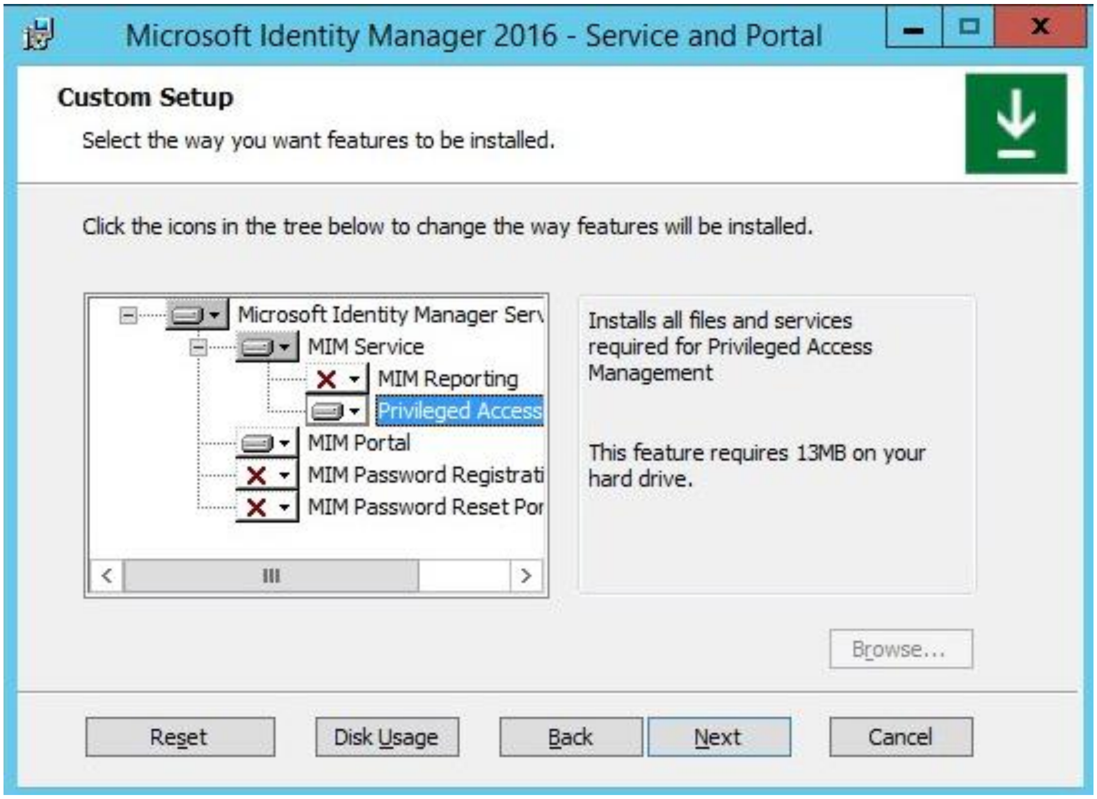


Welcome to the Microsoft Identity Manager Service and Portal Setup Wizard

The Setup Wizard will install Microsoft Identity Manager Service and Portal on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

© 2015 Microsoft Corporation. All rights reserved.

Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.



Microsoft Identity Manager 2016 - Service and Portal

Custom Setup

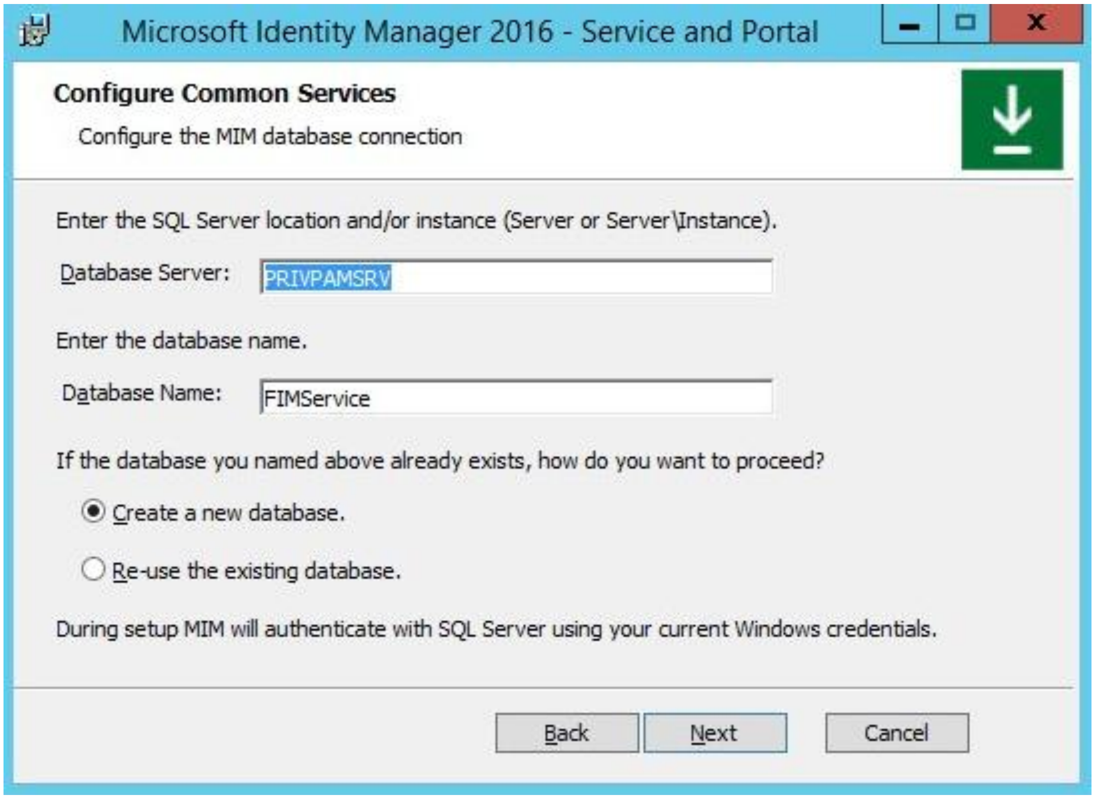
Select the way you want features to be installed.

Click the icons in the tree below to change the way features will be installed.

- Microsoft Identity Manager Serv
  - MIM Service
    - ✗ MIM Reporting
    - Privileged Access
  - MIM Portal
  - ✗ MIM Password Registrati
  - ✗ MIM Password Reset Por

Installs all files and services required for Privileged Access Management

This feature requires 13MB on your hard drive.



Microsoft Identity Manager 2016 - Service and Portal

Configure Common Services

Configure the MIM database connection

Enter the SQL Server location and/or instance (Server or Server\Instance).

Database Server: PRIVPAMSRV

Enter the database name.

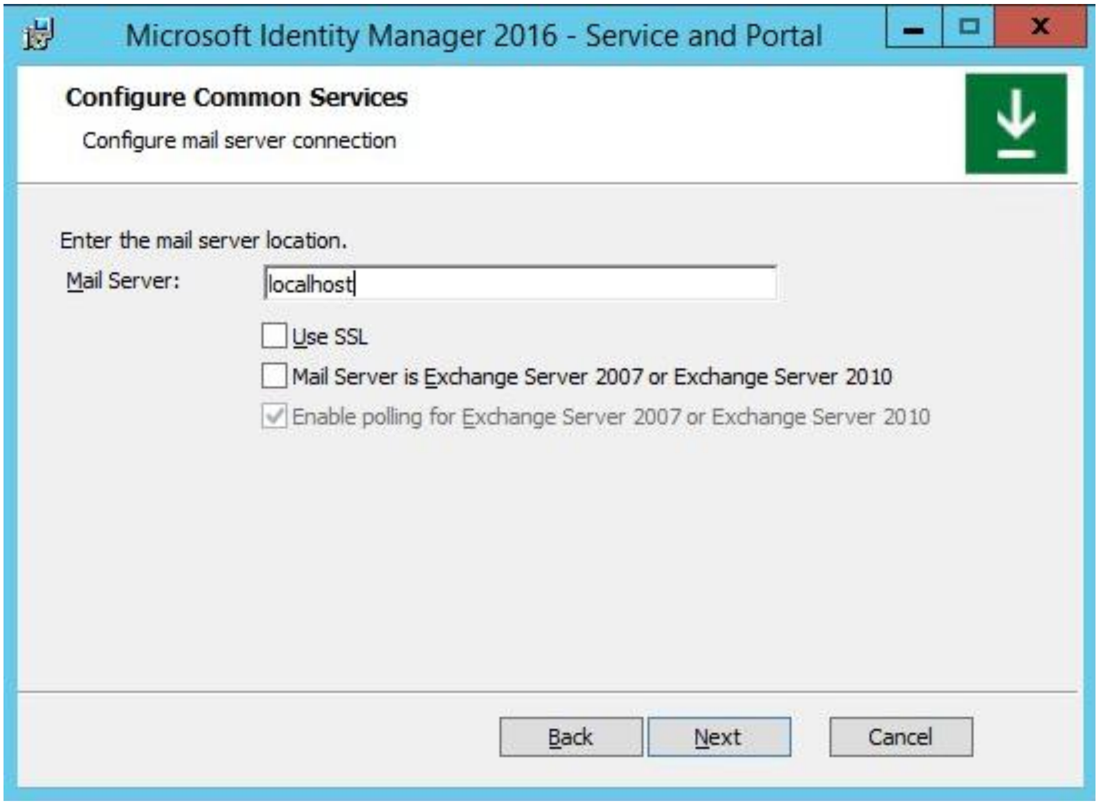
Database Name: FIMService

If the database you named above already exists, how do you want to proceed?

● Create a new database.

○ Re-use the existing database.

During setup MIM will authenticate with SQL Server using your current Windows credentials.



Microsoft Identity Manager 2016 - Service and Portal

Configure Common Services

Configure mail server connection

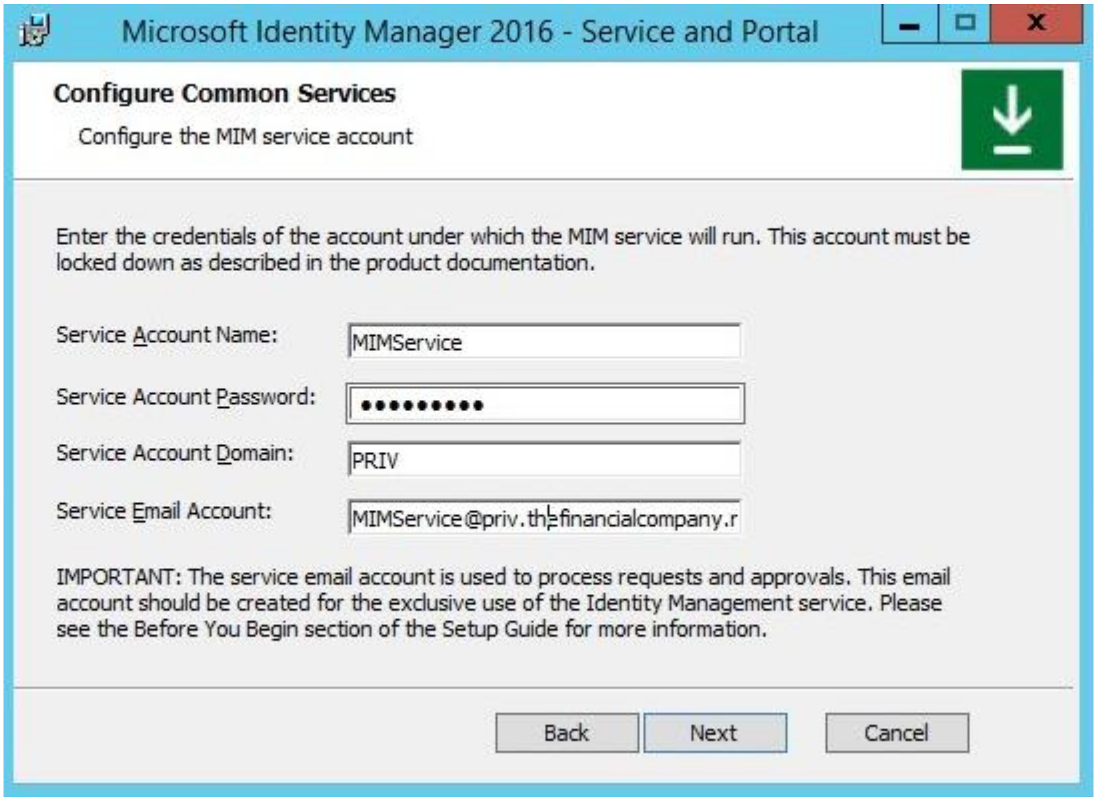
Enter the mail server location.

Mail Server: localhost

□ Use SSL

□ Mail Server is Exchange Server 2007 or Exchange Server 2010

☑ Enable polling for Exchange Server 2007 or Exchange Server 2010



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.

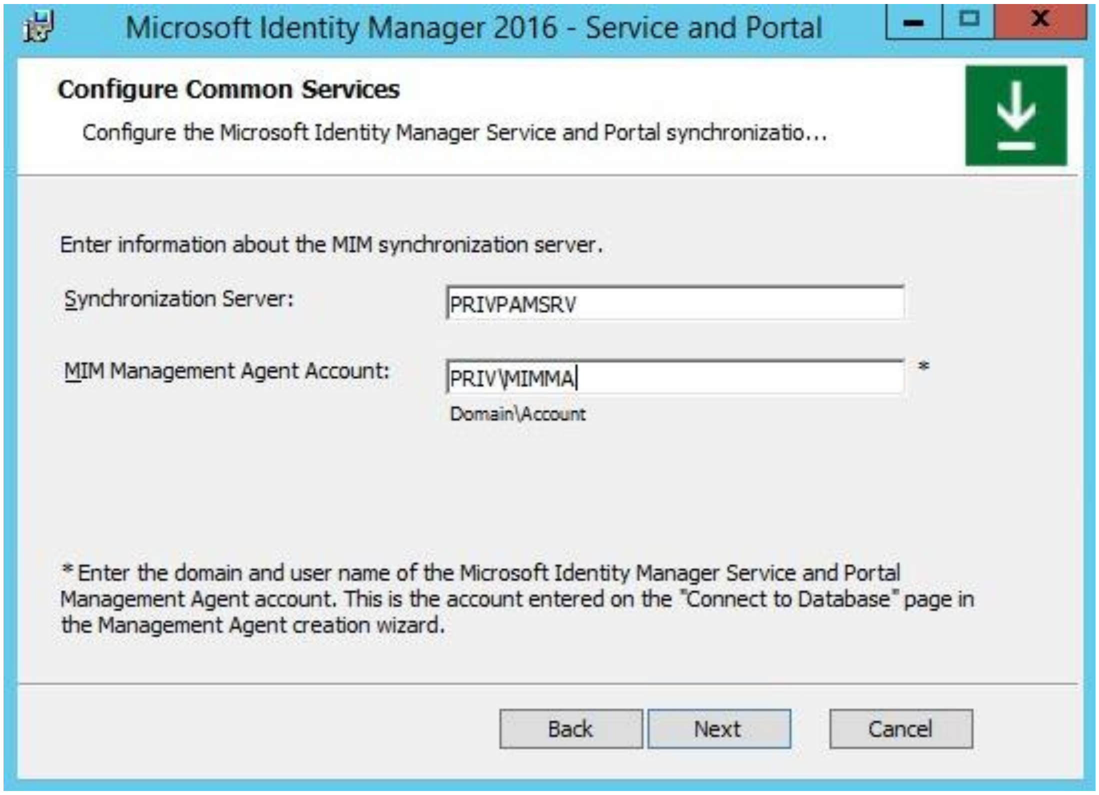
Service Account Name: MIMService

Service Account Password: ••••••••••

Service Account Domain: PRIV

Service Email Account: MIMService@priv.thefinancialcompany.r

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.



Configure Common Services

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

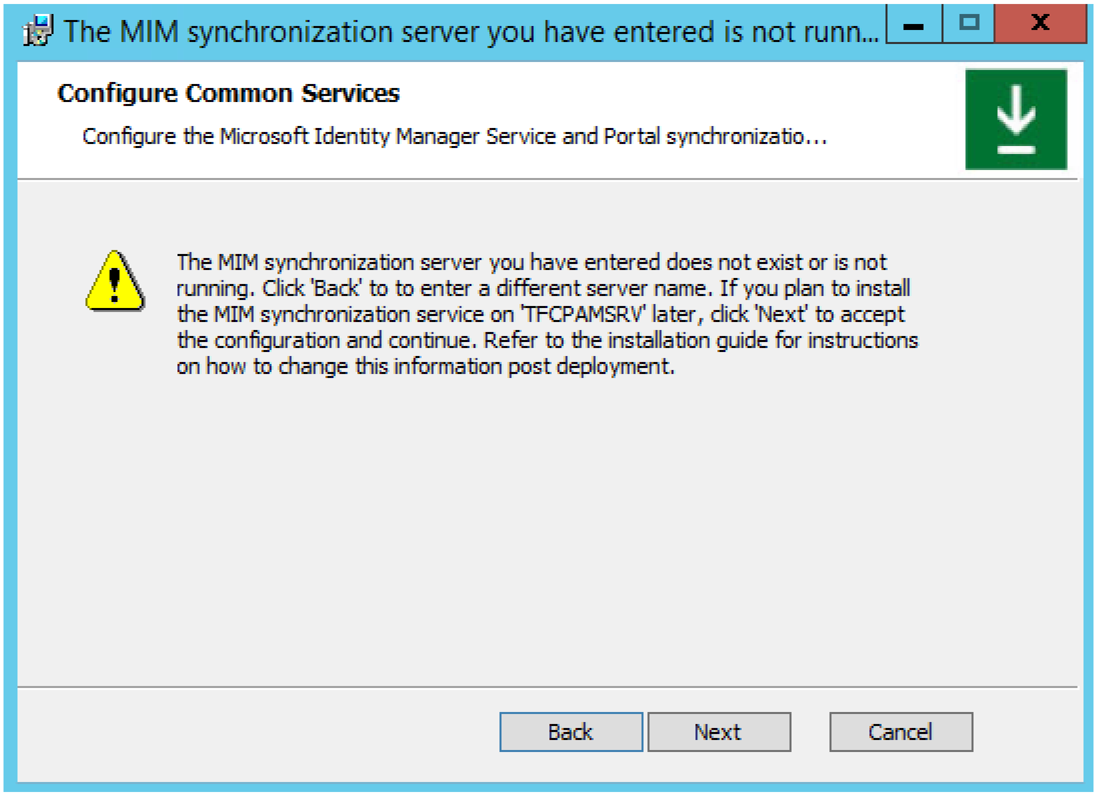
Enter information about the MIM synchronization server.

Synchronization Server: PRIVPAMSRV

MIM Management Agent Account: PRIV\MIMMA *

Domain\Account

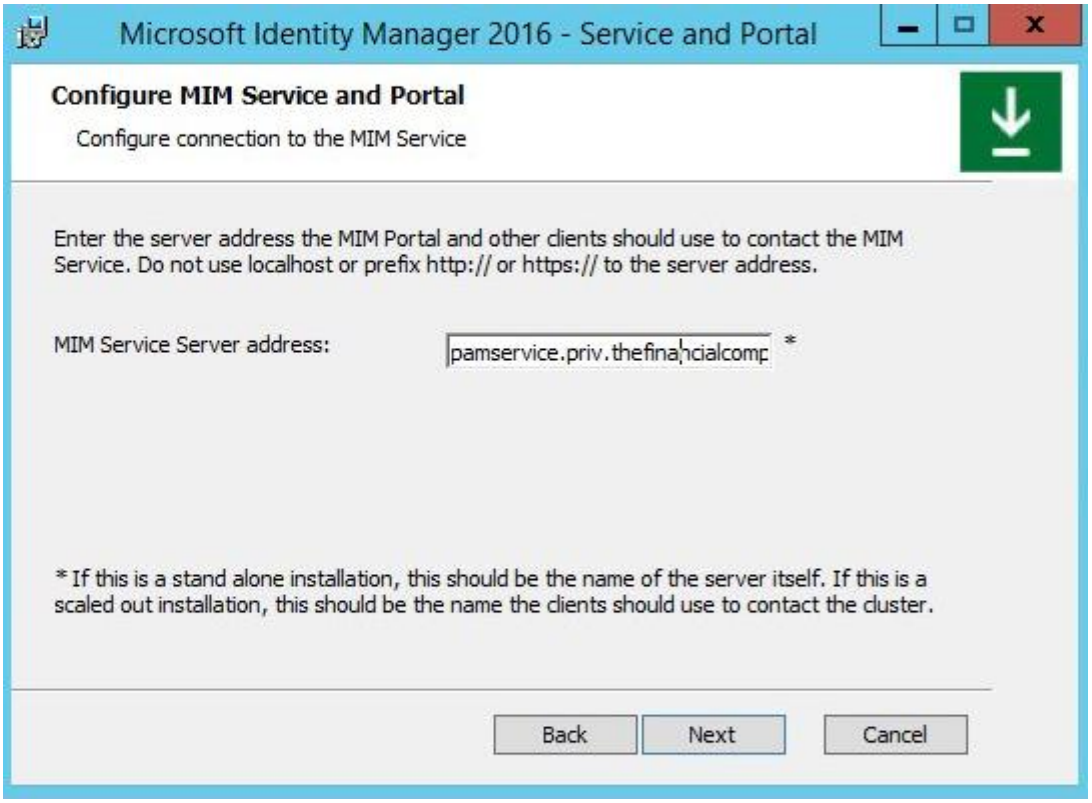
* Enter the domain and user name of the Microsoft Identity Manager Service and Portal Management Agent account. This is the account entered on the "Connect to Database" page in the Management Agent creation wizard.


The MIM synchronization server you have entered is not runn...

Configure Common Services

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

The MIM synchronization server you have entered does not exist or is not running. Click 'Back' to to enter a different server name. If you plan to install the MIM synchronization service on 'TFCPAMSRV' later, click 'Next' to accept the configuration and continue. Refer to the installation guide for instructions on how to change this information post deployment.



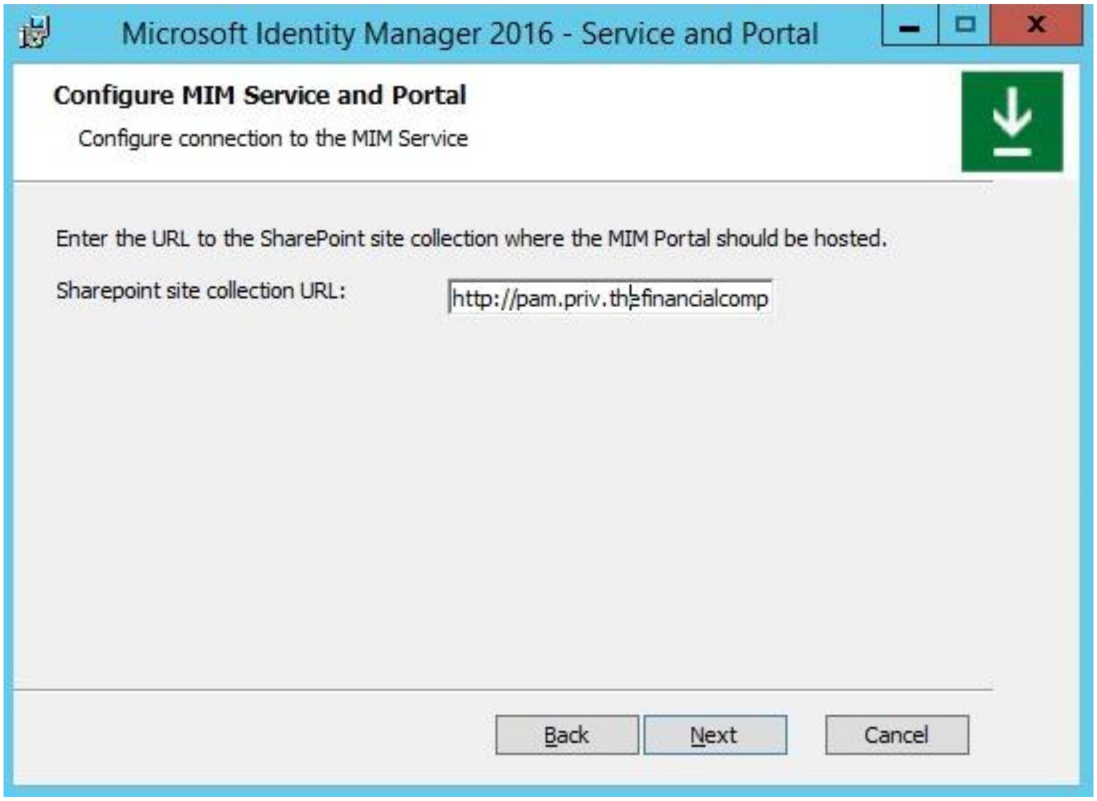
Configure MIM Service and Portal

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: pamservice.priv.thefinancialcomp *

* 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.

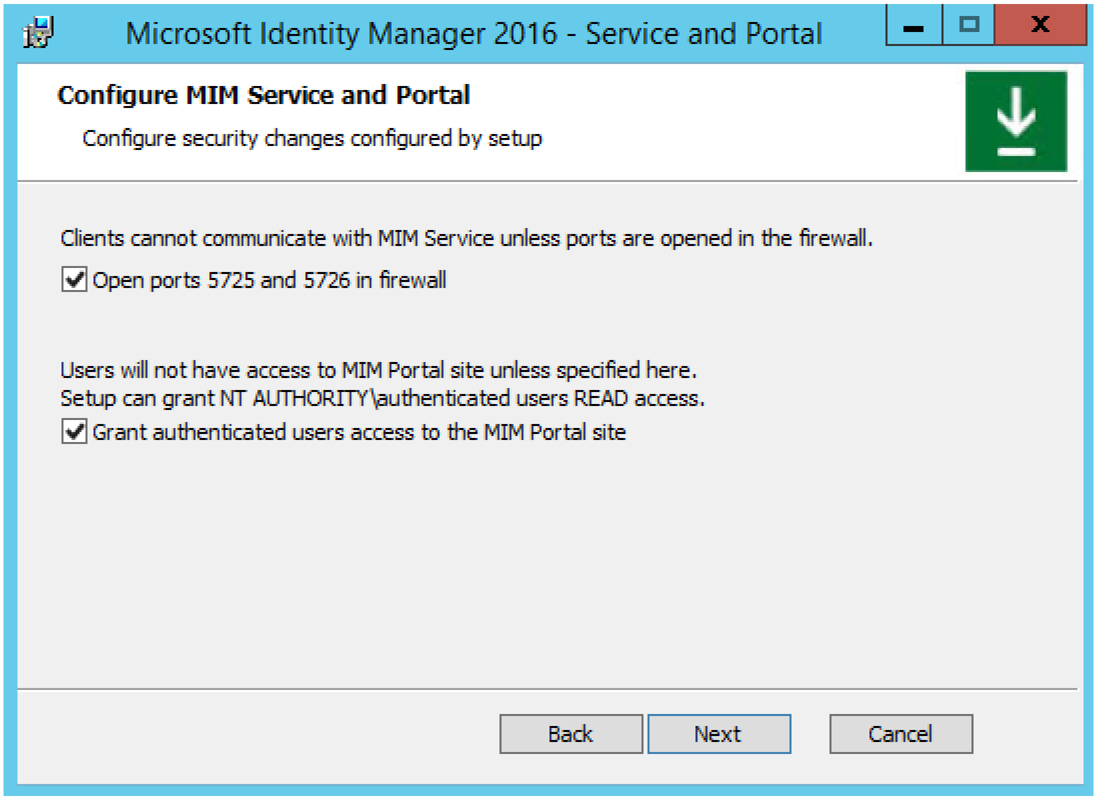


Configure MIM Service and Portal

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: http://pam.priv.thefinancialcomp



Configure MIM Service and Portal

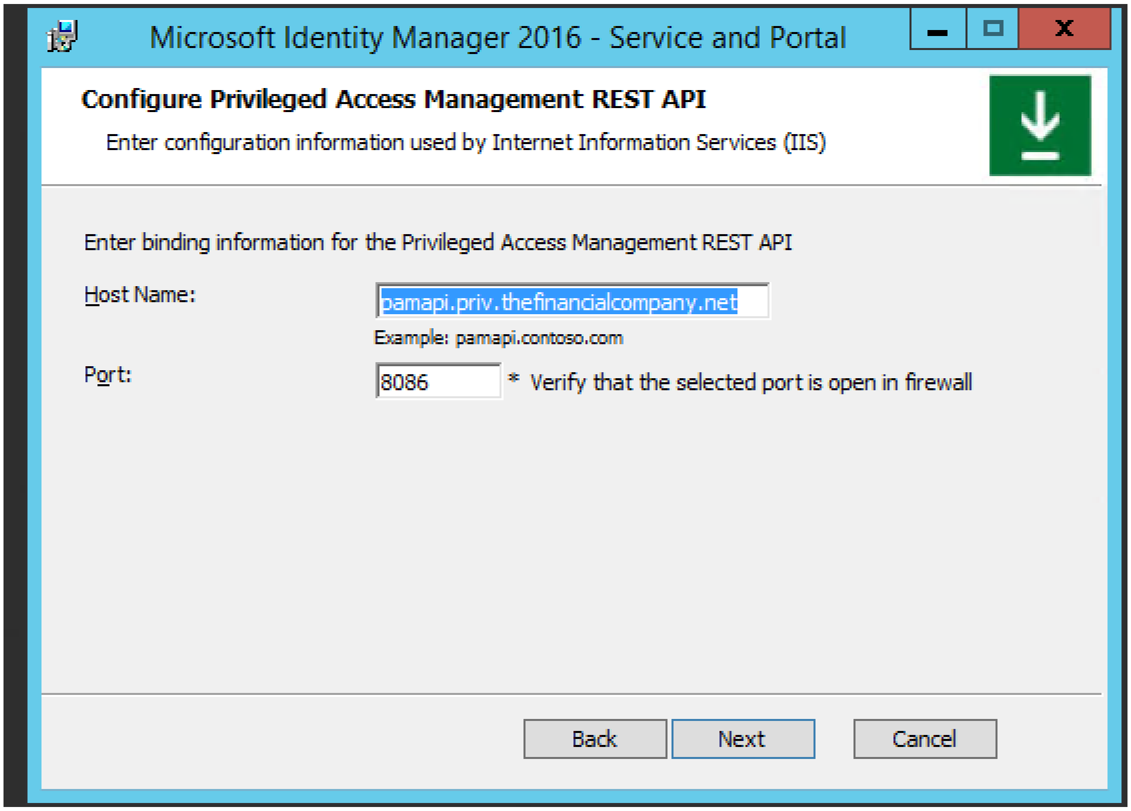
Configure security changes configured by setup

Clients cannot communicate with MIM Service unless ports are opened in the firewall.

☑ Open ports 5725 and 5726 in firewall

Users will not have access to MIM Portal site unless specified here.
Setup can grant NT AUTHORITY\authenticated users READ access.

☑ Grant authenticated users access to the MIM Portal site



Configure Privileged Access Management REST API

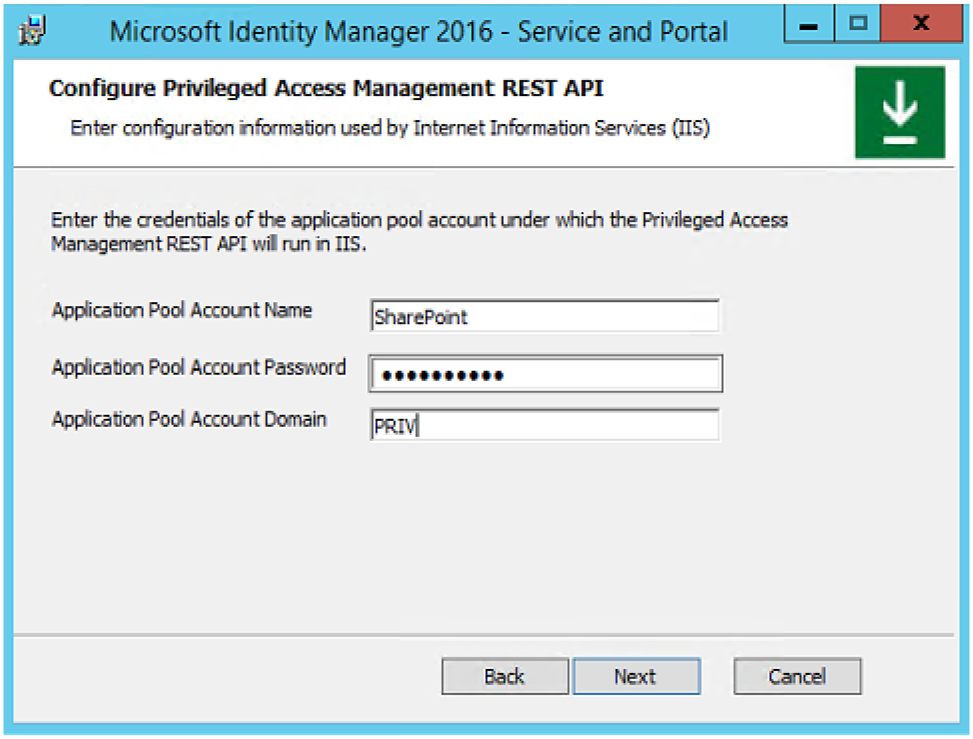
Enter configuration information used by Internet Information Services (IIS)

Enter binding information for the Privileged Access Management REST API

Host Name: pamapi.priv.thefinancialcompany.net

Example: pamapi.contoso.com

Port: 8086 * Verify that the selected port is open in firewall



Microsoft Identity Manager 2016 - Service and Portal

Configure Privileged Access Management REST API

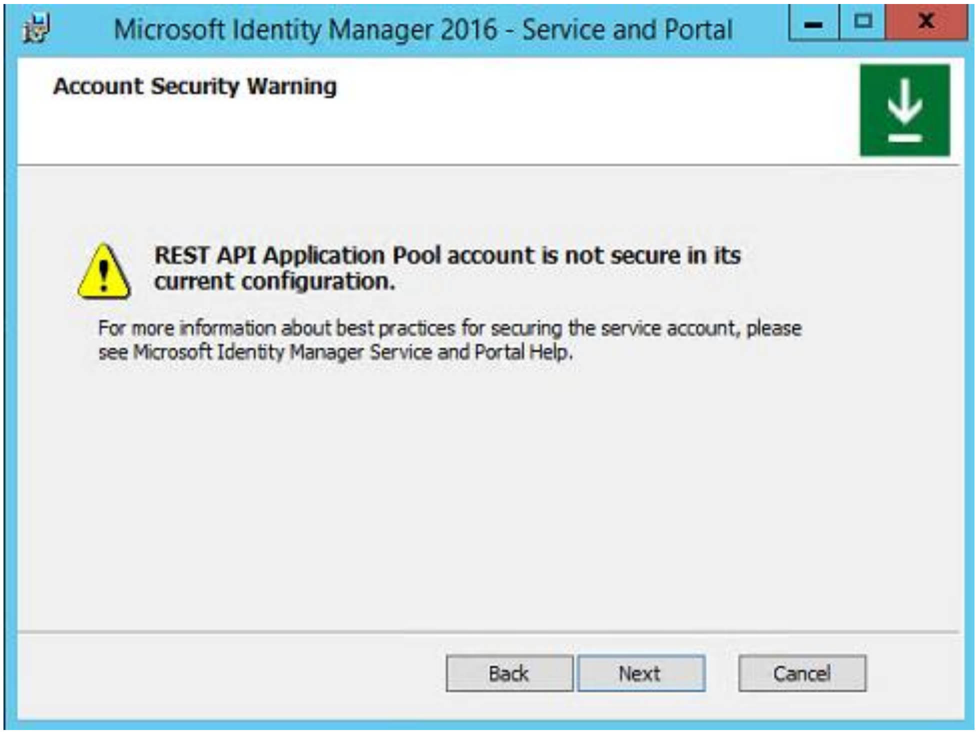
Enter configuration information used by Internet Information Services (IIS)

Enter the credentials of the application pool account under which the Privileged Access Management REST API will run in IIS.

Application Pool Account Name: SharePoint

Application Pool Account Password: ●●●●●●●●●●●

Application Pool Account Domain: PRIV

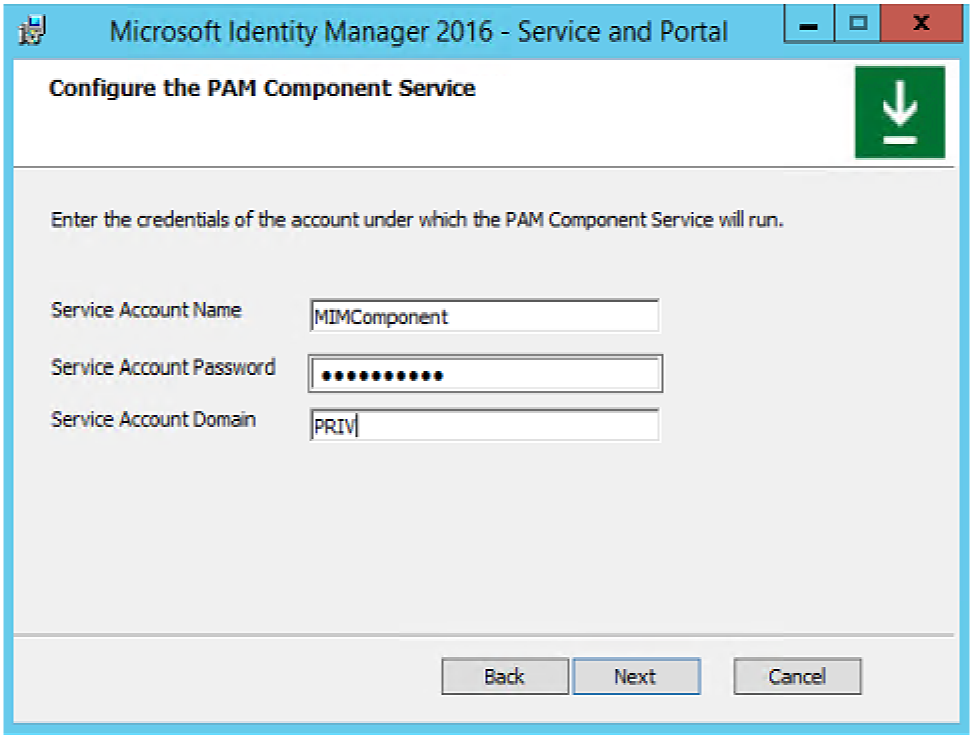


Microsoft Identity Manager 2016 - Service and Portal

Account Security Warning

REST API Application Pool account is not secure in its current configuration.

For more information about best practices for securing the service account, please see Microsoft Identity Manager Service and Portal Help.



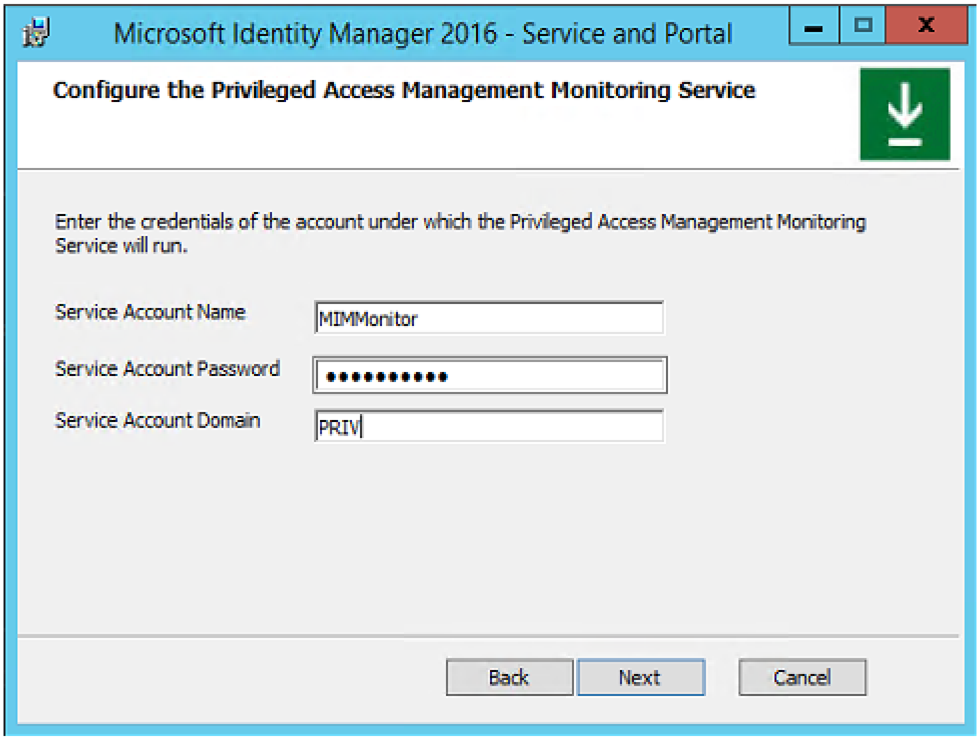
Configure the PAM Component Service

Enter the credentials of the account under which the PAM Component Service will run.

Service Account Name: MIMComponent

Service Account Password: ●●●●●●●●●●●

Service Account Domain: PRIV



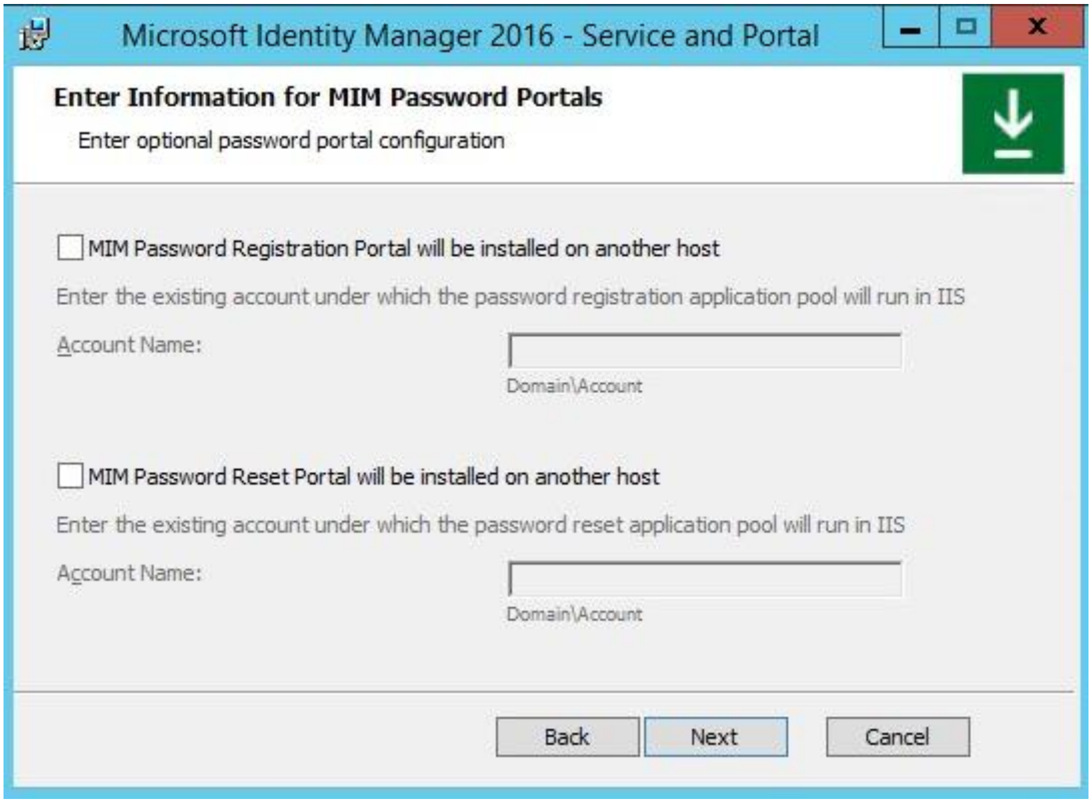
Configure the Privileged Access Management Monitoring Service

Enter the credentials of the account under which the Privileged Access Management Monitoring Service will run.

Service Account Name: MIMMonitor

Service Account Password: ●●●●●●●●●●●

Service Account Domain: PRIV



Enter Information for MIM Password Portals

Enter optional password portal configuration

☐ MIM Password Registration Portal will be installed on another host

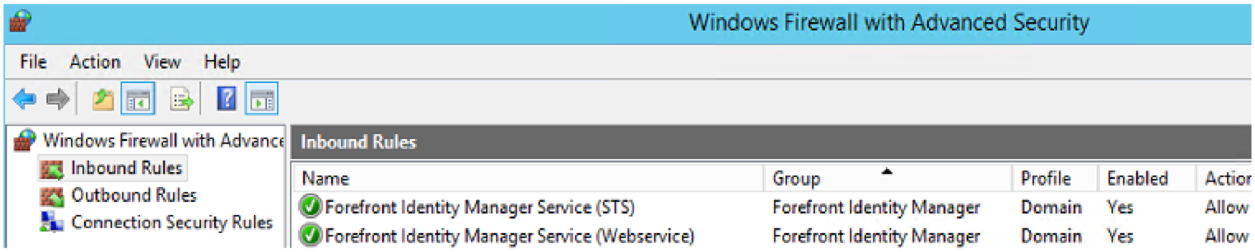
Enter the existing account under which the password registration application pool will run in IIS

Account Name: ______ Domain\Account

☐ MIM Password Reset Portal will be installed on another host

Enter the existing account under which the password reset application pool will run in IIS

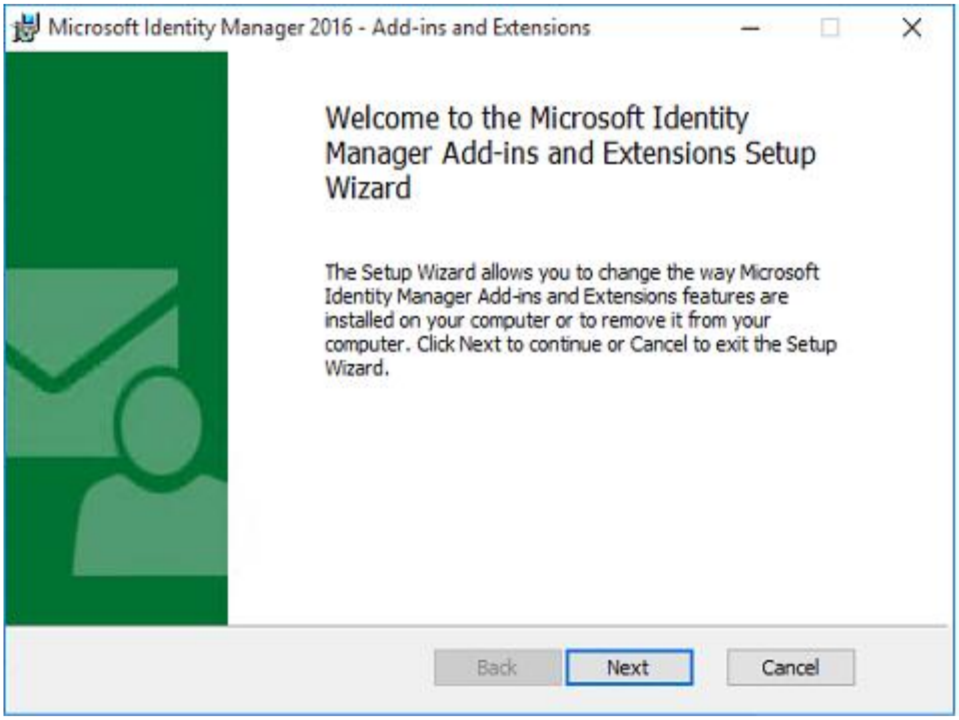
Account Name: ______ Domain\Account



Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advance
Inbound Rules
Outbound Rules
Connection Security Rules

Inbound Rules

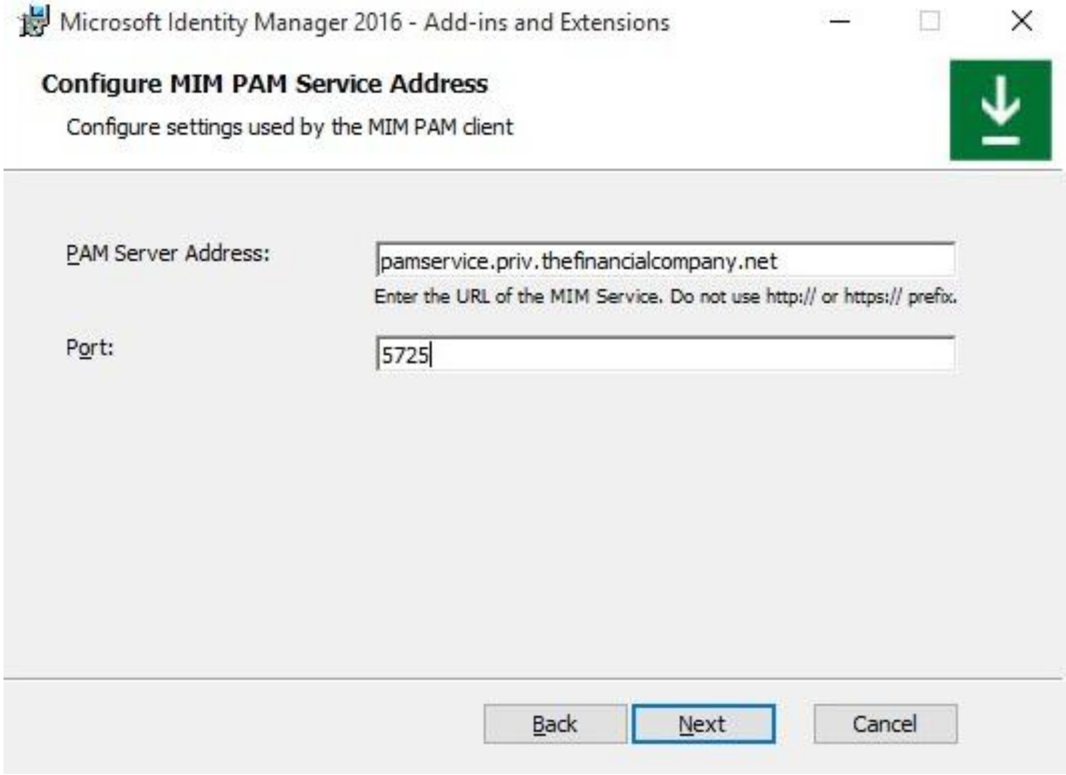
Name	Group	Profile	Enabled	Actior
Forefront Identity Manager Service (STS)	Forefront Identity Manager	Domain	Yes	Allow
Forefront Identity Manager Service (Webservice)	Forefront Identity Manager	Domain	Yes	Allow



Microsoft Identity Manager 2016 - Add-ins and Extensions

Welcome to the Microsoft Identity Manager Add-ins and Extensions Setup Wizard

The Setup Wizard allows you to change the way Microsoft Identity Manager Add-ins and Extensions features are installed on your computer or to remove it from your computer. Click Next to continue or Cancel to exit the Setup Wizard.



Microsoft Identity Manager 2016 - Add-ins and Extensions

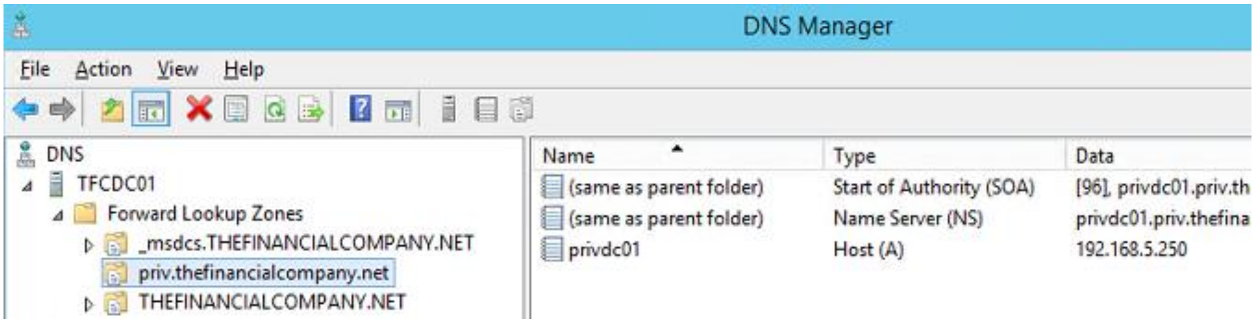
Configure MIM PAM Service Address

Configure settings used by the MIM PAM client

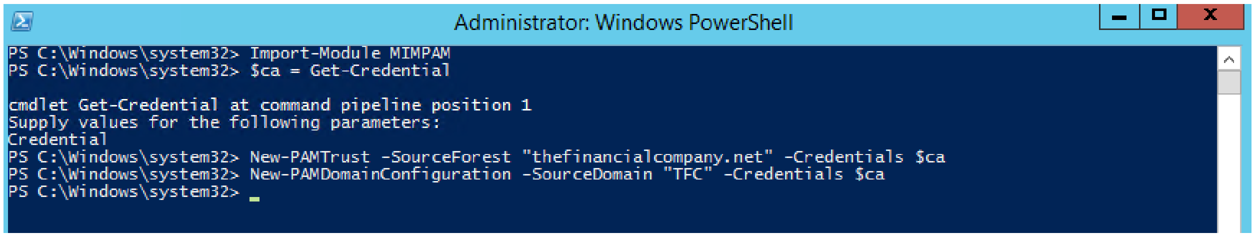
PAM Server Address: pamservice.priv.thefinancialcompany.net

Enter the URL of the MIM Service. Do not use http:// or https:// prefix.

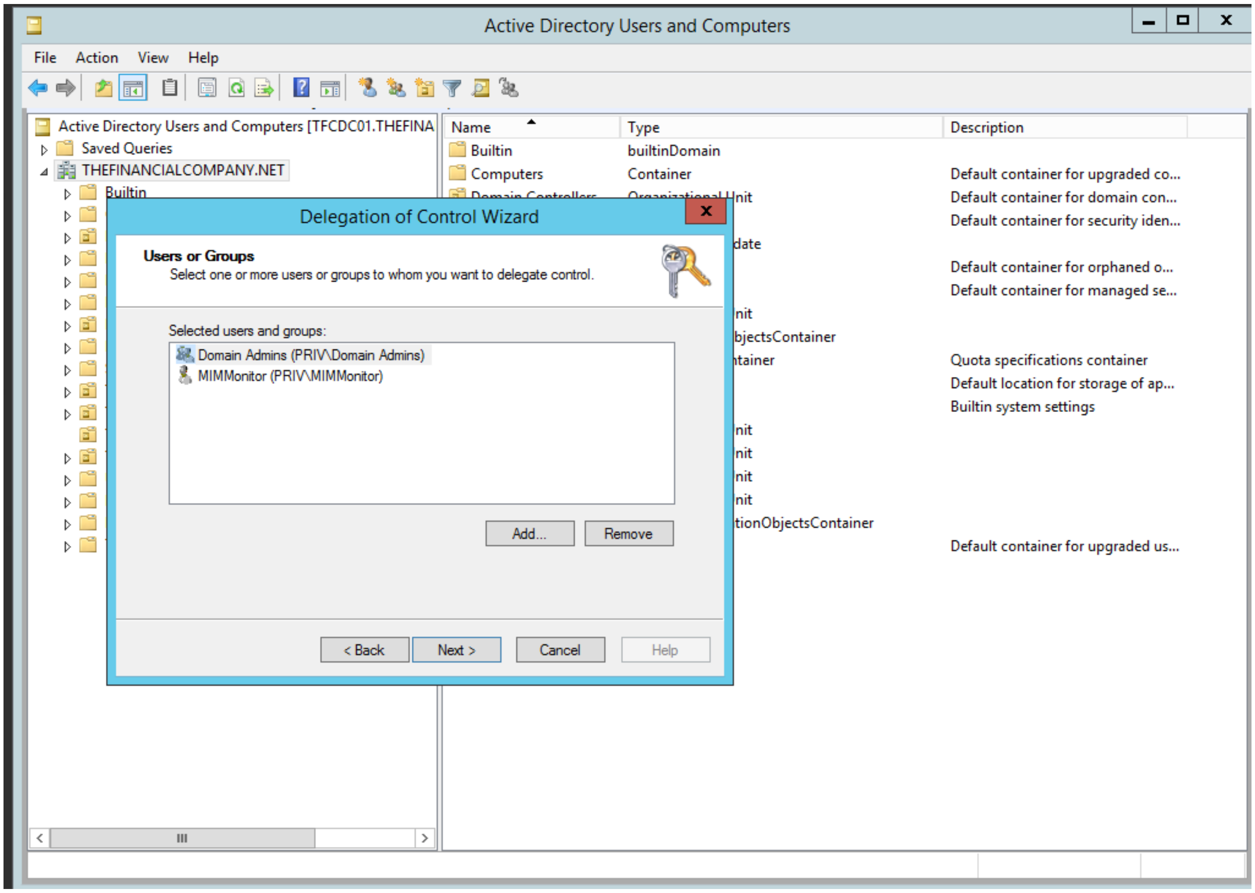
Port: 5725



Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[96], privdc01.priv.th
(same as parent folder)	Name Server (NS)	privdc01.priv.thefina
privdc01	Host (A)	192.168.5.250



```
PS C:\Windows\system32> Import-Module MIMPAM
PS C:\Windows\system32> $ca = Get-Credential

cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
PS C:\Windows\system32> New-PAMTrust -SourceForest "thefinancialcompany.net" -Credentials $ca
PS C:\Windows\system32> New-PAMDomainConfiguration -SourceDomain "TFC" -Credentials $ca
PS C:\Windows\system32> _
```

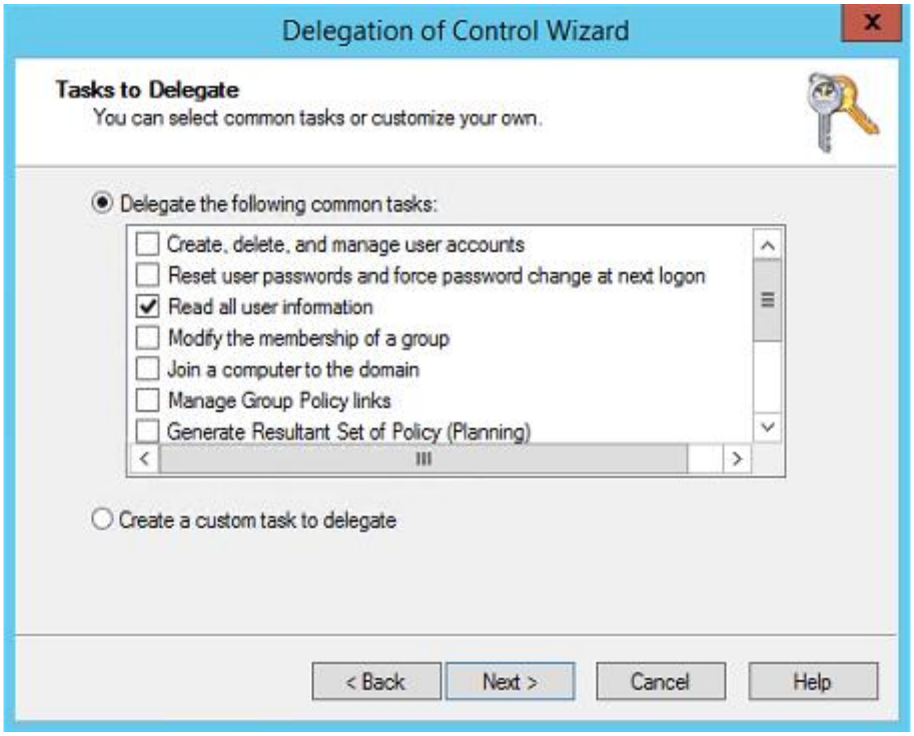

Active Directory Users and Computers
File Action View Help
Active Directory Users and Computers [TFCDC01.THEFINA
Saved Queries
THEFINANCIALCOMPANY.NET
Builtin
Name
Type
Description
Builtin
builtinDomain
Computers
Container
Default container for upgraded co...
Default container for domain con...
Default container for security iden...
Default container for orphaned o...
Default container for managed se...
Quota specifications container
Default location for storage of ap...
Builtin system settings
Default container for upgraded us...
Delegation of Control Wizard
Add...
Remove
< Back
Next >
Cancel
Help

Users or Groups

Select one or more users or groups to whom you want to delegate control.

Selected users and groups:

Domain Admins (PRIV\Domain Admins)
MIMMonitor (PRIV\MIMMonitor)

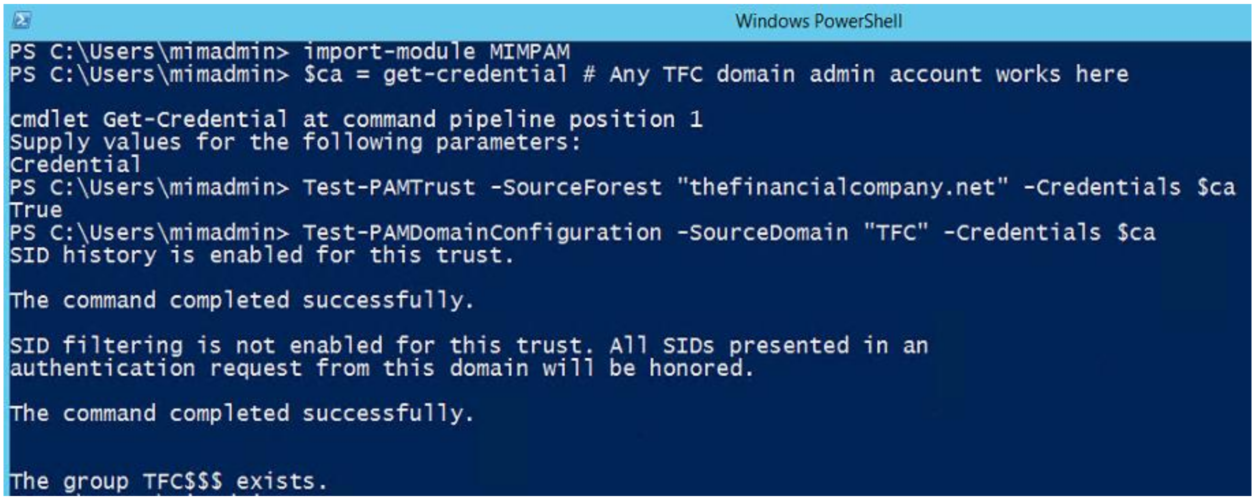


Tasks to Delegate
You can select common tasks or customize your own.

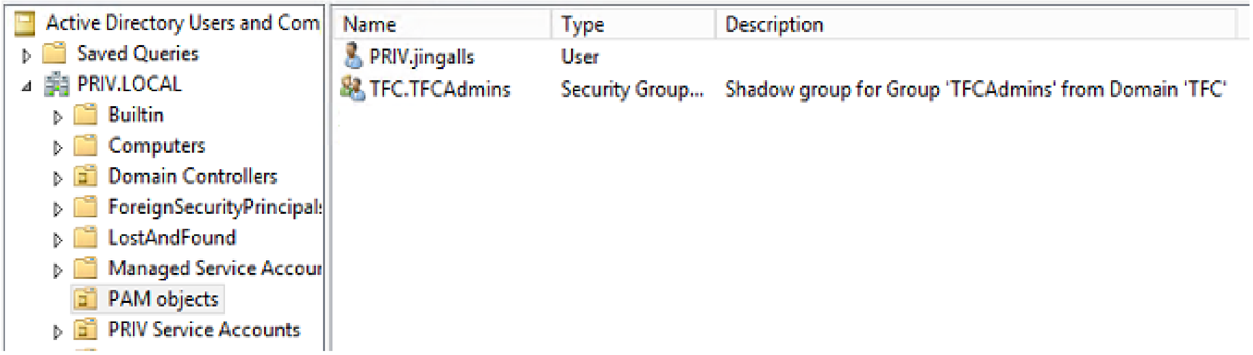
● Delegate the following common tasks:

- ☐ Create, delete, and manage user accounts
- ☐ Reset user passwords and force password change at next logon
- ☑ Read all user information
- ☐ Modify the membership of a group
- ☐ Join a computer to the domain
- ☐ Manage Group Policy links
- ☐ Generate Resultant Set of Policy (Planning)

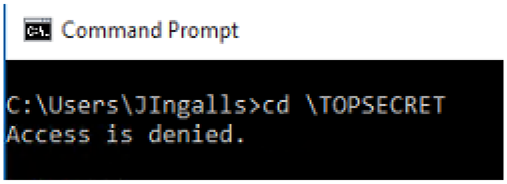
○ Create a custom task to delegate



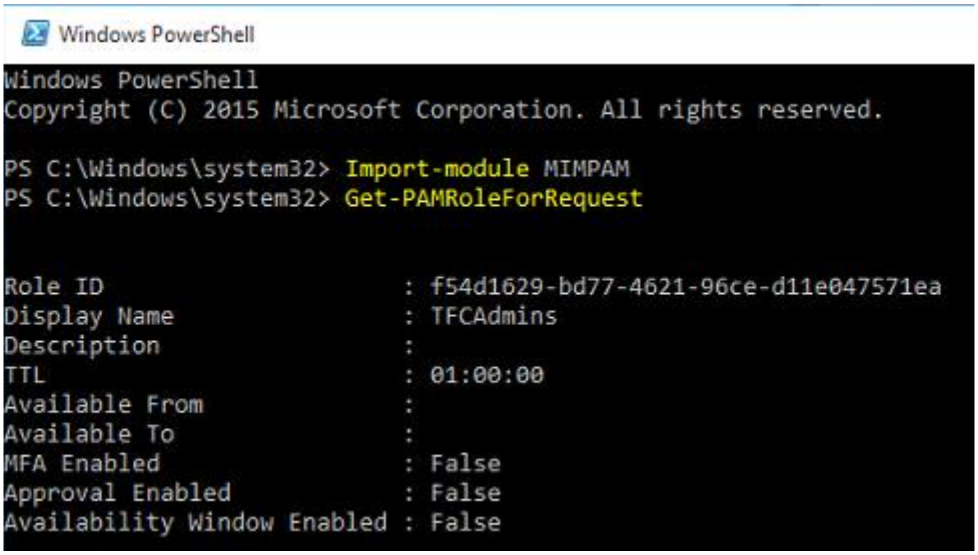
```
PS C:\Users\mimadmin> import-module MIMPAM
PS C:\Users\mimadmin> $ca = get-credential # Any TFC domain admin account works here

cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
PS C:\Users\mimadmin> Test-PAMTrust -SourceForest "thefinancialcompany.net" -Credentials $ca
True
PS C:\Users\mimadmin> Test-PAMDomainConfiguration -SourceDomain "TFC" -Credentials $ca
SID history is enabled for this trust.

The command completed successfully.

SID filtering is not enabled for this trust. All SIDs presented in an
authentication request from this domain will be honored.

The command completed successfully.


The group TFC$$$ exists.
```



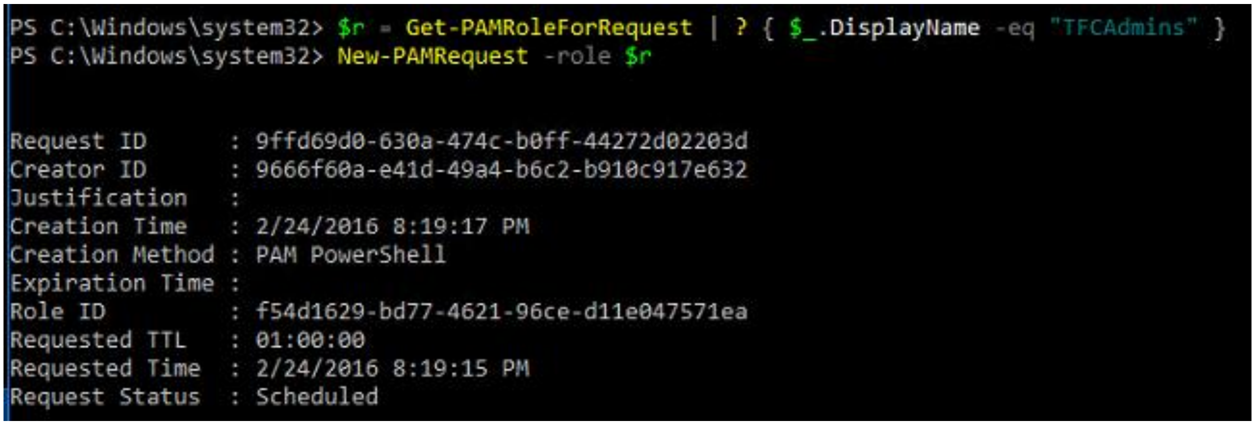
Name	Type	Description
PRIV.jingalls	User	
TFC.TFCAdmins	Security Group...	Shadow group for Group 'TFCAdmins' from Domain 'TFC'



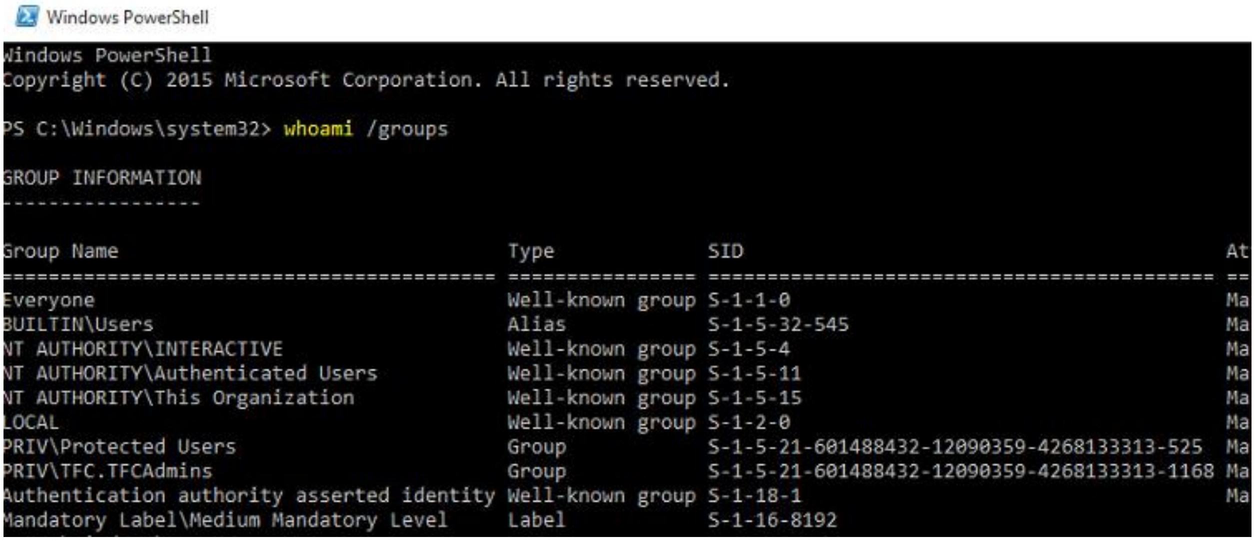
```
C:\Users\JIngalls>cd \TOPSECRET
Access is denied.
```



```
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Import-module MIMPAM
PS C:\Windows\system32> Get-PAMRoleForRequest


Role ID                      : f54d1629-bd77-4621-96ce-d11e047571ea
Display Name                 : TFCAdmins
Description                  :
TTL                          : 01:00:00
Available From               :
Available To                 :
MFA Enabled                  : False
Approval Enabled             : False
Availability Window Enabled  : False
```

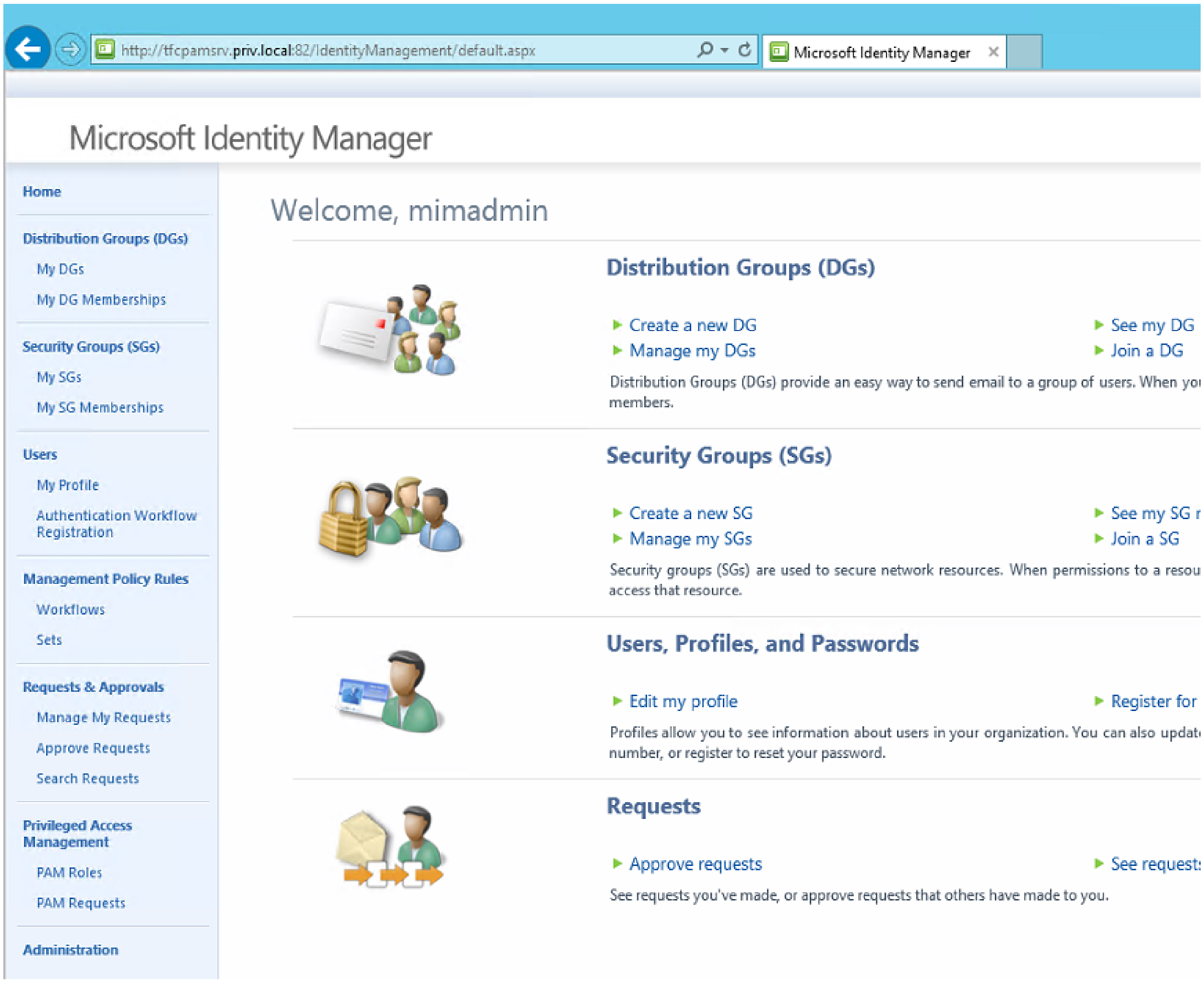


```
PS C:\Windows\system32> $r = Get-PAMRoleForRequest | ? { $_.DisplayName -eq "TFCAdmins" }
PS C:\Windows\system32> New-PAMRequest -role $r


Request ID      : 9ffd69d0-630a-474c-b0ff-44272d02203d
Creator ID      : 9666f60a-e41d-49a4-b6c2-b910c917e632
Justification   :
Creation Time   : 2/24/2016 8:19:17 PM
Creation Method : PAM PowerShell
Expiration Time :
Role ID         : f54d1629-bd77-4621-96ce-d11e047571ea
Requested TTL   : 01:00:00
Requested Time  : 2/24/2016 8:19:15 PM
Request Status  : Scheduled
```



Windows PowerShell

```
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> whoami /groups

GROUP INFORMATION
-----------------

Group Name                                 Type             SID                                            At
========================================== ================ ============================================== ==
Everyone                                   Well-known group S-1-1-0                                        Ma
BUILTIN\Users                              Alias            S-1-5-32-545                                   Ma
NT AUTHORITY\INTERACTIVE                   Well-known group S-1-5-4                                        Ma
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11                                       Ma
NT AUTHORITY\This Organization             Well-known group S-1-5-15                                       Ma
LOCAL                                      Well-known group S-1-2-0                                        Ma
PRIV\Protected Users                       Group            S-1-5-21-601488432-12090359-4268133313-525     Ma
PRIV\TFC.TFCAdmins                         Group            S-1-5-21-601488432-12090359-4268133313-1168    Ma
Authentication authority asserted identity Well-known group S-1-18-1                                       Ma
Mandatory Label\Medium Mandatory Level     Label            S-1-16-8192
```



http://tfcpamsrv.priv.local:82/IdentityManagement/default.aspx

Microsoft Identity Manager

Welcome, mimadmin

Distribution Groups (DGs)

Distribution Groups (DGs) provide an easy way to send email to a group of users. When yo members.

Security Groups (SGs)

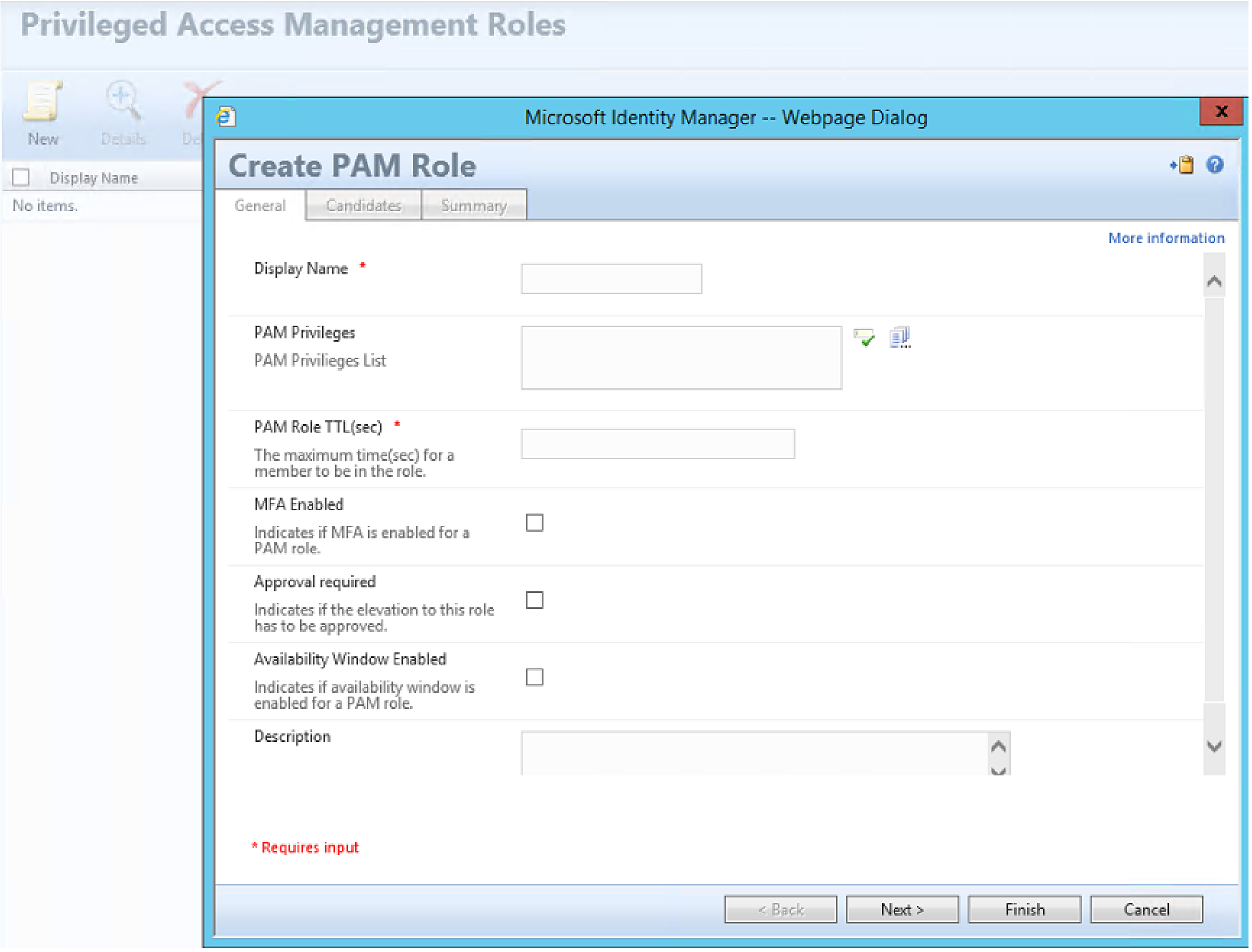
Security groups (SGs) are used to secure network resources. When permissions to a resou access that resource.

Users, Profiles, and Passwords

Profiles allow you to see information about users in your organization. You can also updat number, or register to reset your password.

Requests

See requests you've made, or approve requests that others have made to you.



Create PAM Role

Display Name *

PAM Privileges
PAM Privilieges List

PAM Role TTL(sec) *
The maximum time(sec) for a member to be in the role.

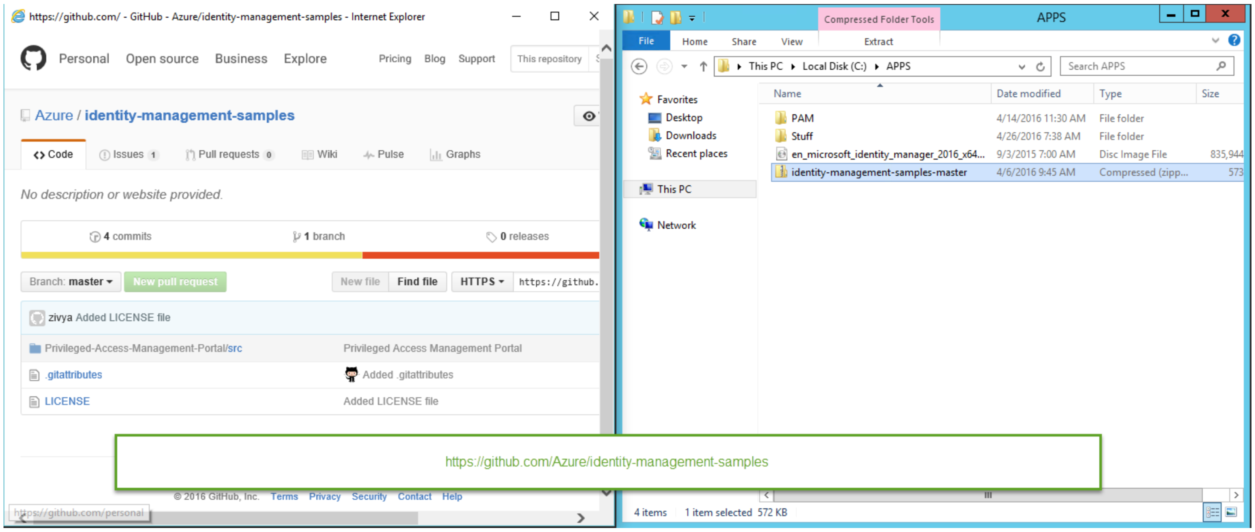
MFA Enabled □
Indicates if MFA is enabled for a PAM role.

Approval required □
Indicates if the elevation to this role has to be approved.

Availability Window Enabled □
Indicates if availability window is enabled for a PAM role.

Description

* Requires input



Azure / identity-management-samples

No description or website provided.

4 commits 1 branch 0 releases

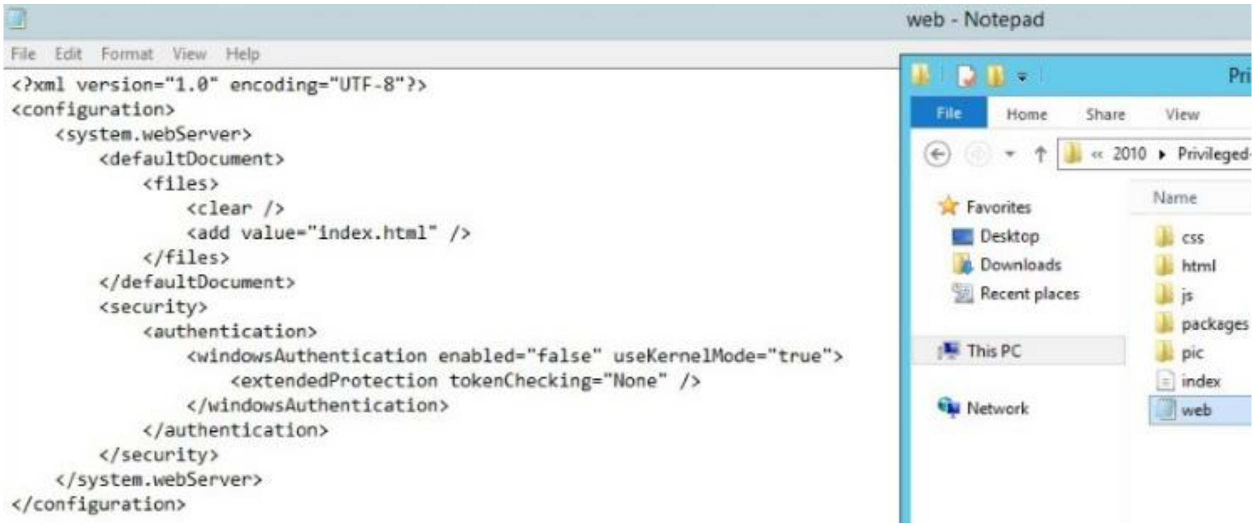
zivya Added LICENSE file

Privileged-Access-Management-Portal/src	Privileged Access Management Portal
.gitattributes	Added .gitattributes
LICENSE	Added LICENSE file

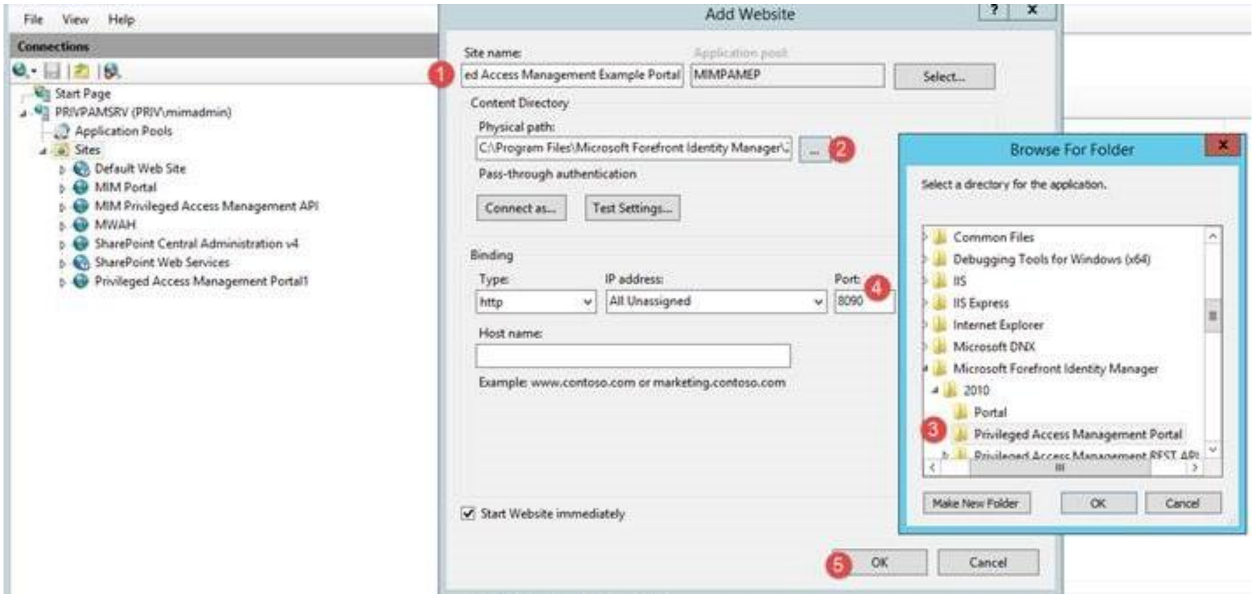
Name	Date modified	Type	Size
PAM	4/14/2016 11:30 AM	File folder	
Stuff	4/26/2016 7:38 AM	File folder	
en_microsoft_identity_manager_2016_x64...	9/3/2015 7:00 AM	Disc Image File	835,944
identity-management-samples-master	4/6/2016 9:45 AM	Compressed (zipp...	573

4 items 1 item selected 572 KB

https://github.com/Azure/identity-management-samples



```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <system.webServer>
        <defaultDocument>
            <files>
                <clear />
                <add value="index.html" />
            </files>
        </defaultDocument>
        <security>
            <authentication>
                <windowsAuthentication enabled="false" useKernelMode="true">
                    <extendedProtection tokenChecking="None" />
                </windowsAuthentication>
            </authentication>
        </security>
    </system.webServer>
</configuration>
```


File View Help
Connections
Start Page
PRIVPAMSRV (PRIV\mimadmin)
Application Pools
Sites
Default Web Site
MIM Portal
MIM Privileged Access Management API
MWAH
SharePoint Central Administration v4
SharePoint Web Services
Privileged Access Management Portal1
Add Website
Select...
Connect as...
Test Settings...
Browse For Folder
Select a directory for the application.
Common Files
Debugging Tools for Windows (x64)
IIS
IIS Express
Internet Explorer
Microsoft DNX
Microsoft Forefront Identity Manager
2010
Portal
Privileged Access Management Portal
Privileged Access Management REST API
Make New Folder
OK
Cancel
OK
Cancel

1 Site name: ed Access Management Example Portal

Application pool: MIMPAMEP

Content Directory

2 Physical path: C:\Program Files\Microsoft Forefront Identity Manager\...

Pass-through authentication

3 Privileged Access Management Portal

Binding

Type: http

IP address: All Unassigned

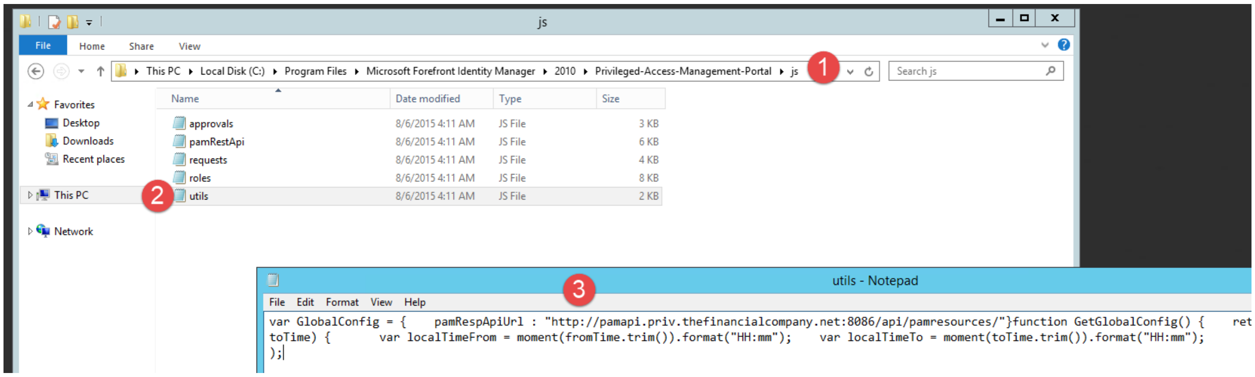
4 Port: 8090

Host name:

Example: www.contoso.com or marketing.contoso.com

☑ Start Website immediately

5 OK

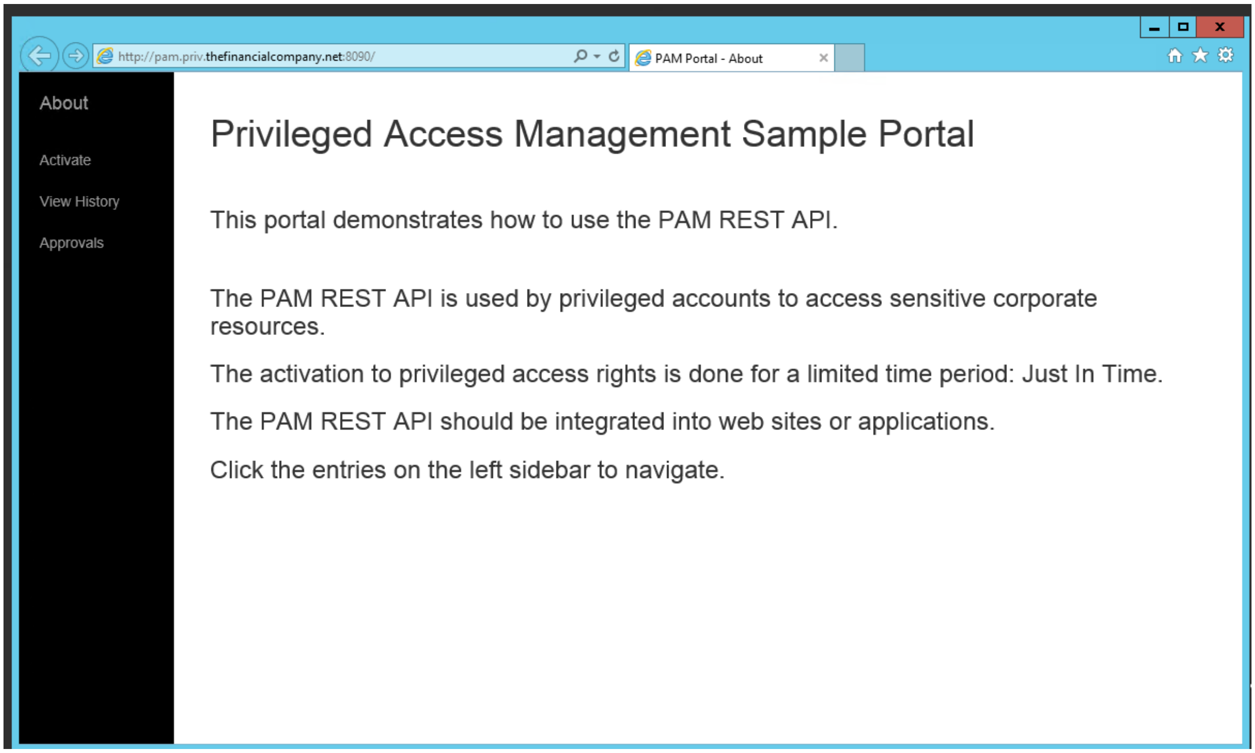


1 This PC ▸ Local Disk (C:) ▸ Program Files ▸ Microsoft Forefront Identity Manager ▸ 2010 ▸ Privileged-Access-Management-Portal ▸ js

Name	Date modified	Type	Size
approvals	8/6/2015 4:11 AM	JS File	3 KB
pamRestApi	8/6/2015 4:11 AM	JS File	6 KB
requests	8/6/2015 4:11 AM	JS File	4 KB
roles	8/6/2015 4:11 AM	JS File	8 KB
2 utils	8/6/2015 4:11 AM	JS File	2 KB

3 utils - Notepad

```
var GlobalConfig = {    pamRespApiUrl : "http://pamapi.priv.thefinancialcompany.net:8086/api/pamresources/"}function GetGlobalConfig() {    ret
toTime) {       var localTimeFrom = moment(fromTime.trim()).format("HH:mm");    var localTimeTo = moment(toTime.trim()).format("HH:mm");
);
```



Privileged Access Management Sample Portal

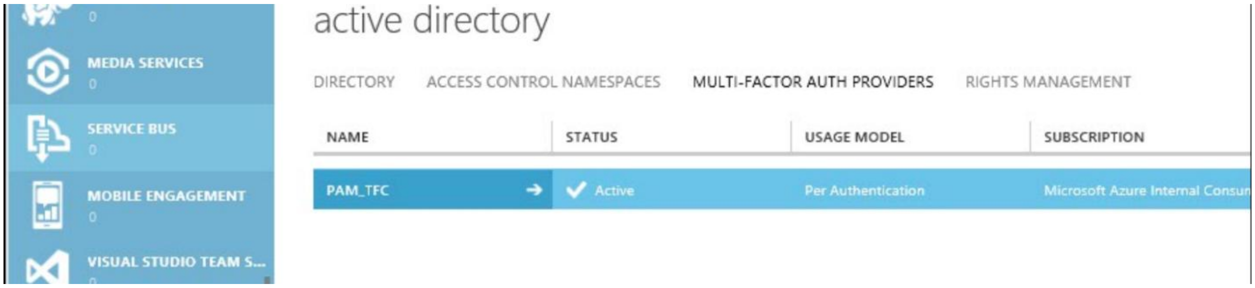
This portal demonstrates how to use the PAM REST API.

The PAM REST API is used by privileged accounts to access sensitive corporate resources.

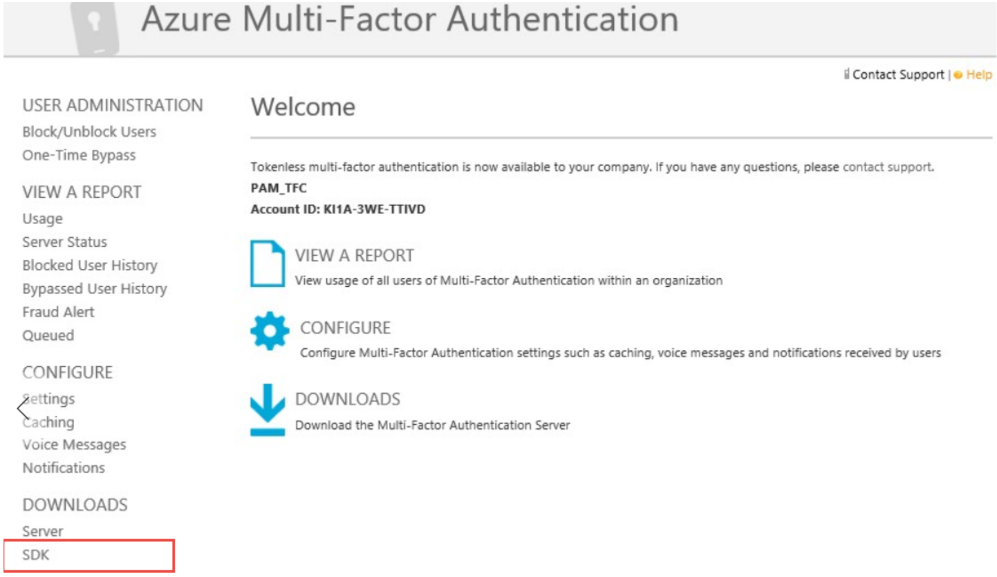
The activation to privileged access rights is done for a limited time period: Just In Time.

The PAM REST API should be integrated into web sites or applications.

Click the entries on the left sidebar to navigate.



NAME	STATUS	USAGE MODEL	SUBSCRIPTION
PAM_TFC	✓ Active	Per Authentication	Microsoft Azure Internal Consun



Welcome

Tokenless multi-factor authentication is now available to your company. If you have any questions, please contact support.

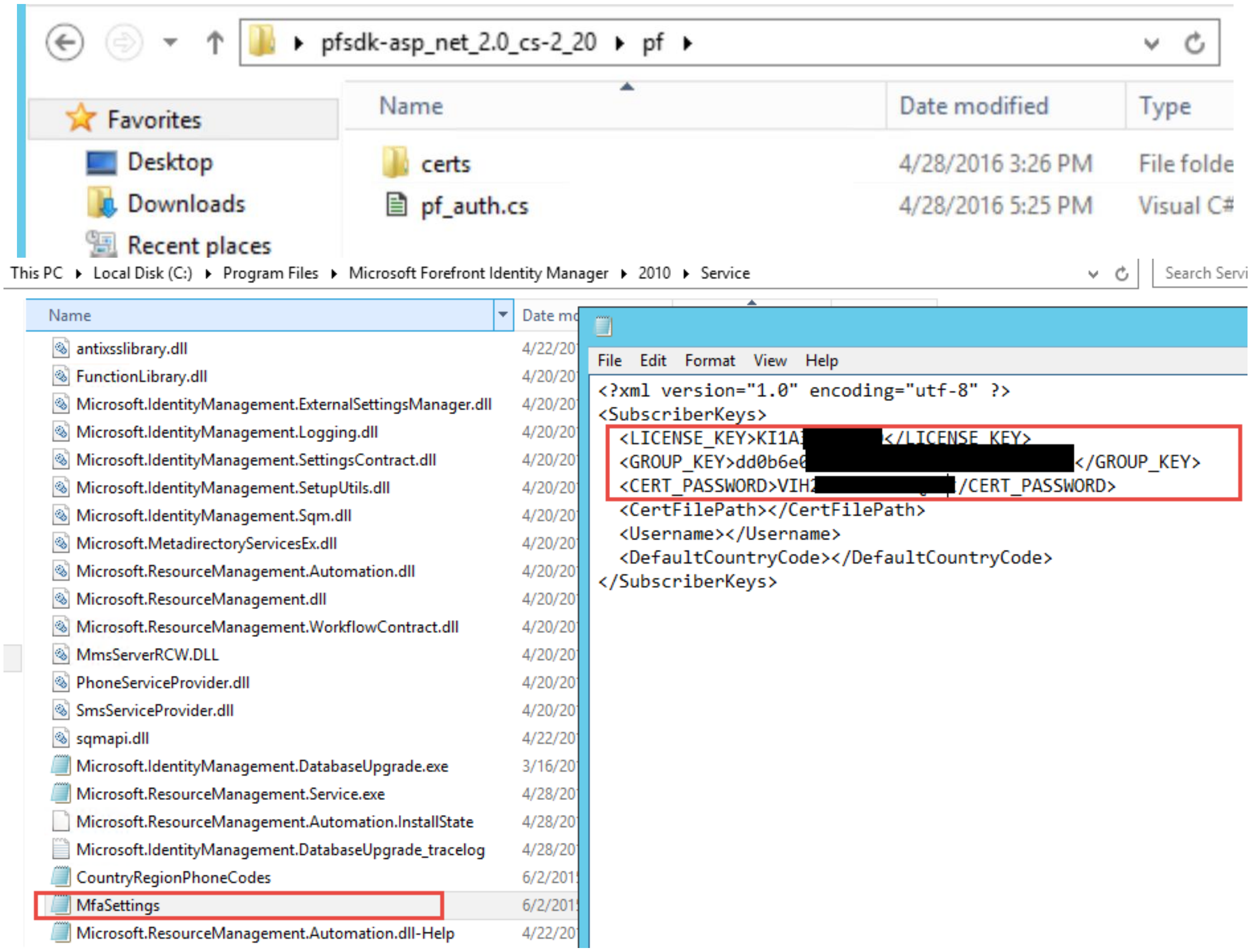
PAM_TFC

Account ID: KI1A-3WE-TTIVD

VIEW A REPORT
View usage of all users of Multi-Factor Authentication within an organization

CONFIGURE
Configure Multi-Factor Authentication settings such as caching, voice messages and notifications received by users

DOWNLOADS
Download the Multi-Factor Authentication Server



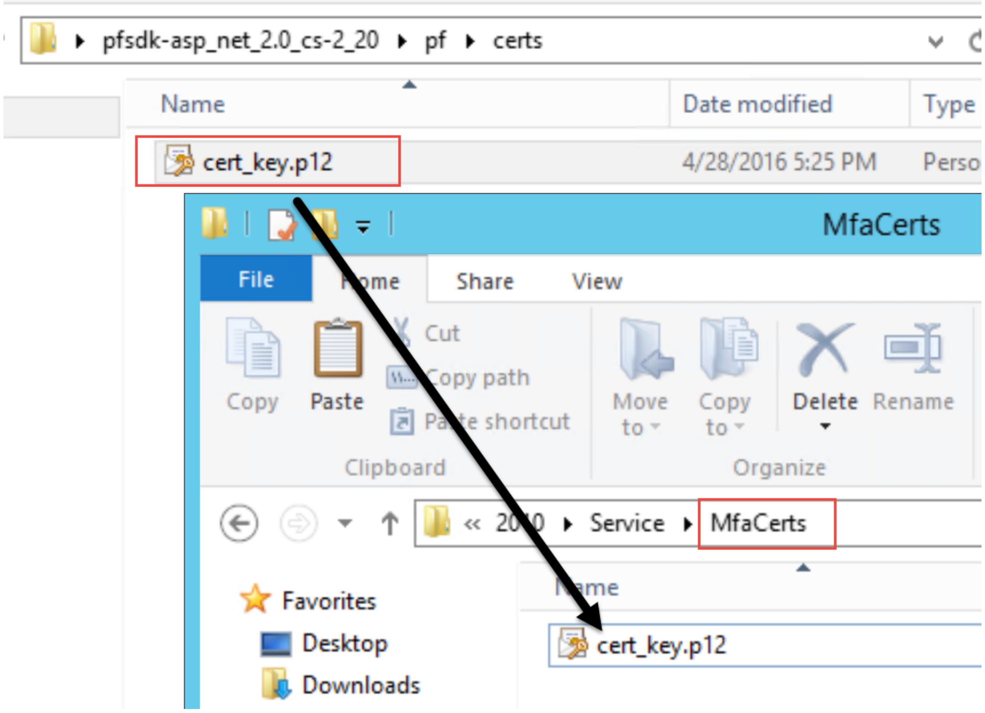
pfsdk-asp_net_2.0_cs-2_20 ▸ pf ▸

Name	Date modified	Type
certs	4/28/2016 3:26 PM	File folde
pf_auth.cs	4/28/2016 5:25 PM	Visual C#

This PC ▸ Local Disk (C:) ▸ Program Files ▸ Microsoft Forefront Identity Manager ▸ 2010 ▸ Service

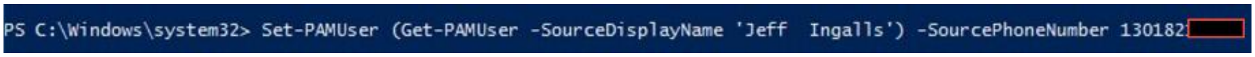
Name	Date mo
antixsslibrary.dll	4/22/20
FunctionLibrary.dll	4/20/20
Microsoft.IdentityManagement.ExternalSettingsManager.dll	4/20/20
Microsoft.IdentityManagement.Logging.dll	4/20/20
Microsoft.IdentityManagement.SettingsContract.dll	4/20/20
Microsoft.IdentityManagement.SetupUtils.dll	4/20/20
Microsoft.IdentityManagement.Sqm.dll	4/20/20
Microsoft.MetadirectoryServicesEx.dll	4/20/20
Microsoft.ResourceManagement.Automation.dll	4/20/20
Microsoft.ResourceManagement.dll	4/20/20
Microsoft.ResourceManagement.WorkflowContract.dll	4/20/20
MmsServerRCW.DLL	4/20/20
PhoneServiceProvider.dll	4/20/20
SmsServiceProvider.dll	4/20/20
sqmapi.dll	4/22/20
Microsoft.IdentityManagement.DatabaseUpgrade.exe	3/16/20
Microsoft.ResourceManagement.Service.exe	4/28/20
Microsoft.ResourceManagement.Automation.InstallState	4/28/20
Microsoft.IdentityManagement.DatabaseUpgrade_tracelog	4/28/20
CountryRegionPhoneCodes	6/2/201
MfaSettings	6/2/201
Microsoft.ResourceManagement.Automation.dll-Help	4/22/20

```
<?xml version="1.0" encoding="utf-8" ?>
<SubscriberKeys>
  <LICENSE_KEY>KI1A[redacted]</LICENSE_KEY>
  <GROUP_KEY>dd0b6e[redacted]</GROUP_KEY>
  <CERT_PASSWORD>VIH[redacted]/CERT_PASSWORD>
  <CertFilePath></CertFilePath>
  <Username></Username>
  <DefaultCountryCode></DefaultCountryCode>
</SubscriberKeys>
```

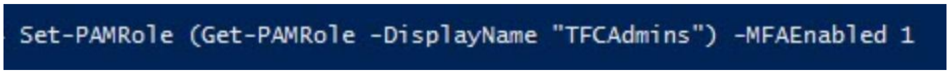


pfsdk-asp_net_2.0_cs-2_20 ▸ pf ▸ certs

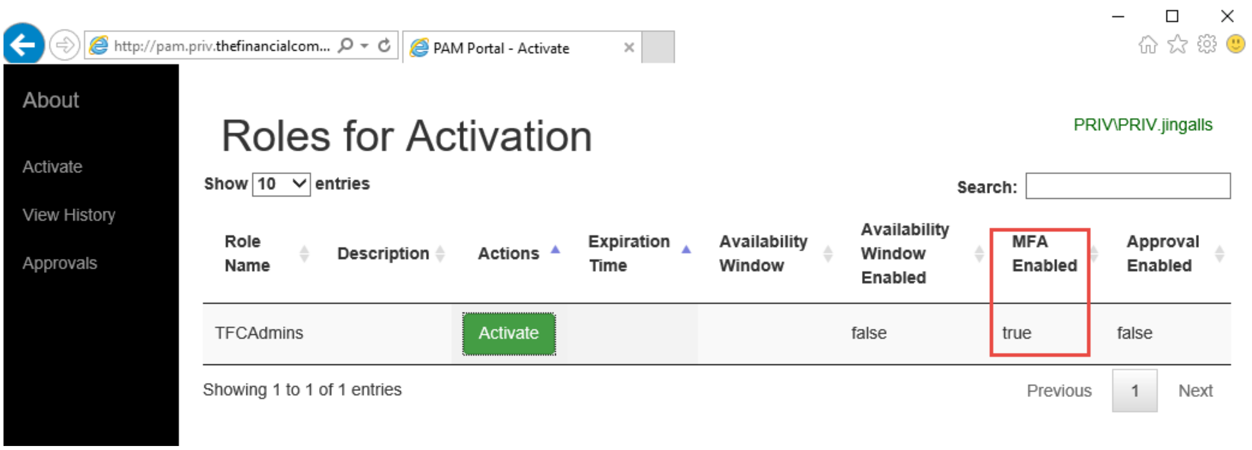
Name	Date modified	Type
cert_key.p12	4/28/2016 5:25 PM	Perso



```
PS C:\Windows\system32> Set-PAMUser (Get-PAMUser -SourceDisplayName 'Jeff  Ingalls') -SourcePhoneNumber 130182[redacted]
```



```
Set-PAMRole (Get-PAMRole -DisplayName "TFCAdmins") -MFAEnabled 1
```



Roles for Activation

PRIV\PRIV.jingalls

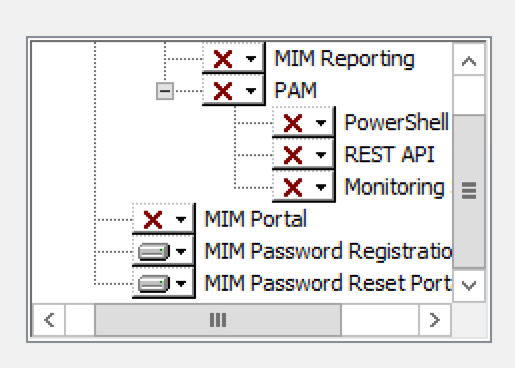
Show 10 entries

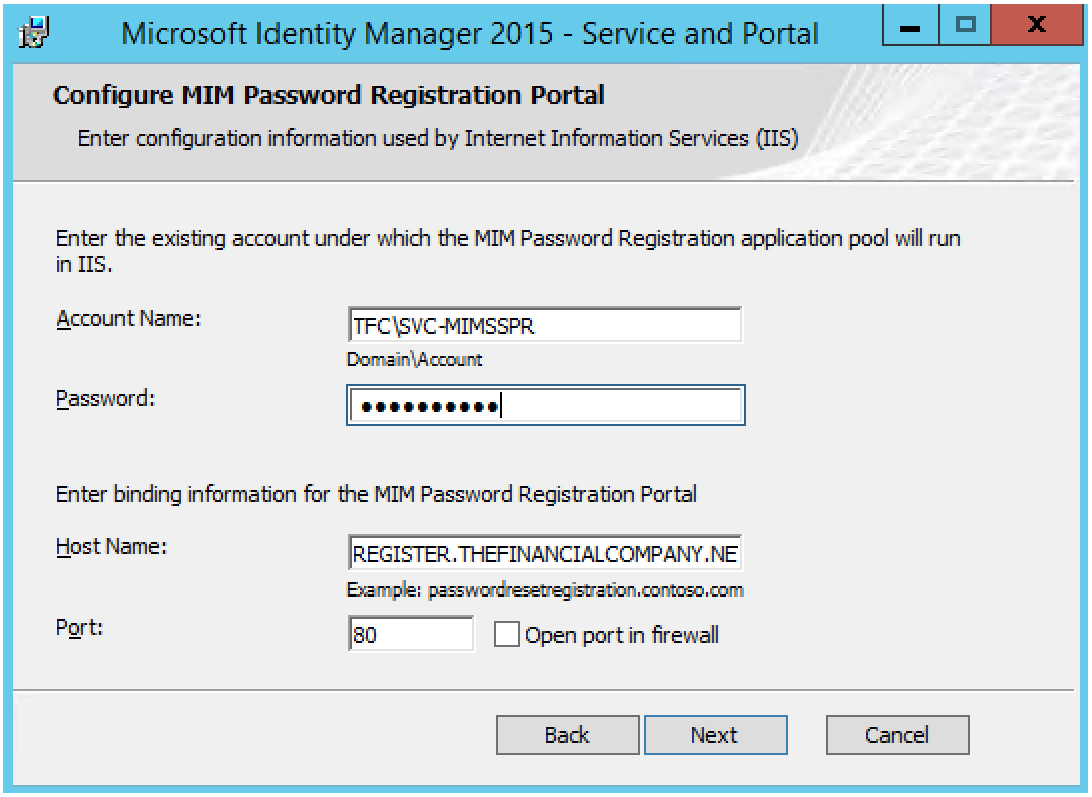
Search:

Role Name	Description	Actions	Expiration Time	Availability Window	Availability Window Enabled	MFA Enabled	Approval Enabled
TFCAdmins		Activate			false	true	false

Showing 1 to 1 of 1 entries

Previous 1 Next





Microsoft Identity Manager 2015 - Service and Portal

Configure MIM Password Registration Portal

Enter configuration information used by Internet Information Services (IIS)

Enter the existing account under which the MIM Password Registration application pool will run in IIS.

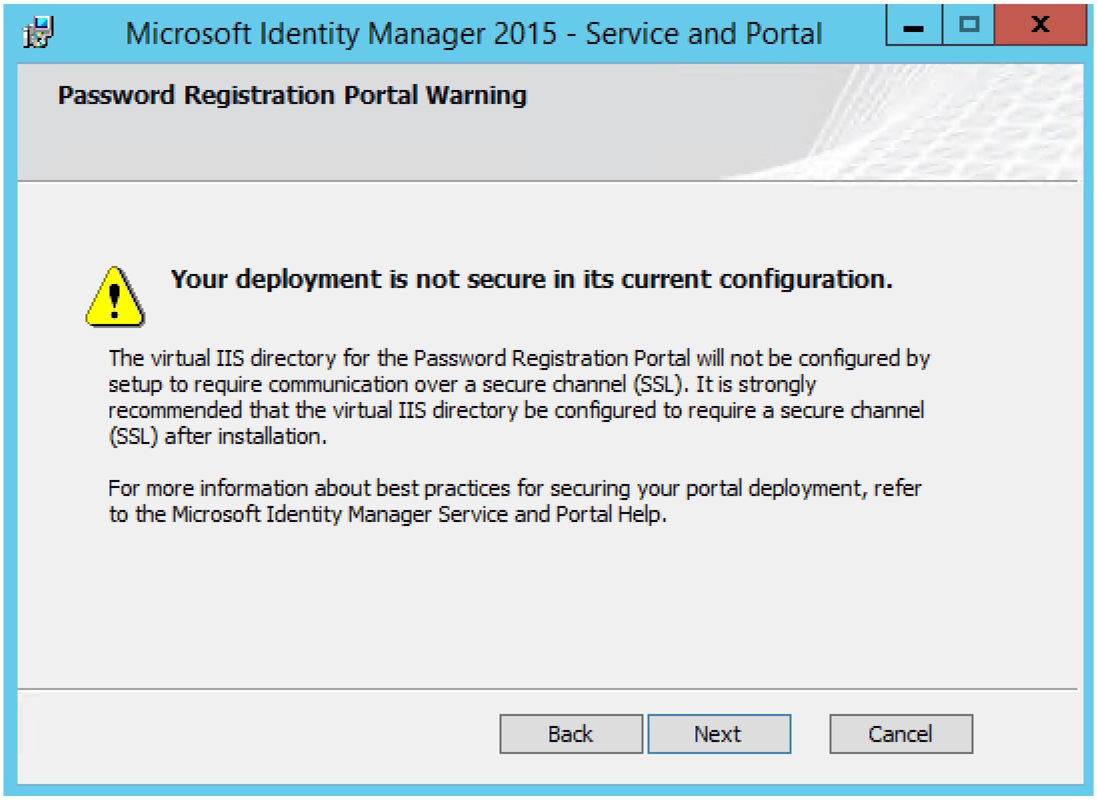
Account Name: TFC\SVC-MIMSSPR
Domain\Account

Password: ●●●●●●●●●●

Enter binding information for the MIM Password Registration Portal

Host Name: REGISTER.THEFINANCIALCOMPANY.NE
Example: passwordresetregistration.contoso.com

Port: 80 □ Open port in firewall

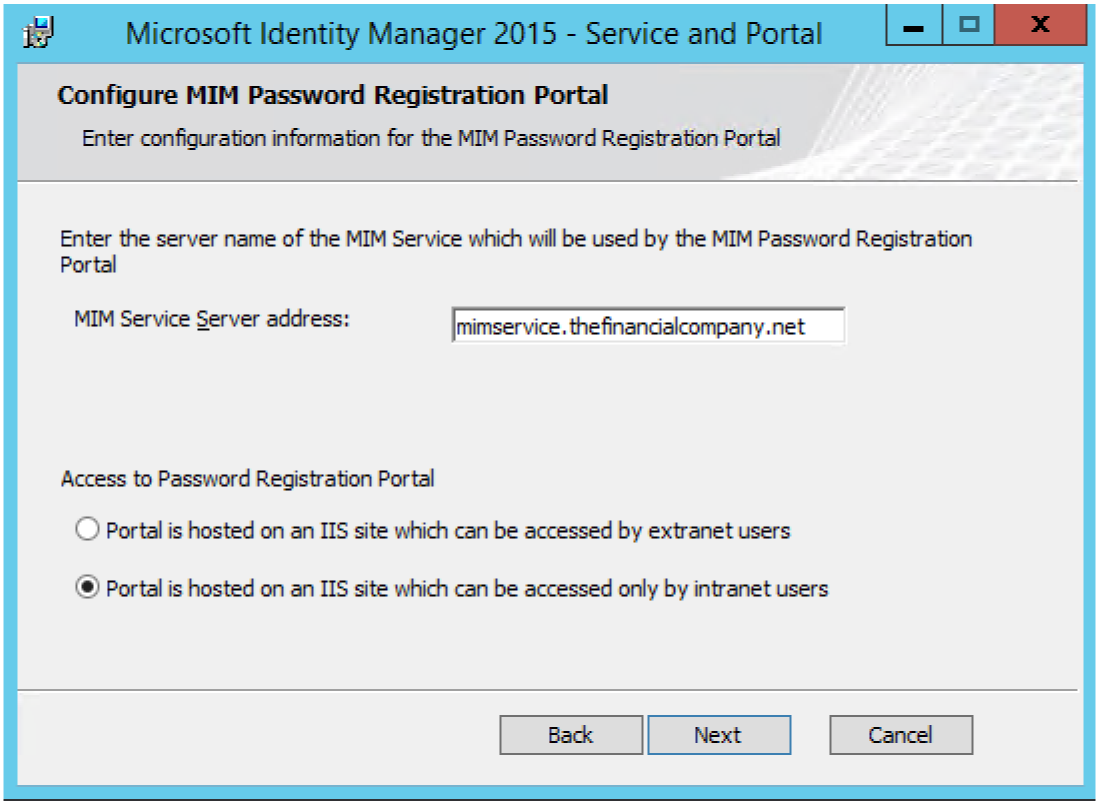


Password Registration Portal Warning

Your deployment is not secure in its current configuration.

The virtual IIS directory for the Password Registration Portal will not be configured by setup to require communication over a secure channel (SSL). It is strongly recommended that the virtual IIS directory be configured to require a secure channel (SSL) after installation.

For more information about best practices for securing your portal deployment, refer to the Microsoft Identity Manager Service and Portal Help.



Configure MIM Password Registration Portal

Enter configuration information for the MIM Password Registration Portal

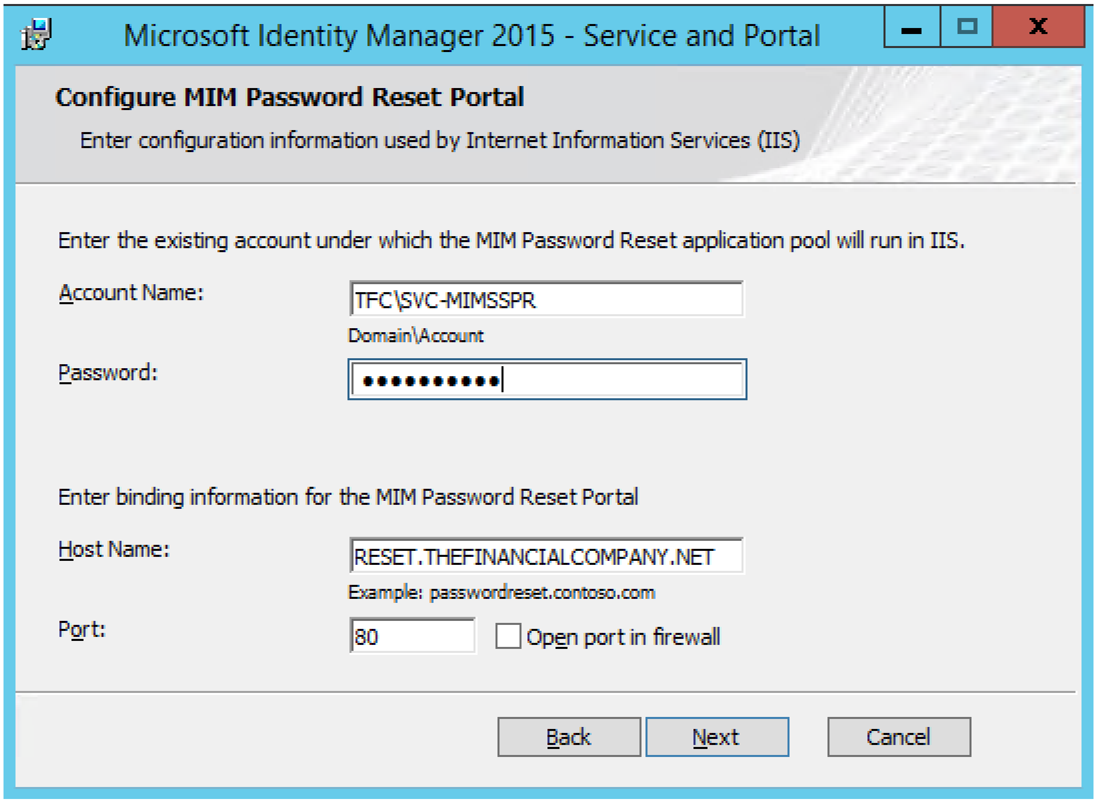
Enter the server name of the MIM Service which will be used by the MIM Password Registration Portal

MIM Service Server address: mimservice.thefinancialcompany.net

Access to Password Registration Portal

○ Portal is hosted on an IIS site which can be accessed by extranet users

● Portal is hosted on an IIS site which can be accessed only by intranet users



Microsoft Identity Manager 2015 - Service and Portal

Configure MIM Password Reset Portal

Enter configuration information used by Internet Information Services (IIS)

Enter the existing account under which the MIM Password Reset application pool will run in IIS.

Account Name: TFC\SVC-MIMSSPR

Domain\Account

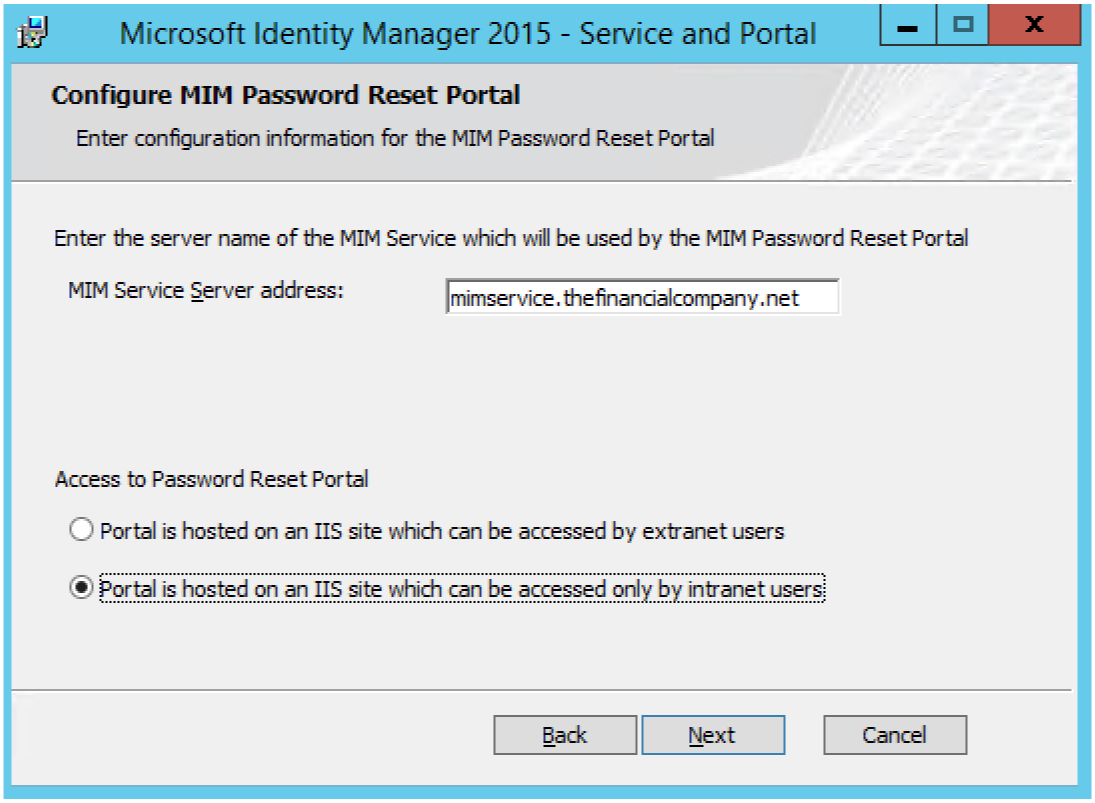
Password: ●●●●●●●●●●●

Enter binding information for the MIM Password Reset Portal

Host Name: RESET.THEFINANCIALCOMPANY.NET

Example: passwordreset.contoso.com

Port: 80 □ Open port in firewall



Microsoft Identity Manager 2015 - Service and Portal

Configure MIM Password Reset Portal

Enter configuration information for the MIM Password Reset Portal

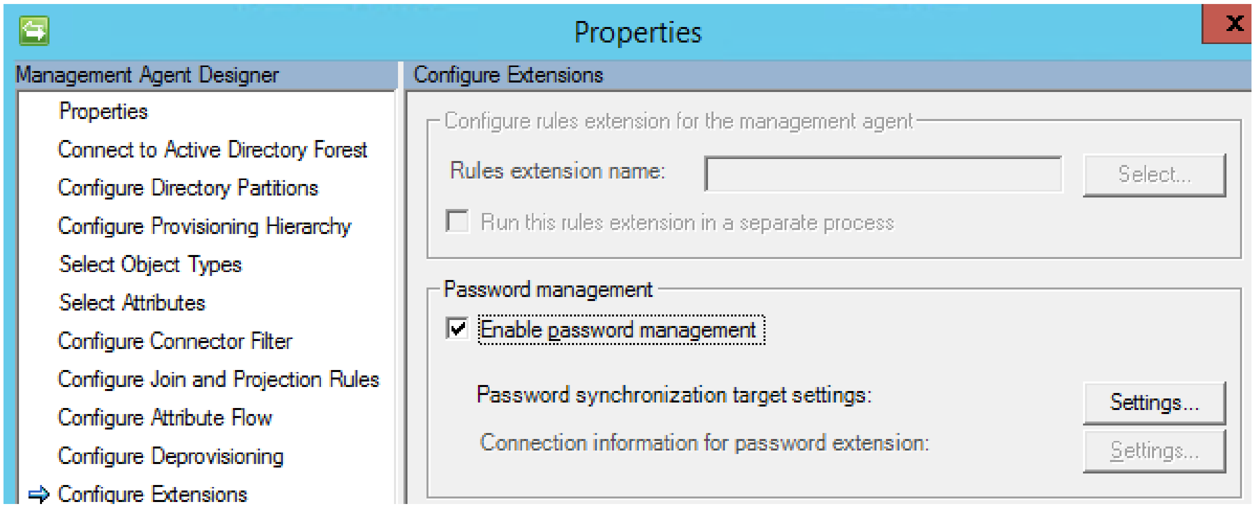
Enter the server name of the MIM Service which will be used by the MIM Password Reset Portal

MIM Service Server address: mimservice.thefinancialcompany.net

Access to Password Reset Portal

○ Portal is hosted on an IIS site which can be accessed by extranet users

● Portal is hosted on an IIS site which can be accessed only by intranet users


Properties
Management Agent Designer
Properties
Connect to Active Directory Forest
Configure Directory Partitions
Configure Provisioning Hierarchy
Select Object Types
Select Attributes
Configure Connector Filter
Configure Join and Projection Rules
Configure Attribute Flow
Configure Deprovisioning
Configure Extensions
Select...
Settings...
Settings...

Configure Extensions

Configure rules extension for the management agent

Rules extension name:

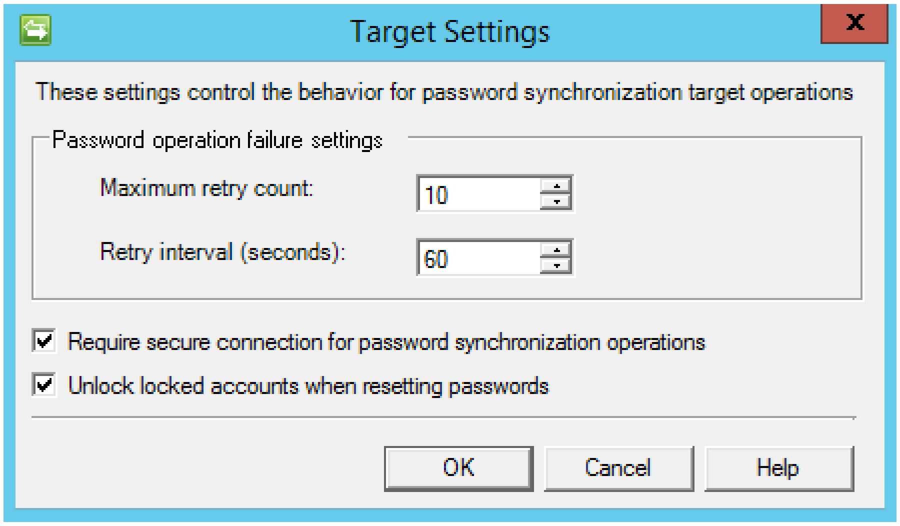
□ Run this rules extension in a separate process

Password management

☑ Enable password management

Password synchronization target settings:

Connection information for password extension:



These settings control the behavior for password synchronization target operations

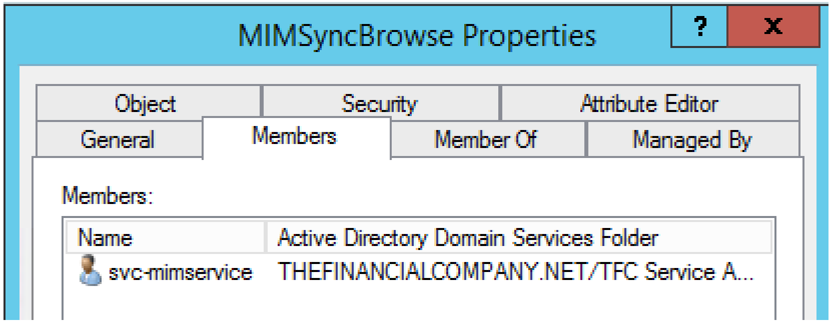
Password operation failure settings

Maximum retry count: 10

Retry interval (seconds): 60

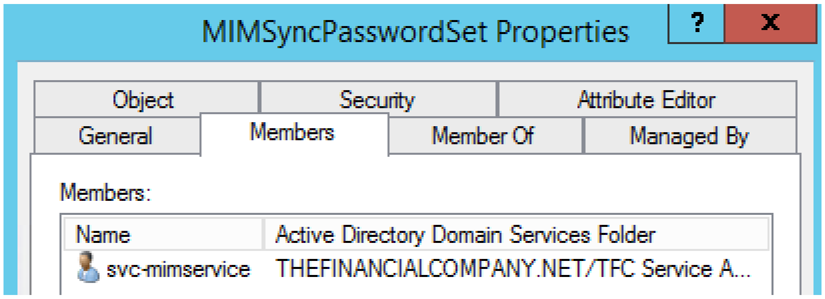
☑ Require secure connection for password synchronization operations

☑ Unlock locked accounts when resetting passwords



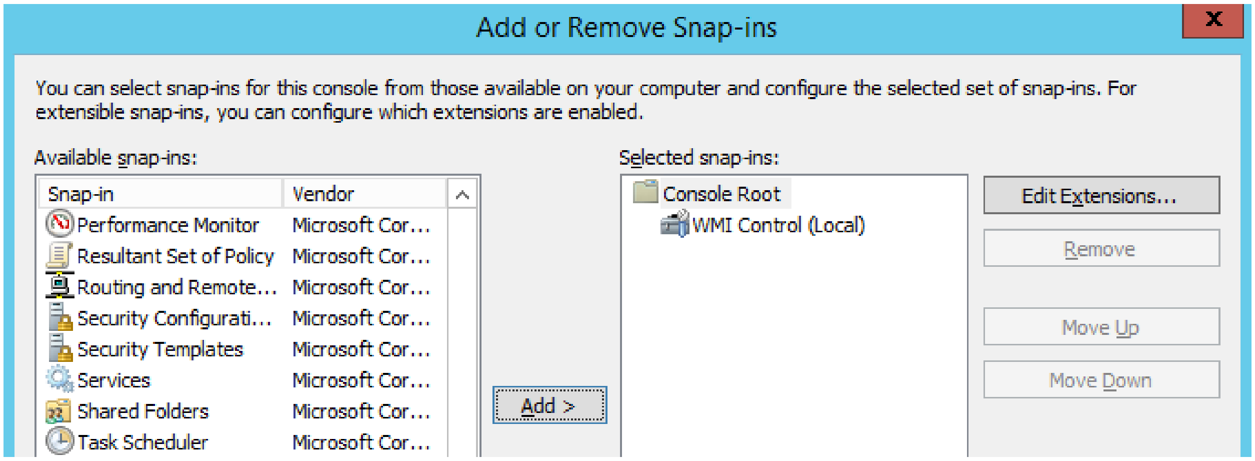
Members:

Name	Active Directory Domain Services Folder
svc-mimservice	THEFINANCIALCOMPANY.NET/TFC Service A...



Members:

Name	Active Directory Domain Services Folder
svc-mimservice	THEFINANCIALCOMPANY.NET/TFC Service A...


Add or Remove Snap-ins

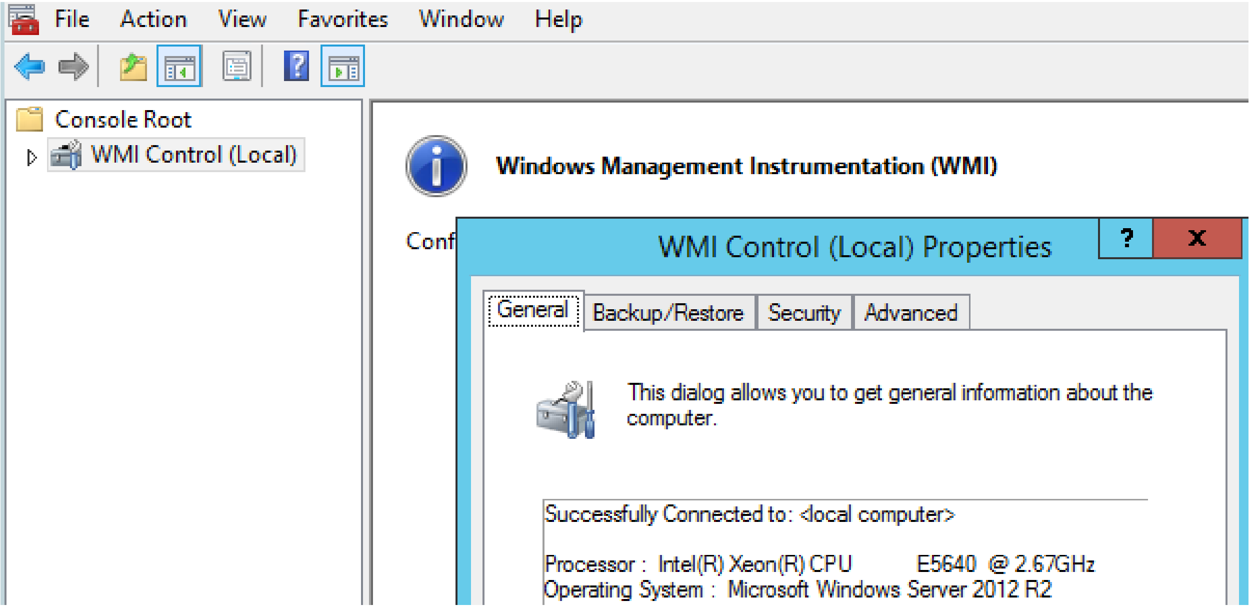
You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
Performance Monitor	Microsoft Cor...
Resultant Set of Policy	Microsoft Cor...
Routing and Remote...	Microsoft Cor...
Security Configurati...	Microsoft Cor...
Security Templates	Microsoft Cor...
Services	Microsoft Cor...
Shared Folders	Microsoft Cor...
Task Scheduler	Microsoft Cor...

Selected snap-ins:

- Console Root
  - WMI Control (Local)



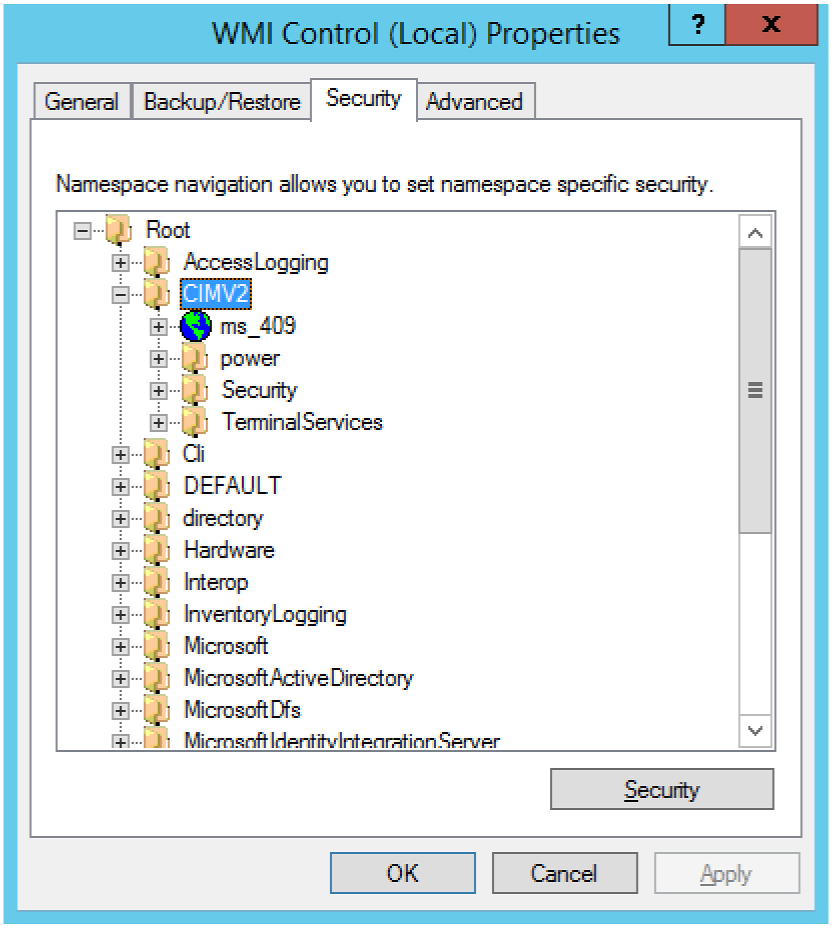
Windows Management Instrumentation (WMI)

WMI Control (Local) Properties

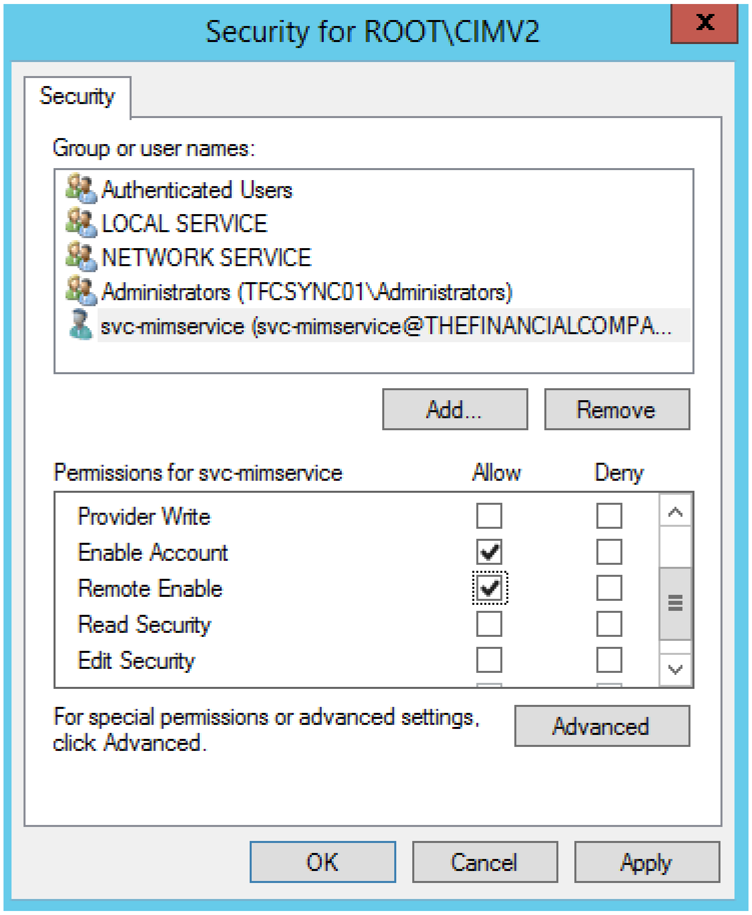
This dialog allows you to get general information about the computer.

Successfully Connected to: <local computer>

Processor : Intel(R) Xeon(R) CPU E5640 @ 2.67GHz
Operating System : Microsoft Windows Server 2012 R2



Namespace navigation allows you to set namespace specific security.



Security for ROOT\CIMV2

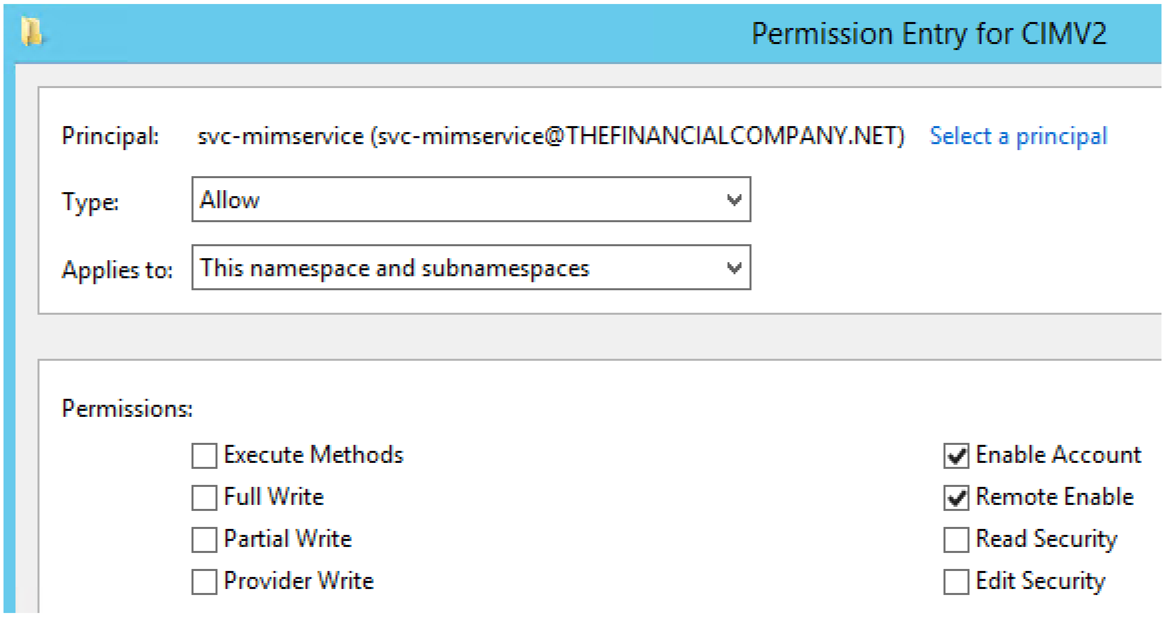
Security

Group or user names:

- Authenticated Users
- LOCAL SERVICE
- NETWORK SERVICE
- Administrators (TFCSYNC01\Administrators)
- svc-mimservice (svc-mimservice@THEFINANCIALCOMPA...

Permissions for svc-mimservice	Allow	Deny
Provider Write	□	□
Enable Account	☑	□
Remote Enable	☑	□
Read Security	□	□
Edit Security	□	□

For special permissions or advanced settings, click Advanced.



Permission Entry for CIMV2

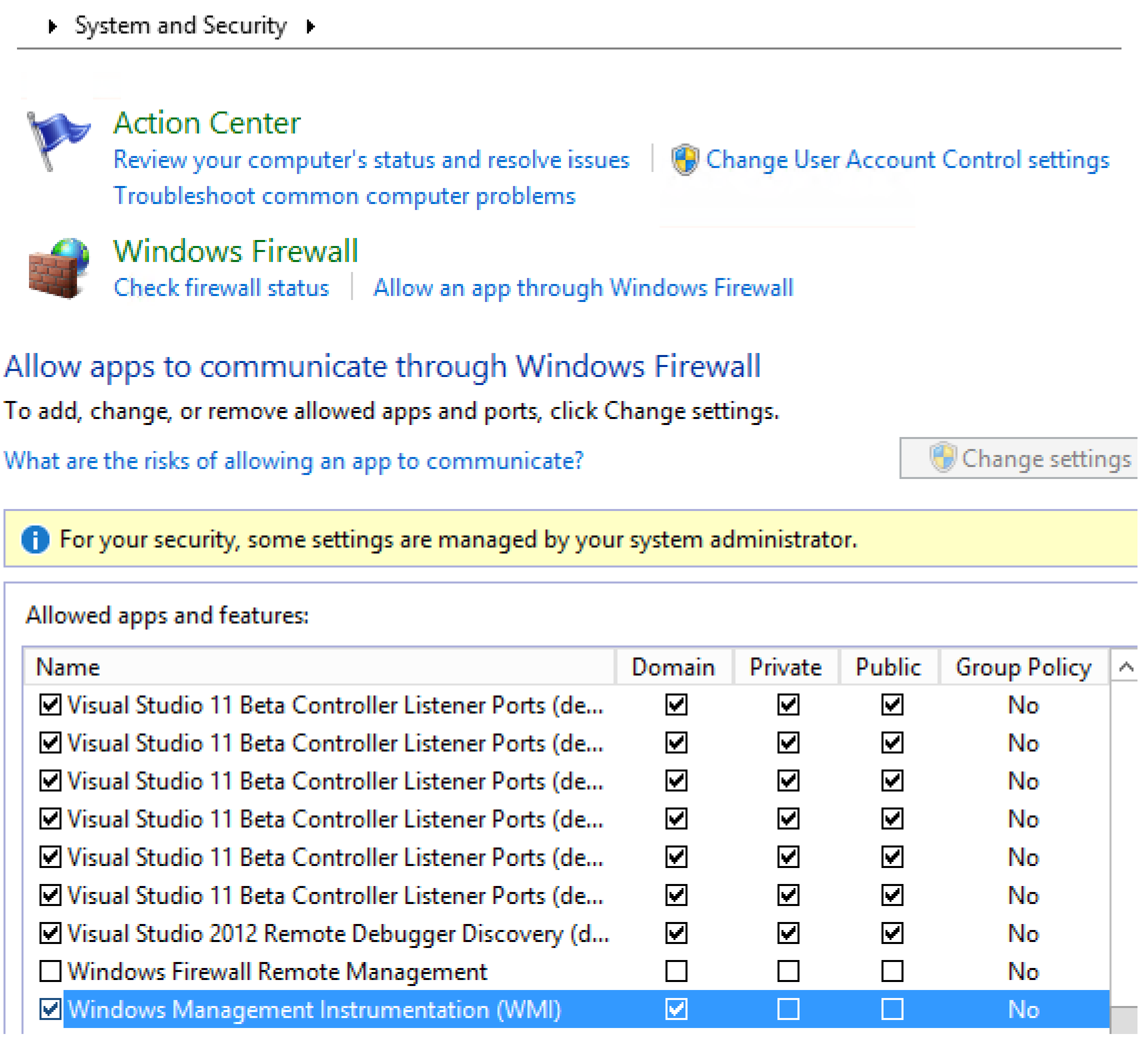
Principal: svc-mimservice (svc-mimservice@THEFINANCIALCOMPANY.NET)

Type: Allow

Applies to: This namespace and subnamespaces

Permissions:

□ Execute Methods	☑ Enable Account
□ Full Write	☑ Remote Enable
□ Partial Write	□ Read Security
□ Provider Write	□ Edit Security



Review your computer's status and resolve issues | Change User Account Control settings

Troubleshoot common computer problems

Check firewall status | Allow an app through Windows Firewall

Allow apps to communicate through Windows Firewall

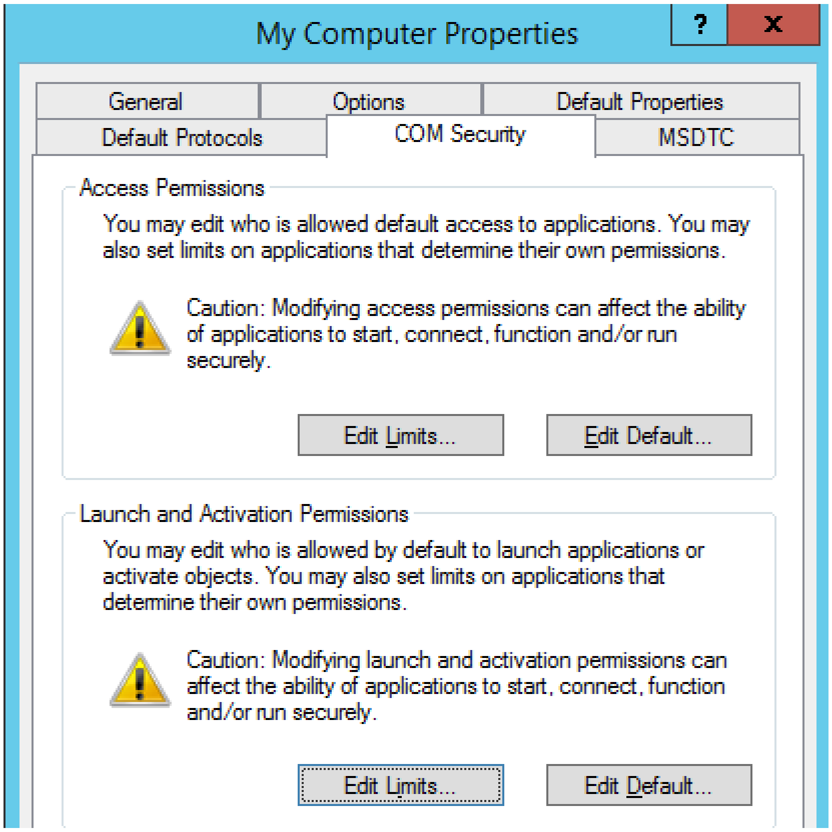
To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

For your security, some settings are managed by your system administrator.

Allowed apps and features:

Name	Domain	Private	Public	Group Policy
☑ Visual Studio 11 Beta Controller Listener Ports (de...	☑	☑	☑	No
☑ Visual Studio 11 Beta Controller Listener Ports (de...	☑	☑	☑	No
☑ Visual Studio 11 Beta Controller Listener Ports (de...	☑	☑	☑	No
☑ Visual Studio 11 Beta Controller Listener Ports (de...	☑	☑	☑	No
☑ Visual Studio 11 Beta Controller Listener Ports (de...	☑	☑	☑	No
☑ Visual Studio 11 Beta Controller Listener Ports (de...	☑	☑	☑	No
☑ Visual Studio 2012 Remote Debugger Discovery (d...	☑	☑	☑	No
□ Windows Firewall Remote Management	□	□	□	No
☑ Windows Management Instrumentation (WMI)	☑	□	□	No



Access Permissions

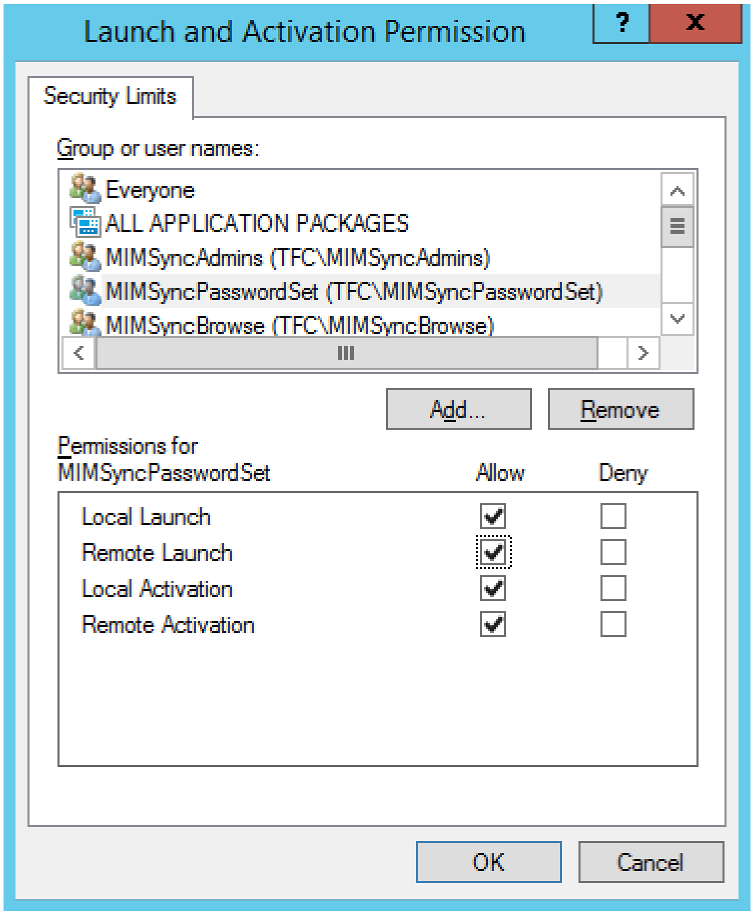
You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions.

Caution: Modifying access permissions can affect the ability of applications to start, connect, function and/or run securely.

Launch and Activation Permissions

You may edit who is allowed by default to launch applications or activate objects. You may also set limits on applications that determine their own permissions.

Caution: Modifying launch and activation permissions can affect the ability of applications to start, connect, function and/or run securely.



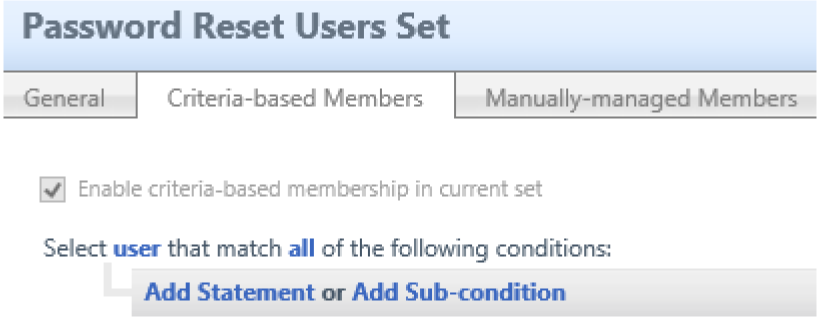
Launch and Activation Permission

Security Limits

Group or user names:

- Everyone
- ALL APPLICATION PACKAGES
- MIMSyncAdmins (TFC\MIMSyncAdmins)
- MIMSyncPasswordSet (TFC\MIMSyncPasswordSet)
- MIMSyncBrowse (TFC\MIMSyncBrowse)

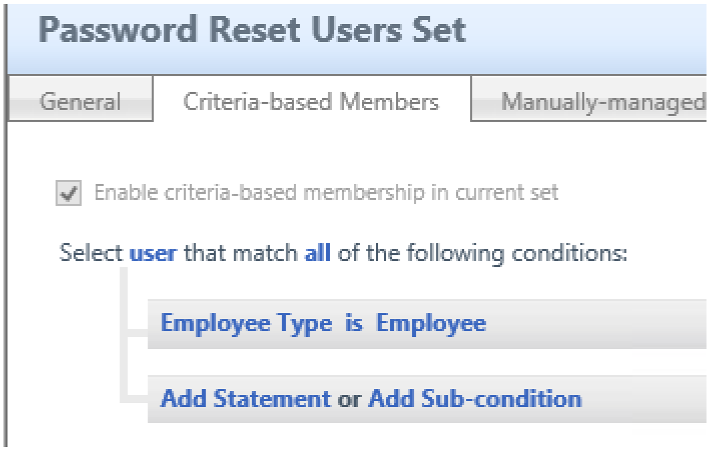
Permissions for MIMSyncPasswordSet	Allow	Deny
Local Launch	☑	□
Remote Launch	☑	□
Local Activation	☑	□
Remote Activation	☑	□



Password Reset Users Set

☑ Enable criteria-based membership in current set

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



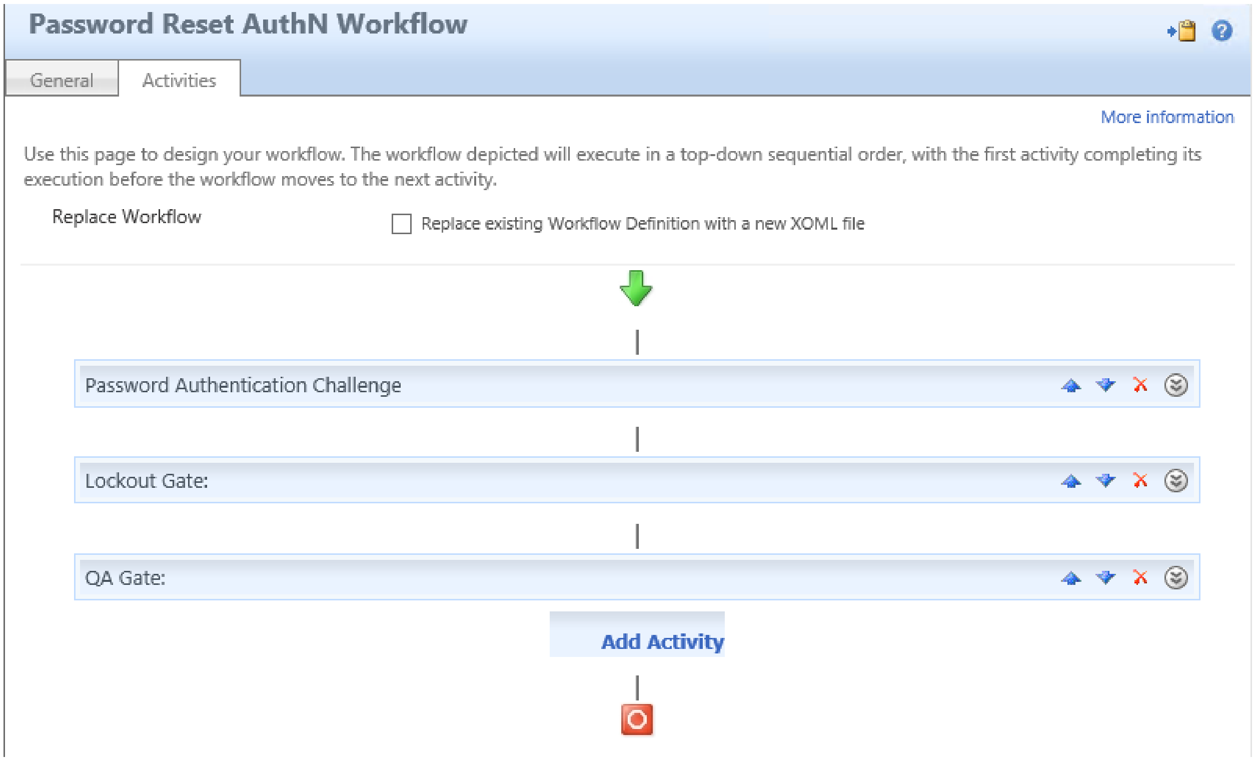
Password Reset Users Set

☑ Enable criteria-based membership in current set

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

Employee Type is Employee

Add Statement or Add Sub-condition



Password Reset AuthN Workflow

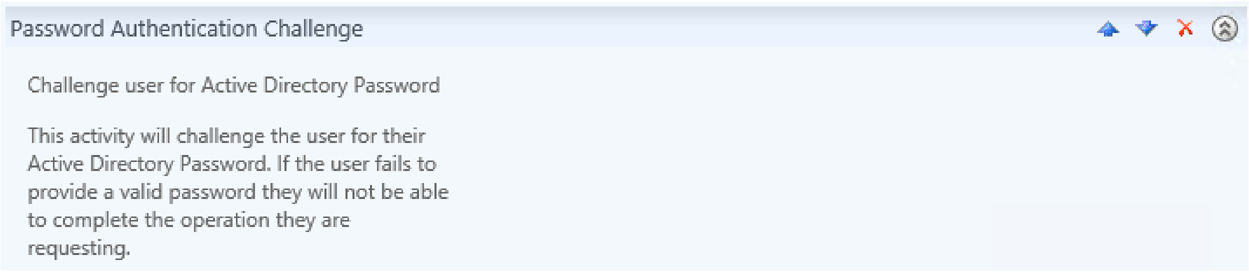
Use this page to design your workflow. The workflow depicted will execute in a top-down sequential order, with the first activity completing its execution before the workflow moves to the next activity.

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

Password Authentication Challenge

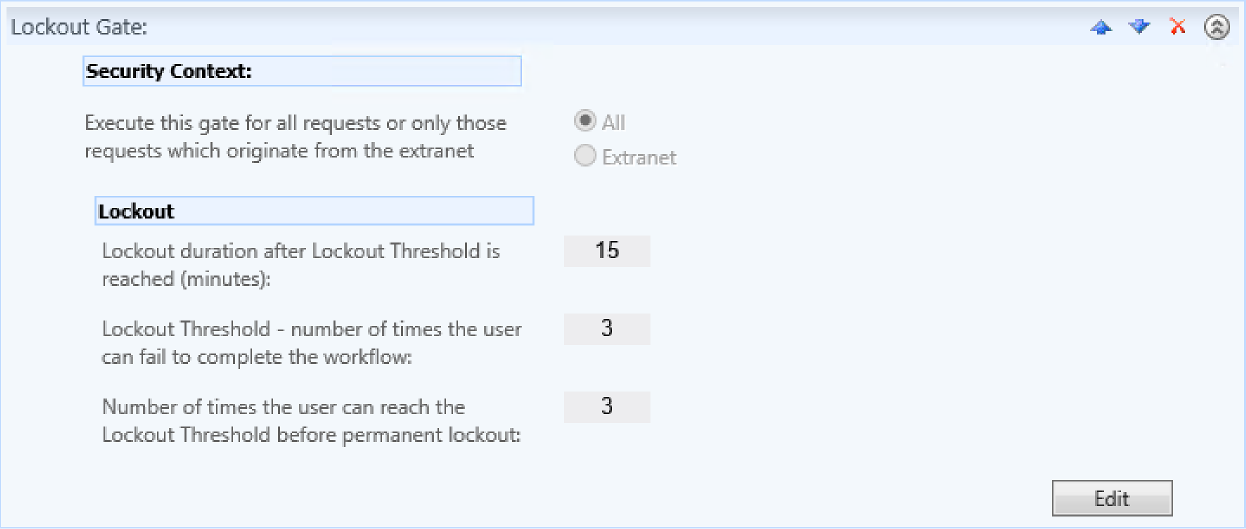
Lockout Gate:

QA Gate:


Password Authentication Challenge

Challenge user for Active Directory Password

This activity will challenge the user for their Active Directory Password. If the user fails to provide a valid password they will not be able to complete the operation they are requesting.



Lockout Gate:

Security Context:

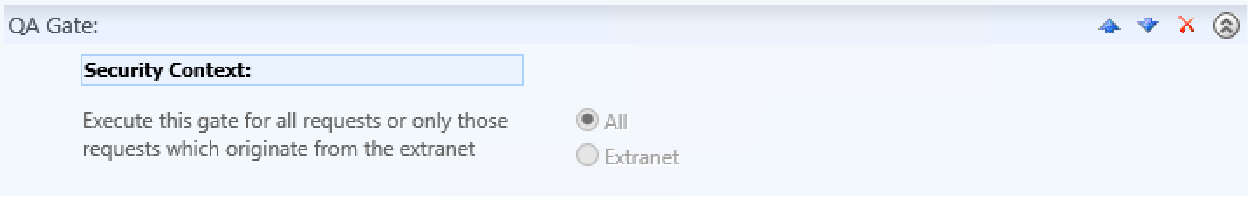
Execute this gate for all requests or only those requests which originate from the extranet ● All ○ Extranet

Lockout

Lockout duration after Lockout Threshold is reached (minutes): 15

Lockout Threshold - number of times the user can fail to complete the workflow: 3

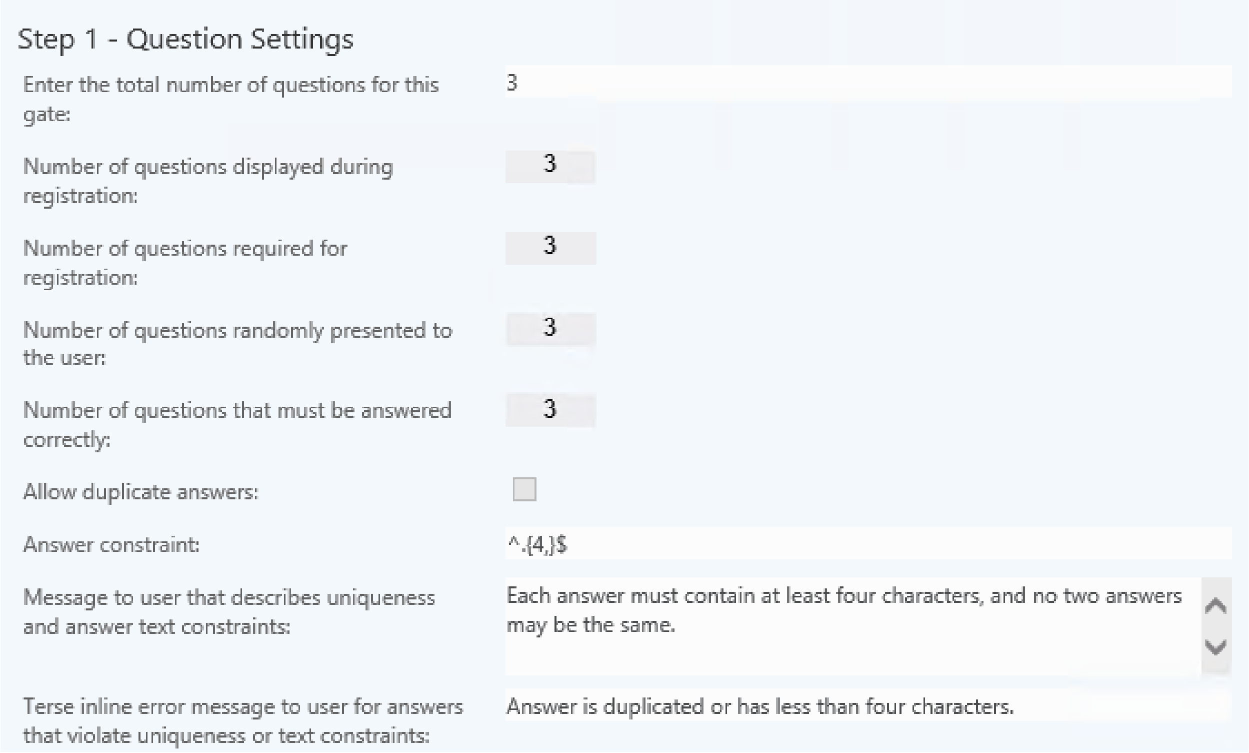
Number of times the user can reach the Lockout Threshold before permanent lockout: 3



QA Gate:

Security Context:

Execute this gate for all requests or only those requests which originate from the extranet ● All ○ Extranet



Step 1 - Question Settings

Enter the total number of questions for this gate: 3

Number of questions displayed during registration: 3

Number of questions required for registration: 3

Number of questions randomly presented to the user: 3

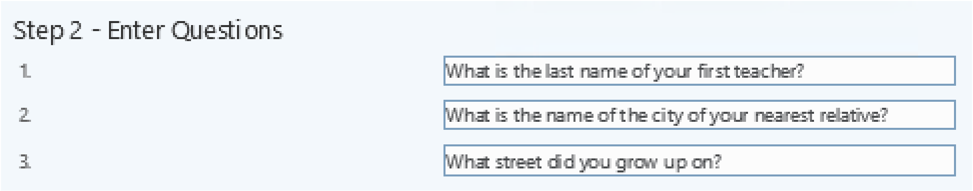
Number of questions that must be answered correctly: 3

Allow duplicate answers: □

Answer constraint: ^.{4,}$

Message to user that describes uniqueness and answer text constraints: Each answer must contain at least four characters, and no two answers may be the same.

Terse inline error message to user for answers that violate uniqueness or text constraints: Answer is duplicated or has less than four characters.

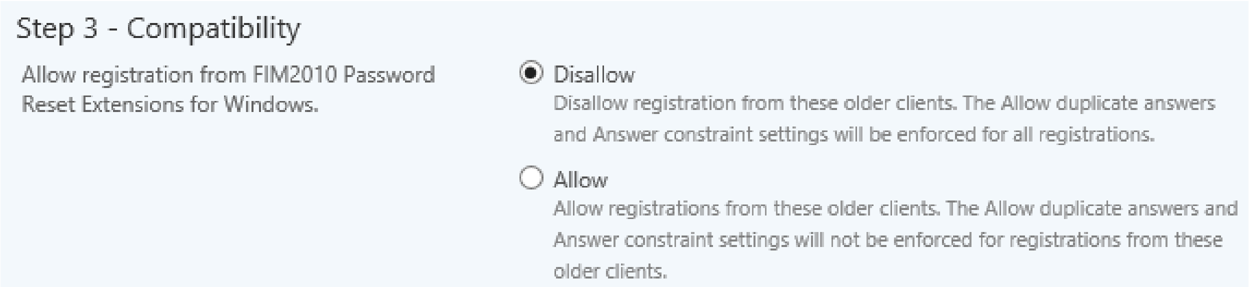


Step 2 - Enter Questions

1. What is the last name of your first teacher?

2. What is the name of the city of your nearest relative?

3. What street did you grow up on?

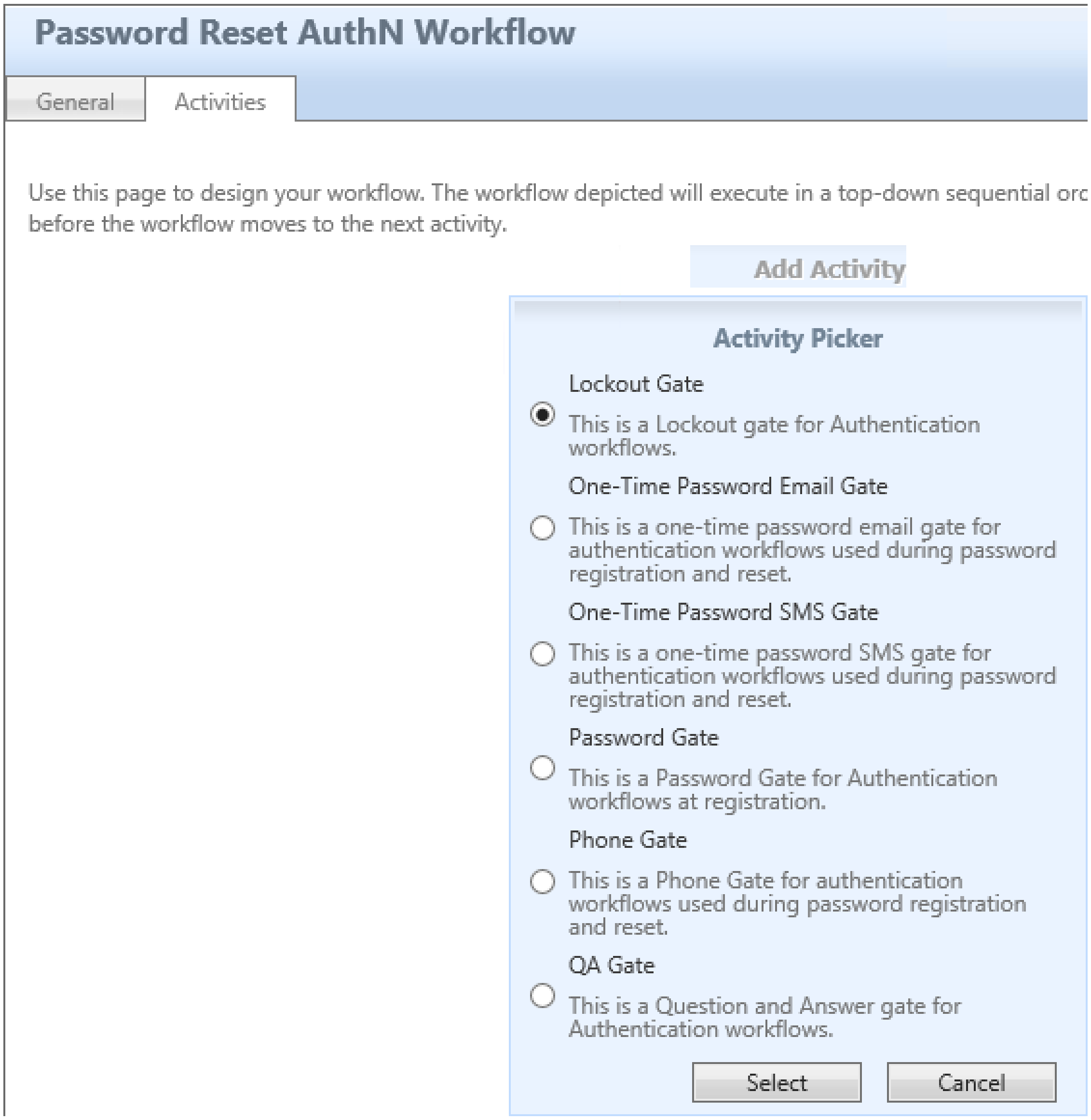


Step 3 - Compatibility

Allow registration from FIM2010 Password Reset Extensions for Windows.

● Disallow
Disallow registration from these older clients. The Allow duplicate answers and Answer constraint settings will be enforced for all registrations.

○ Allow
Allow registrations from these older clients. The Allow duplicate answers and Answer constraint settings will not be enforced for registrations from these older clients.



Password Reset AuthN Workflow

Use this page to design your workflow. The workflow depicted will execute in a top-down sequential orc
before the workflow moves to the next activity.

Activity Picker

● Lockout Gate
This is a Lockout gate for Authentication workflows.

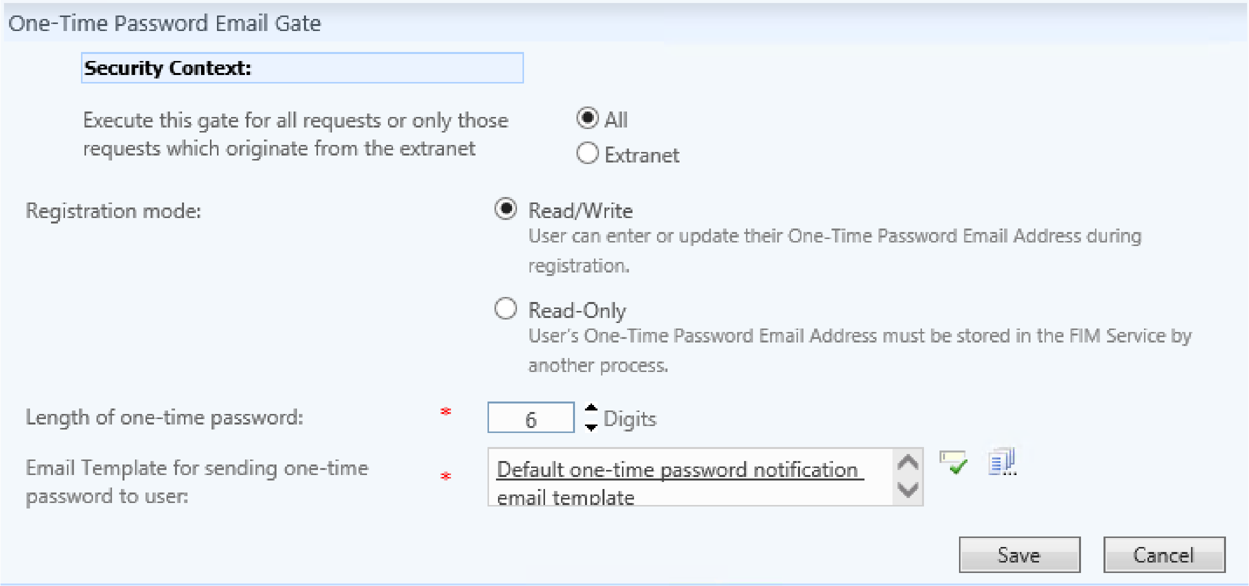
○ One-Time Password Email Gate
This is a one-time password email gate for authentication workflows used during password registration and reset.

○ One-Time Password SMS Gate
This is a one-time password SMS gate for authentication workflows used during password registration and reset.

○ Password Gate
This is a Password Gate for Authentication workflows at registration.

○ Phone Gate
This is a Phone Gate for authentication workflows used during password registration and reset.

○ QA Gate
This is a Question and Answer gate for Authentication workflows.



One-Time Password Email Gate

Security Context:

Execute this gate for all requests or only those requests which originate from the extranet ● All ○ Extranet

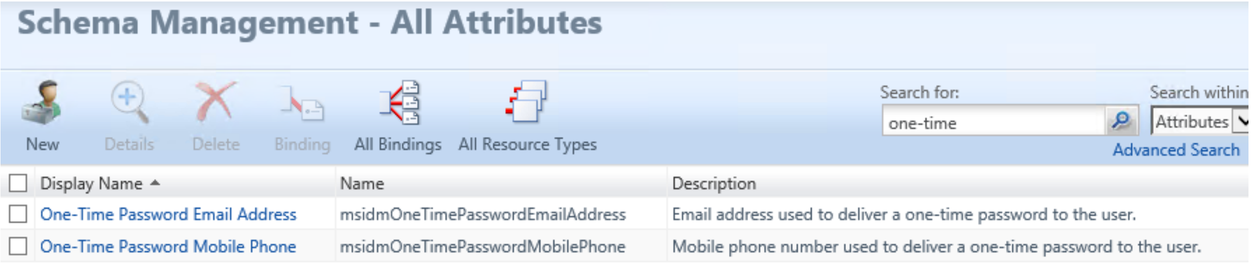
Registration mode:

● Read/Write
User can enter or update their One-Time Password Email Address during registration.

○ Read-Only
User's One-Time Password Email Address must be stored in the FIM Service by another process.

Length of one-time password: * 6 Digits

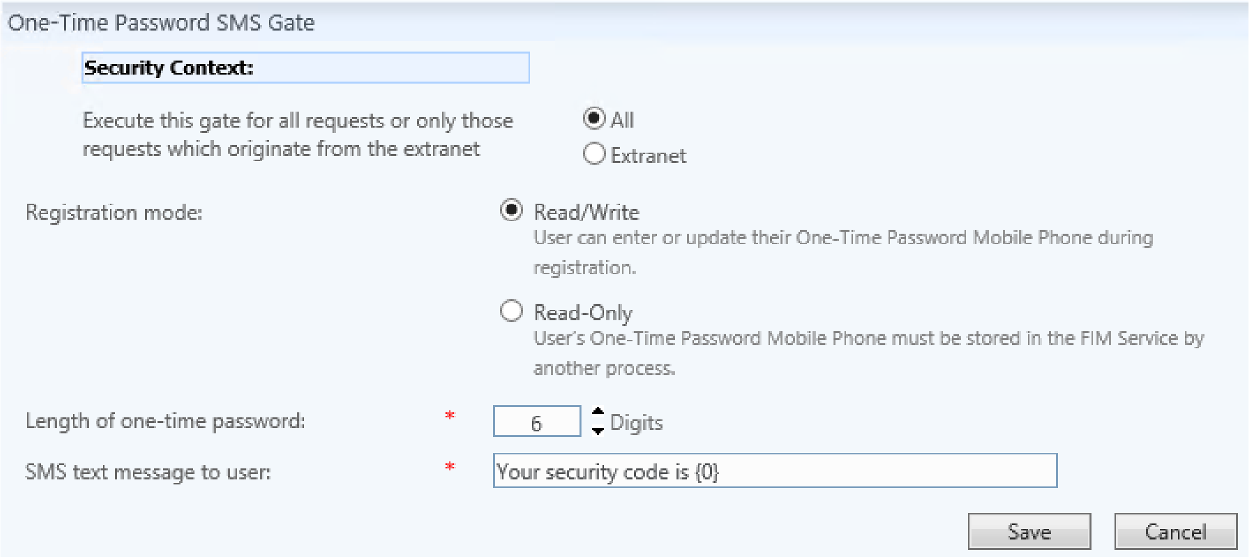
Email Template for sending one-time password to user: * Default one-time password notification email template



Schema Management - All Attributes

Search for: one-time

□	Display Name ▲	Name	Description
□	One-Time Password Email Address	msidmOneTimePasswordEmailAddress	Email address used to deliver a one-time password to the user.
□	One-Time Password Mobile Phone	msidmOneTimePasswordMobilePhone	Mobile phone number used to deliver a one-time password to the user.



One-Time Password SMS Gate

Security Context:

Execute this gate for all requests or only those requests which originate from the extranet ● All ○ Extranet

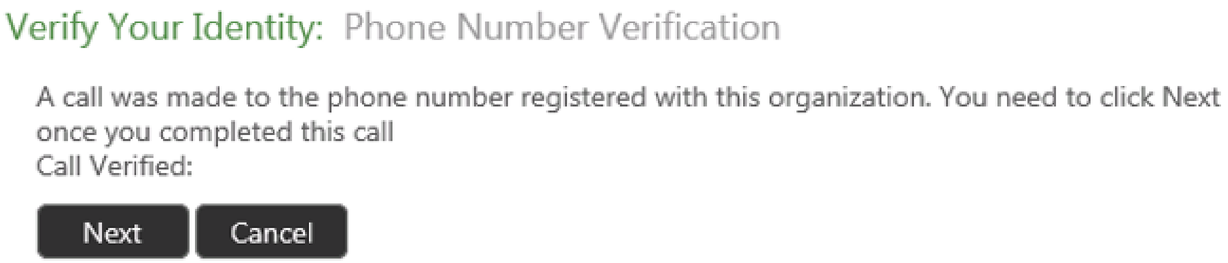
Registration mode:

● Read/Write
User can enter or update their One-Time Password Mobile Phone during registration.

○ Read-Only
User's One-Time Password Mobile Phone must be stored in the FIM Service by another process.

Length of one-time password: * 6 Digits

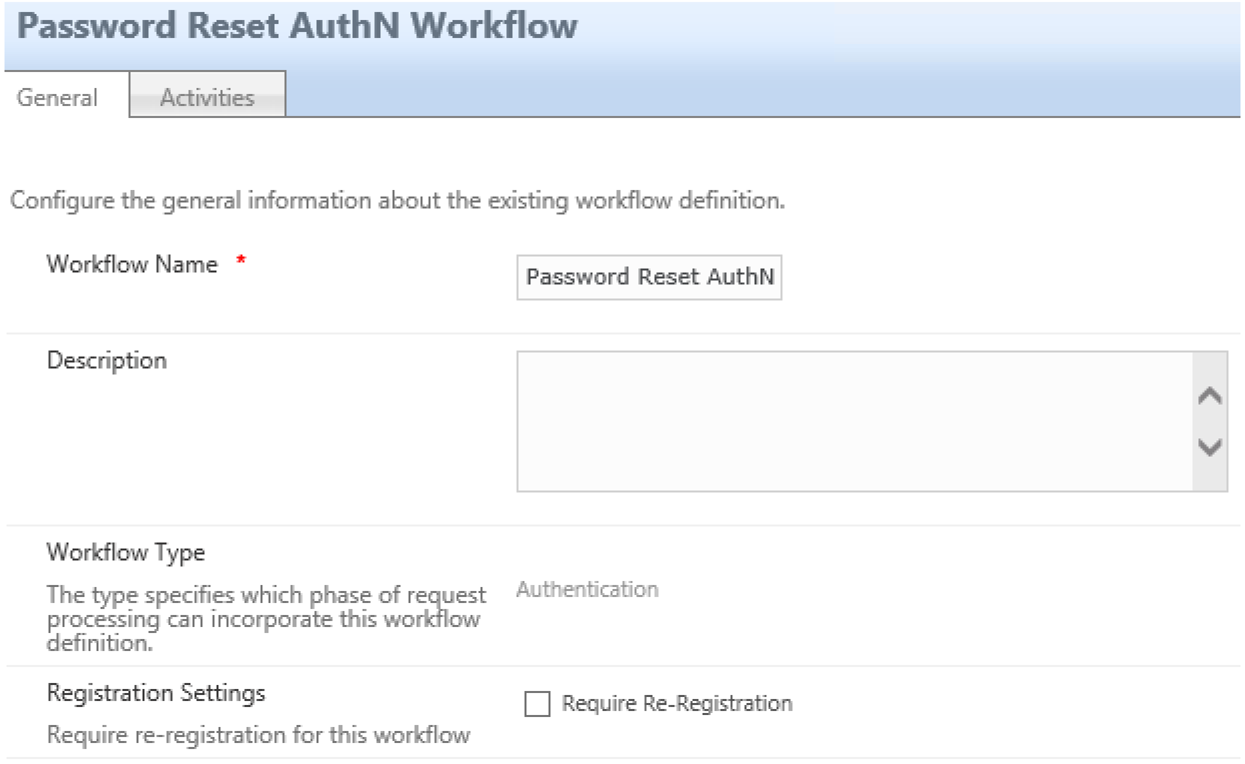
SMS text message to user: * Your security code is {0}



Verify Your Identity: Phone Number Verification

A call was made to the phone number registered with this organization. You need to click Next once you completed this call

Call Verified:



Password Reset AuthN Workflow

Configure the general information about the existing workflow definition.

Workflow Name * : Password Reset AuthN

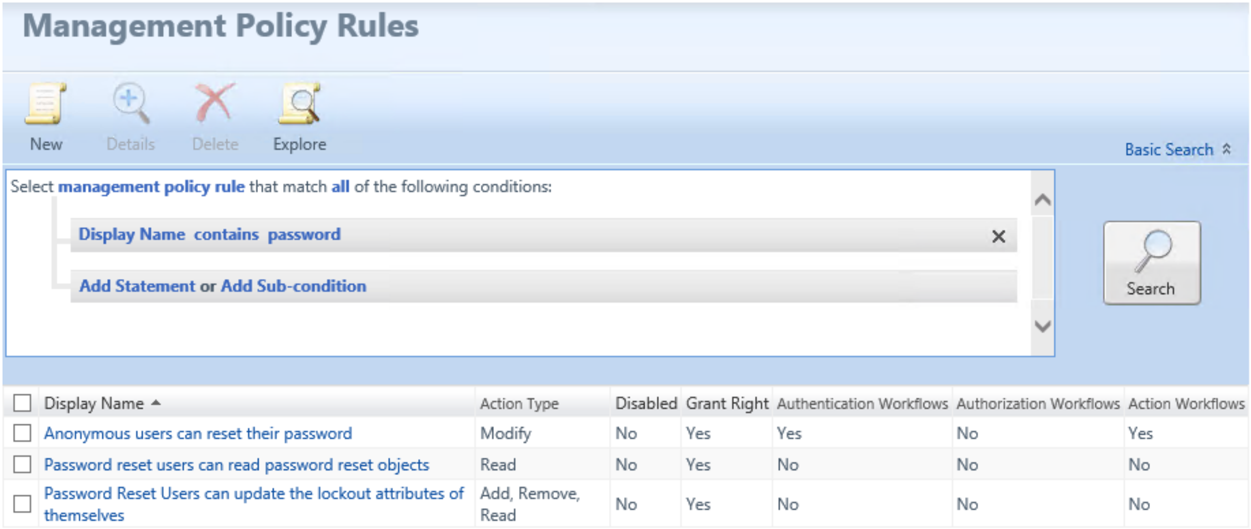
Description:

Workflow Type: Authentication

The type specifies which phase of request processing can incorporate this workflow definition.

Registration Settings: □ Require Re-Registration

Require re-registration for this workflow



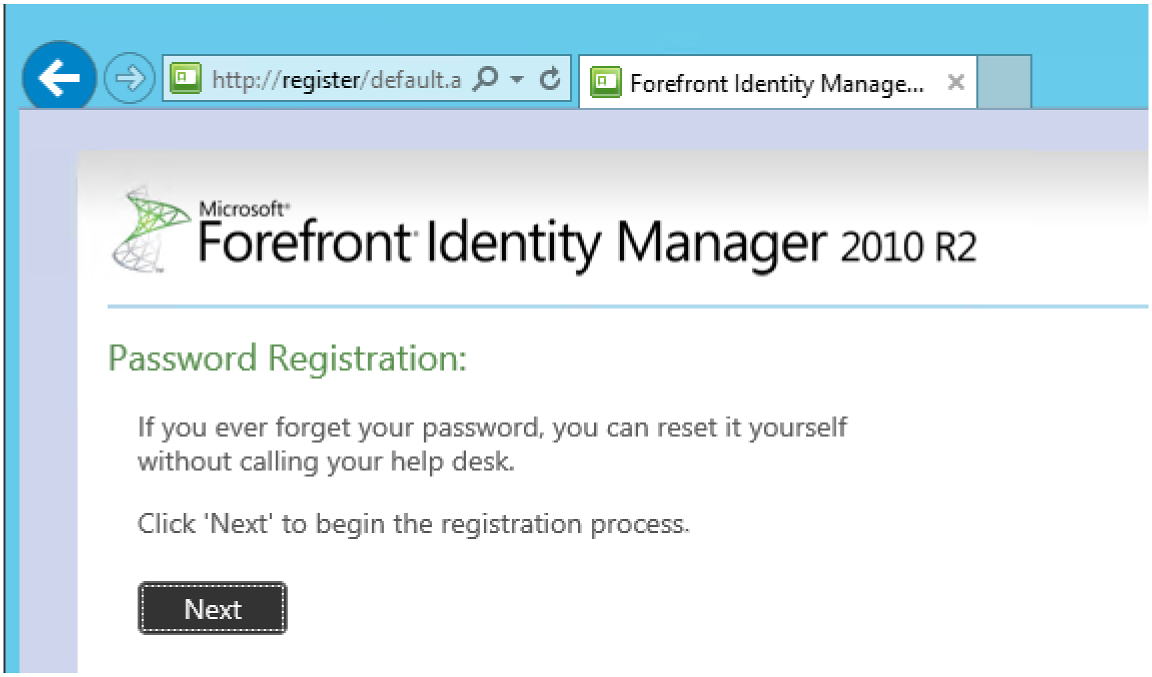
Management Policy Rules

Select management policy rule that match all of the following conditions:

Display Name contains password

Add Statement or Add Sub-condition

□	Display Name	Action Type	Disabled	Grant Right	Authentication Workflows	Authorization Workflows	Action Workflows
□	Anonymous users can reset their password	Modify	No	Yes	Yes	No	Yes
□	Password reset users can read password reset objects	Read	No	Yes	No	No	No
□	Password Reset Users can update the lockout attributes of themselves	Add, Remove, Read	No	Yes	No	No	No

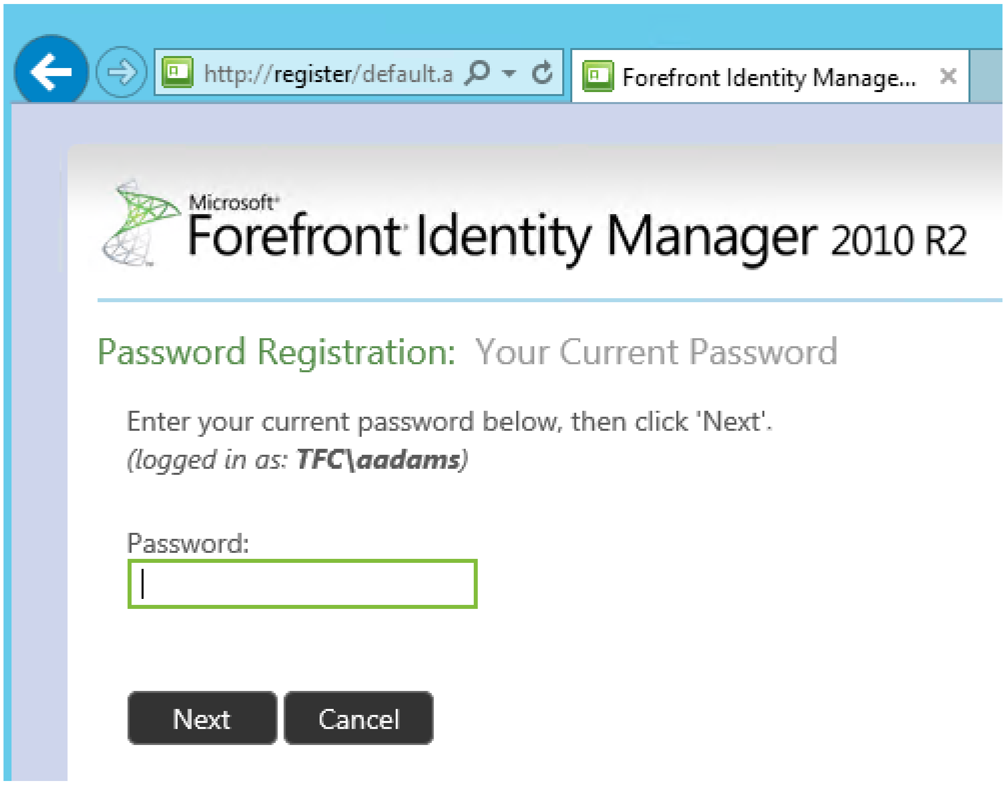


http://register/default.a
Forefront Identity Manage...
Microsoft
Forefront Identity Manager 2010 R2

Password Registration:

If you ever forget your password, you can reset it yourself without calling your help desk.

Click 'Next' to begin the registration process.

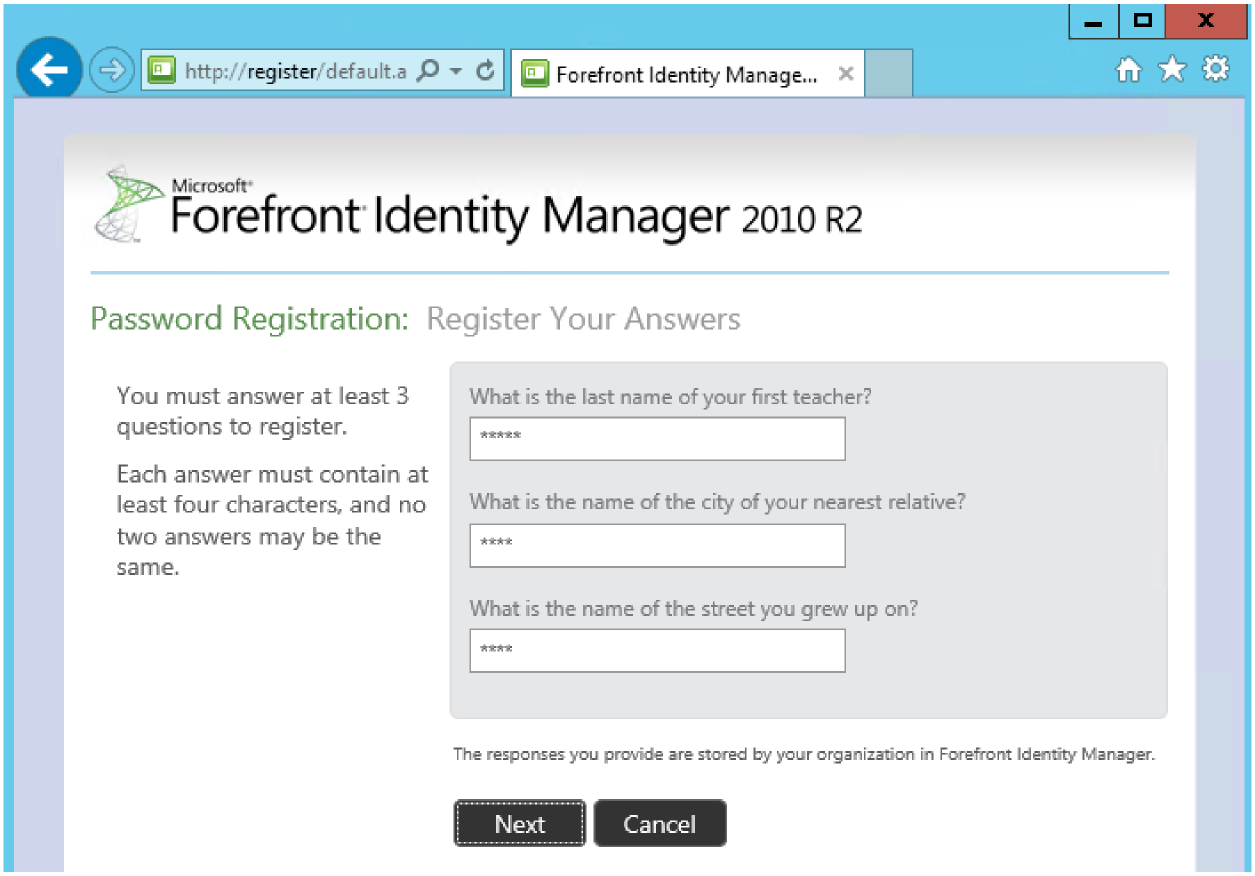


http://register/default.a
Forefront Identity Manage...
Microsoft
Forefront Identity Manager 2010 R2

Password Registration: Your Current Password

Enter your current password below, then click 'Next'.
*(logged in as: **TFC\aadams**)*

Password:


http://register/default.a
Forefront Identity Manage...
Microsoft
Forefront Identity Manager 2010 R2

Password Registration: Register Your Answers

You must answer at least 3 questions to register.

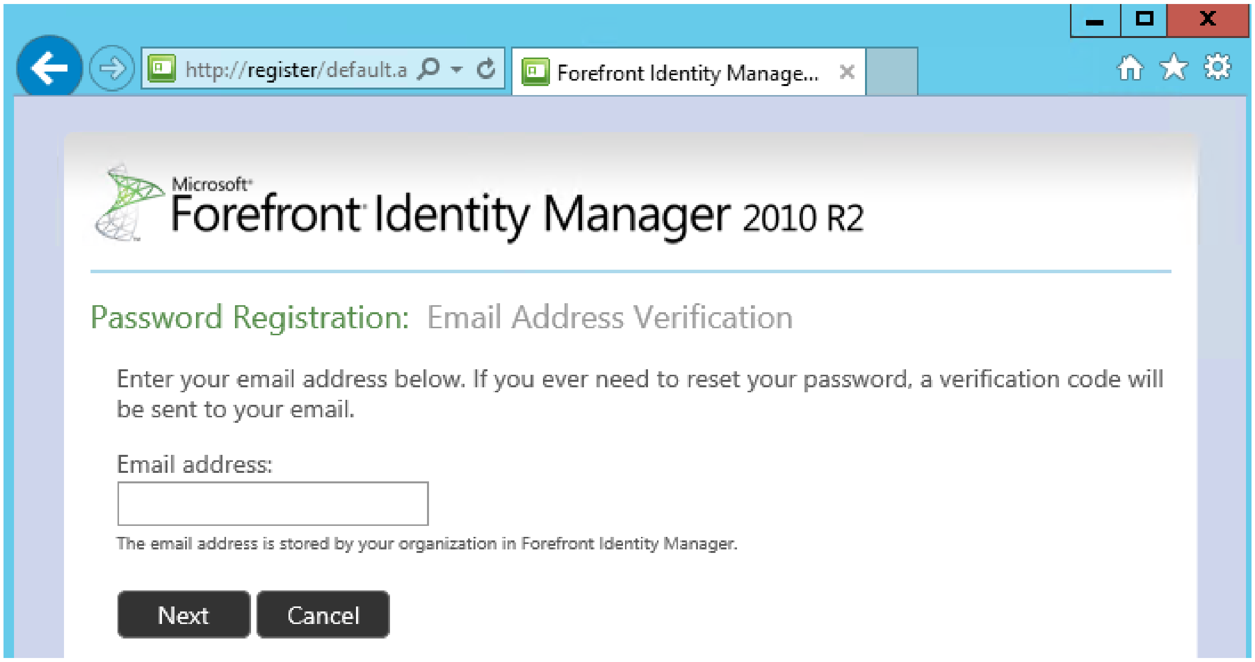
Each answer must contain at least four characters, and no two answers may be the same.

What is the last name of your first teacher?
*****

What is the name of the city of your nearest relative?
****

What is the name of the street you grew up on?
****

The responses you provide are stored by your organization in Forefront Identity Manager.

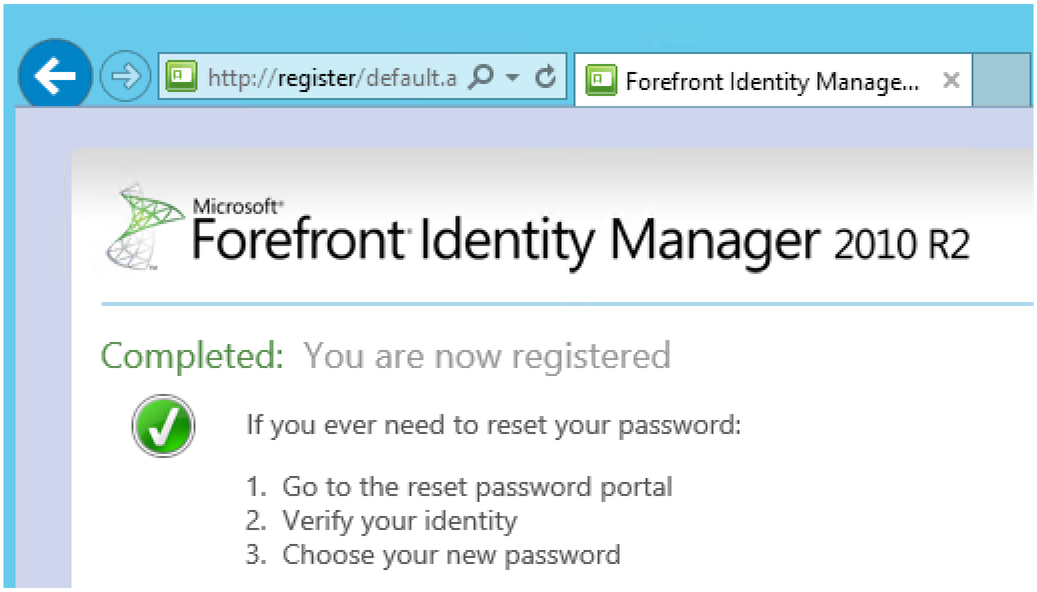

http://register/default.a
Forefront Identity Manage...
Microsoft
Forefront Identity Manager 2010 R2

Password Registration: Email Address Verification

Enter your email address below. If you ever need to reset your password, a verification code will be sent to your email.

Email address:

The email address is stored by your organization in Forefront Identity Manager.

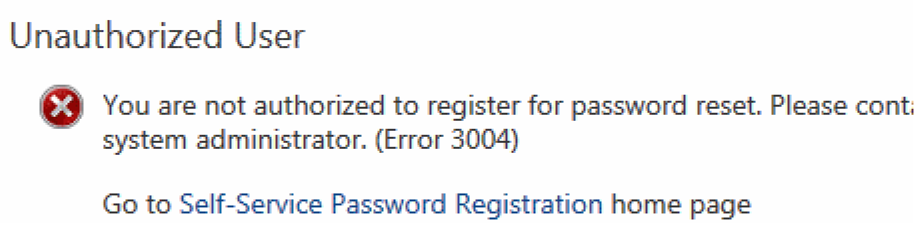


Microsoft Forefront Identity Manager 2010 R2

Completed: You are now registered

If you ever need to reset your password:

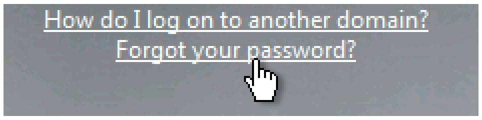
1. Go to the reset password portal
2. Verify your identity
3. Choose your new password

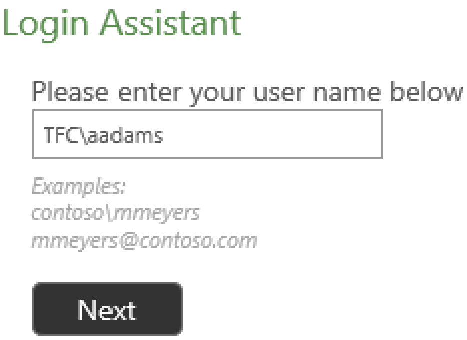


Unauthorized User

You are not authorized to register for password reset. Please cont system administrator. (Error 3004)

Go to Self-Service Password Registration home page



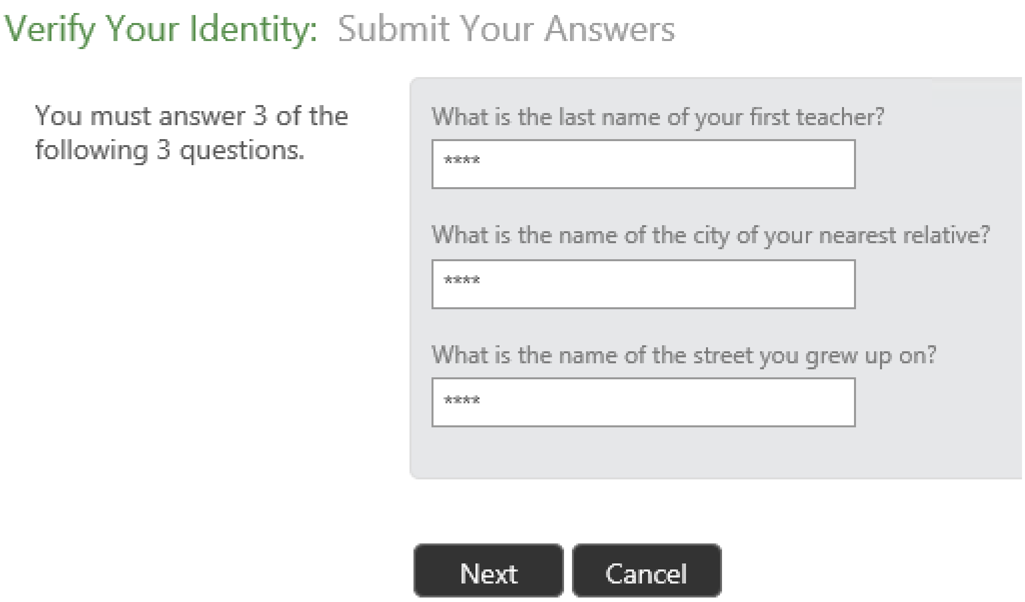


Login Assistant

Please enter your user name below

TFC\aadams

Examples:
contoso\mmeyers
mmeyers@contoso.com



Verify Your Identity: Submit Your Answers

You must answer 3 of the following 3 questions.

What is the last name of your first teacher?

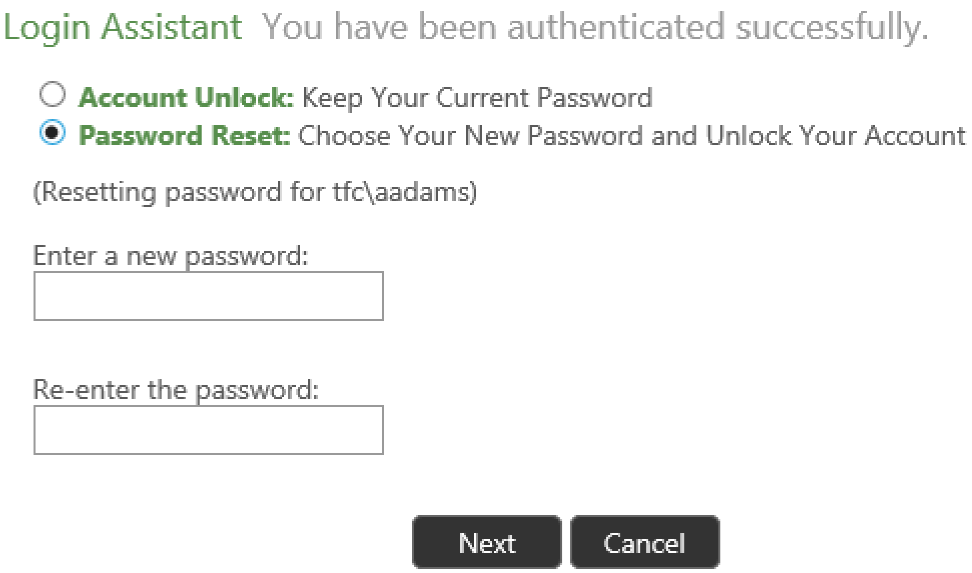
****

What is the name of the city of your nearest relative?

****

What is the name of the street you grew up on?

****



Login Assistant You have been authenticated successfully.

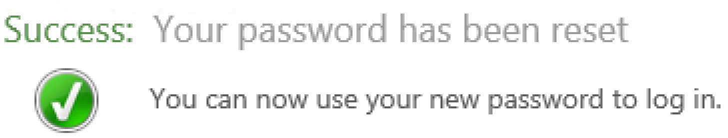
○ **Account Unlock:** Keep Your Current Password

● **Password Reset:** Choose Your New Password and Unlock Your Account

(Resetting password for tfc\aadams)

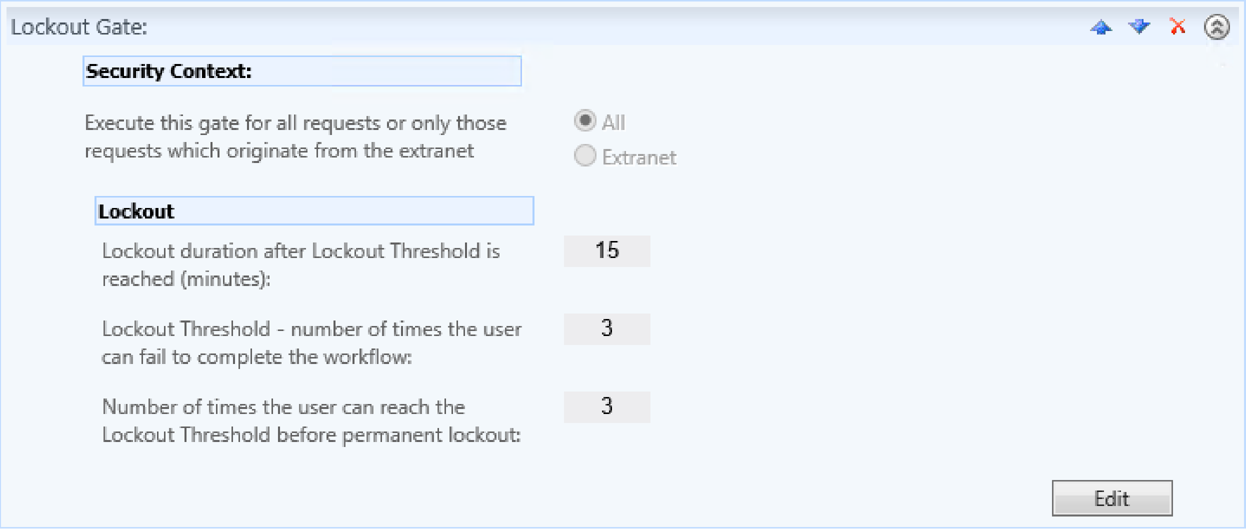
Enter a new password:

Re-enter the password:



Success: Your password has been reset

✓ You can now use your new password to log in.



Lockout Gate:

Security Context:

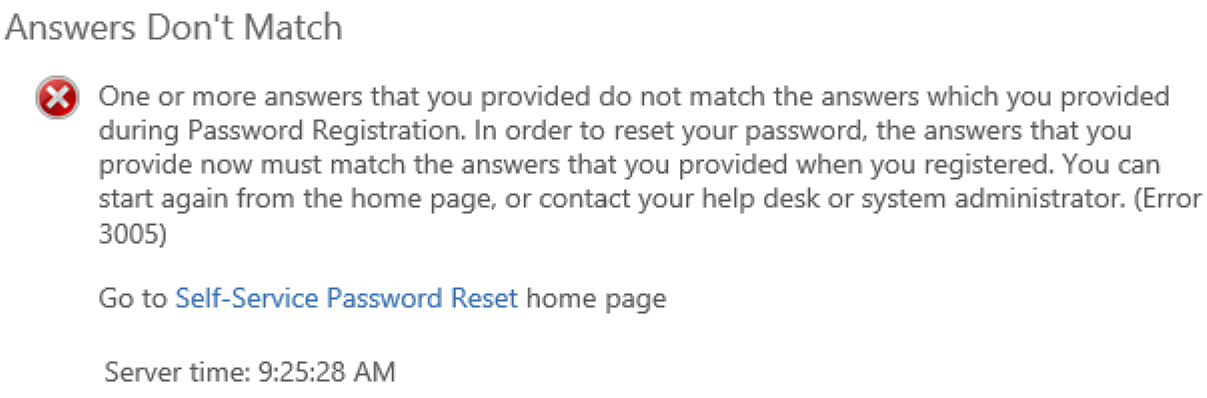
Execute this gate for all requests or only those requests which originate from the extranet ● All ○ Extranet

Lockout

Lockout duration after Lockout Threshold is reached (minutes): 15

Lockout Threshold - number of times the user can fail to complete the workflow: 3

Number of times the user can reach the Lockout Threshold before permanent lockout: 3

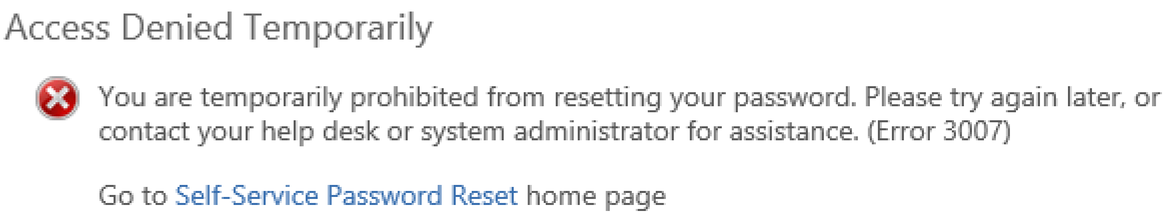


Answers Don't Match

One or more answers that you provided do not match the answers which you provided during Password Registration. In order to reset your password, the answers that you provide now must match the answers that you provided when you registered. You can start again from the home page, or contact your help desk or system administrator. (Error 3005)

Go to Self-Service Password Reset home page

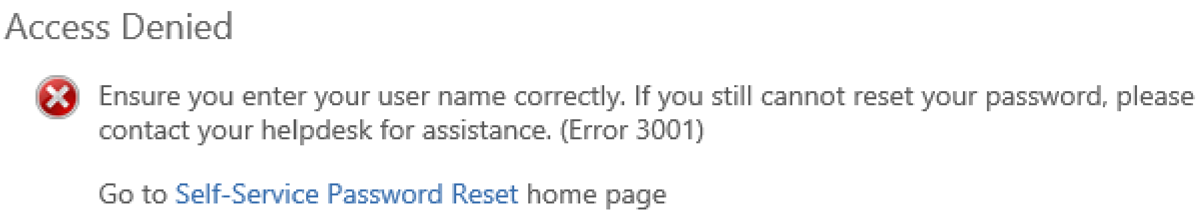
Server time: 9:25:28 AM



Access Denied Temporarily

You are temporarily prohibited from resetting your password. Please try again later, or contact your help desk or system administrator for assistance. (Error 3007)

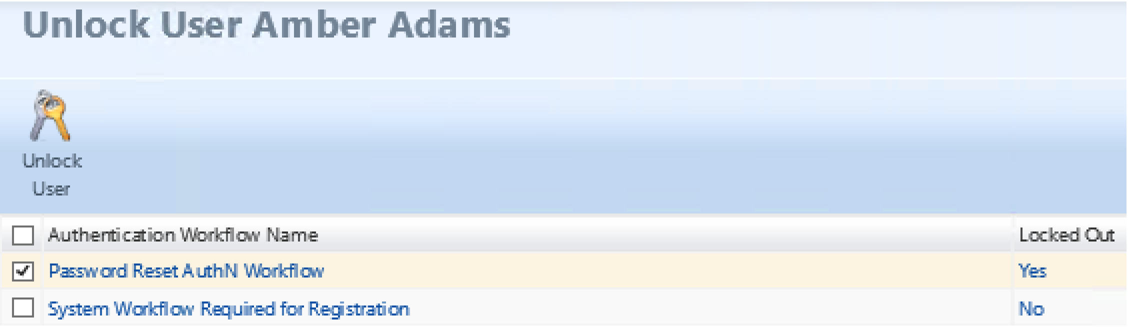
Go to Self-Service Password Reset home page



Access Denied

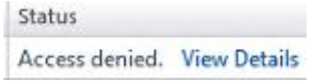
Ensure you enter your user name correctly. If you still cannot reset your password, please contact your helpdesk for assistance. (Error 3001)

Go to Self-Service Password Reset home page



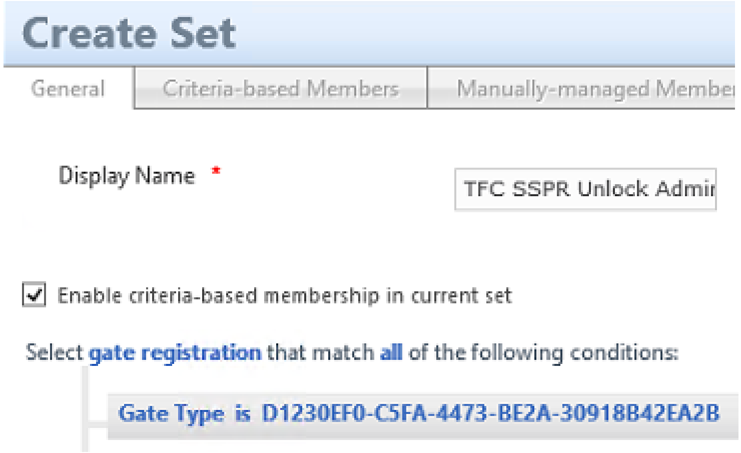
Unlock User Amber Adams

☐	Authentication Workflow Name	Locked Out
☑	Password Reset AuthN Workflow	Yes
☐	System Workflow Required for Registration	No



Status

Access denied. View Details



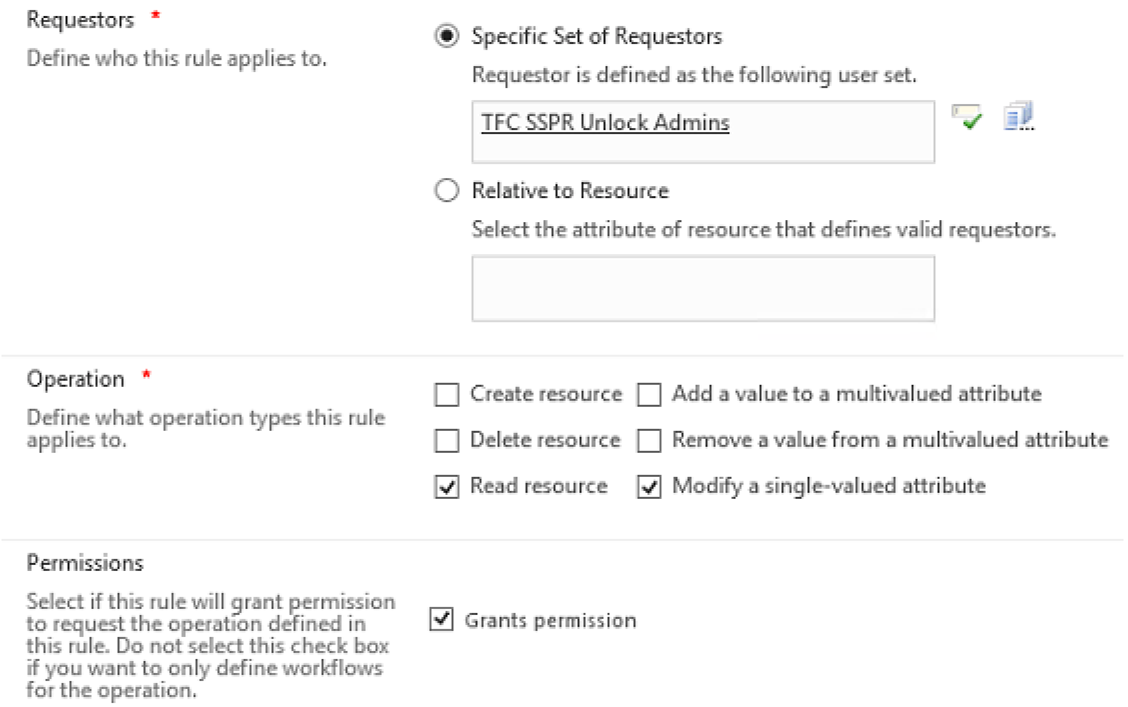
Create Set

Display Name * TFC SSPR Unlock Admir

☑ Enable criteria-based membership in current set

Select **gate registration** that match **all** of the following conditions:

Gate Type is D1230EF0-C5FA-4473-BE2A-30918B42EA2B



Requestors *

Define who this rule applies to.

● Specific Set of Requestors

Requestor is defined as the following user set.

TFC SSPR Unlock Admins

○ Relative to Resource

Select the attribute of resource that defines valid requestors.

Operation *

Define what operation types this rule applies to.

☐ Create resource ☐ Add a value to a multivalued attribute

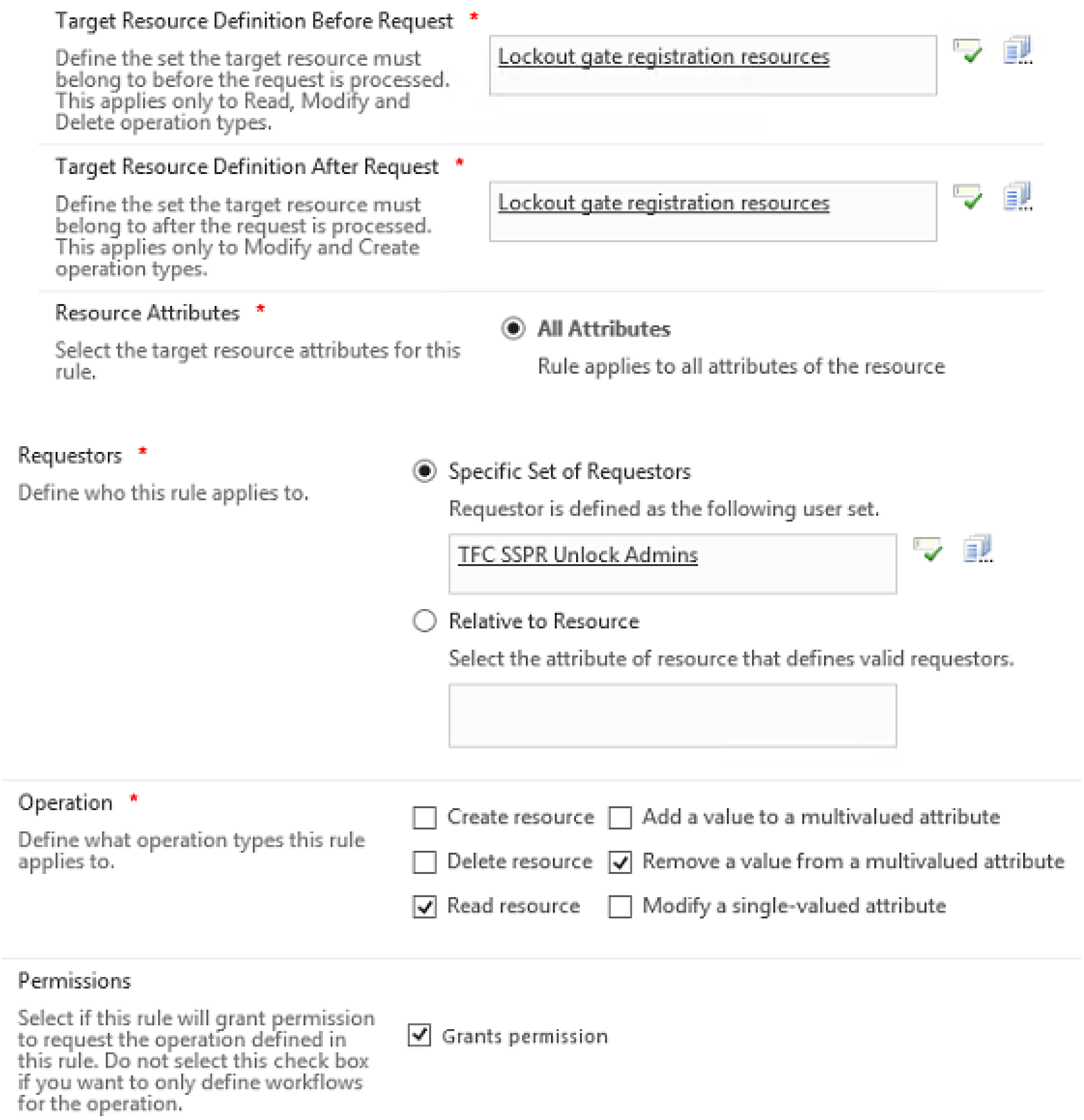
☐ Delete resource ☐ Remove a value from a multivalued attribute

☑ 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 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.

Lockout gate registration resources

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.

Lockout gate registration resources

Resource Attributes *

Select the target resource attributes for this rule.

● **All Attributes**

Rule applies to all attributes of the resource

Requestors *

Define who this rule applies to.

● Specific Set of Requestors

Requestor is defined as the following user set.

TFC SSPR Unlock Admins

○ Relative to Resource

Select the attribute of resource that defines valid requestors.

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

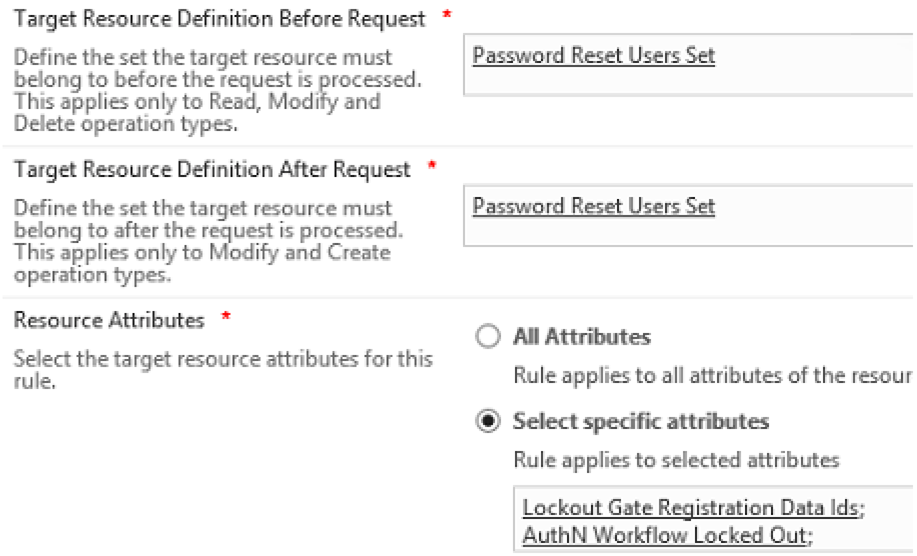
☑ Read resource

□ 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 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.

Password Reset Users Set

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.

Password Reset Users Set

Resource Attributes *

Select the target resource attributes for this rule.

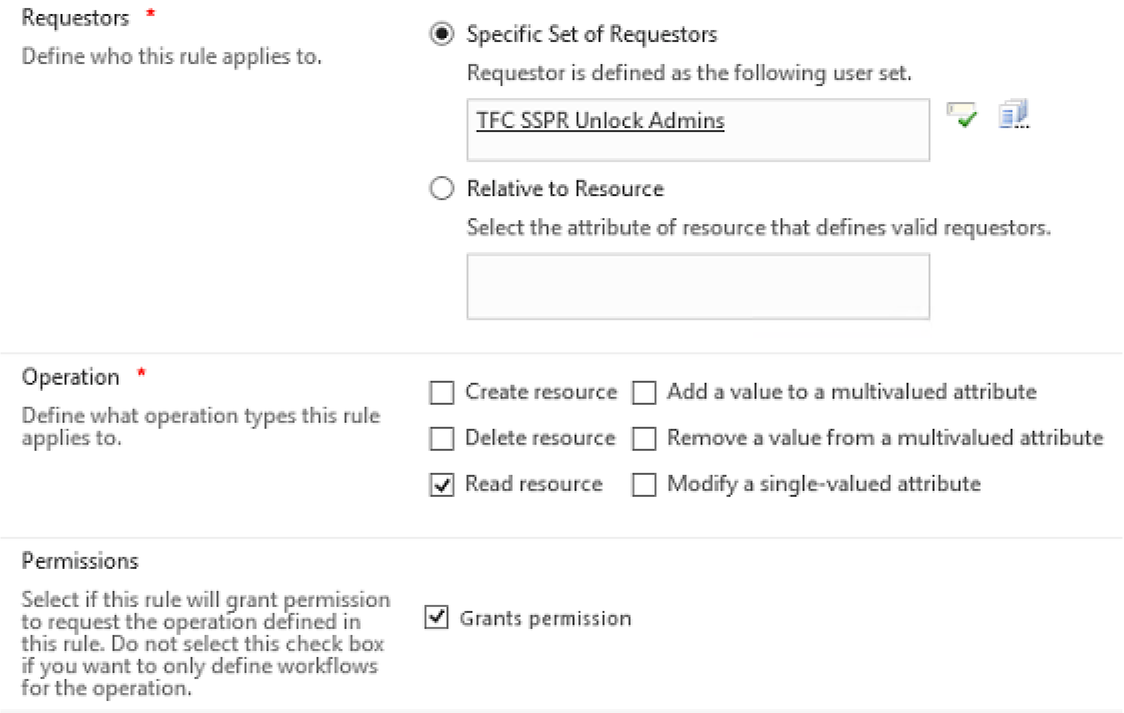
○ **All Attributes**

Rule applies to all attributes of the resour

● **Select specific attributes**

Rule applies to selected attributes

Lockout Gate Registration Data Ids;
AuthN Workflow Locked Out;



Requestors *

Define who this rule applies to.

● Specific Set of Requestors

Requestor is defined as the following user set.

TFC SSPR Unlock Admins

○ Relative to Resource

Select the attribute of resource that defines valid requestors.

Operation *

Define what operation types this rule applies to.

☐ Create resource ☐ Add a value to a multivalued attribute

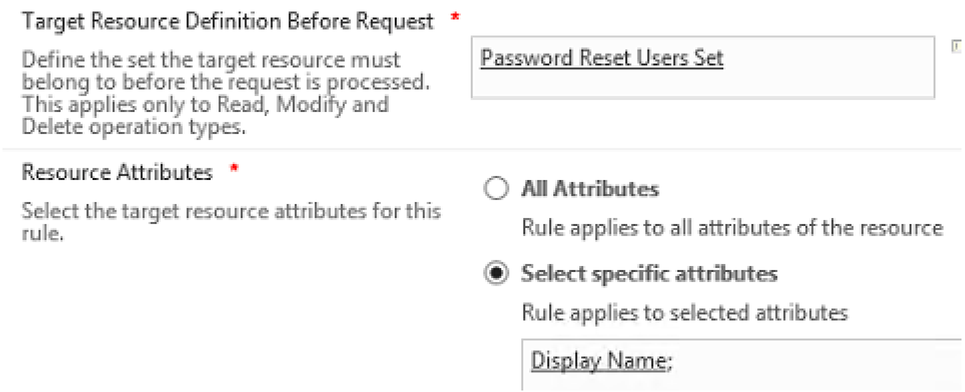
☐ Delete resource ☐ Remove a value from a multivalued attribute

☑ 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 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.

Password Reset Users Set

Resource Attributes *

Select the target resource attributes for this rule.

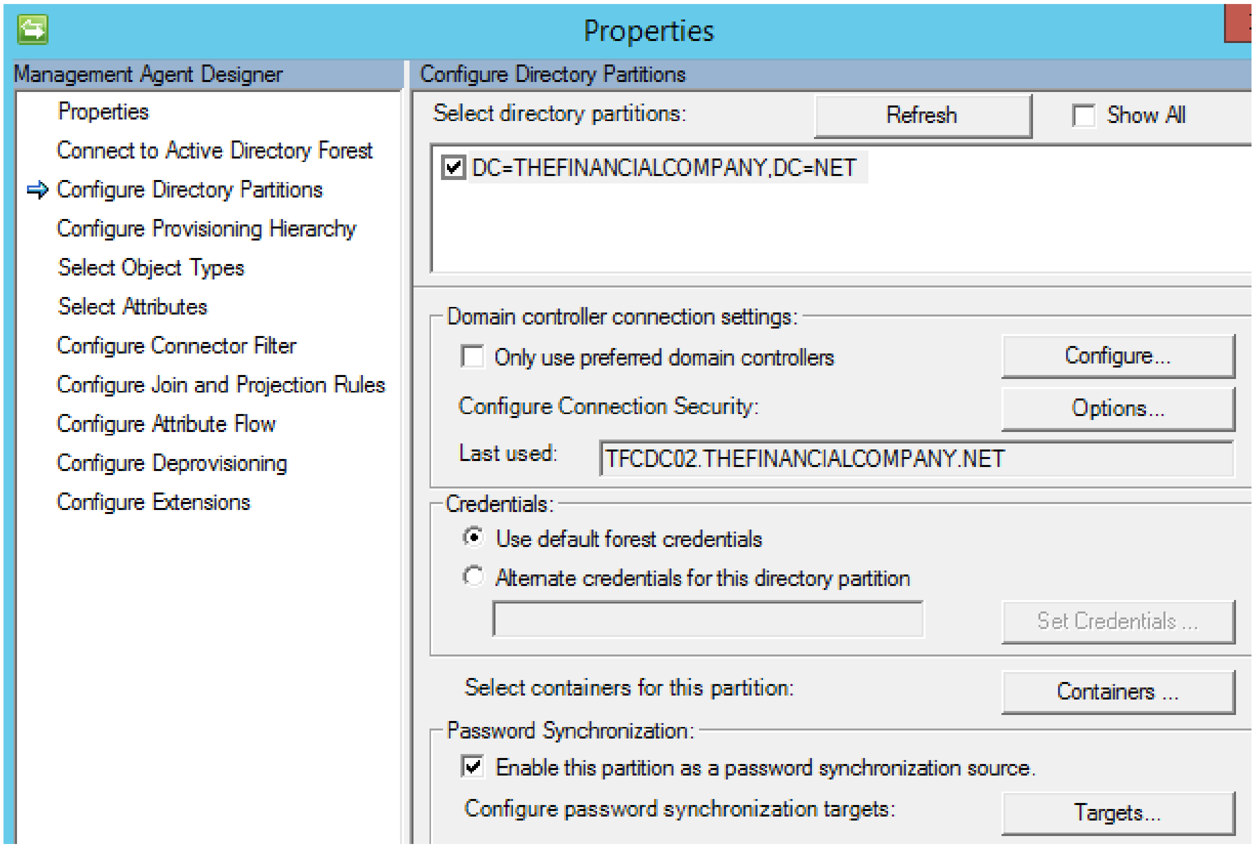
○ **All Attributes**

Rule applies to all attributes of the resource

● **Select specific attributes**

Rule applies to selected attributes

Display Name;



Properties

Management Agent Designer

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

Configure Directory Partitions

Select directory partitions: Refresh □ Show All

☑ DC=THEFINANCIALCOMPANY,DC=NET

Domain controller connection settings:

□ Only use preferred domain controllers Configure...

Configure Connection Security: Options...

Last used: TFCDC02.THEFINANCIALCOMPANY.NET

Credentials:

● Use default forest credentials

○ Alternate credentials for this directory partition

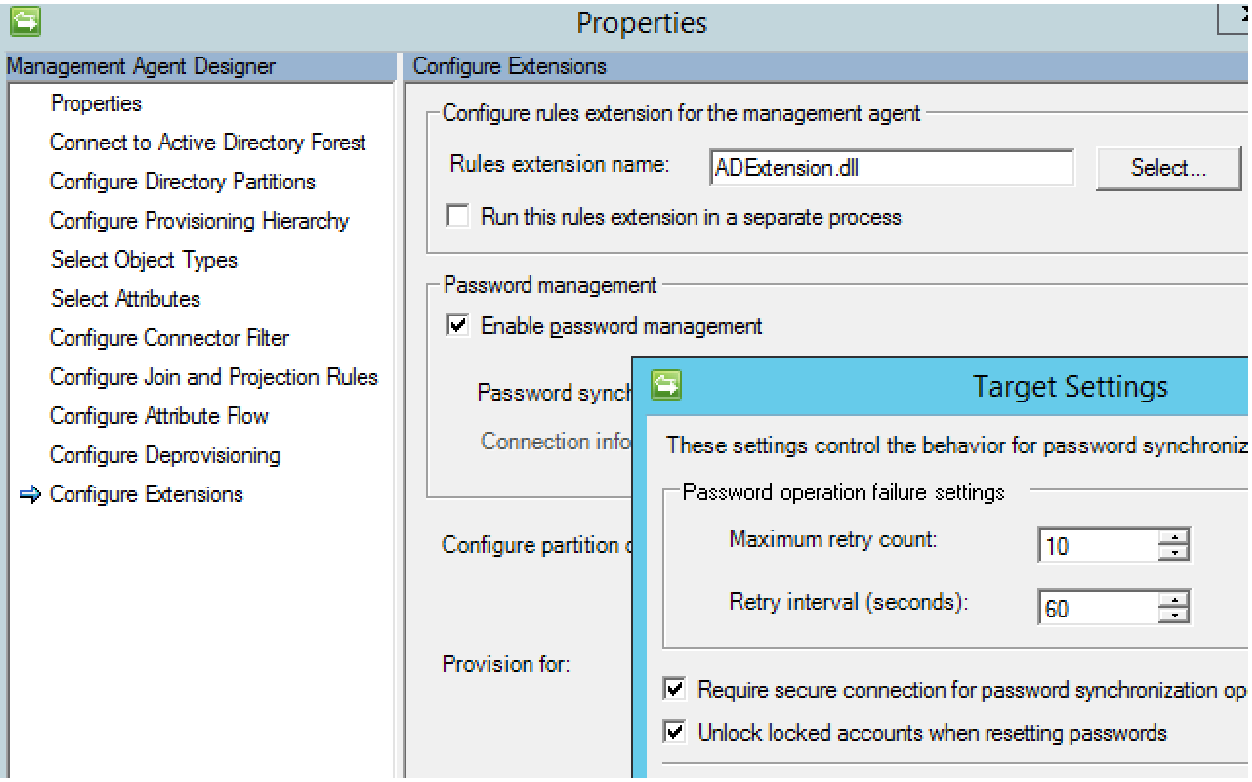
Set Credentials ...

Select containers for this partition: Containers ...

Password Synchronization:

☑ Enable this partition as a password synchronization source.

Configure password synchronization targets: Targets...



Properties

Management Agent Designer

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

Configure Extensions

Configure rules extension for the management agent

Rules extension name: ADExtension.dll

□ Run this rules extension in a separate process

Password management

☑ Enable password management

Password synch

Connection info

Configure partition c

Provision for:

Target Settings

These settings control the behavior for password synchroniz

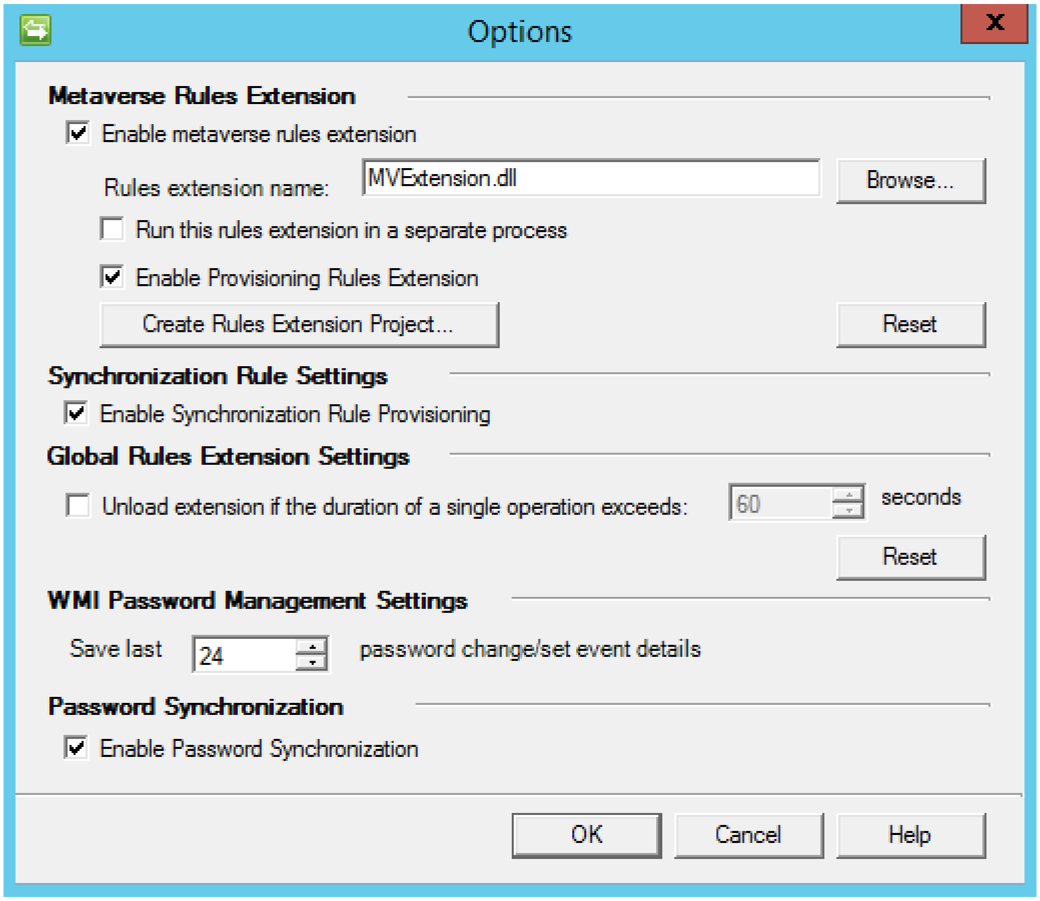
Password operation failure settings

Maximum retry count: 10

Retry interval (seconds): 60

☑ Require secure connection for password synchronization op

☑ Unlock locked accounts when resetting passwords



Options

Metaverse Rules Extension

☑ Enable metaverse rules extension

Rules extension name: MVExtension.dll

□ Run this rules extension in a separate process

☑ Enable Provisioning Rules Extension

Synchronization Rule Settings

☑ Enable Synchronization Rule Provisioning

Global Rules Extension Settings

□ Unload extension if the duration of a single operation exceeds: 60 seconds

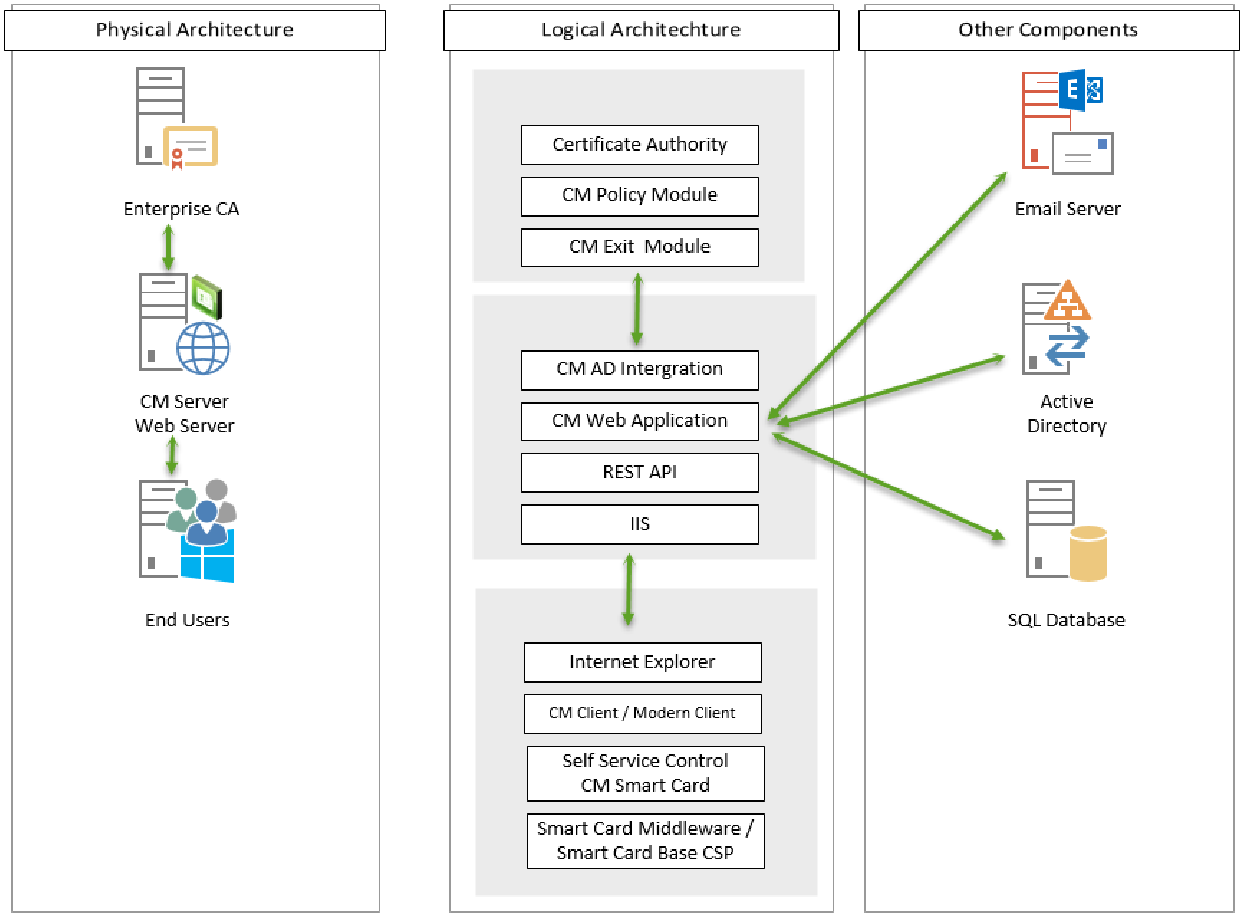
WMI Password Management Settings

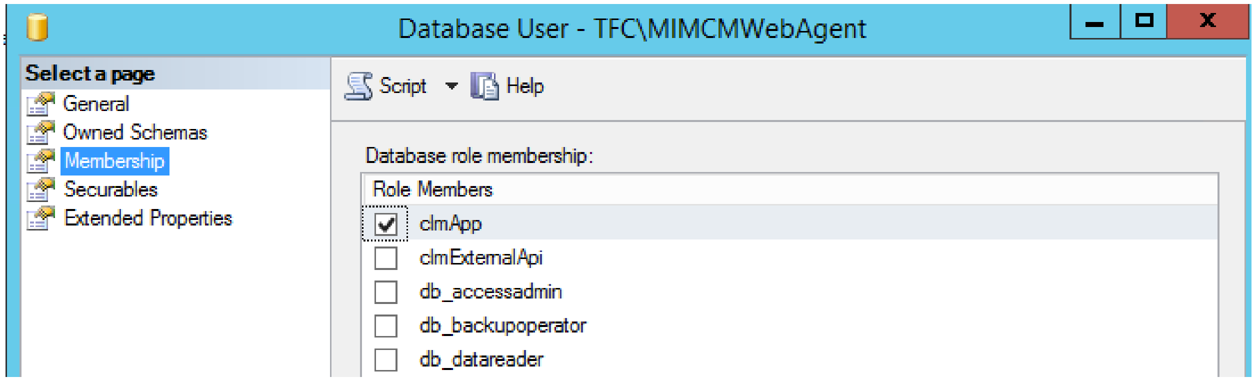
Save last 24 password change/set event details

Password Synchronization

☑ Enable Password Synchronization

Chapter 10: Overview of Certificate Management



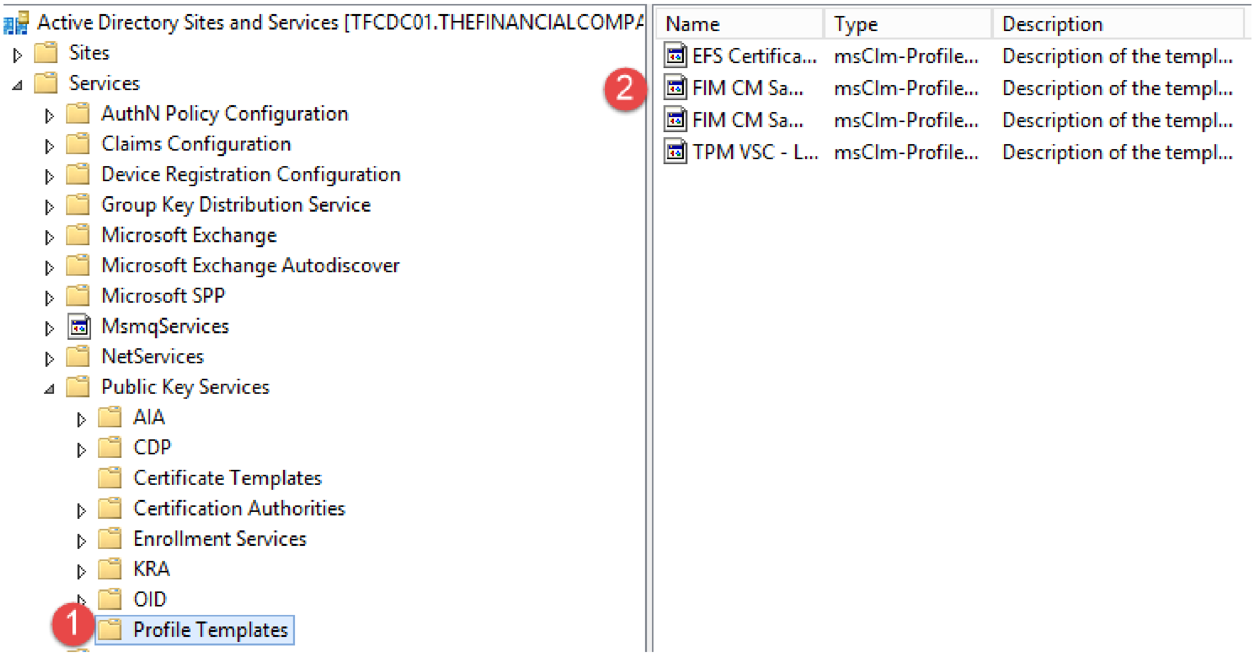

Database User - TFC\MIMCMWebAgent

Select a page
- General
- Owned Schemas
- Membership
- Securables
- Extended Properties

Script ▾ Help

Database role membership:

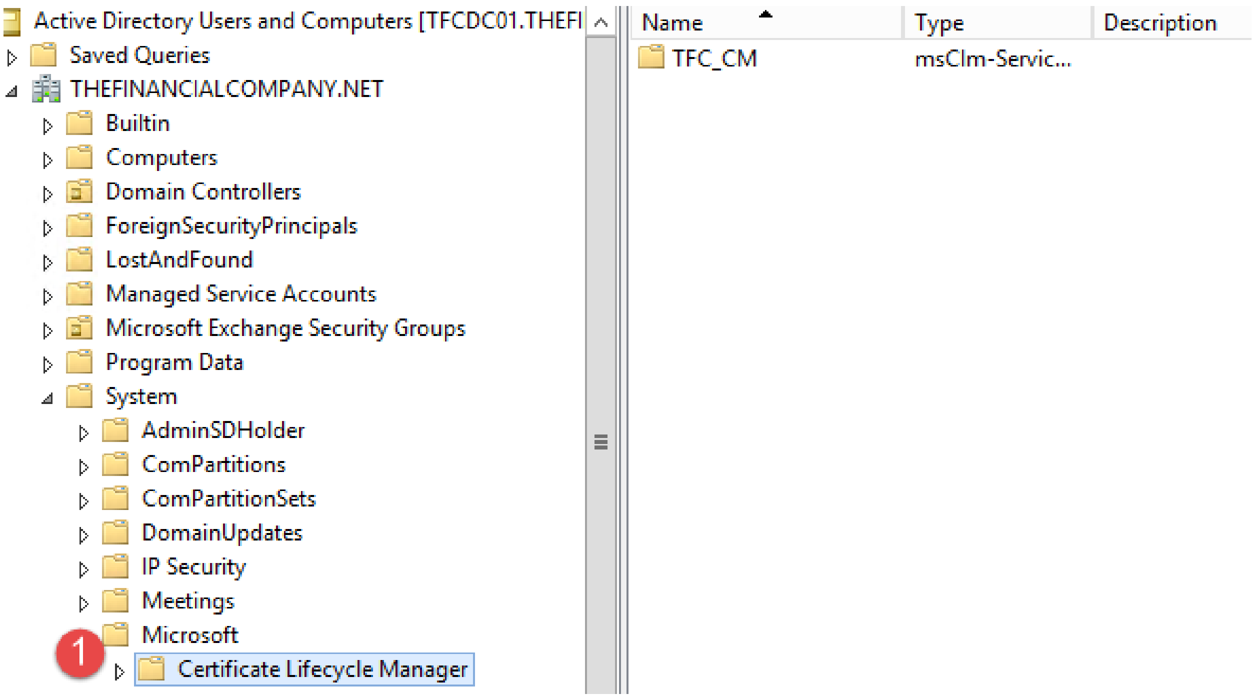
Role Members
- ☑ clmApp
- ☐ clmExternalApi
- ☐ db_accessadmin
- ☐ db_backupoperator
- ☐ db_datareader



Active Directory Sites and Services [TFCDC01.THEFINANCIALCOMPA

- Sites
- Services
  - AuthN Policy Configuration
  - Claims Configuration
  - Device Registration Configuration
  - Group Key Distribution Service
  - Microsoft Exchange
  - Microsoft Exchange Autodiscover
  - Microsoft SPP
  - MsmqServices
  - NetServices
  - Public Key Services
    - AIA
    - CDP
    - Certificate Templates
    - Certification Authorities
    - Enrollment Services
    - KRA
    - OID
    - Profile Templates

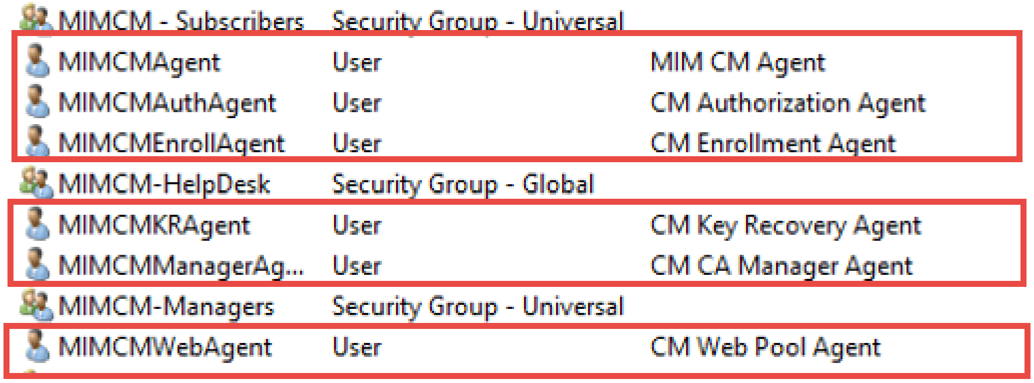
Name	Type	Description
EFS Certifica...	msClm-Profile...	Description of the templ...
FIM CM Sa...	msClm-Profile...	Description of the templ...
FIM CM Sa...	msClm-Profile...	Description of the templ...
TPM VSC - L...	msClm-Profile...	Description of the templ...



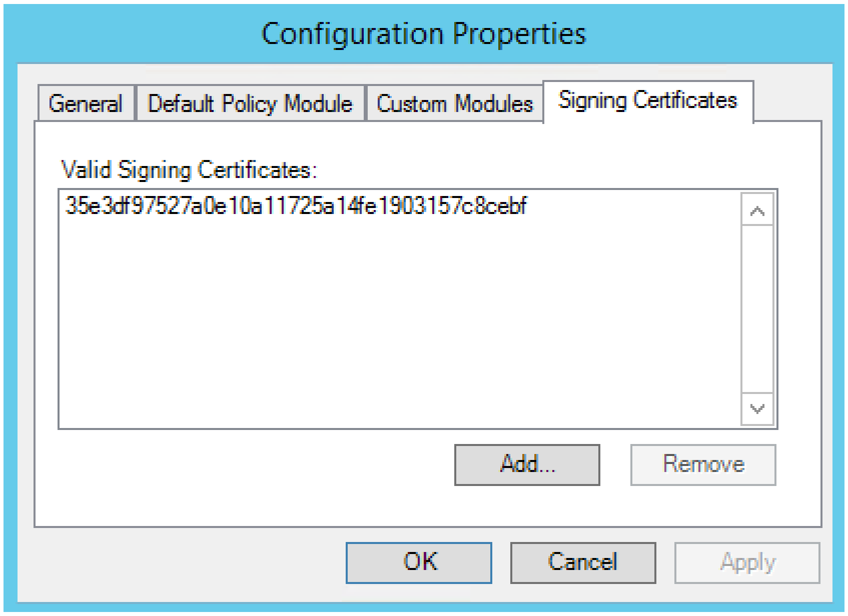
Active Directory Users and Computers [TFCDC01.THEFI

- Saved Queries
- THEFINANCIALCOMPANY.NET
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - LostAndFound
  - Managed Service Accounts
  - Microsoft Exchange Security Groups
  - Program Data
  - System
    - AdminSDHolder
    - ComPartitions
    - ComPartitionSets
    - DomainUpdates
    - IP Security
    - Meetings
    - Microsoft
      - Certificate Lifecycle Manager

Name	Type	Description
TFC_CM	msClm-Servic...	



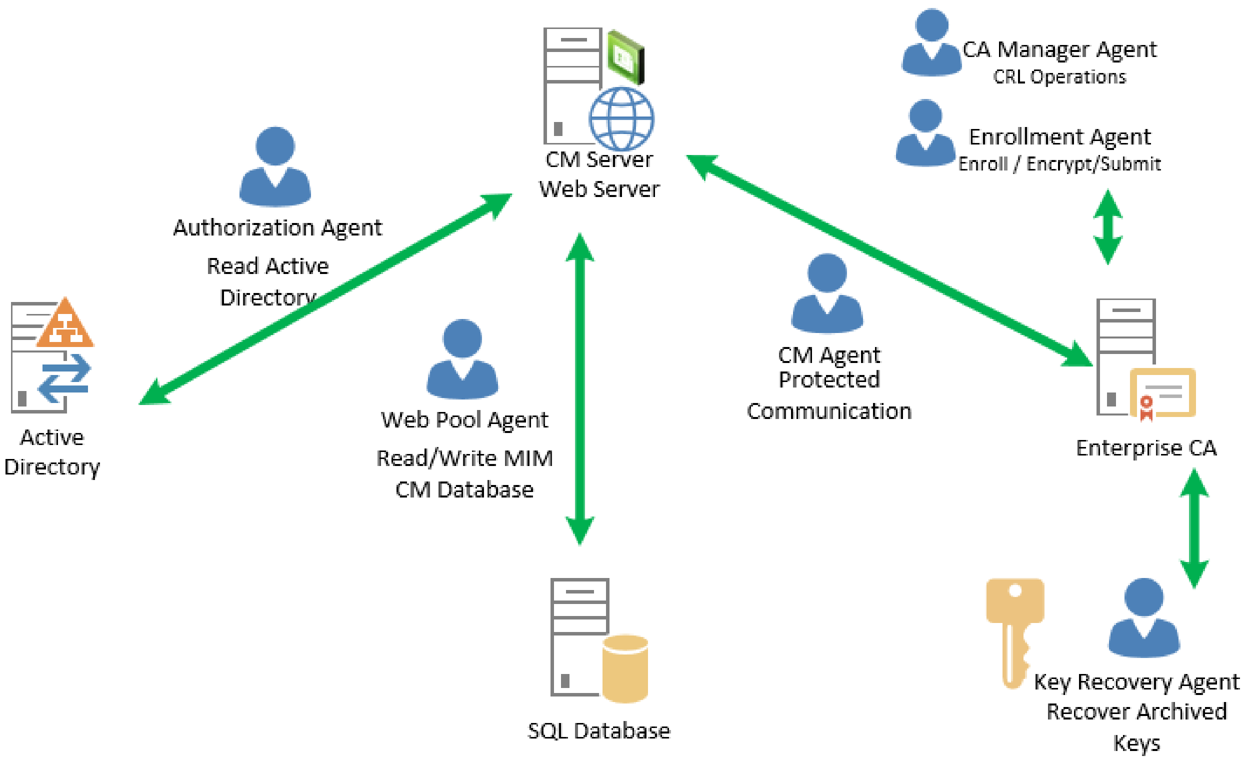
MIMCM - Subscribers	Security Group - Universal	
MIMCMAgent	User	MIM CM Agent
MIMCMAuthAgent	User	CM Authorization Agent
MIMCMEnrollAgent	User	CM Enrollment Agent
MIMCM-HelpDesk	Security Group - Global	
MIMCMKRAgent	User	CM Key Recovery Agent
MIMCMManagerAg...	User	CM CA Manager Agent
MIMCM-Managers	Security Group - Universal	
MIMCMWebAgent	User	CM Web Pool Agent

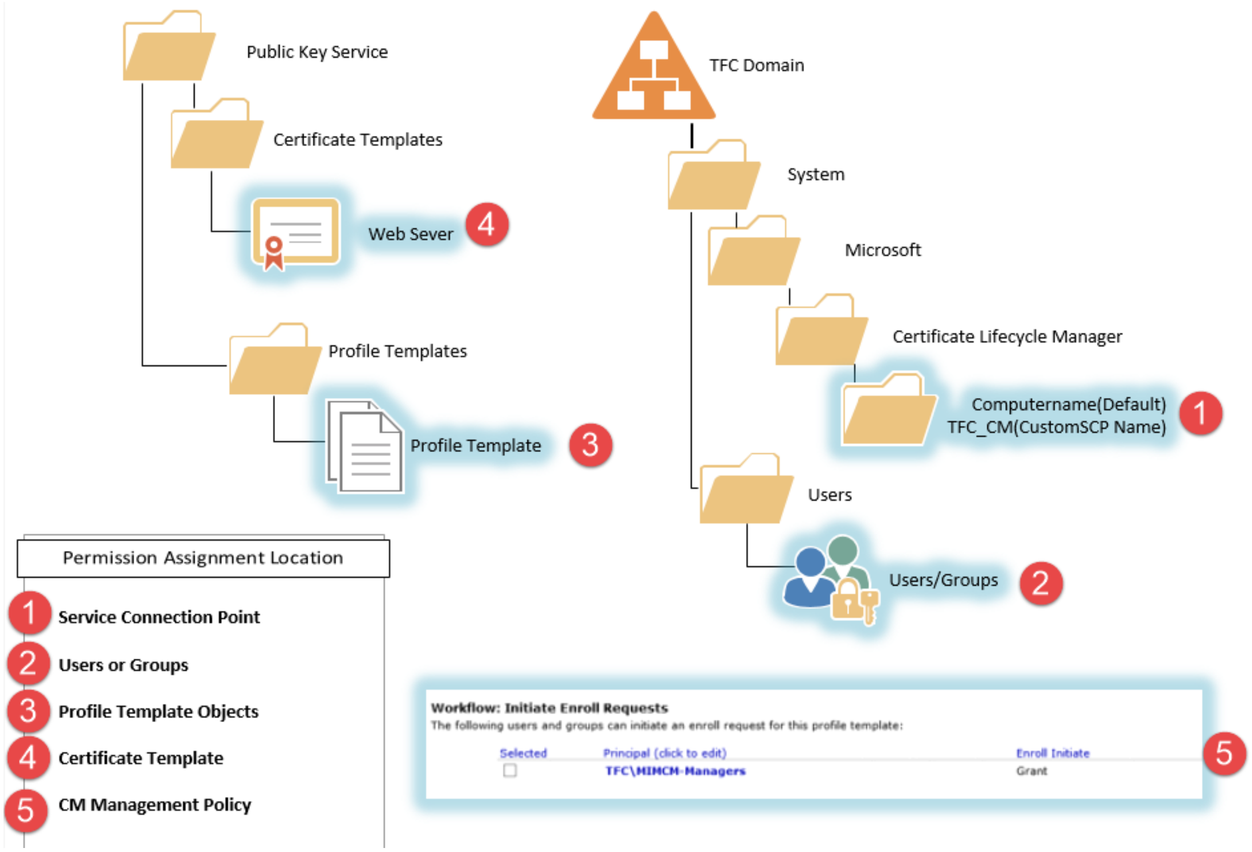


Configuration Properties

Valid Signing Certificates:

35e3df97527a0e10a11725a14fe1903157c8cebf

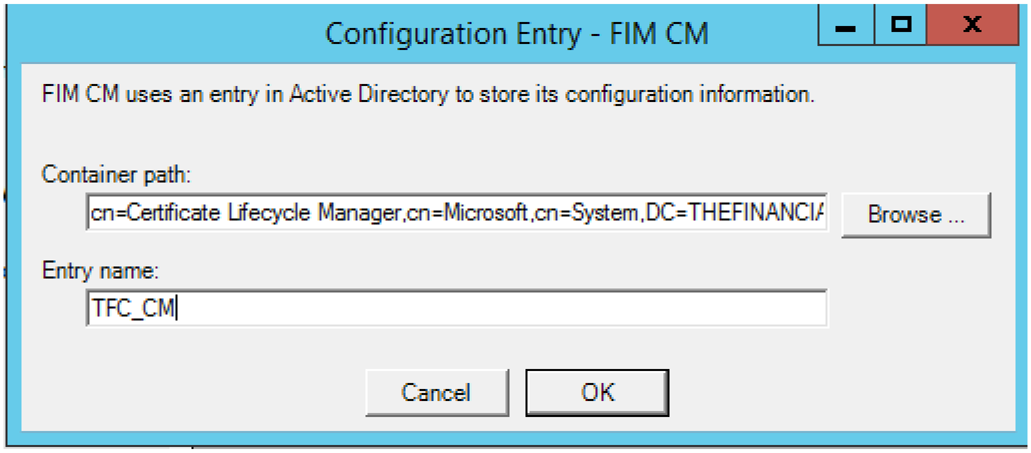




Workflow: Initiate Enroll Requests

The following users and groups can initiate an enroll request for this profile template:

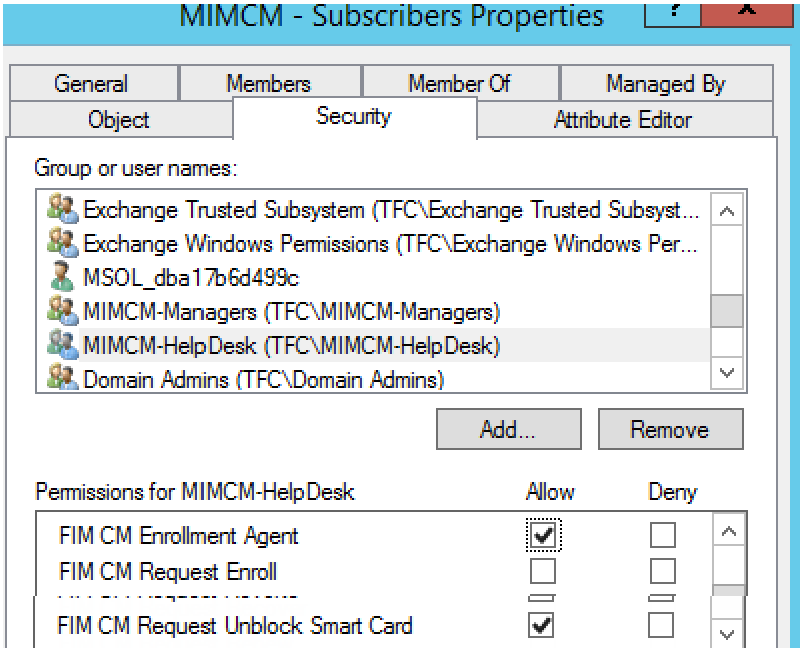
Selected	Principal (click to edit)	Enroll Initiate
□	**TFC\MIMCM-Managers**	Grant



FIM CM uses an entry in Active Directory to store its configuration information.

Container path:
cn=Certificate Lifecycle Manager,cn=Microsoft,cn=System,DC=THEFINANCIA

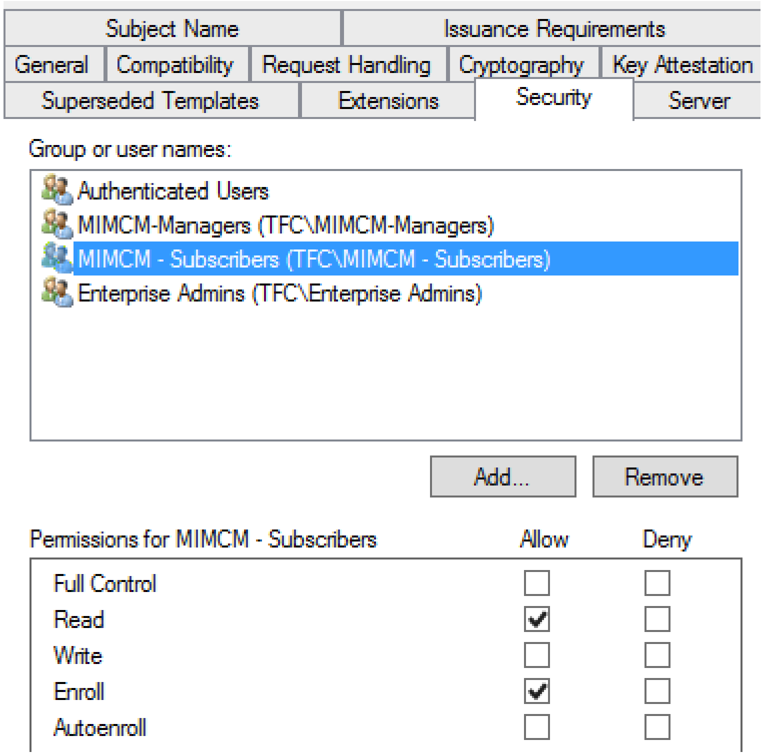
Entry name:
TFC_CM



Group or user names:

- Exchange Trusted Subsystem (TFC\Exchange Trusted Subsyst...
- Exchange Windows Permissions (TFC\Exchange Windows Per...
- MSOL_dba17b6d499c
- MIMCM-Managers (TFC\MIMCM-Managers)
- MIMCM-HelpDesk (TFC\MIMCM-HelpDesk)
- Domain Admins (TFC\Domain Admins)

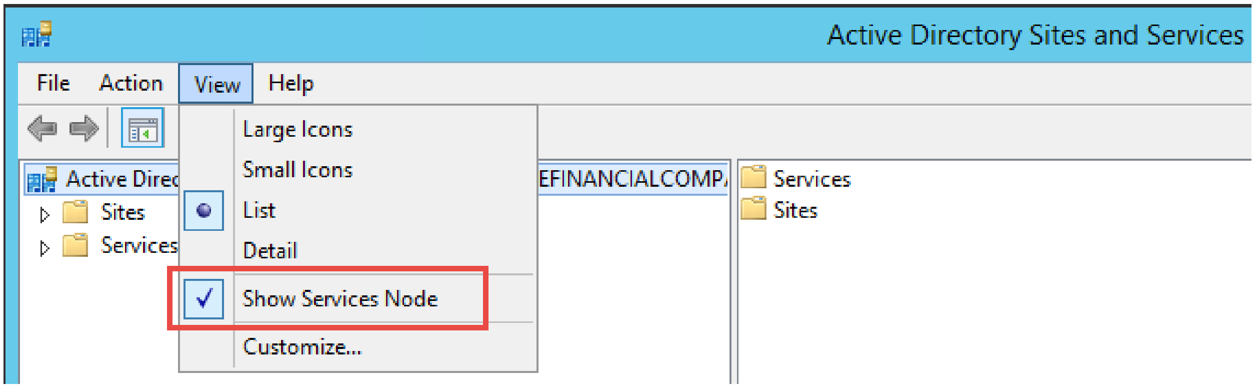
Permissions for MIMCM-HelpDesk	Allow	Deny
FIM CM Enrollment Agent	☑	□
FIM CM Request Enroll	□	□
FIM CM Request Unblock Smart Card	☑	□

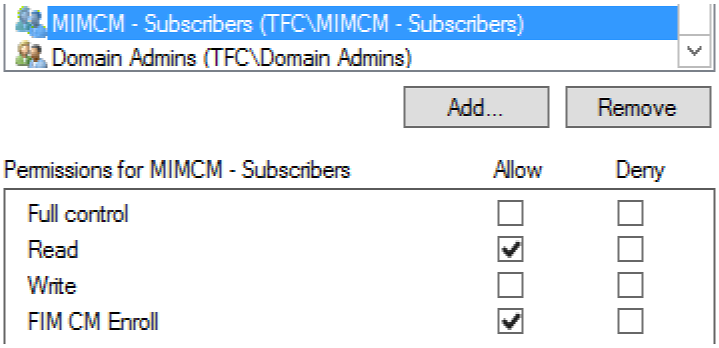


Group or user names:

- Authenticated Users
- MIMCM-Managers (TFC\MIMCM-Managers)
- MIMCM - Subscribers (TFC\MIMCM - Subscribers)
- Enterprise Admins (TFC\Enterprise Admins)

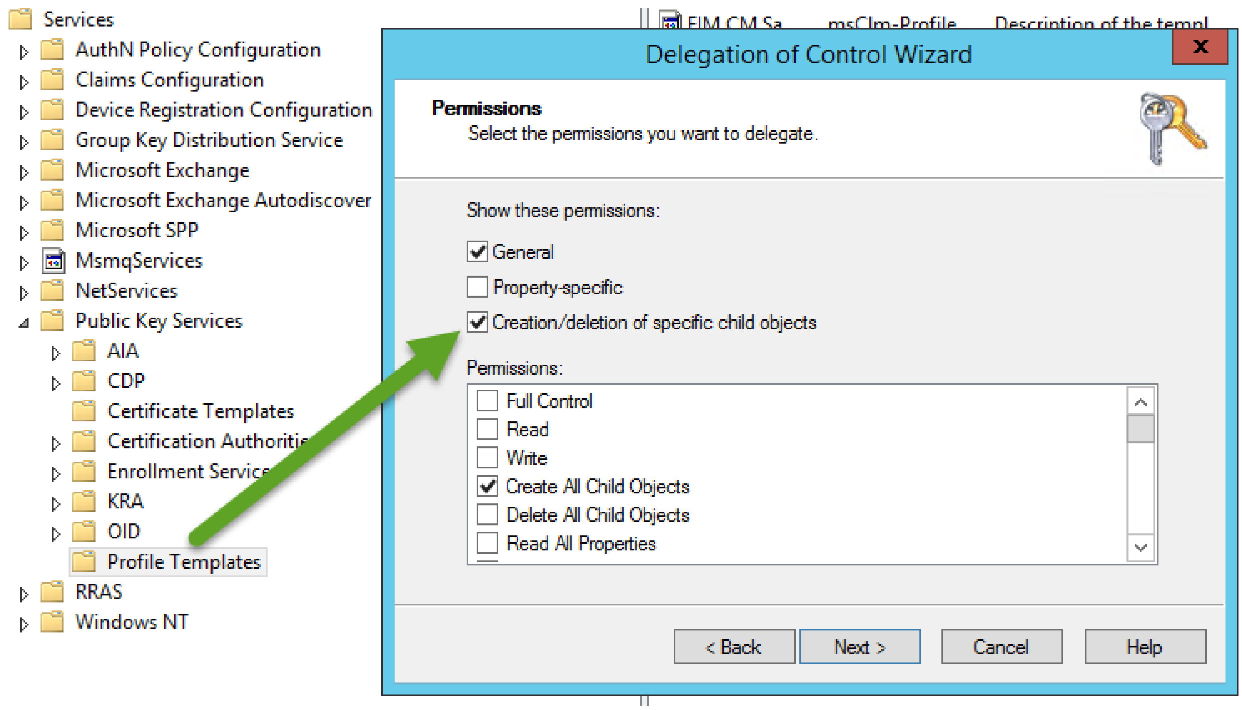
Permissions for MIMCM - Subscribers	Allow	Deny
Full Control	□	□
Read	☑	□
Write	□	□
Enroll	☑	□
Autoenroll	□	□





- MIMCM - Subscribers (TFC\MIMCM - Subscribers)
- Domain Admins (TFC\Domain Admins)

Permissions for MIMCM - Subscribers	Allow	Deny
Full control	□	□
Read	☑	□
Write	□	□
FIM CM Enroll	☑	□



- Services
  - AuthN Policy Configuration
  - Claims Configuration
  - Device Registration Configuration
  - Group Key Distribution Service
  - Microsoft Exchange
  - Microsoft Exchange Autodiscover
  - Microsoft SPP
  - MsmqServices
  - NetServices
  - Public Key Services
    - AIA
    - CDP
    - Certificate Templates
    - Certification Authoriti
    - Enrollment Service
    - KRA
    - OID
    - Profile Templates
  - RRAS
  - Windows NT

FIM CM Sa msClm-Profile Description of the templ

Delegation of Control Wizard

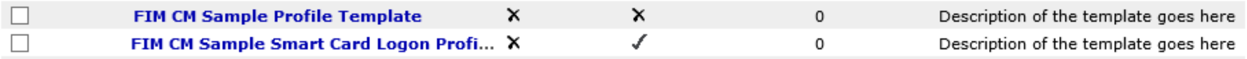
Permissions
Select the permissions you want to delegate.

Show these permissions:

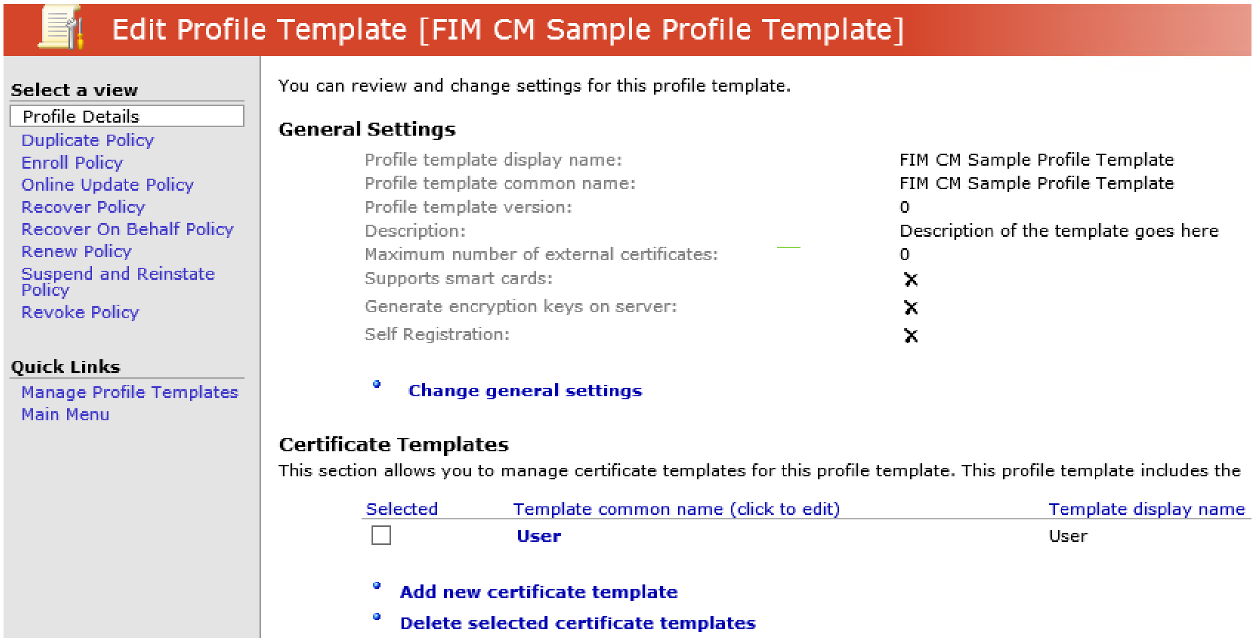
☑ General
☐ Property-specific
☑ Creation/deletion of specific child objects

Permissions:

☐ Full Control
☐ Read
☐ Write
☑ Create All Child Objects
☐ Delete All Child Objects
☐ Read All Properties



☐	FIM CM Sample Profile Template	✗	✗	0	Description of the template goes here
☐	FIM CM Sample Smart Card Logon Profi...	✗	✓	0	Description of the template goes here



Edit Profile Template [FIM CM Sample Profile Template]

Select a view

- Profile Details
- Duplicate Policy
- Enroll Policy
- Online Update Policy
- Recover Policy
- Recover On Behalf Policy
- Renew Policy
- Suspend and Reinstate Policy
- Revoke Policy

Quick Links

- Manage Profile Templates
- Main Menu

You can review and change settings for this profile template.

General Settings

Profile template display name:	FIM CM Sample Profile Template
Profile template common name:	FIM CM Sample Profile Template
Profile template version:	0
Description:	Description of the template goes here
Maximum number of external certificates:	0
Supports smart cards:	✗
Generate encryption keys on server:	✗
Self Registration:	✗

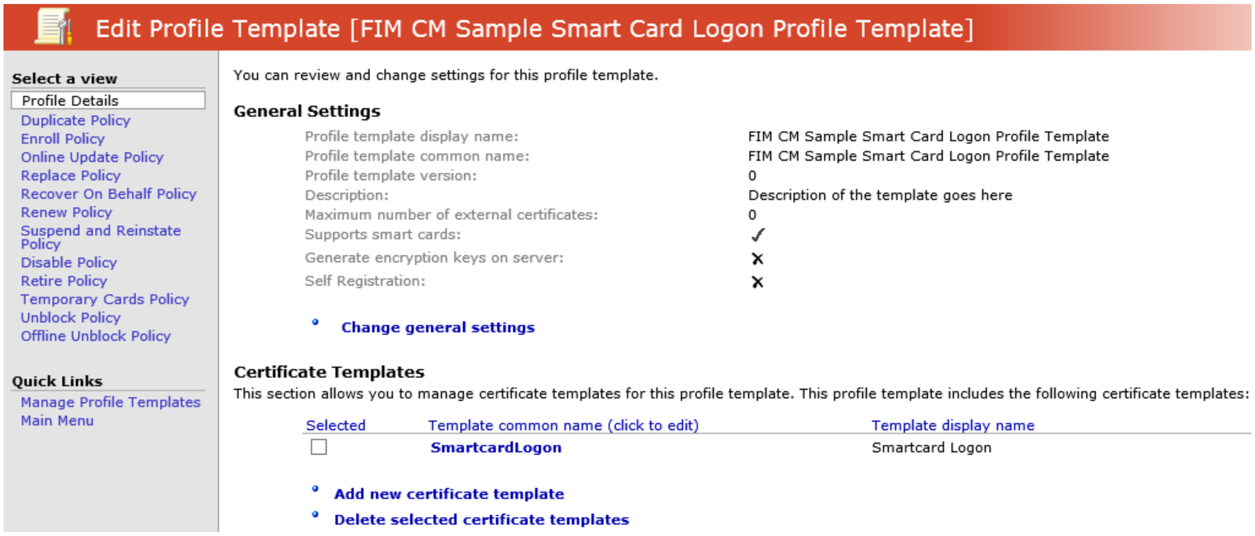
- **Change general settings**

Certificate Templates

This section allows you to manage certificate templates for this profile template. This profile template includes the

Selected	Template common name (click to edit)	Template display name
☐	**User**	User

- **Add new certificate template**
- **Delete selected certificate templates**



Edit Profile Template [FIM CM Sample Smart Card Logon Profile Template]

Select a view

- Profile Details
- Duplicate Policy
- Enroll Policy
- Online Update Policy
- Replace Policy
- Recover On Behalf Policy
- Renew Policy
- Suspend and Reinstate Policy
- Disable Policy
- Retire Policy
- Temporary Cards Policy
- Unblock Policy
- Offline Unblock Policy

Quick Links

- Manage Profile Templates
- Main Menu

You can review and change settings for this profile template.

General Settings

Profile template display name:	FIM CM Sample Smart Card Logon Profile Template
Profile template common name:	FIM CM Sample Smart Card Logon Profile Template
Profile template version:	0
Description:	Description of the template goes here
Maximum number of external certificates:	0
Supports smart cards:	✓
Generate encryption keys on server:	✗
Self Registration:	✗

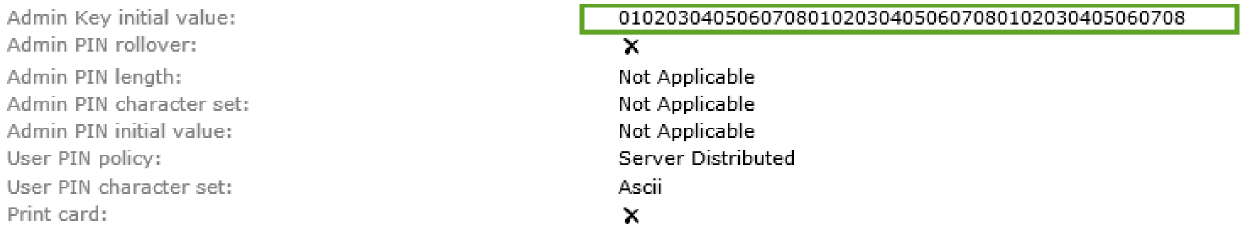
- **Change general settings**

Certificate Templates

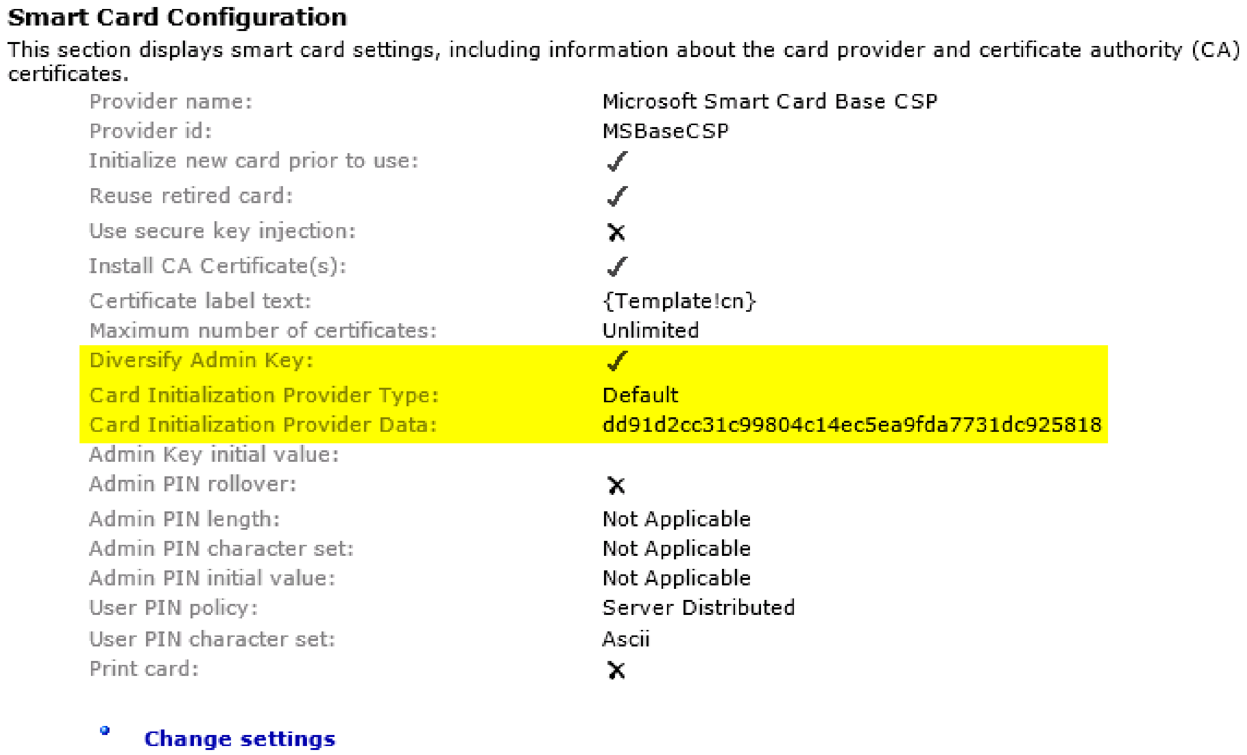
This section allows you to manage certificate templates for this profile template. This profile template includes the following certificate templates:

Selected	Template common name (click to edit)	Template display name
☐	**SmartcardLogon**	Smartcard Logon

- **Add new certificate template**
- **Delete selected certificate templates**



Admin Key initial value:	010203040506070801020304050607080102030405060708
Admin PIN rollover:	✗
Admin PIN length:	Not Applicable
Admin PIN character set:	Not Applicable
Admin PIN initial value:	Not Applicable
User PIN policy:	Server Distributed
User PIN character set:	Ascii
Print card:	✗



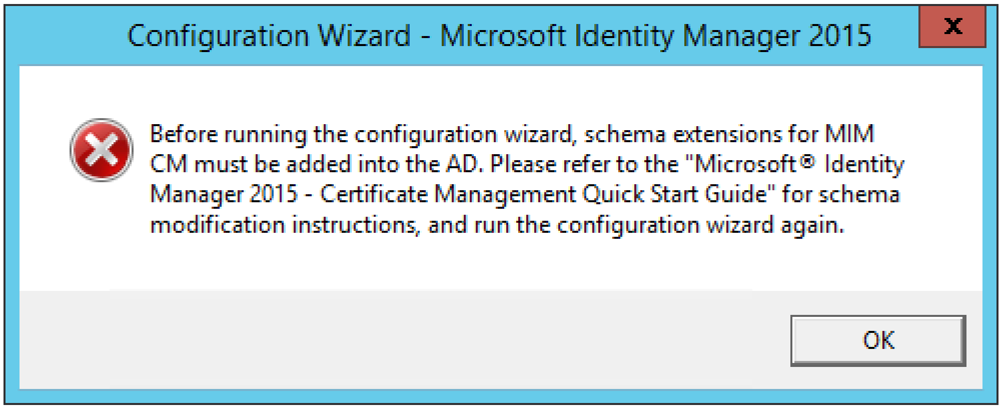
Smart Card Configuration

This section displays smart card settings, including information about the card provider and certificate authority (CA) certificates.

Provider name:	Microsoft Smart Card Base CSP
Provider id:	MSBaseCSP
Initialize new card prior to use:	✓
Reuse retired card:	✓
Use secure key injection:	✗
Install CA Certificate(s):	✓
Certificate label text:	{Template!cn}
Maximum number of certificates:	Unlimited
Diversify Admin Key:	✓
Card Initialization Provider Type:	Default
Card Initialization Provider Data:	dd91d2cc31c99804c14ec5ea9fda7731dc925818
Admin Key initial value:	
Admin PIN rollover:	✗
Admin PIN length:	Not Applicable
Admin PIN character set:	Not Applicable
Admin PIN initial value:	Not Applicable
User PIN policy:	Server Distributed
User PIN character set:	Ascii
Print card:	✗

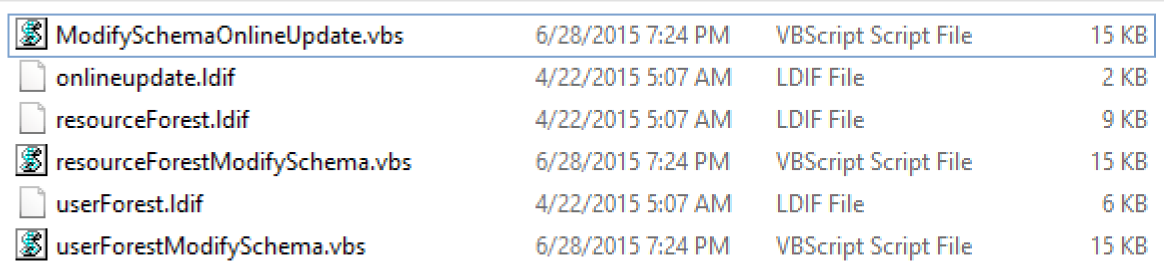
- **Change settings**

Chapter 11: Installation and the Client Side of Certificate Management

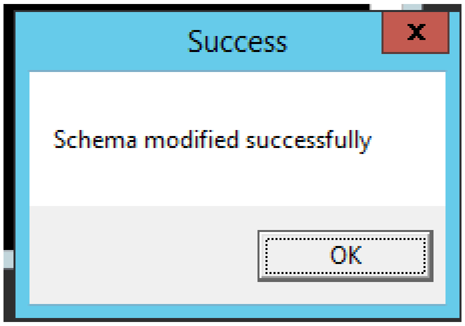


Configuration Wizard - Microsoft Identity Manager 2015

Before running the configuration wizard, schema extensions for MIM CM must be added into the AD. Please refer to the "Microsoft® Identity Manager 2015 - Certificate Management Quick Start Guide" for schema modification instructions, and run the configuration wizard again.

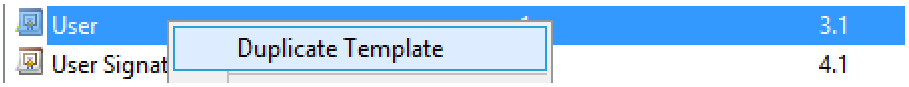


ModifySchemaOnlineUpdate.vbs	6/28/2015 7:24 PM	VBScript Script File	15 KB
onlineupdate.ldif	4/22/2015 5:07 AM	LDIF File	2 KB
resourceForest.ldif	4/22/2015 5:07 AM	LDIF File	9 KB
resourceForestModifySchema.vbs	6/28/2015 7:24 PM	VBScript Script File	15 KB
userForest.ldif	4/22/2015 5:07 AM	LDIF File	6 KB
userForestModifySchema.vbs	6/28/2015 7:24 PM	VBScript Script File	15 KB

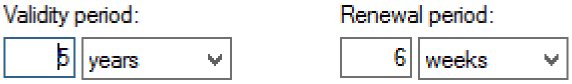


Success

Schema modified successfully

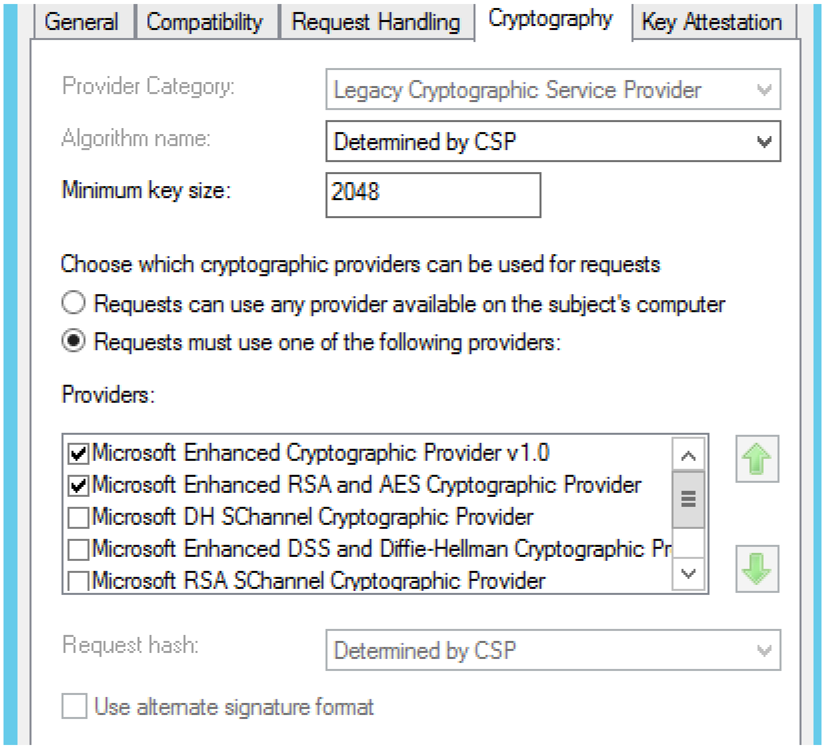


User	3.1
User Signat	4.1



Validity period: 5 years

Renewal period: 6 weeks



Provider Category: Legacy Cryptographic Service Provider

Algorithm name: Determined by CSP

Minimum key size: 2048

Choose which cryptographic providers can be used for requests

○ Requests can use any provider available on the subject's computer

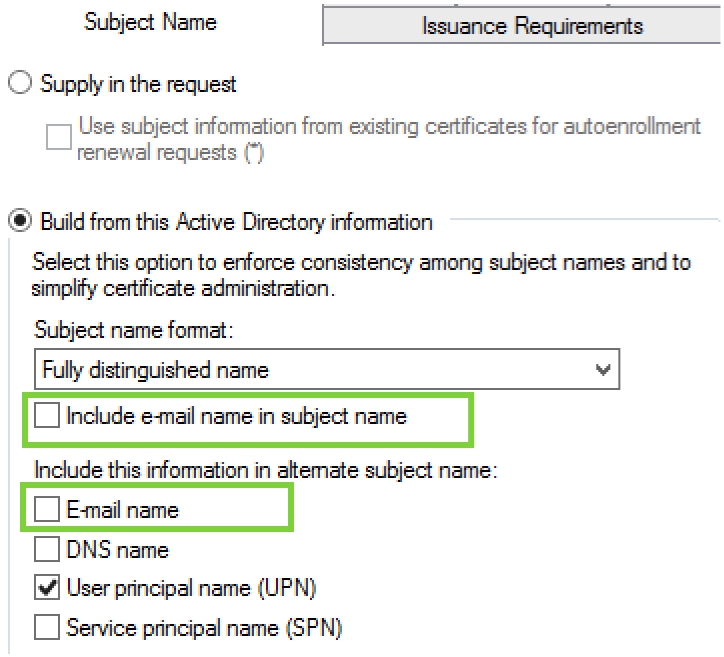
● Requests must use one of the following providers:

Providers:

☑ Microsoft Enhanced Cryptographic Provider v1.0
☑ Microsoft Enhanced RSA and AES Cryptographic Provider
☐ Microsoft DH SChannel Cryptographic Provider
☐ Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Pr
☐ Microsoft RSA SChannel Cryptographic Provider

Request hash: Determined by CSP

☐ Use alternate signature format



○ Supply in the request

☐ Use subject information from existing certificates for autoenrollment renewal requests (*)

● Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

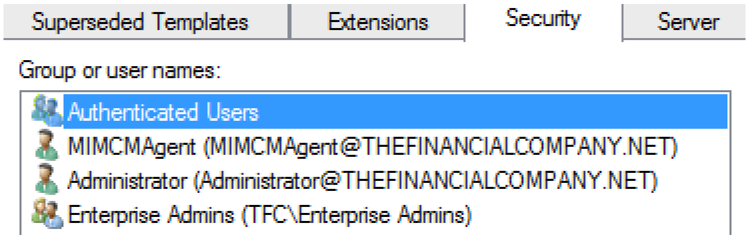
Subject name format:

Fully distinguished name

☐ Include e-mail name in subject name

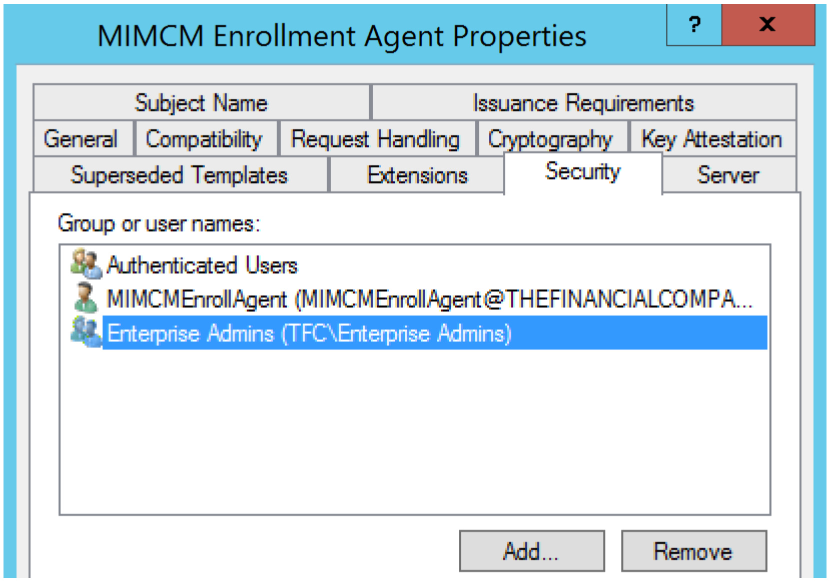
Include this information in alternate subject name:

☐ E-mail name
☐ DNS name
☑ User principal name (UPN)
☐ Service principal name (SPN)



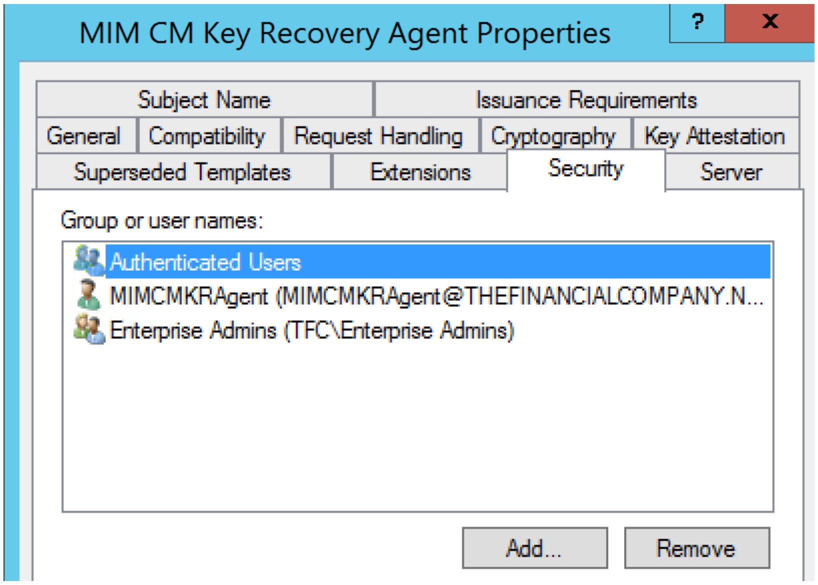
Group or user names:

Authenticated Users
MIMCMAgent (MIMCMAgent@THEFINANCIALCOMPANY.NET)
Administrator (Administrator@THEFINANCIALCOMPANY.NET)
Enterprise Admins (TFC\Enterprise Admins)



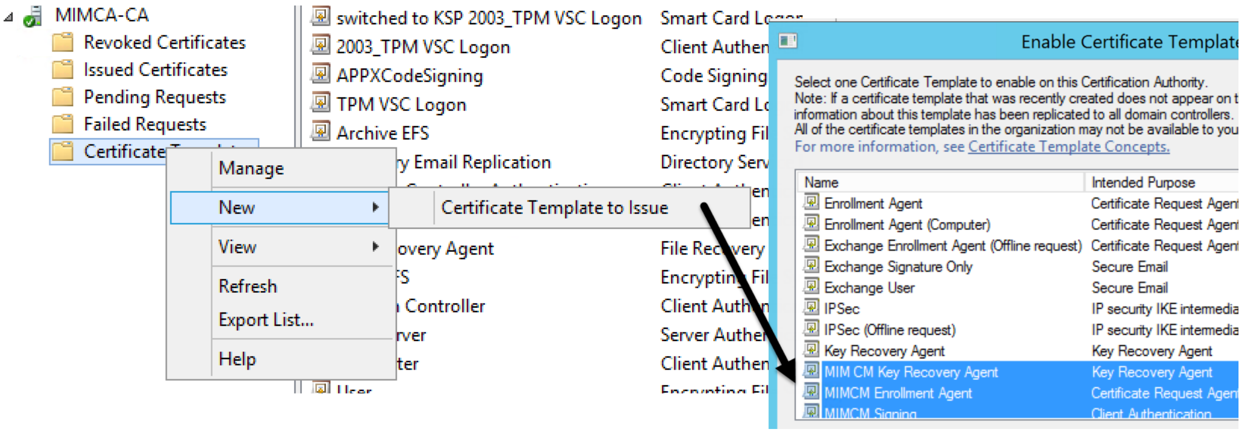
Group or user names:

- Authenticated Users
- MIMCMEnrollAgent (MIMCMEnrollAgent@THEFINANCIALCOMPA...
- Enterprise Admins (TFC\Enterprise Admins)



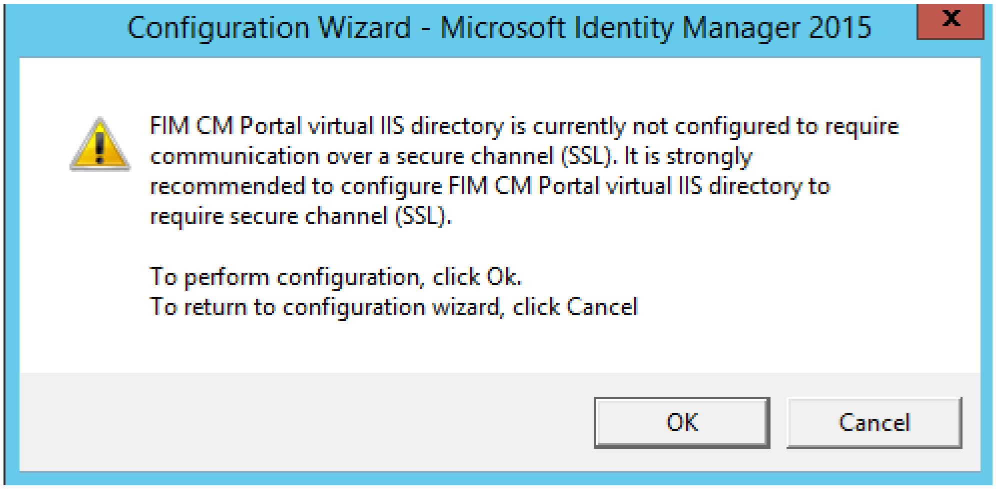
Group or user names:

- Authenticated Users
- MIMCMKRAgent (MIMCMKRAgent@THEFINANCIALCOMPANY.N...
- Enterprise Admins (TFC\Enterprise Admins)



Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on t
information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to you
For more information, see Certificate Template Concepts.

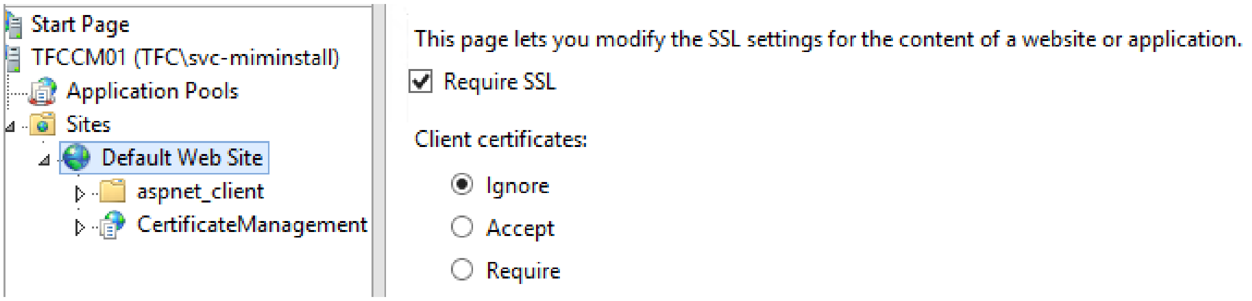
Name	Intended Purpose
Enrollment Agent	Certificate Request Agent
Enrollment Agent (Computer)	Certificate Request Agent
Exchange Enrollment Agent (Offline request)	Certificate Request Agent
Exchange Signature Only	Secure Email
Exchange User	Secure Email
IPSec	IP security IKE intermedia
IPSec (Offline request)	IP security IKE intermedia
Key Recovery Agent	Key Recovery Agent
MIM CM Key Recovery Agent	Key Recovery Agent
MIMCM Enrollment Agent	Certificate Request Agent
MIMCM Signing	Client Authentication



Configuration Wizard - Microsoft Identity Manager 2015

FIM CM Portal virtual IIS directory is currently not configured to require communication over a secure channel (SSL). It is strongly recommended to configure FIM CM Portal virtual IIS directory to require secure channel (SSL).

To perform configuration, click Ok.
To return to configuration wizard, click Cancel

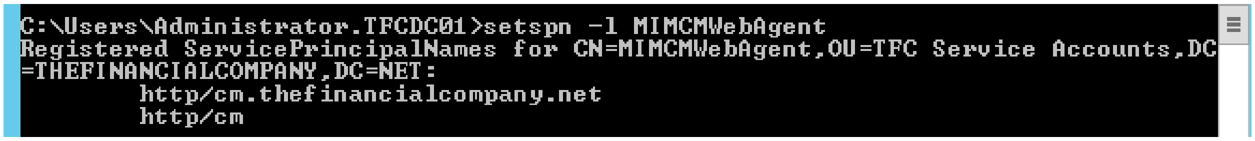


This page lets you modify the SSL settings for the content of a website or application.

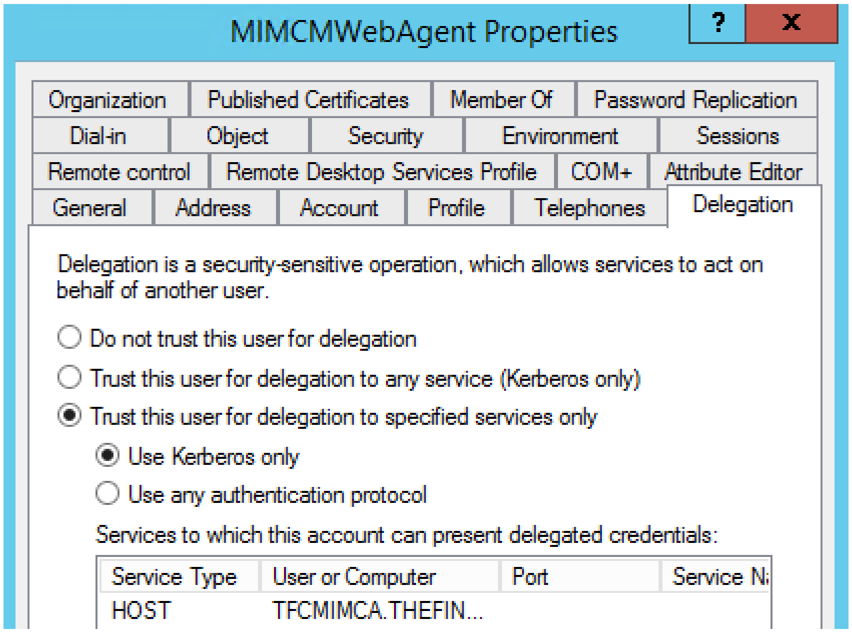
☑ Require SSL

Client certificates:

● Ignore
○ Accept
○ Require



```
C:\Users\Administrator.TFCDC01>setspn -l MIMCMWebAgent
Registered ServicePrincipalNames for CN=MIMCMWebAgent,OU=TFC Service Accounts,DC
=THEFINANCIALCOMPANY,DC=NET:
        http/cm.thefinancialcompany.net
        http/cm
```



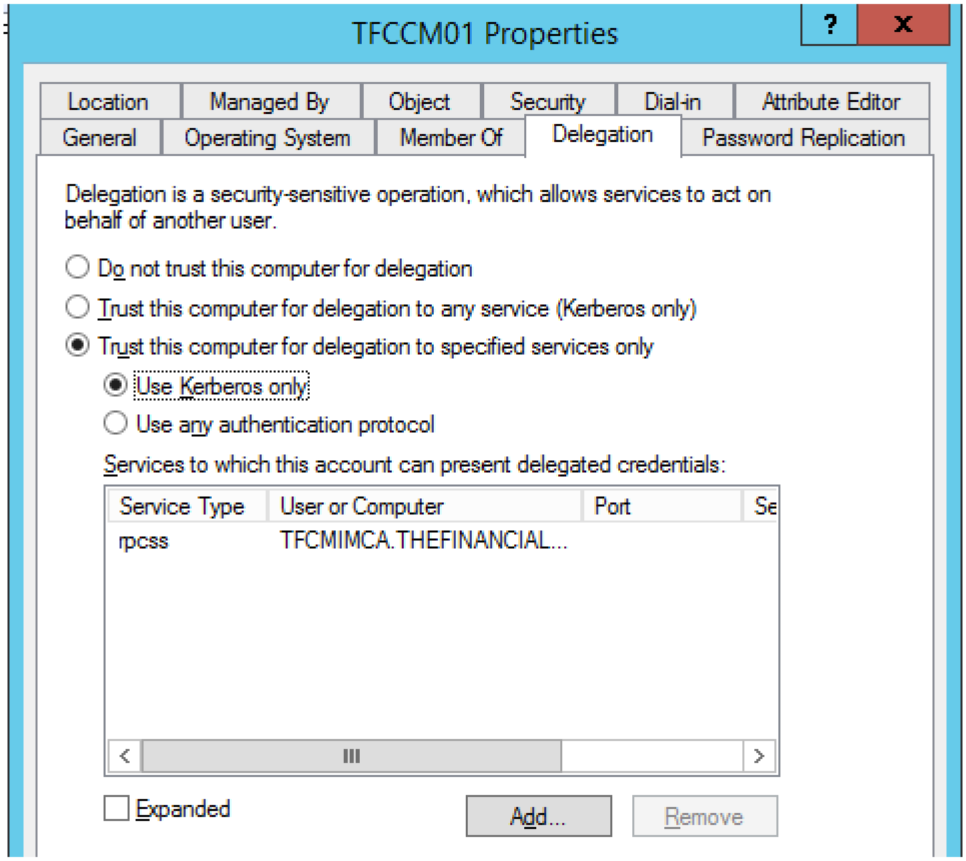
MIMCMWebAgent Properties

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

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service N
HOST	TFCMIMCA.THEFIN...		



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

○ Do not trust this computer for delegation

○ Trust this computer for delegation to any service (Kerberos only)

● Trust this computer for delegation to specified services only

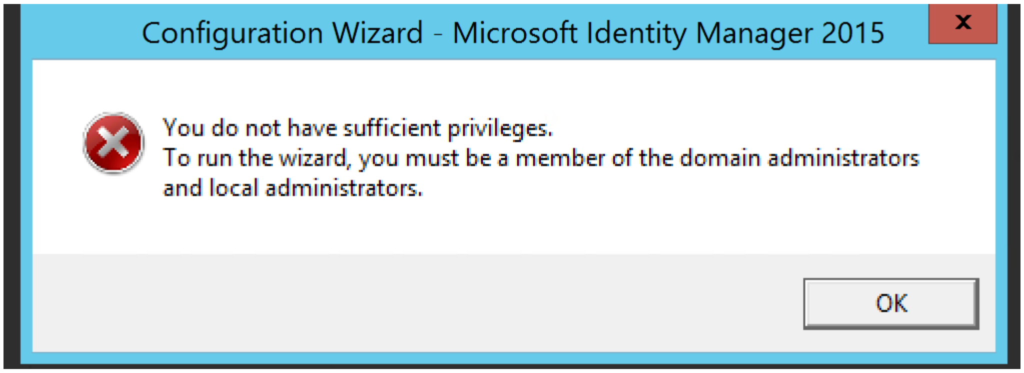
● Use Kerberos only

○ Use any authentication protocol

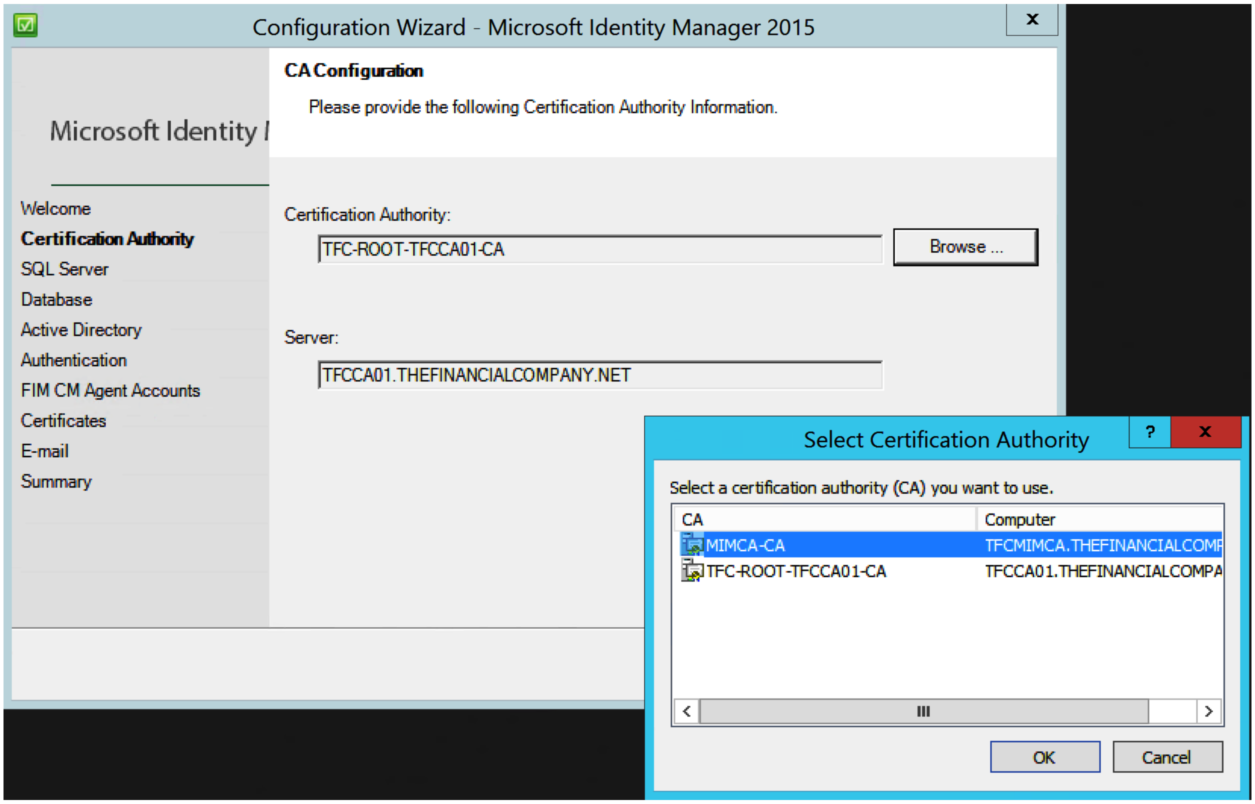
Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Se
rpcss	TFCMIMCA.THEFINANCIAL...		

□ Expanded



You do not have sufficient privileges.
To run the wizard, you must be a member of the domain administrators and local administrators.



Configuration Wizard - Microsoft Identity Manager 2015

CA Configuration

Please provide the following Certification Authority Information.

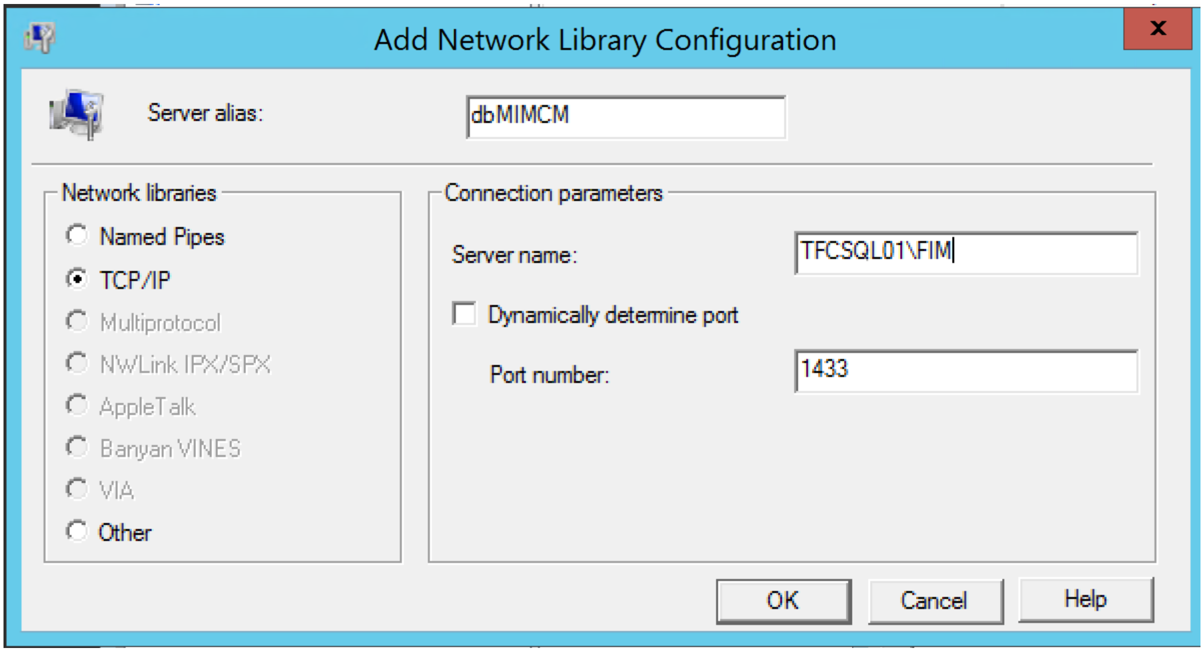
Certification Authority: TFC-ROOT-TFCCA01-CA

Server: TFCCA01.THEFINANCIALCOMPANY.NET

Select Certification Authority

Select a certification authority (CA) you want to use.

CA	Computer
MIMCA-CA	TFCMIMCA.THEFINANCIALCOMP
TFC-ROOT-TFCCA01-CA	TFCCA01.THEFINANCIALCOMPA



Add Network Library Configuration

Server alias: dbMIMCM

Network libraries

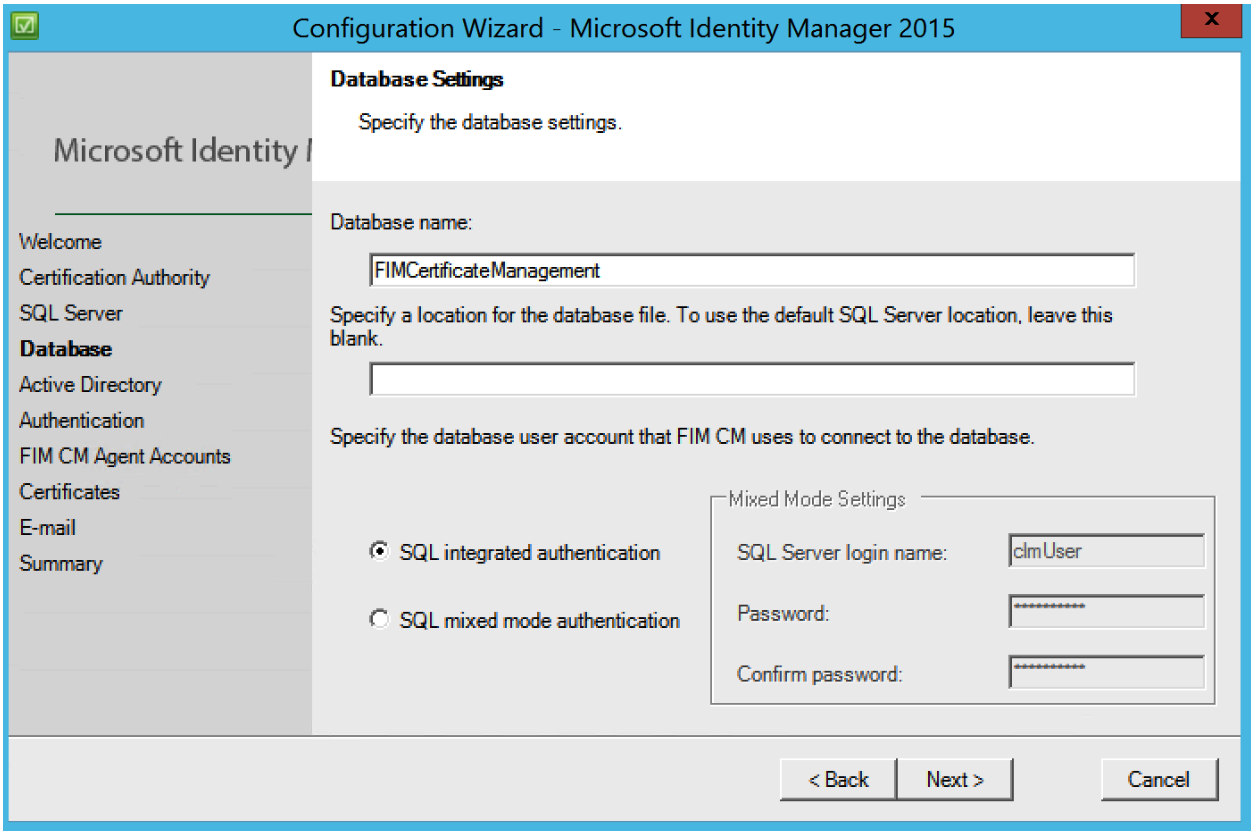
- ○ Named Pipes
- ● TCP/IP
- ○ Multiprotocol
- ○ NWLink IPX/SPX
- ○ AppleTalk
- ○ Banyan VINES
- ○ VIA
- ○ Other

Connection parameters

Server name: TFCSQL01\FIM

□ Dynamically determine port

Port number: 1433



Database Settings

Specify the database settings.

Database name:

FIMCertificateManagement

Specify a location for the database file. To use the default SQL Server location, leave this blank.

Specify the database user account that FIM CM uses to connect to the database.

● SQL integrated authentication

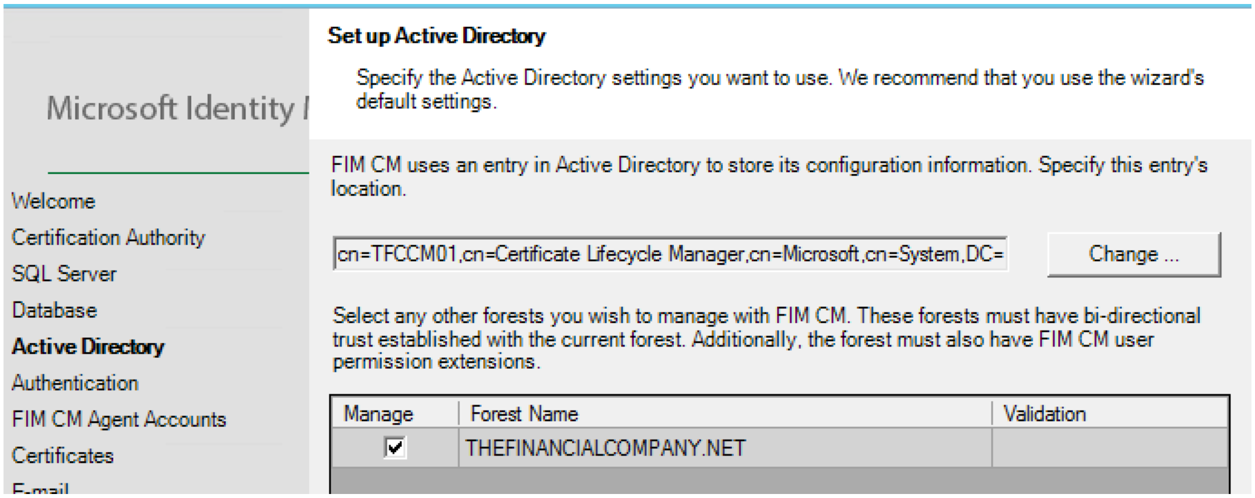
○ SQL mixed mode authentication

Mixed Mode Settings

SQL Server login name: clmUser

Password: ***********

Confirm password: ***********



Set up Active Directory

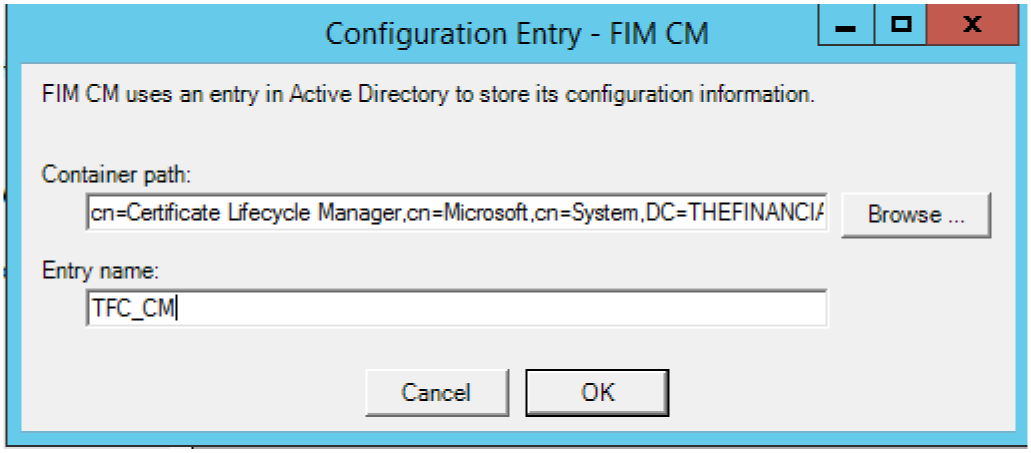
Specify the Active Directory settings you want to use. We recommend that you use the wizard's default settings.

FIM CM uses an entry in Active Directory to store its configuration information. Specify this entry's location.

cn=TFCCM01,cn=Certificate Lifecycle Manager,cn=Microsoft,cn=System,DC=

Select any other forests you wish to manage with FIM CM. These forests must have bi-directional trust established with the current forest. Additionally, the forest must also have FIM CM user permission extensions.

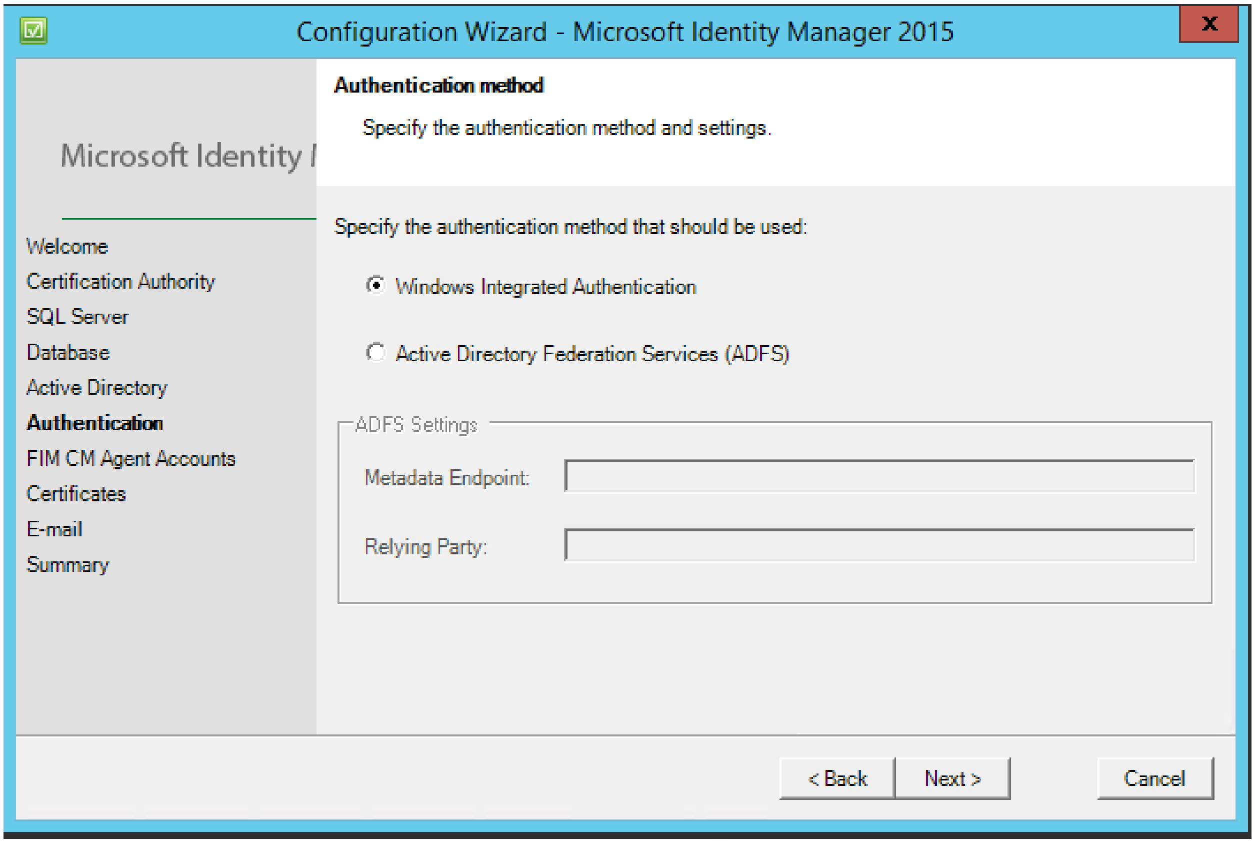
Manage	Forest Name	Validation
☑	THEFINANCIALCOMPANY.NET	



FIM CM uses an entry in Active Directory to store its configuration information.

Container path: cn=Certificate Lifecycle Manager,cn=Microsoft,cn=System,DC=THEFINANCI/

Entry name: TFC_CM



Authentication method

Specify the authentication method and settings.

Specify the authentication method that should be used:

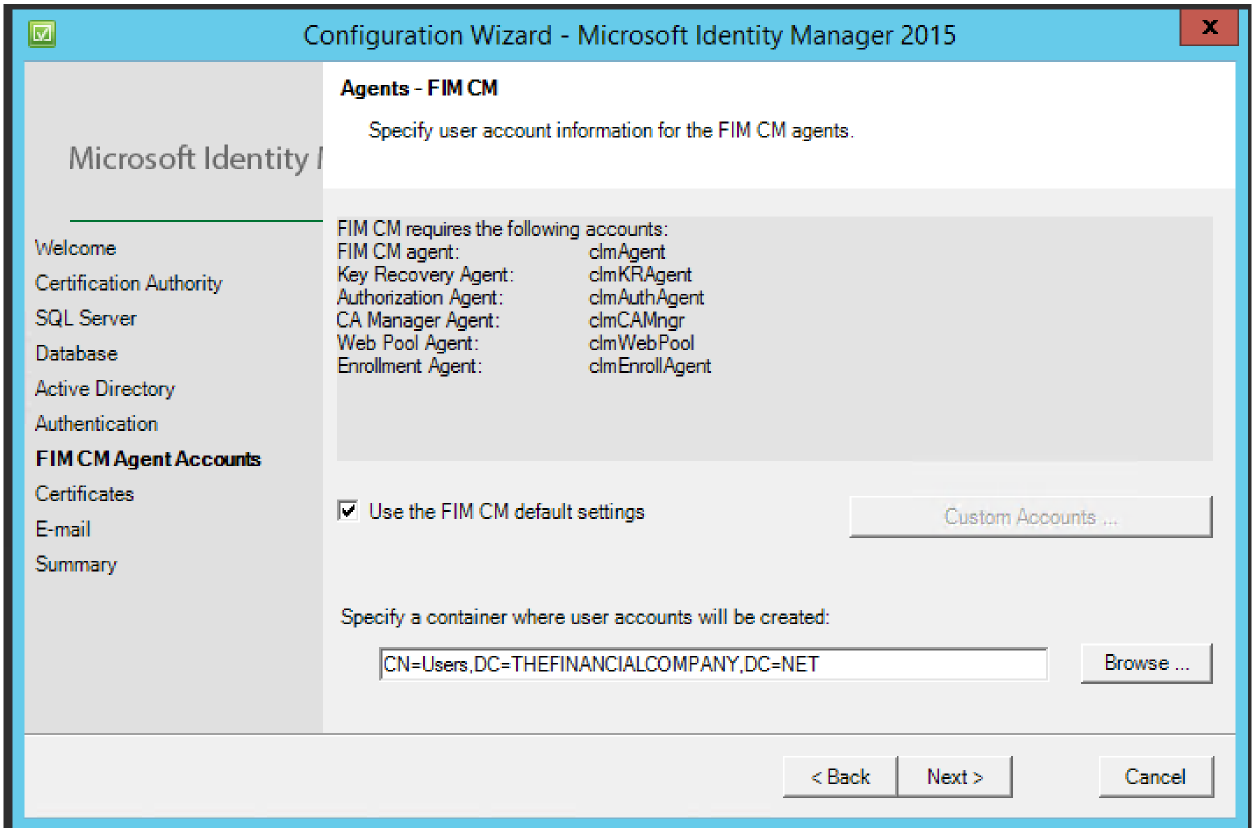
● Windows Integrated Authentication

○ Active Directory Federation Services (ADFS)

ADFS Settings

Metadata Endpoint:

Relying Party:



Configuration Wizard - Microsoft Identity Manager 2015

Agents - FIM CM

Specify user account information for the FIM CM agents.

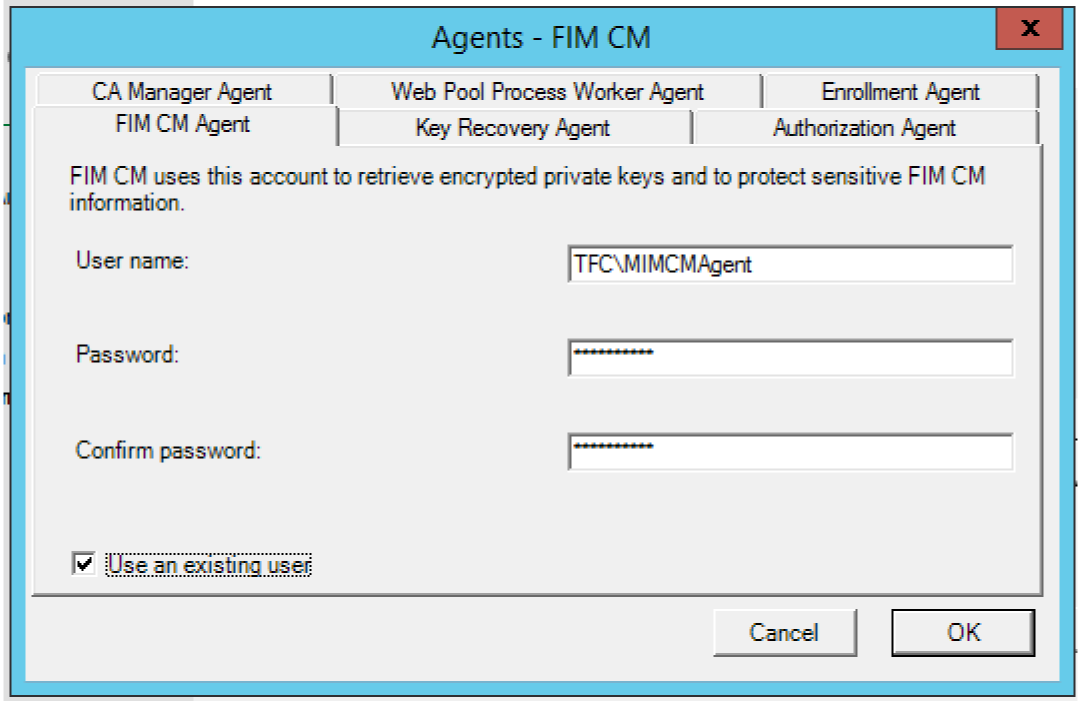
FIM CM requires the following accounts:

FIM CM agent:	clmAgent
Key Recovery Agent:	clmKRAgent
Authorization Agent:	clmAuthAgent
CA Manager Agent:	clmCAMngr
Web Pool Agent:	clmWebPool
Enrollment Agent:	clmEnrollAgent

☑ Use the FIM CM default settings

Specify a container where user accounts will be created:

CN=Users,DC=THEFINANCIALCOMPANY,DC=NET



Agents - FIM CM

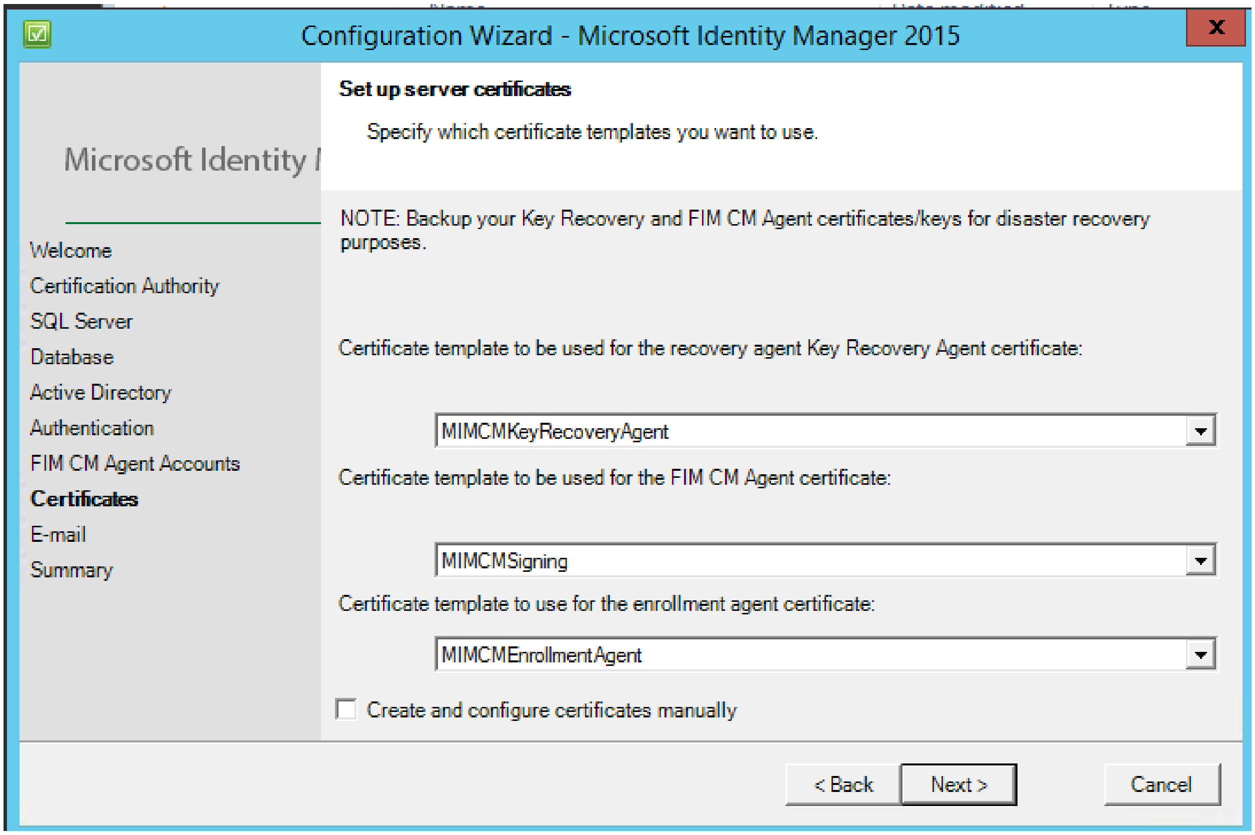
FIM CM uses this account to retrieve encrypted private keys and to protect sensitive FIM CM information.

User name: TFC\MIMCMAgent

Password: ***********

Confirm password: ***********

☑ Use an existing user



Set up server certificates

Specify which certificate templates you want to use.

NOTE: Backup your Key Recovery and FIM CM Agent certificates/keys for disaster recovery purposes.

Certificate template to be used for the recovery agent Key Recovery Agent certificate:

MIMCMKeyRecoveryAgent

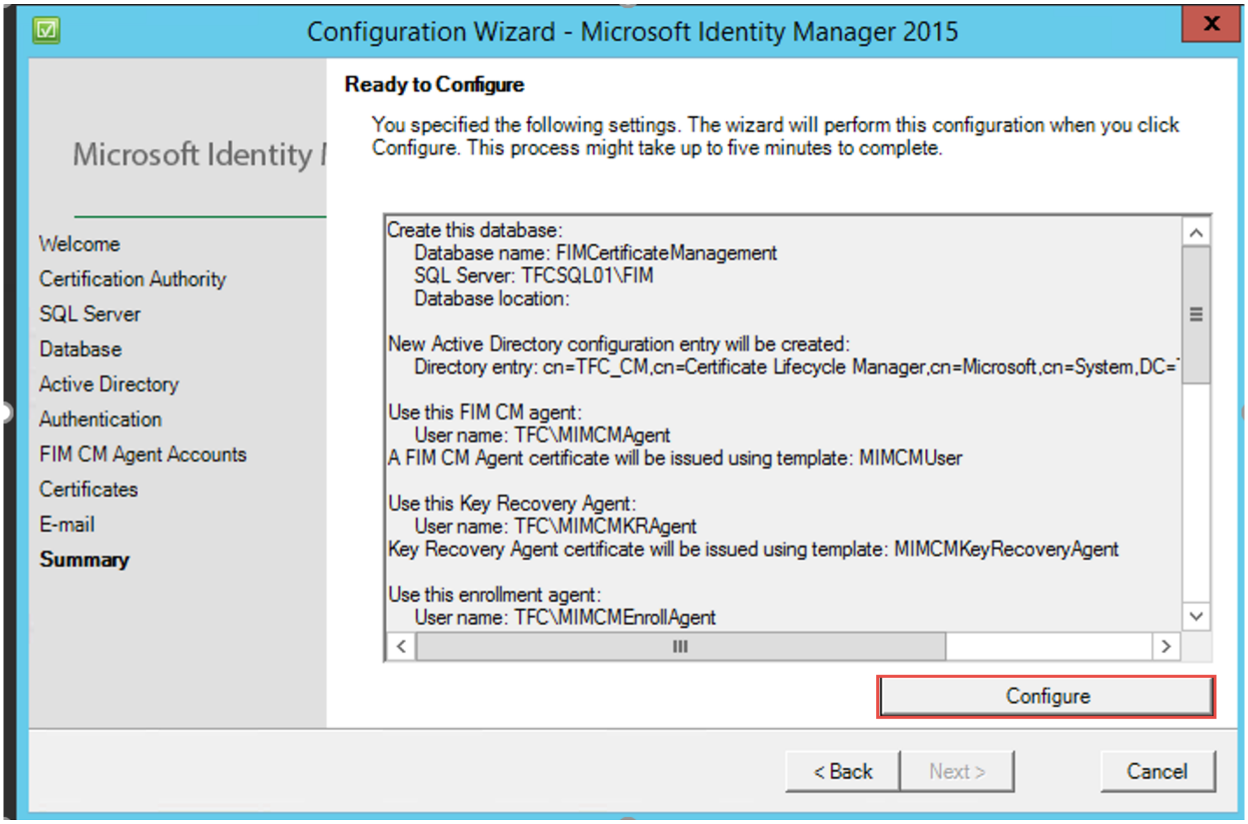
Certificate template to be used for the FIM CM Agent certificate:

MIMCMSigning

Certificate template to use for the enrollment agent certificate:

MIMCMEnrollmentAgent

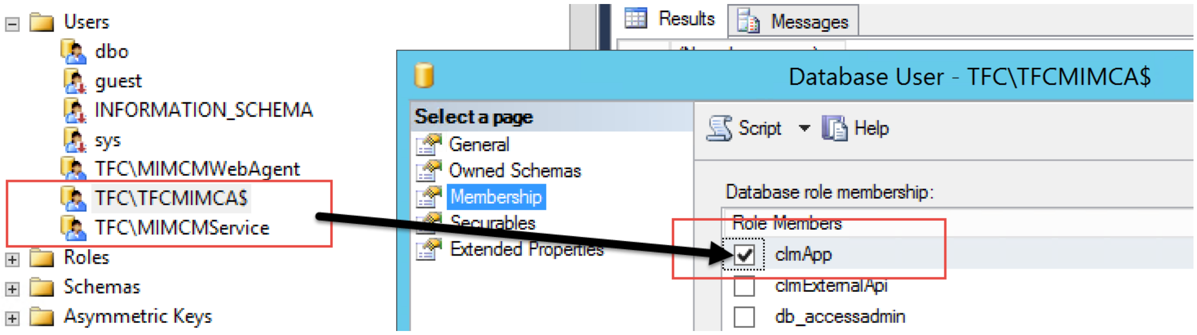
□ Create and configure certificates manually



Ready to Configure

You specified the following settings. The wizard will perform this configuration when you click Configure. This process might take up to five minutes to complete.

```
Create this database:
    Database name: FIMCertificateManagement
    SQL Server: TFCSQL01\FIM
    Database location:

New Active Directory configuration entry will be created:
    Directory entry: cn=TFC_CM,cn=Certificate Lifecycle Manager,cn=Microsoft,cn=System,DC=

Use this FIM CM agent:
    User name: TFC\MIMCMAgent
A FIM CM Agent certificate will be issued using template: MIMCMUser

Use this Key Recovery Agent:
    User name: TFC\MIMCMKRAgent
Key Recovery Agent certificate will be issued using template: MIMCMKeyRecoveryAgent

Use this enrollment agent:
    User name: TFC\MIMCMEnrollAgent
```



Users
- dbo
- guest
- INFORMATION_SCHEMA
- sys
- TFC\MIMCMWebAgent
- TFC\TFCMIMCA$
- TFC\MIMCMService

Roles

Schemas

Asymmetric Keys

Results | Messages

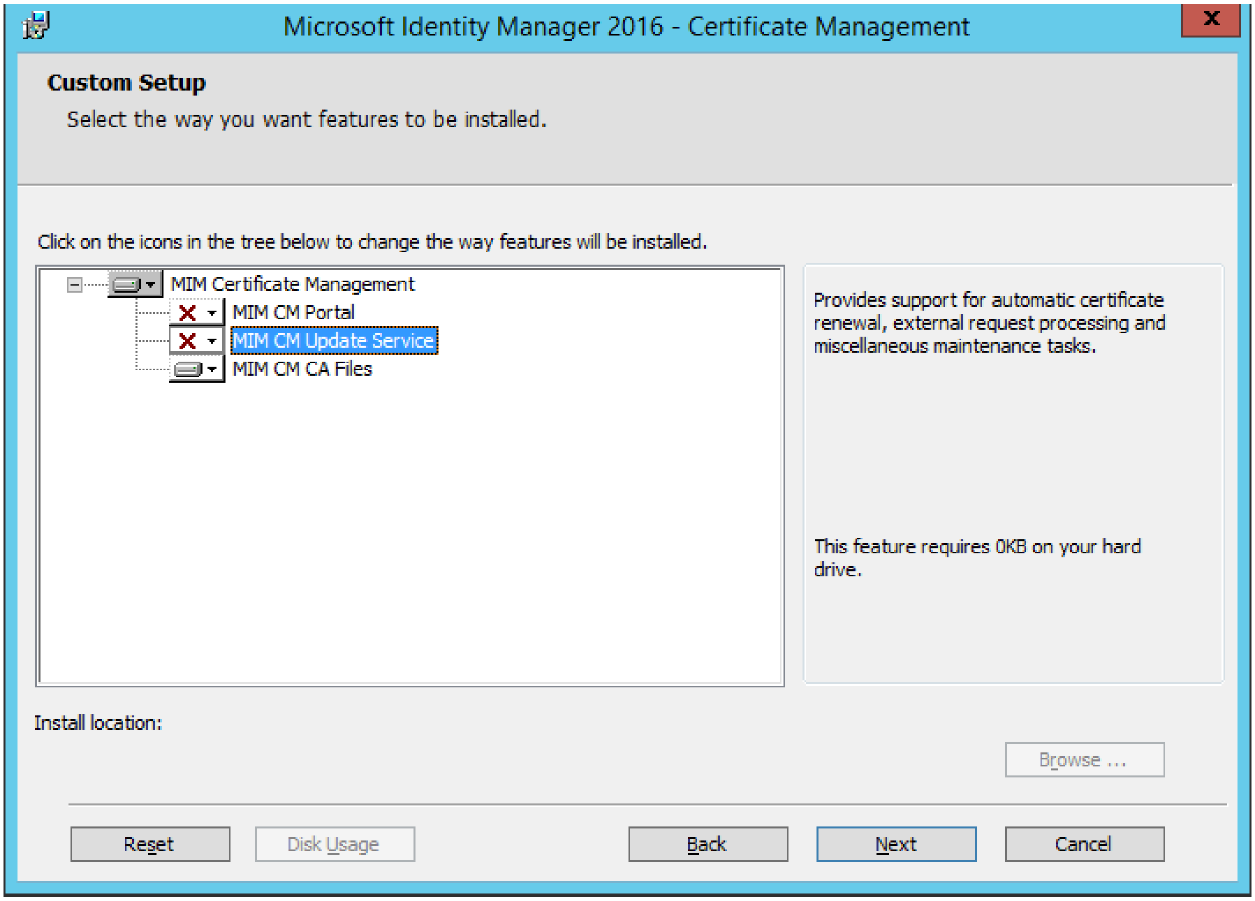
Database User - TFC\TFCMIMCA$

Select a page
- General
- Owned Schemas
- Membership
- Securables
- Extended Properties

Script | Help

Database role membership:

Role Members
- ☑ clmApp
- □ clmExternalApi
- □ db_accessadmin



Microsoft Identity Manager 2016 - Certificate Management

Custom Setup

Select the way you want features to be installed.

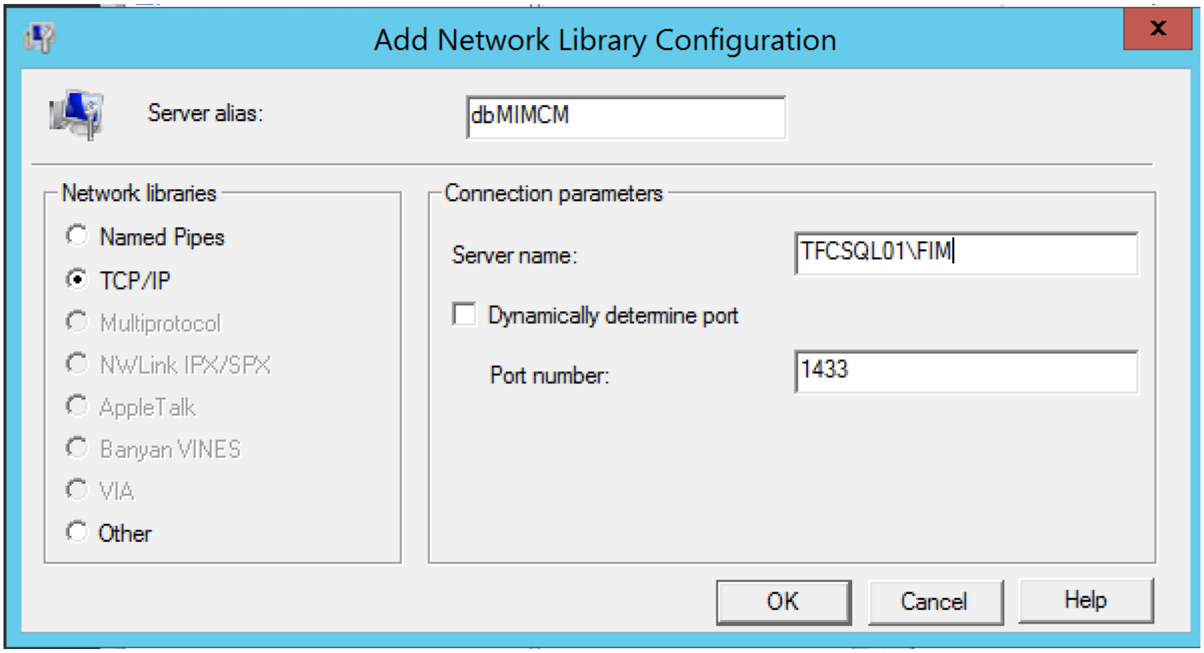
Click on the icons in the tree below to change the way features will be installed.

- MIM Certificate Management
  - ☒ MIM CM Portal
  - ☒ MIM CM Update Service
  - MIM CM CA Files

Provides support for automatic certificate renewal, external request processing and miscellaneous maintenance tasks.

This feature requires 0KB on your hard drive.

Install location:



Add Network Library Configuration

Server alias: dbMIMCM

Network libraries

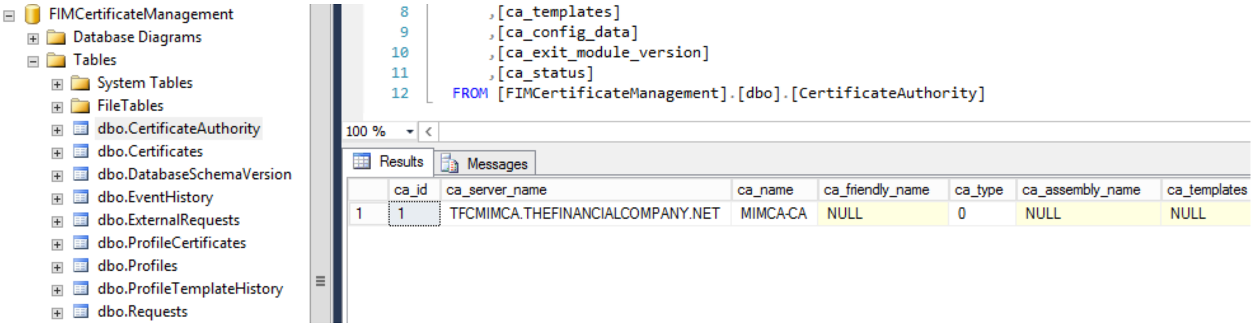
- ○ Named Pipes
- ● TCP/IP
- ○ Multiprotocol
- ○ NWLink IPX/SPX
- ○ AppleTalk
- ○ Banyan VINES
- ○ VIA
- ○ Other

Connection parameters

Server name: TFCSQL01\FIM

□ Dynamically determine port

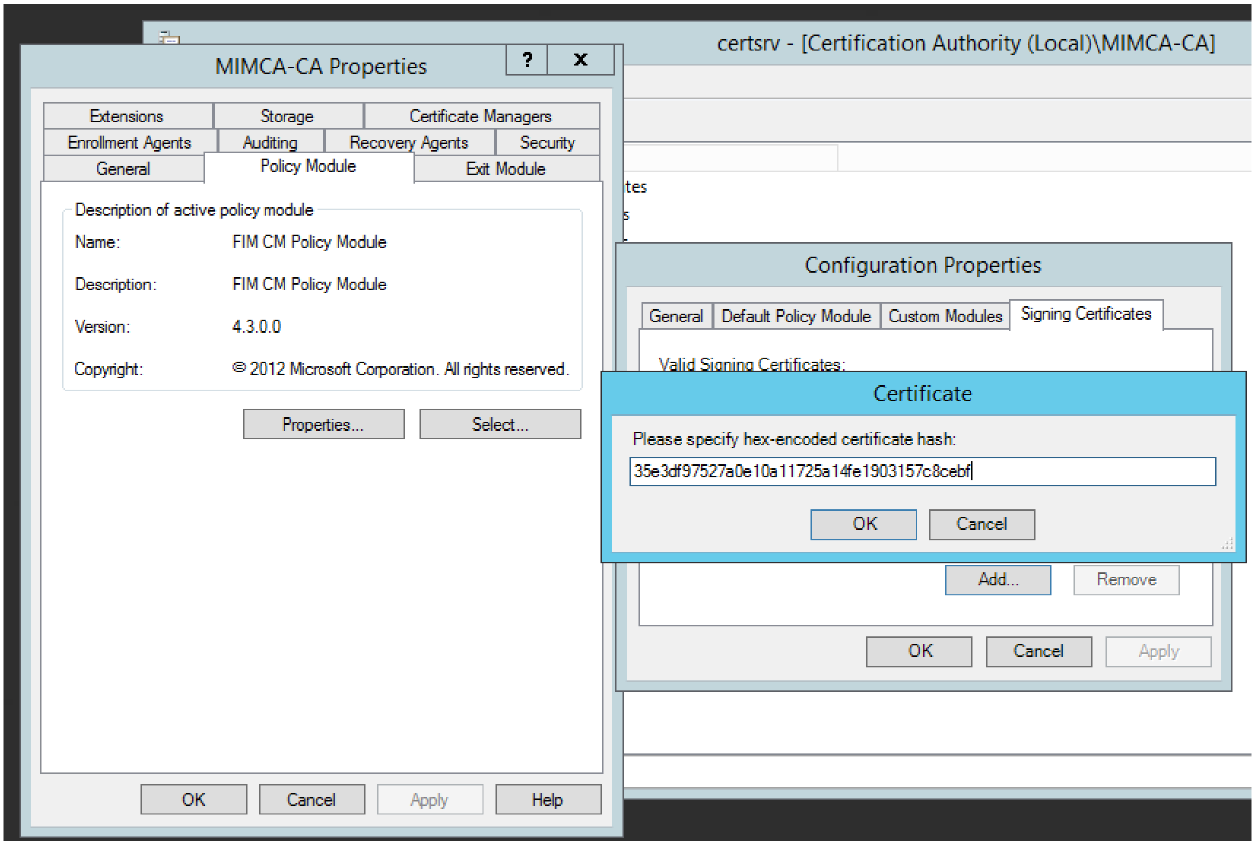
Port number: 1433



```
FIMCertificateManagement
  Database Diagrams
  Tables
    System Tables
    FileTables
    dbo.CertificateAuthority
    dbo.Certificates
    dbo.DatabaseSchemaVersion
    dbo.EventHistory
    dbo.ExternalRequests
    dbo.ProfileCertificates
    dbo.Profiles
    dbo.ProfileTemplateHistory
    dbo.Requests
```

```
      ,[ca_templates]
      ,[ca_config_data]
      ,[ca_exit_module_version]
      ,[ca_status]
  FROM [FIMCertificateManagement].[dbo].[CertificateAuthority]
```

	ca_id	ca_server_name	ca_name	ca_friendly_name	ca_type	ca_assembly_name	ca_templates
1	1	TFCMIMCA.THEFINANCIALCOMPANY.NET	MIMCA-CA	NULL	0	NULL	NULL



Description of active policy module

Name: FIM CM Policy Module

Description: FIM CM Policy Module

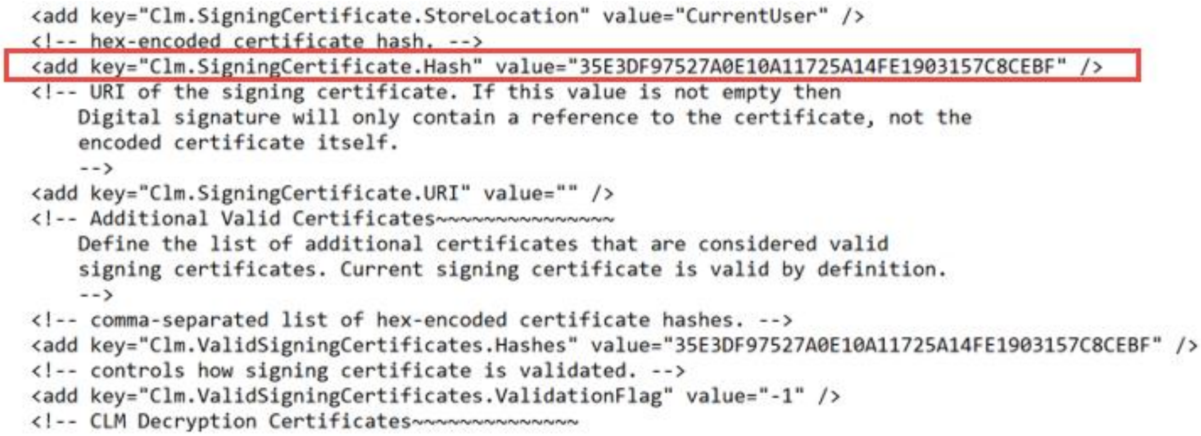
Version: 4.3.0.0

Copyright: © 2012 Microsoft Corporation. All rights reserved.

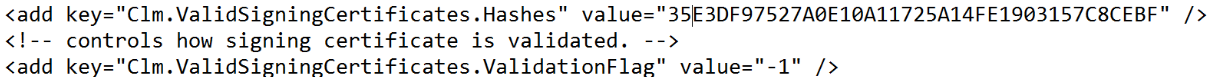
Valid Signing Certificates:

Please specify hex-encoded certificate hash:

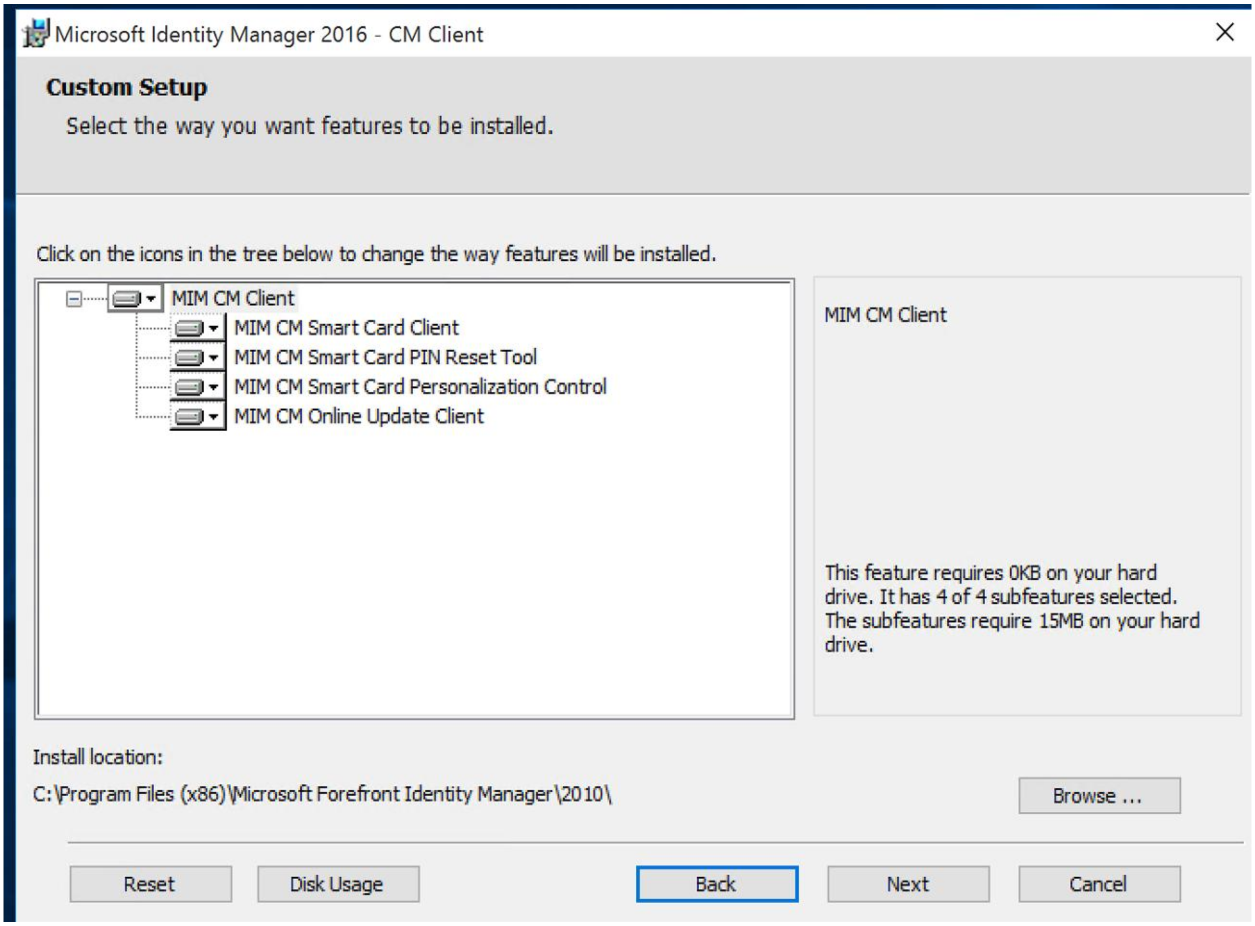
35e3df97527a0e10a11725a14fe1903157c8cebf



```
<add key="Clm.SigningCertificate.StoreLocation" value="CurrentUser" />
<!-- hex-encoded certificate hash. -->
<add key="Clm.SigningCertificate.Hash" value="35E3DF97527A0E10A11725A14FE1903157C8CEBF" />
<!-- URI of the signing certificate. If this value is not empty then
    Digital signature will only contain a reference to the certificate, not the
    encoded certificate itself.
    -->
<add key="Clm.SigningCertificate.URI" value="" />
<!-- Additional Valid Certificates~~~~~~~~~~~~~~~
    Define the list of additional certificates that are considered valid
    signing certificates. Current signing certificate is valid by definition.
    -->
<!-- comma-separated list of hex-encoded certificate hashes. -->
<add key="Clm.ValidSigningCertificates.Hashes" value="35E3DF97527A0E10A11725A14FE1903157C8CEBF" />
<!-- controls how signing certificate is validated. -->
<add key="Clm.ValidSigningCertificates.ValidationFlag" value="-1" />
<!-- CLM Decryption Certificates~~~~~~~~~~~~~~~
```



```
<add key="Clm.ValidSigningCertificates.Hashes" value="35E3DF97527A0E10A11725A14FE1903157C8CEBF" />
<!-- controls how signing certificate is validated. -->
<add key="Clm.ValidSigningCertificates.ValidationFlag" value="-1" />
```



Microsoft Identity Manager 2016 - CM Client

Custom Setup

Select the way you want features to be installed.

Click on the icons in the tree below to change the way features will be installed.

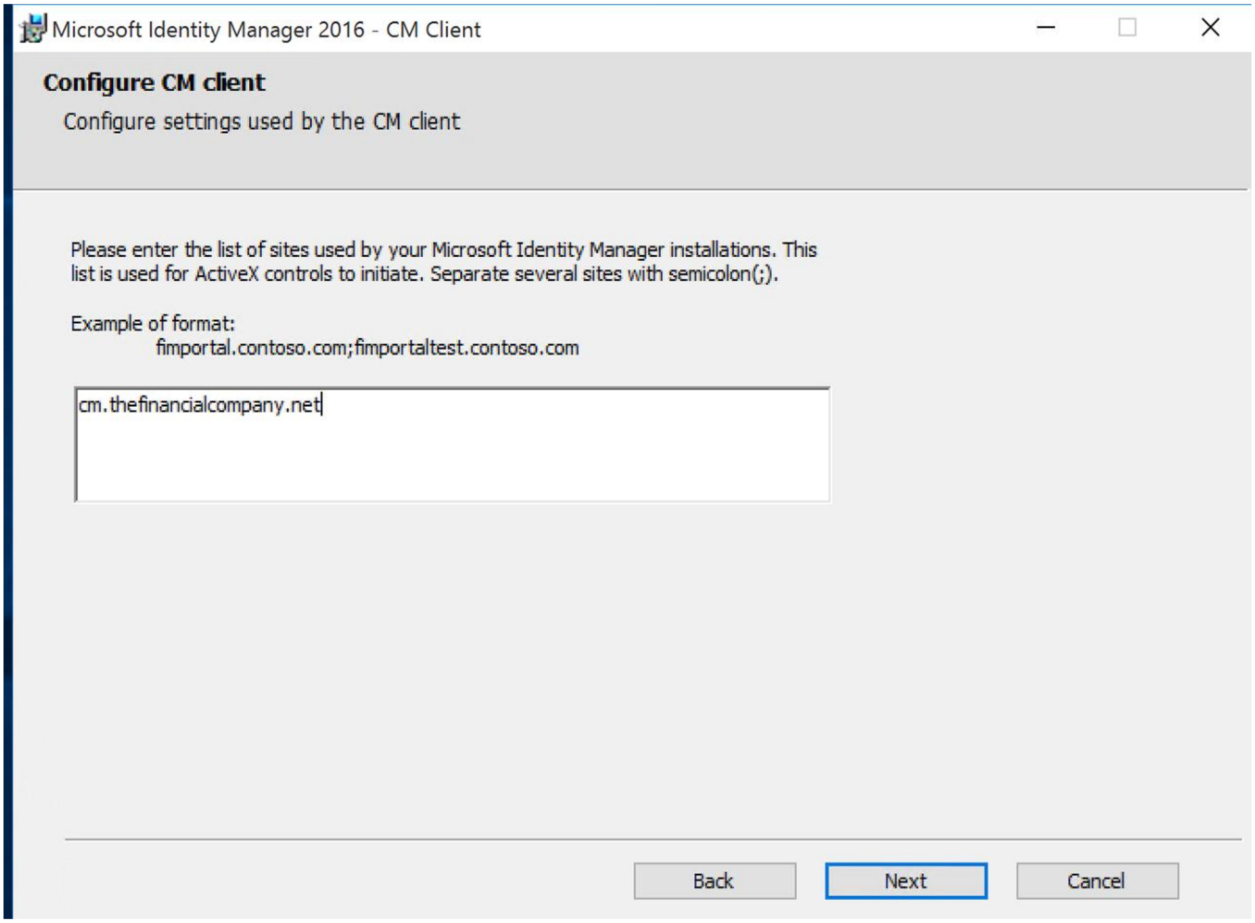
- MIM CM Client
  - MIM CM Smart Card Client
  - MIM CM Smart Card PIN Reset Tool
  - MIM CM Smart Card Personalization Control
  - MIM CM Online Update Client

MIM CM Client

This feature requires 0KB on your hard drive. It has 4 of 4 subfeatures selected. The subfeatures require 15MB on your hard drive.

Install location:

C:\Program Files (x86)\Microsoft Forefront Identity Manager\2010\



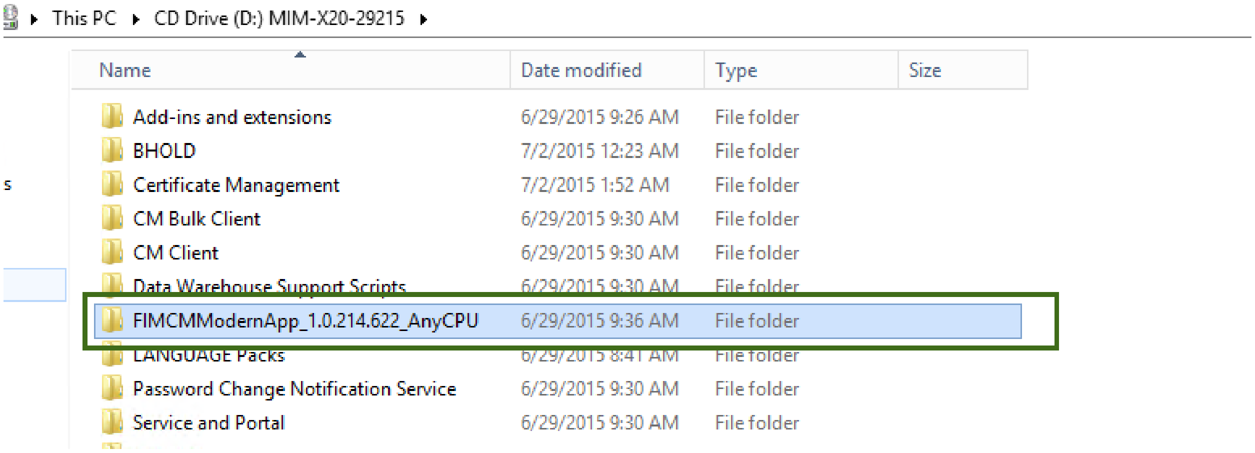
Configure CM client

Configure settings used by the CM client

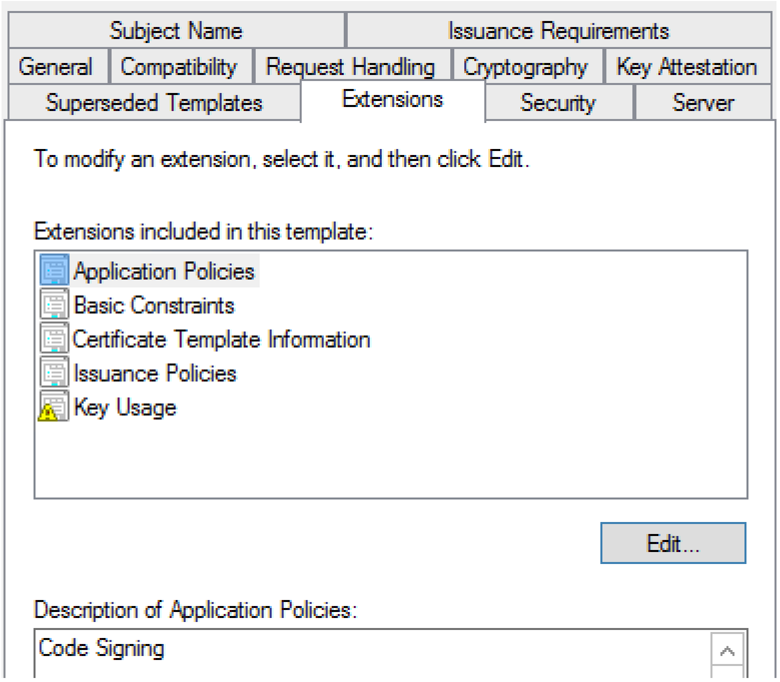
Please enter the list of sites used by your Microsoft Identity Manager installations. This list is used for ActiveX controls to initiate. Separate several sites with semicolon(;).

Example of format:
fimportal.contoso.com;fimportaltest.contoso.com

cm.thefinancialcompany.net



Name	Date modified	Type	Size
Add-ins and extensions	6/29/2015 9:26 AM	File folder	
BHOLD	7/2/2015 12:23 AM	File folder	
Certificate Management	7/2/2015 1:52 AM	File folder	
CM Bulk Client	6/29/2015 9:30 AM	File folder	
CM Client	6/29/2015 9:30 AM	File folder	
Data Warehouse Support Scripts	6/29/2015 9:30 AM	File folder	
FIMCMModernApp_1.0.214.622_AnyCPU	6/29/2015 9:36 AM	File folder	
LANGUAGE Packs	6/29/2015 8:41 AM	File folder	
Password Change Notification Service	6/29/2015 9:30 AM	File folder	
Service and Portal	6/29/2015 9:30 AM	File folder	



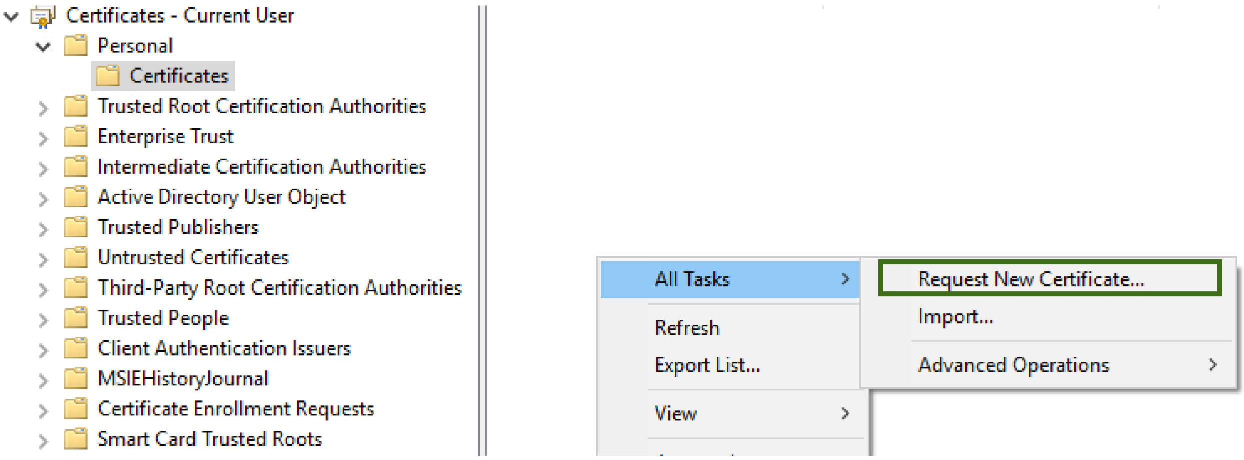
To modify an extension, select it, and then click Edit.

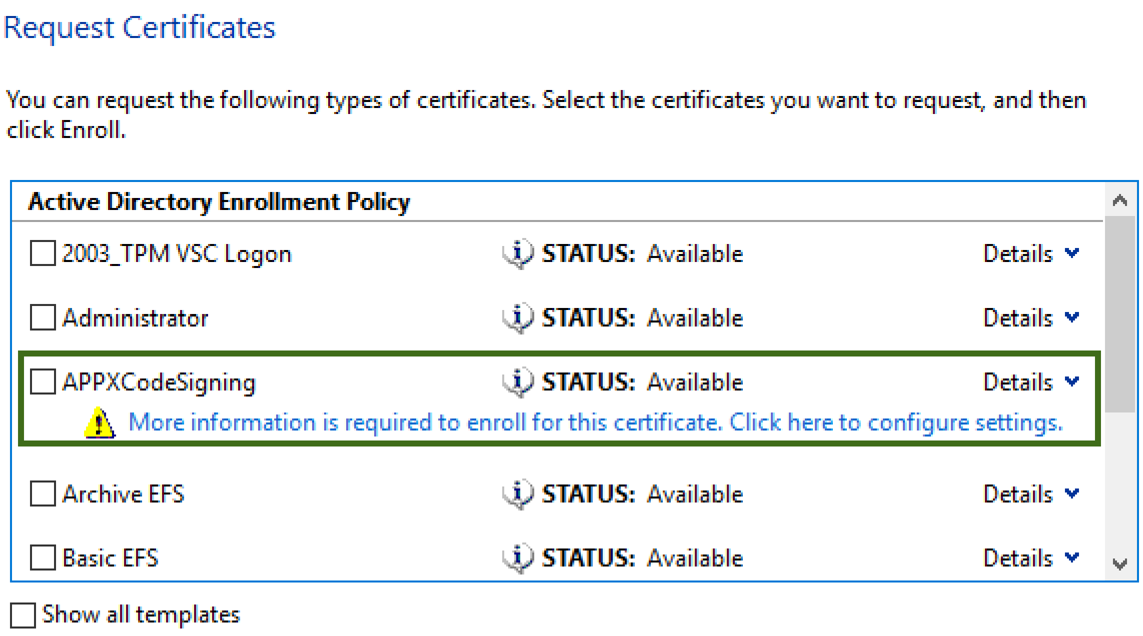
Extensions included in this template:

- Application Policies
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage

Description of Application Policies:

Code Signing


Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
MSIEHistoryJournal
Certificate Enrollment Requests
Smart Card Trusted Roots
All Tasks
Refresh
Export List...
View
Request New Certificate...
Import...
Advanced Operations



Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

Active Directory Enrollment Policy

□ 2003_TPM VSC Logon — **STATUS:** Available — Details

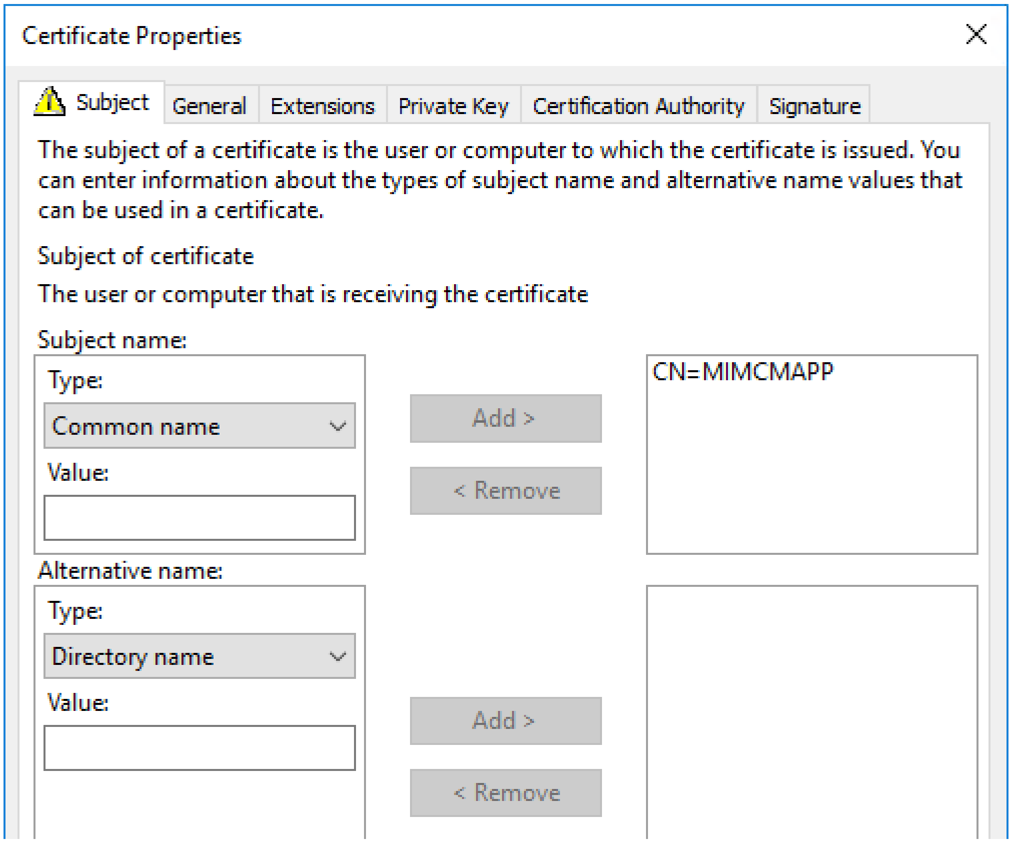
□ Administrator — **STATUS:** Available — Details

□ APPXCodeSigning — **STATUS:** Available — Details
⚠ More information is required to enroll for this certificate. Click here to configure settings.

□ Archive EFS — **STATUS:** Available — Details

□ Basic EFS — **STATUS:** Available — Details

□ Show all templates



Certificate Properties

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate

The user or computer that is receiving the certificate

Subject name:

Type: Common name

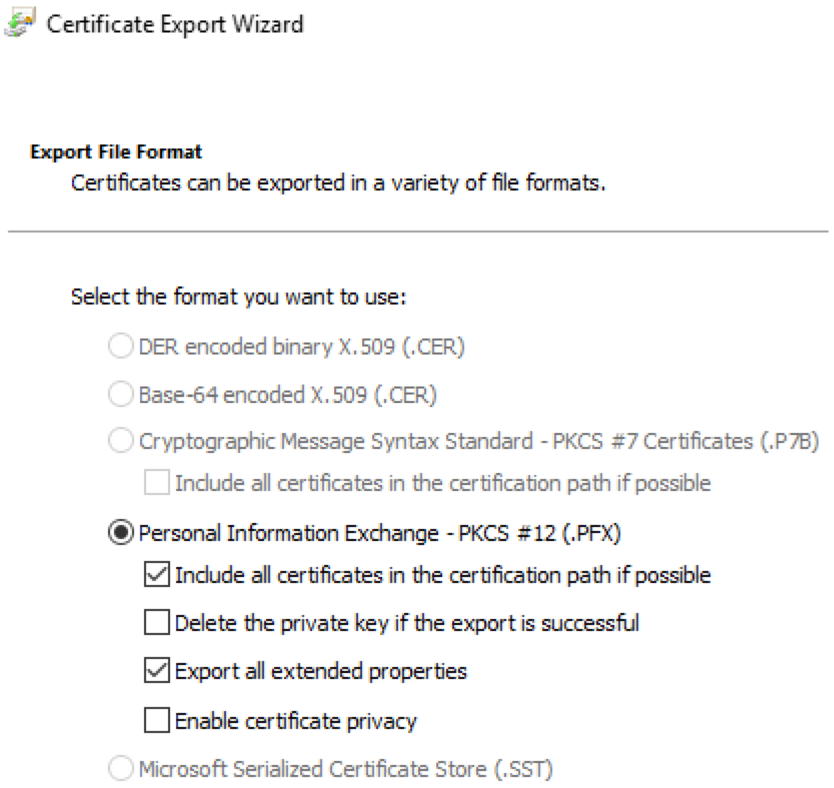
Value:

CN=MIMCMAPP

Alternative name:

Type: Directory name

Value:



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

● Personal Information Exchange - PKCS #12 (.PFX)

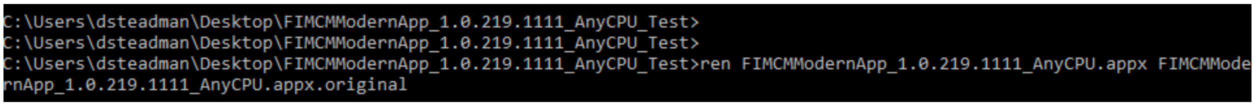
☑ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

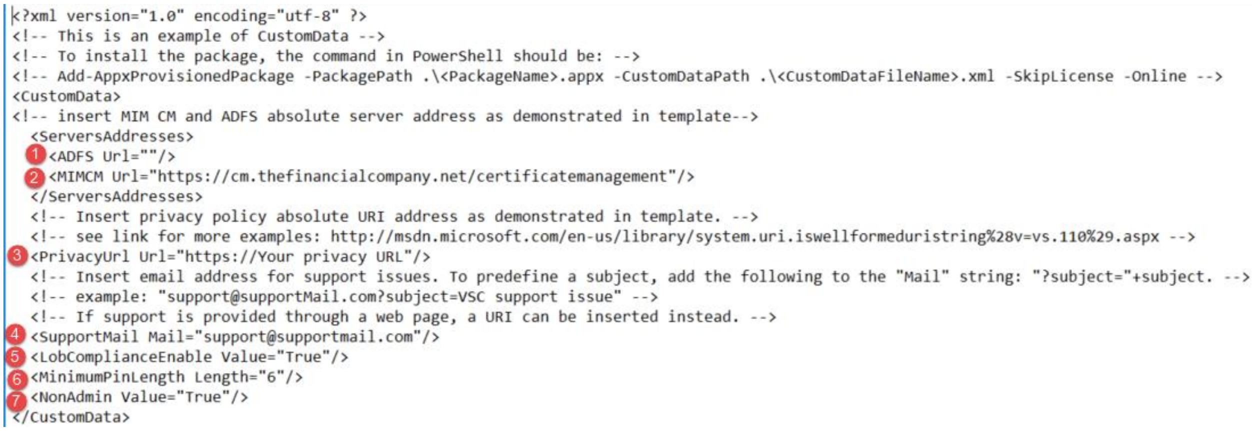
☑ Export all extended properties

□ Enable certificate privacy

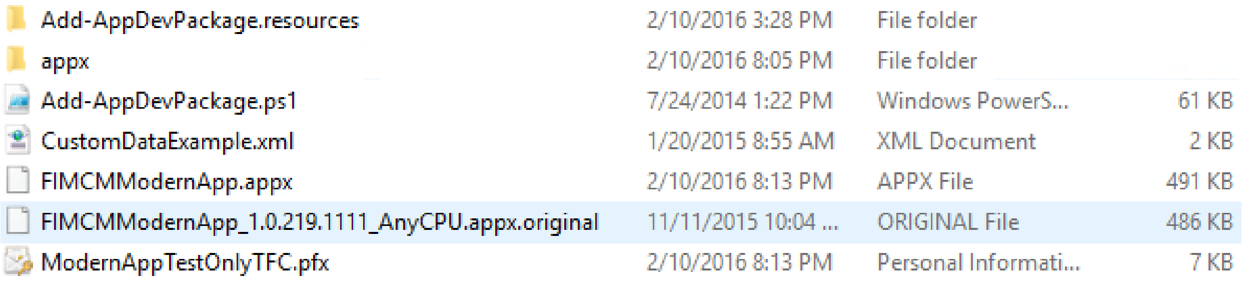
○ Microsoft Serialized Certificate Store (.SST)



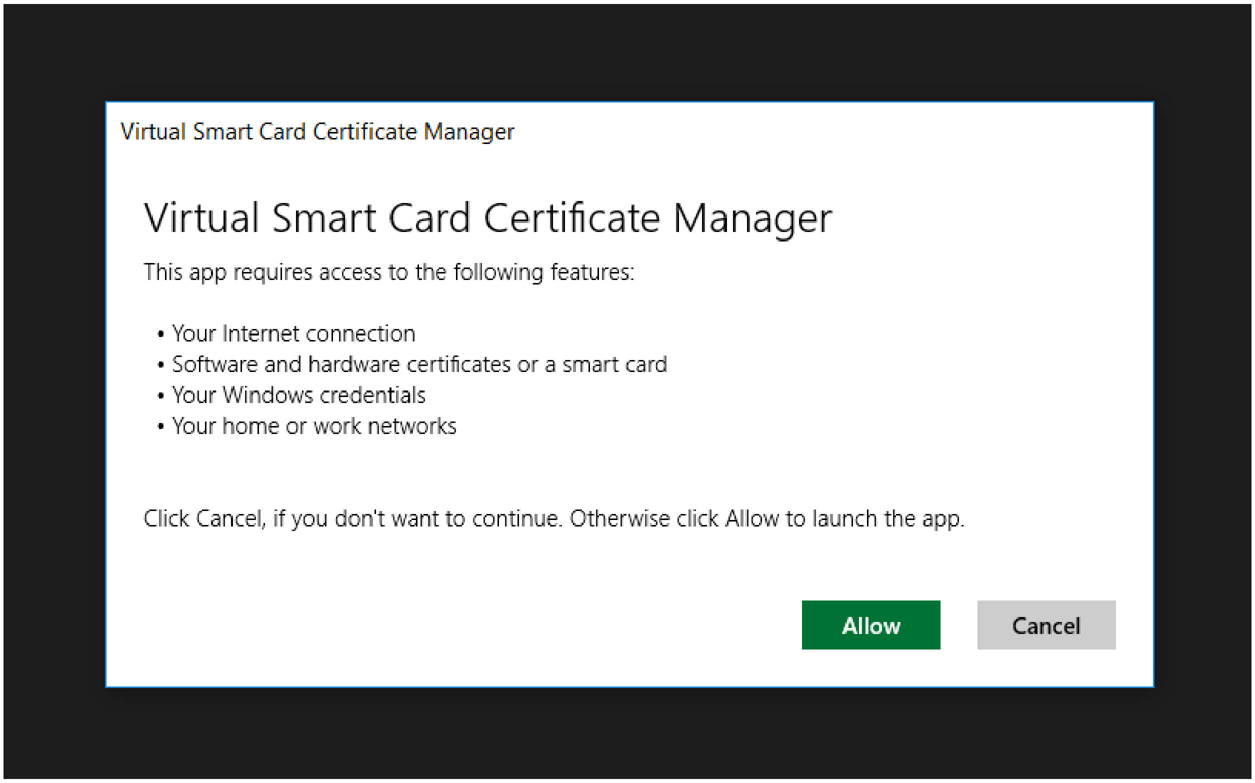
```
C:\Users\dsteadman\Desktop\FIMCMModernApp_1.0.219.1111_AnyCPU_Test>
C:\Users\dsteadman\Desktop\FIMCMModernApp_1.0.219.1111_AnyCPU_Test>
C:\Users\dsteadman\Desktop\FIMCMModernApp_1.0.219.1111_AnyCPU_Test>ren FIMCMModernApp_1.0.219.1111_AnyCPU.appx FIMCMMode
rnApp_1.0.219.1111_AnyCPU.appx.original
```



```
<?xml version="1.0" encoding="utf-8" ?>
<!-- This is an example of CustomData -->
<!-- To install the package, the command in PowerShell should be: -->
<!-- Add-AppxProvisionedPackage -PackagePath .\<PackageName>.appx -CustomDataPath .\<CustomDataFileName>.xml -SkipLicense -Online -->
<CustomData>
<!-- insert MIM CM and ADFS absolute server address as demonstrated in template-->
  <ServersAddresses>
1   <ADFS Url=""/>
2   <MIMCM Url="https://cm.thefinancialcompany.net/certificatemanagement"/>
  </ServersAddresses>
  <!-- Insert privacy policy absolute URI address as demonstrated in template. -->
  <!-- see link for more examples: http://msdn.microsoft.com/en-us/library/system.uri.iswellformeduristring%28v=vs.110%29.aspx -->
3 <PrivacyUrl Url="https://Your privacy URL"/>
  <!-- Insert email address for support issues. To predefine a subject, add the following to the "Mail" string: "?subject="+subject. -->
  <!-- example: "support@supportMail.com?subject=VSC support issue" -->
  <!-- If support is provided through a web page, a URI can be inserted instead. -->
4 <SupportMail Mail="support@supportmail.com"/>
5 <LobComplianceEnable Value="True"/>
6 <MinimumPinLength Length="6"/>
7 <NonAdmin Value="True"/>
</CustomData>
```



Add-AppDevPackage.resources	2/10/2016 3:28 PM	File folder	
appx	2/10/2016 8:05 PM	File folder	
Add-AppDevPackage.ps1	7/24/2014 1:22 PM	Windows PowerS...	61 KB
CustomDataExample.xml	1/20/2015 8:55 AM	XML Document	2 KB
FIMCMModernApp.appx	2/10/2016 8:13 PM	APPX File	491 KB
FIMCMModernApp_1.0.219.1111_AnyCPU.appx.original	11/11/2015 10:04 ...	ORIGINAL File	486 KB
ModernAppTestOnlyTFC.pfx	2/10/2016 8:13 PM	Personal Informati...	7 KB



Virtual Smart Card Certificate Manager

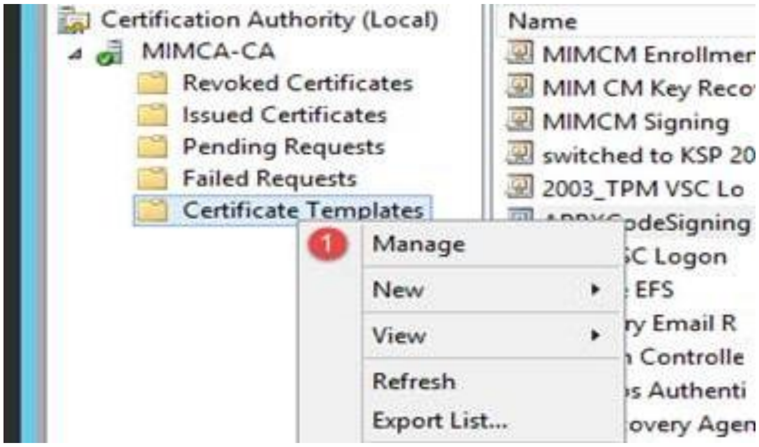
Virtual Smart Card Certificate Manager

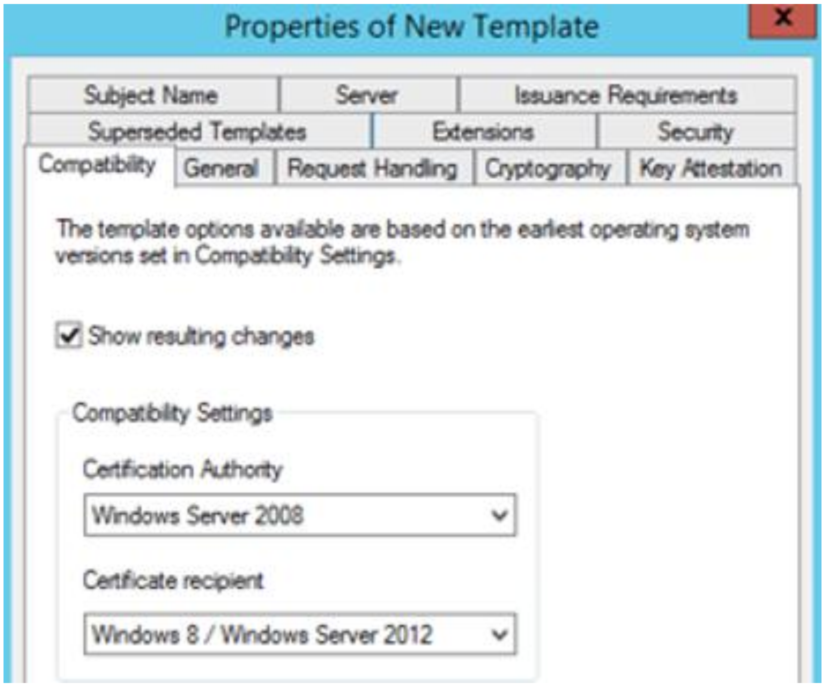
This app requires access to the following features:

- Your Internet connection
- Software and hardware certificates or a smart card
- Your Windows credentials
- Your home or work networks

Click Cancel, if you don't want to continue. Otherwise click Allow to launch the app.

```
  <!--
The FIM CM Web API provides a RESTful interface against which clients can perform
management and enrollment.
-->
  <add key="Clm.WebApi.Enabled" value="true" />
  <!--
```





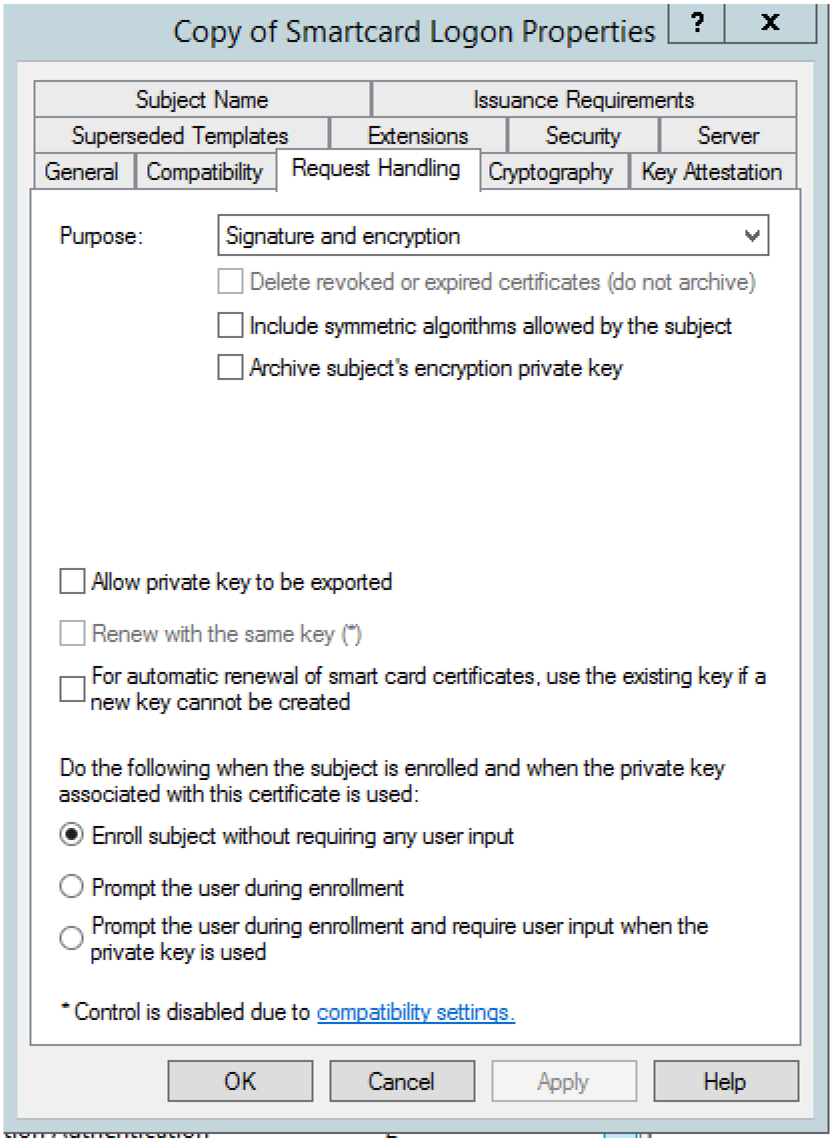
The template options available are based on the earliest operating system versions set in Compatibility Settings.

☑ Show resulting changes

Compatibility Settings

Certification Authority: Windows Server 2008

Certificate recipient: Windows 8 / Windows Server 2012



Purpose: Signature and encryption

□ Delete revoked or expired certificates (do not archive)

□ Include symmetric algorithms allowed by the subject

□ Archive subject's encryption private key

□ Allow private key to be exported

□ Renew with the same key (*)

□ For automatic renewal of smart card certificates, use the existing key if a new key cannot be created

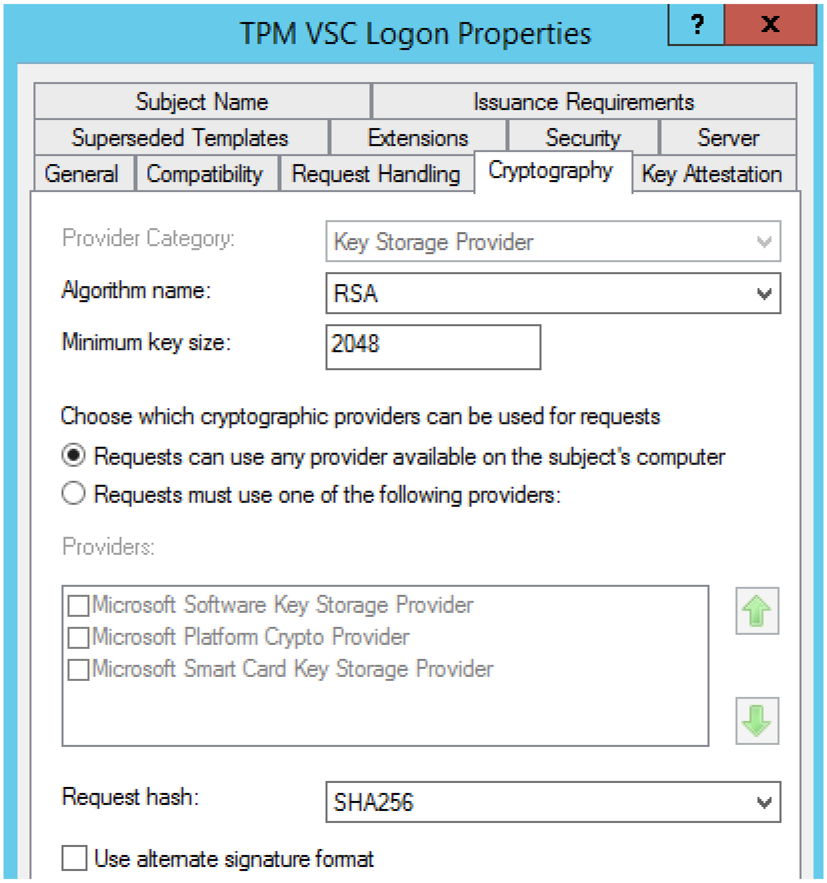
Do the following when the subject is enrolled and when the private key associated with this certificate is used:

● Enroll subject without requiring any user input

○ Prompt the user during enrollment

○ Prompt the user during enrollment and require user input when the private key is used

* Control is disabled due to compatibility settings.



Provider Category: Key Storage Provider

Algorithm name: RSA

Minimum key size: 2048

Choose which cryptographic providers can be used for requests

● Requests can use any provider available on the subject's computer

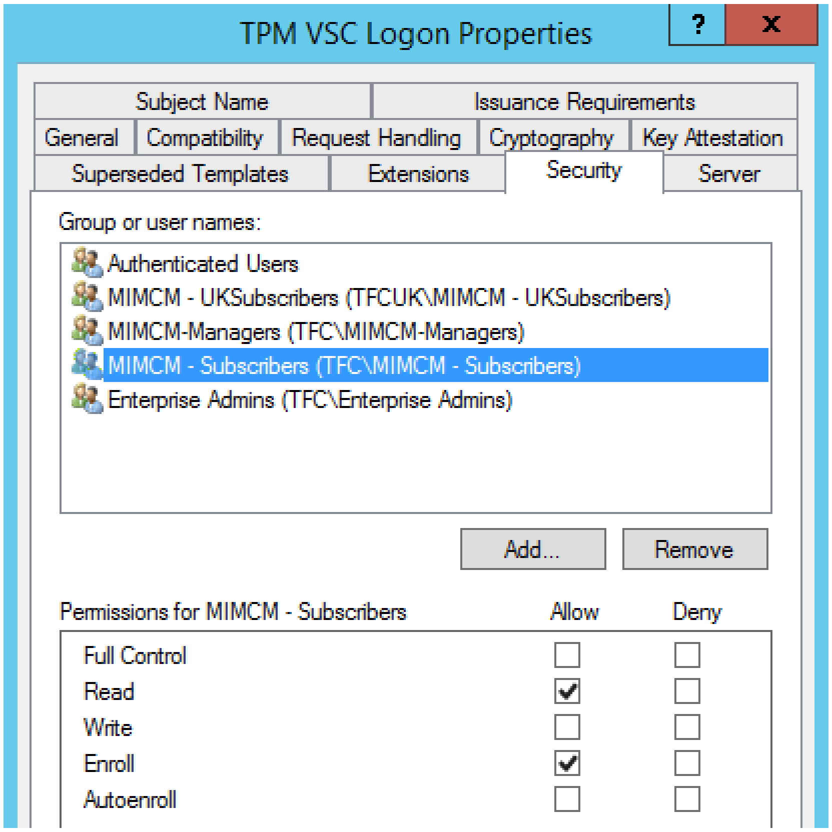
○ Requests must use one of the following providers:

Providers:

□ Microsoft Software Key Storage Provider
□ Microsoft Platform Crypto Provider
□ Microsoft Smart Card Key Storage Provider

Request hash: SHA256

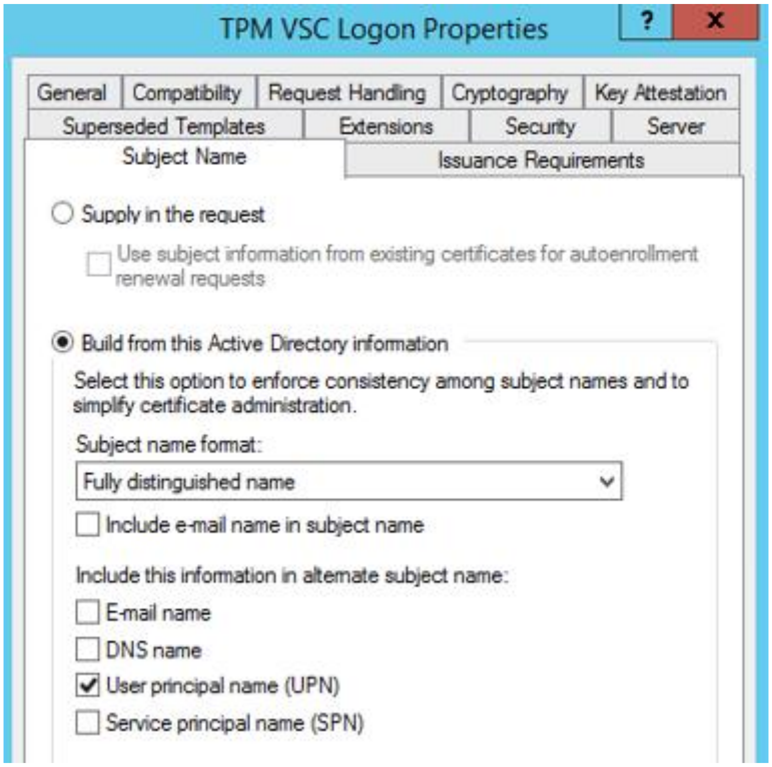
□ Use alternate signature format



Group or user names:

- Authenticated Users
- MIMCM - UKSubscribers (TFCUK\MIMCM - UKSubscribers)
- MIMCM-Managers (TFC\MIMCM-Managers)
- MIMCM - Subscribers (TFC\MIMCM - Subscribers)
- Enterprise Admins (TFC\Enterprise Admins)

Permissions for MIMCM - Subscribers	Allow	Deny
Full Control	□	□
Read	☑	□
Write	□	□
Enroll	☑	□
Autoenroll	□	□



○ Supply in the request

□ Use subject information from existing certificates for autoenrollment renewal requests

● Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

Fully distinguished name

□ Include e-mail name in subject name

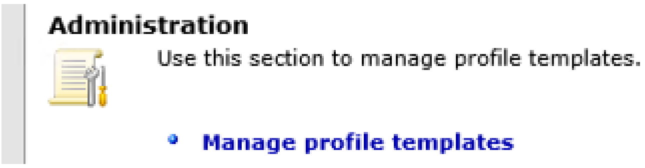
Include this information in alternate subject name:

□ E-mail name

□ DNS name

☑ User principal name (UPN)

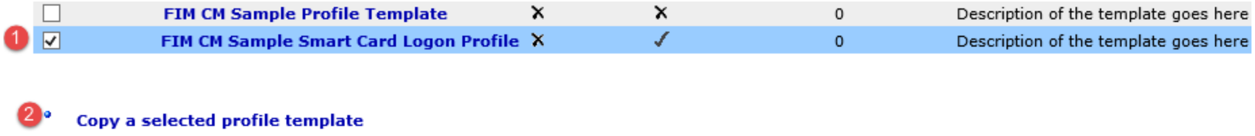
□ Service principal name (SPN)



Administration

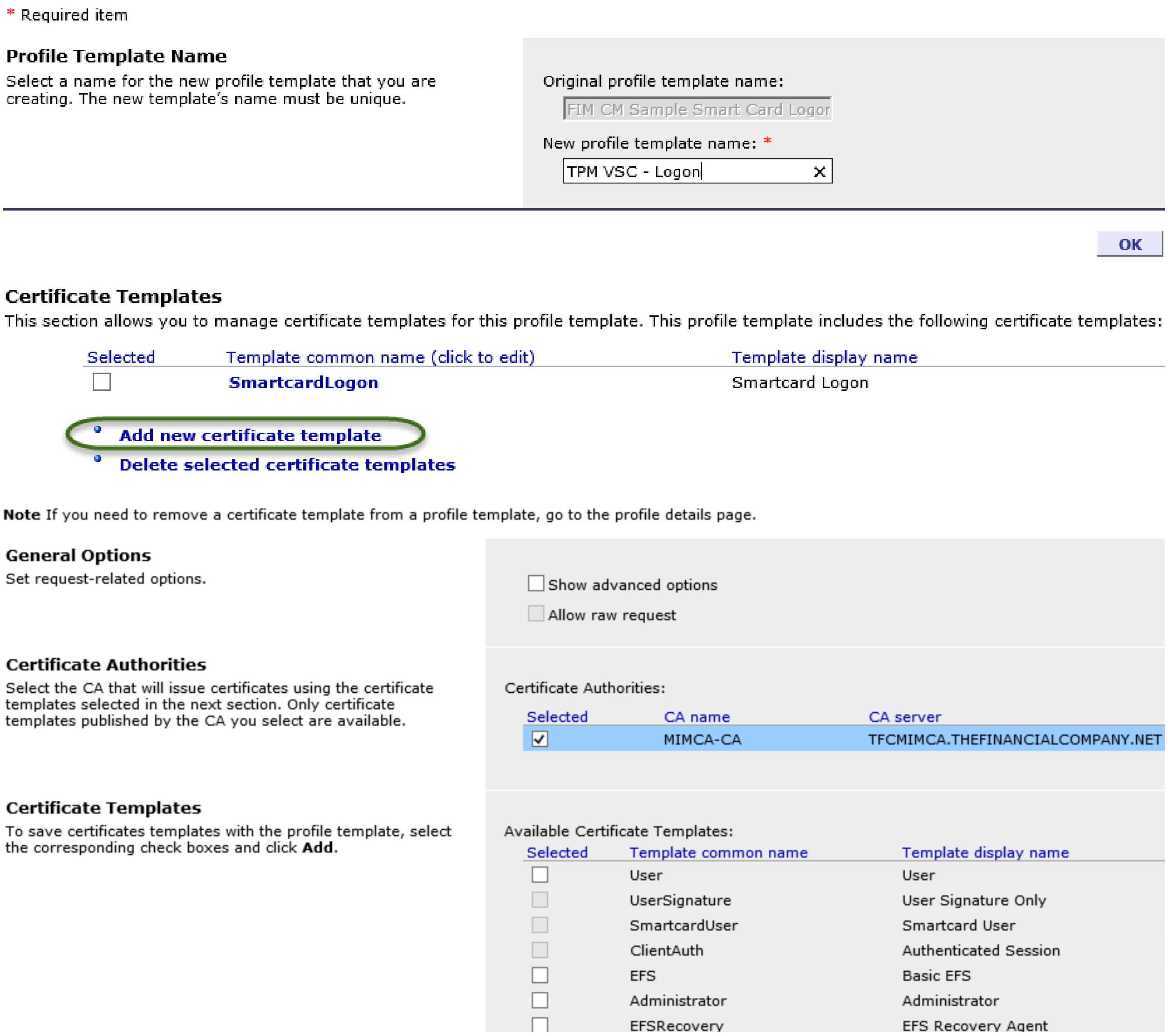
Use this section to manage profile templates.

- Manage profile templates



□	FIM CM Sample Profile Template	✗	✗	0	Description of the template goes here
☑	FIM CM Sample Smart Card Logon Profile	✗	✓	0	Description of the template goes here

- Copy a selected profile template



* Required item

Profile Template Name

Select a name for the new profile template that you are creating. The new template's name must be unique.

Original profile template name:

FIM CM Sample Smart Card Logor

New profile template name: *

TPM VSC - Logon

OK

Certificate Templates

This section allows you to manage certificate templates for this profile template. This profile template includes the following certificate templates:

Selected	Template common name (click to edit)	Template display name
□	SmartcardLogon	Smartcard Logon

- Add new certificate template
- Delete selected certificate templates

Note If you need to remove a certificate template from a profile template, go to the profile details page.

General Options

Set request-related options.

□ Show advanced options

□ Allow raw request

Certificate Authorities

Select the CA that will issue certificates using the certificate templates selected in the next section. Only certificate templates published by the CA you select are available.

Certificate Authorities:

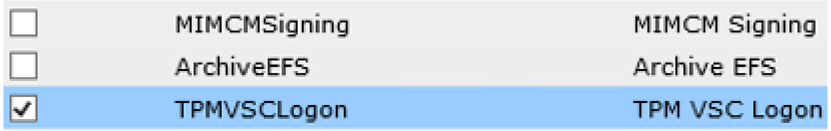
Selected	CA name	CA server
☑	MIMCA-CA	TFCMIMCA.THEFINANCIALCOMPANY.NET

Certificate Templates

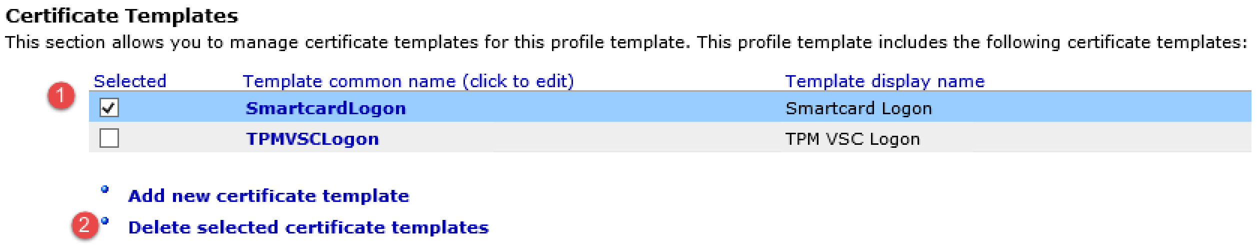
To save certificates templates with the profile template, select the corresponding check boxes and click **Add**.

Available Certificate Templates:

Selected	Template common name	Template display name
□	User	User
□	UserSignature	User Signature Only
□	SmartcardUser	Smartcard User
□	ClientAuth	Authenticated Session
□	EFS	Basic EFS
□	Administrator	Administrator
□	EFSRecovery	EFS Recovery Agent



□	MIMCMSigning	MIMCM Signing
□	ArchiveEFS	Archive EFS
☑	TPMVSCLogon	TPM VSC Logon

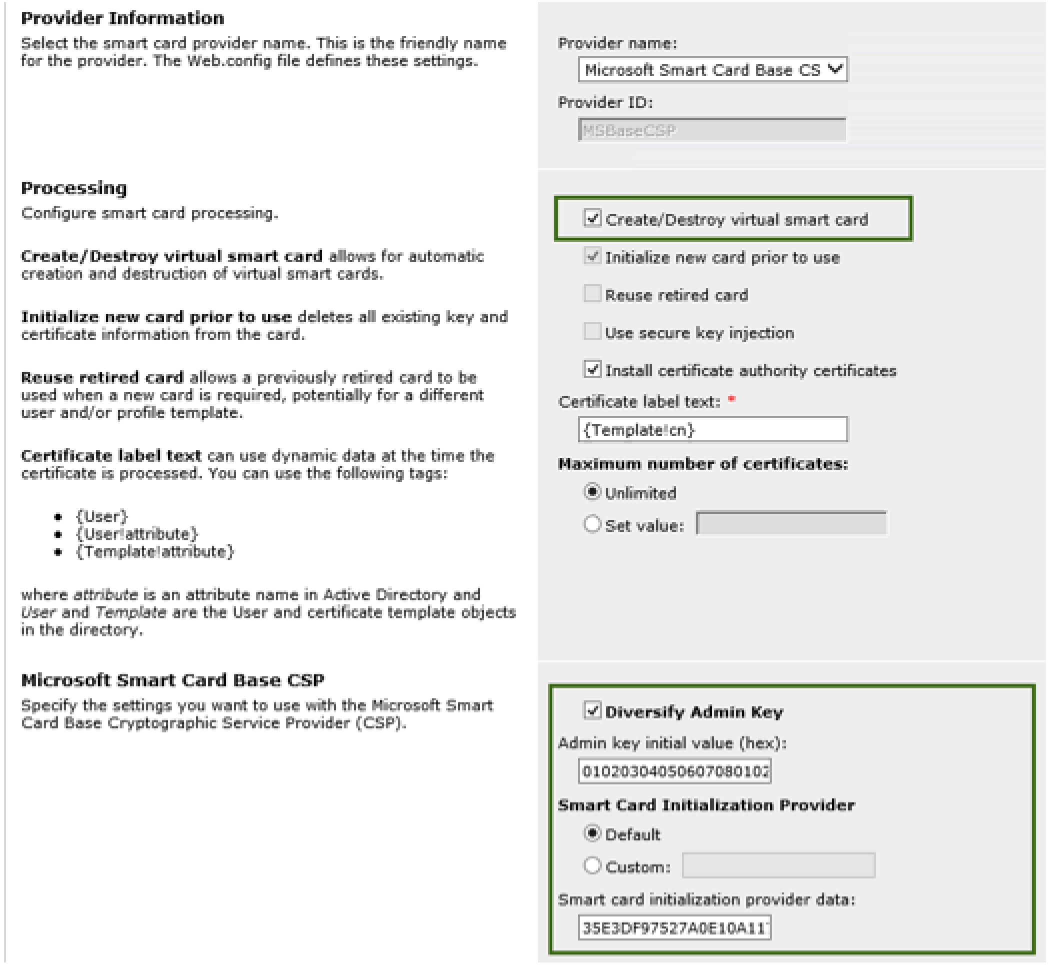


Certificate Templates

This section allows you to manage certificate templates for this profile template. This profile template includes the following certificate templates:

Selected	Template common name (click to edit)	Template display name
1 ☑	**SmartcardLogon**	Smartcard Logon
□	**TPMVSCLogon**	TPM VSC Logon

- **Add new certificate template**
- 2 **Delete selected certificate templates**



Provider Information

Select the smart card provider name. This is the friendly name for the provider. The Web.config file defines these settings.

Provider name: Microsoft Smart Card Base CS

Provider ID: MSBaseCSP

Processing

Configure smart card processing.

Create/Destroy virtual smart card allows for automatic creation and destruction of virtual smart cards.

Initialize new card prior to use deletes all existing key and certificate information from the card.

Reuse retired card allows a previously retired card to be used when a new card is required, potentially for a different user and/or profile template.

Certificate label text can use dynamic data at the time the certificate is processed. You can use the following tags:

- {User}
- {User!attribute}
- {Template!attribute}

where *attribute* is an attribute name in Active Directory and *User* and *Template* are the User and certificate template objects in the directory.

☑ Create/Destroy virtual smart card

☑ Initialize new card prior to use

□ Reuse retired card

□ Use secure key injection

☑ Install certificate authority certificates

Certificate label text: *

{Template!cn}

Maximum number of certificates:

● Unlimited

○ Set value:

Microsoft Smart Card Base CSP

Specify the settings you want to use with the Microsoft Smart Card Base Cryptographic Service Provider (CSP).

☑ **Diversify Admin Key**

Admin key initial value (hex):

01020304050607080102

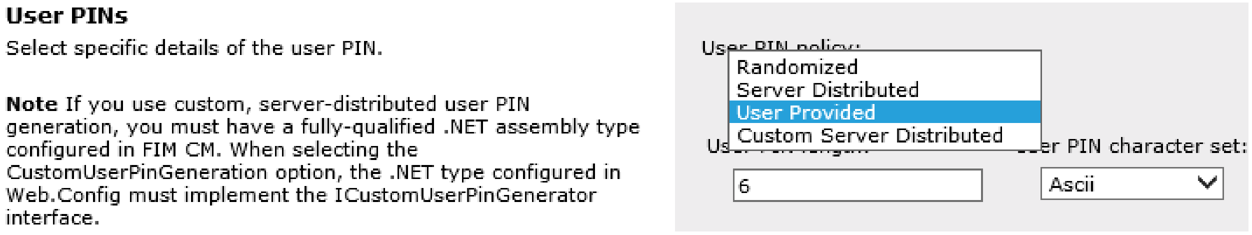
Smart Card Initialization Provider

● Default

○ Custom:

Smart card initialization provider data:

35E3DF97527A0E10A11



User PINs

Select specific details of the user PIN.

Note If you use custom, server-distributed user PIN generation, you must have a fully-qualified .NET assembly type configured in FIM CM. When selecting the CustomUserPinGeneration option, the .NET type configured in Web.Config must implement the ICustomUserPinGenerator interface.

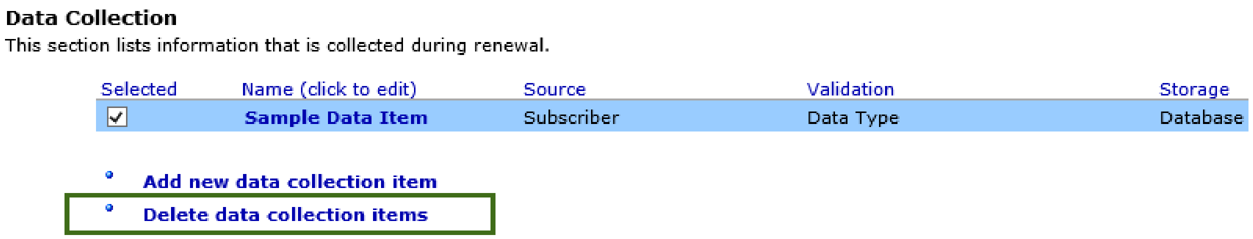
User PIN policy:

Us

6

er PIN character set:

Ascii

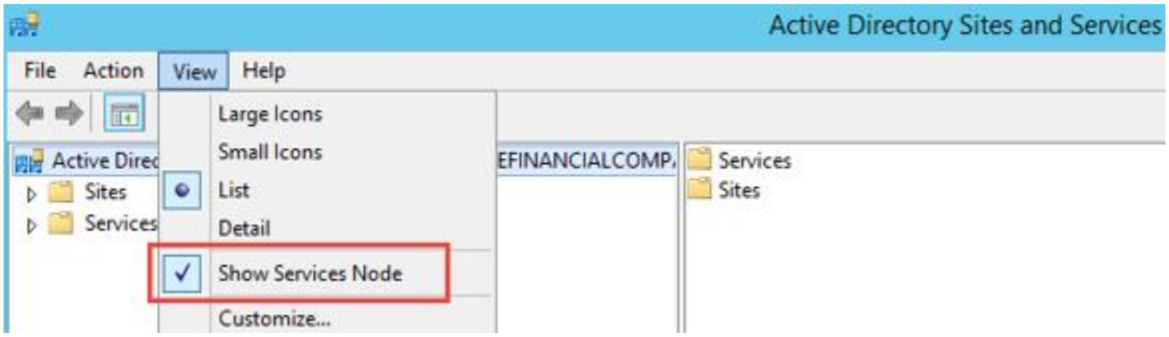


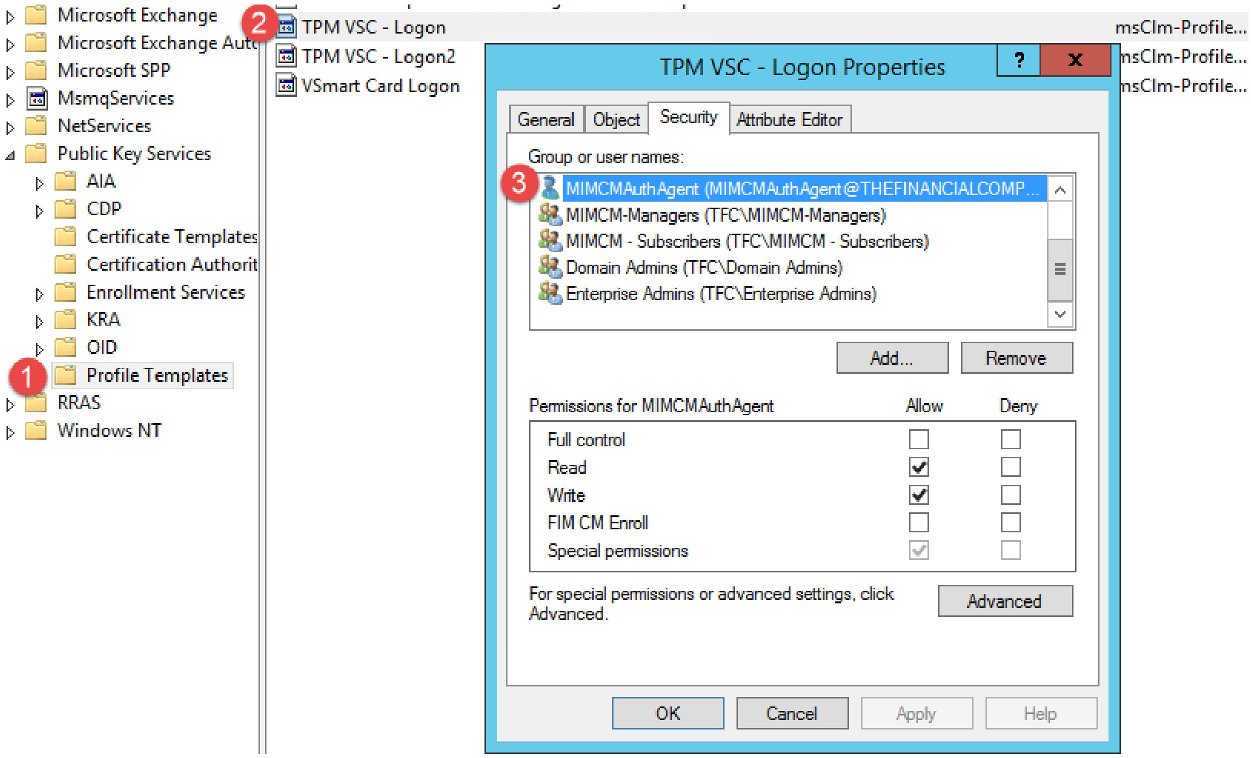
Data Collection

This section lists information that is collected during renewal.

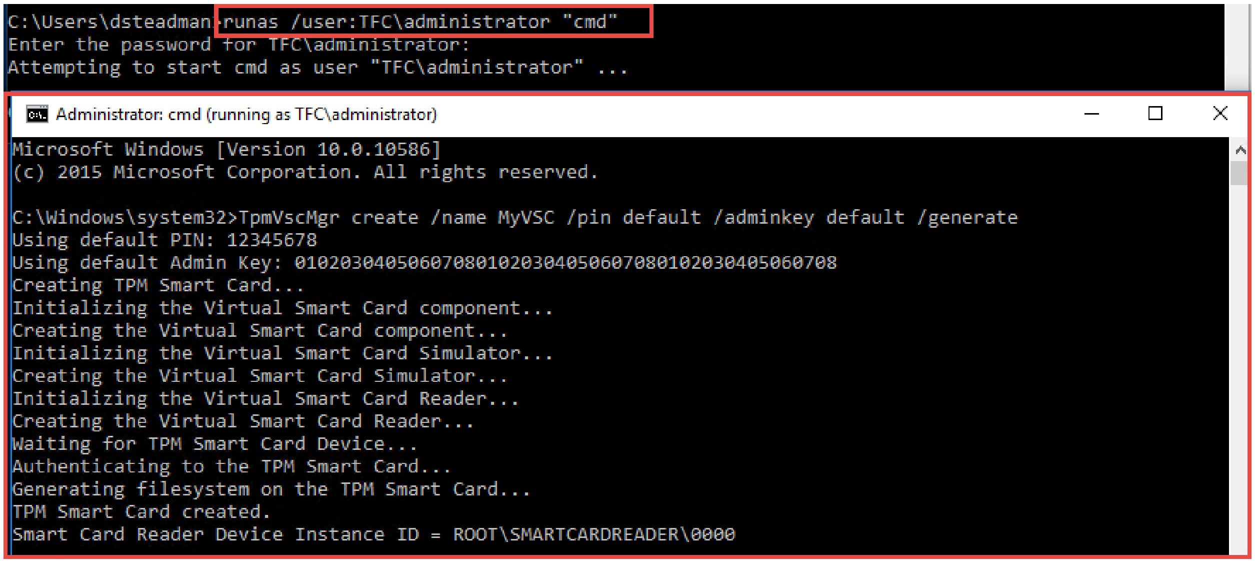
Selected	Name (click to edit)	Source	Validation	Storage
☑	**Sample Data Item**	Subscriber	Data Type	Database

- **Add new data collection item**
- **Delete data collection items**



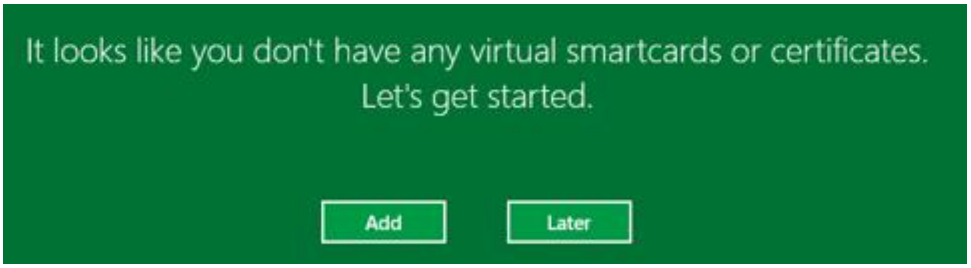


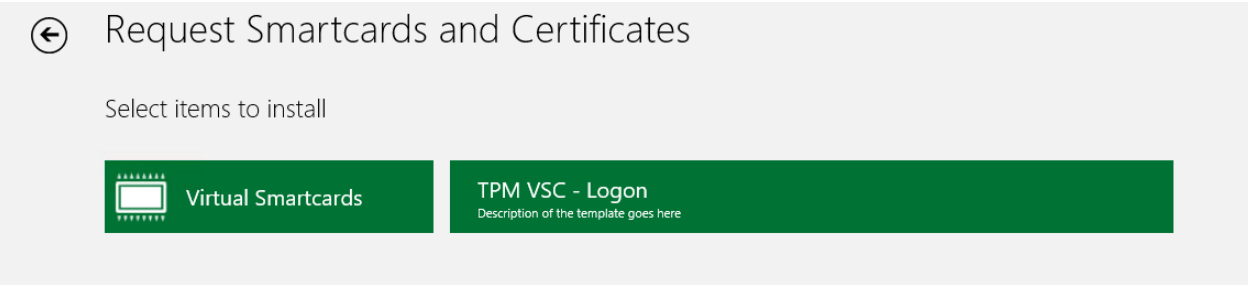
Permissions for MIMCMAuthAgent	Allow	Deny
Full control	□	□
Read	☑	□
Write	☑	□
FIM CM Enroll	□	□
Special permissions	☑	□



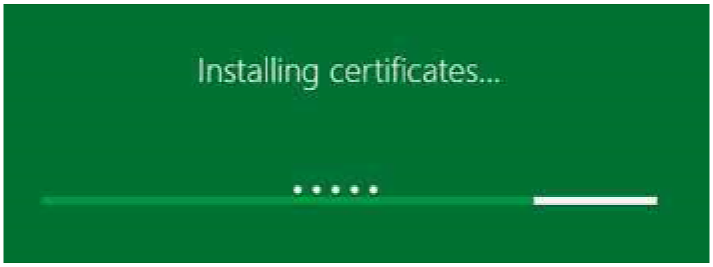
```
C:\Users\dsteadman>runas /user:TFC\administrator "cmd"
Enter the password for TFC\administrator:
Attempting to start cmd as user "TFC\administrator" ...
```

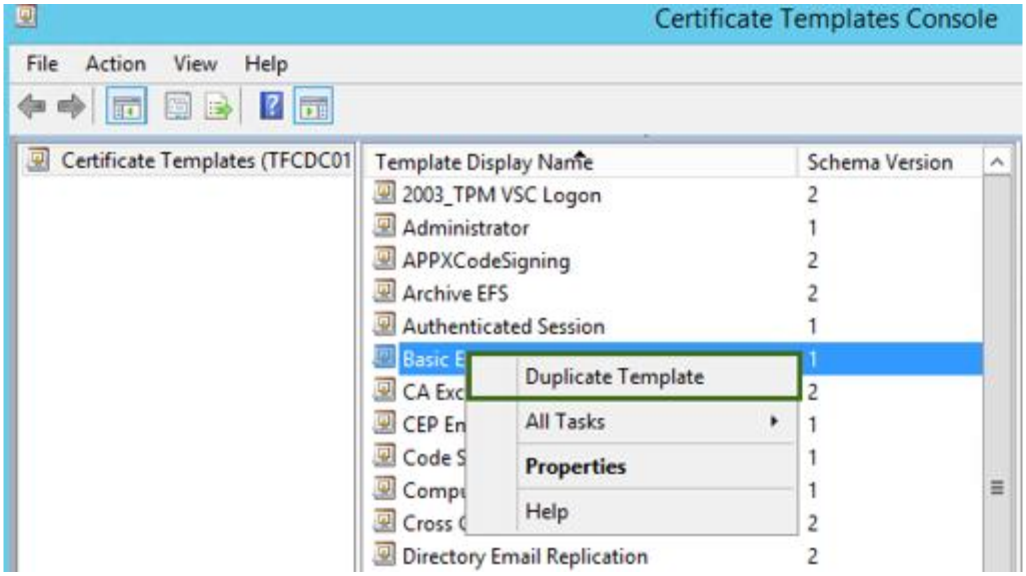
```
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>TpmVscMgr create /name MyVSC /pin default /adminkey default /generate
Using default PIN: 12345678
Using default Admin Key: 010203040506070801020304050607080102030405060708
Creating TPM Smart Card...
Initializing the Virtual Smart Card component...
Creating the Virtual Smart Card component...
Initializing the Virtual Smart Card Simulator...
Creating the Virtual Smart Card Simulator...
Initializing the Virtual Smart Card Reader...
Creating the Virtual Smart Card Reader...
Waiting for TPM Smart Card Device...
Authenticating to the TPM Smart Card...
Generating filesystem on the TPM Smart Card...
TPM Smart Card created.
Smart Card Reader Device Instance ID = ROOT\SMARTCARDREADER\0000
```


It looks like you don't have any virtual smartcards or certificates. Let's get started.

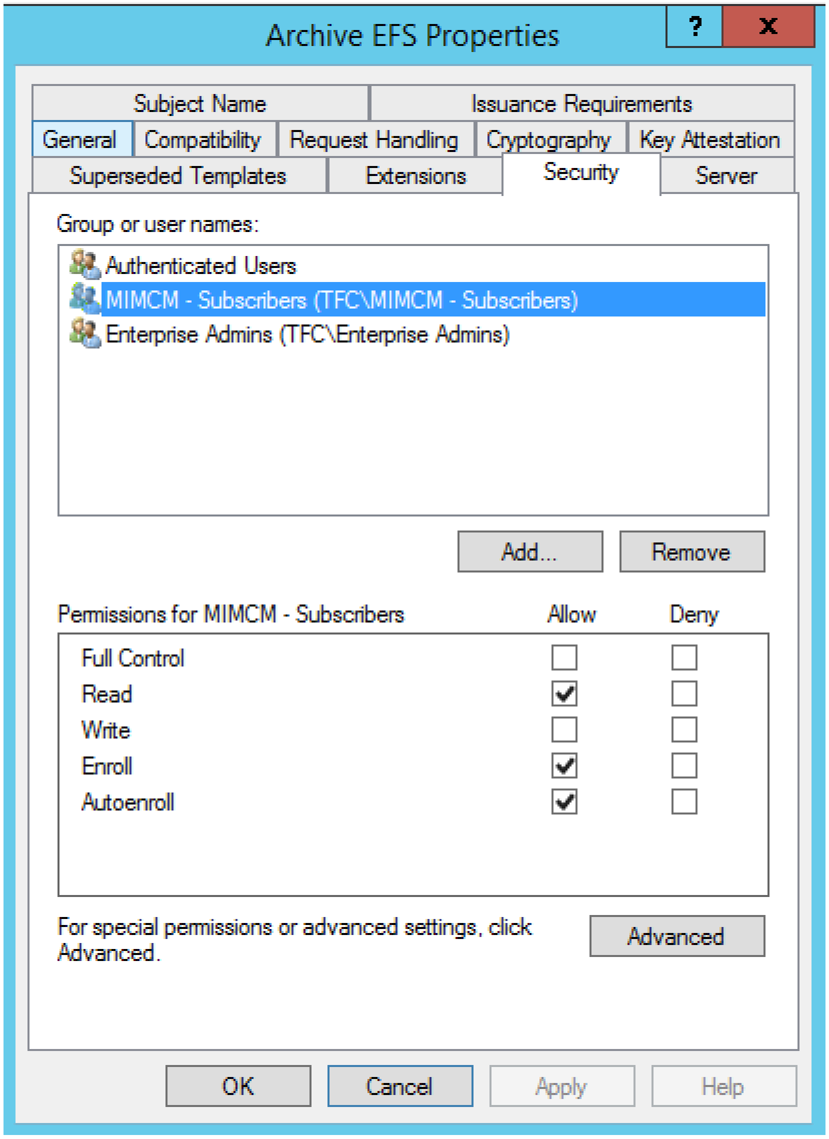

Request Smartcards and Certificates

Select items to install


Installing certificates...



Template Display Name	Schema Version
2003_TPM VSC Logon	2
Administrator	1
APPXCodeSigning	2
Archive EFS	2
Authenticated Session	1
Basic E	1
CA Exc	2
CEP En	1
Code S	1
Compu	1
Cross C	2
Directory Email Replication	2

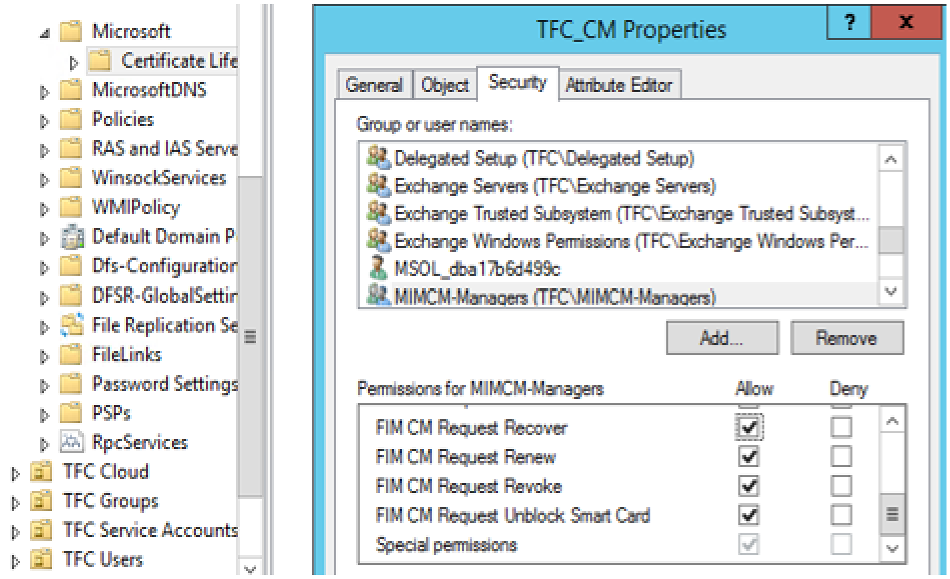


Group or user names:

- Authenticated Users
- MIMCM - Subscribers (TFC\MIMCM - Subscribers)
- Enterprise Admins (TFC\Enterprise Admins)

Permissions for MIMCM - Subscribers	Allow	Deny
Full Control	□	□
Read	☑	□
Write	□	□
Enroll	☑	□
Autoenroll	☑	□

For special permissions or advanced settings, click Advanced.



- Microsoft
  - Certificate Life
- MicrosoftDNS
- Policies
- RAS and IAS Serve
- WinsockServices
- WMIPolicy
- Default Domain P
- Dfs-Configuration
- DFSR-GlobalSettin
- File Replication Se
- FileLinks
- Password Settings
- PSPs
- RpcServices
- TFC Cloud
- TFC Groups
- TFC Service Accounts
- TFC Users

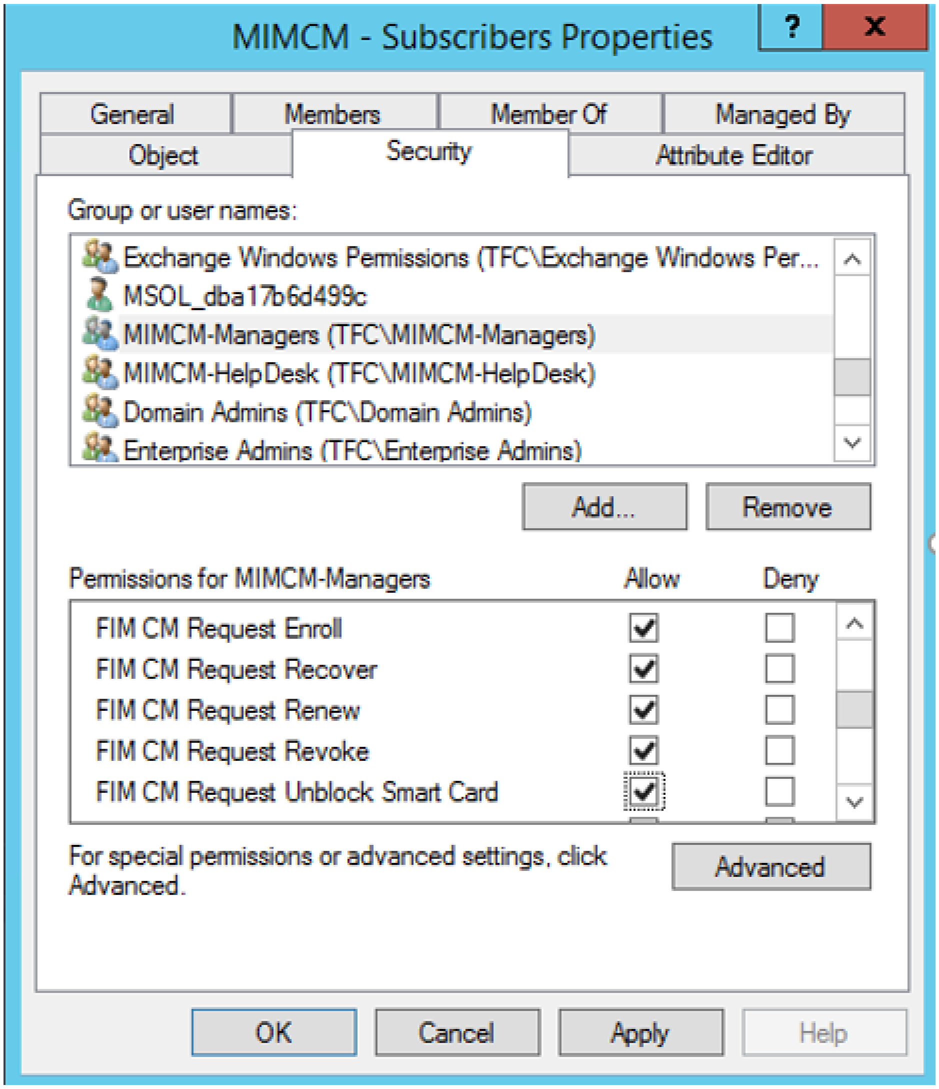
TFC_CM Properties

General | Object | Security | Attribute Editor

Group or user names:

- Delegated Setup (TFC\Delegated Setup)
- Exchange Servers (TFC\Exchange Servers)
- Exchange Trusted Subsystem (TFC\Exchange Trusted Subsyst...
- Exchange Windows Permissions (TFC\Exchange Windows Per...
- MSOL_dba17b6d499c
- MIMCM-Managers (TFC\MIMCM-Managers)

Permissions for MIMCM-Managers	Allow	Deny
FIM CM Request Recover	☑	☐
FIM CM Request Renew	☑	☐
FIM CM Request Revoke	☑	☐
FIM CM Request Unblock Smart Card	☑	☐
Special permissions	☑	☐



MIMCM - Subscribers Properties

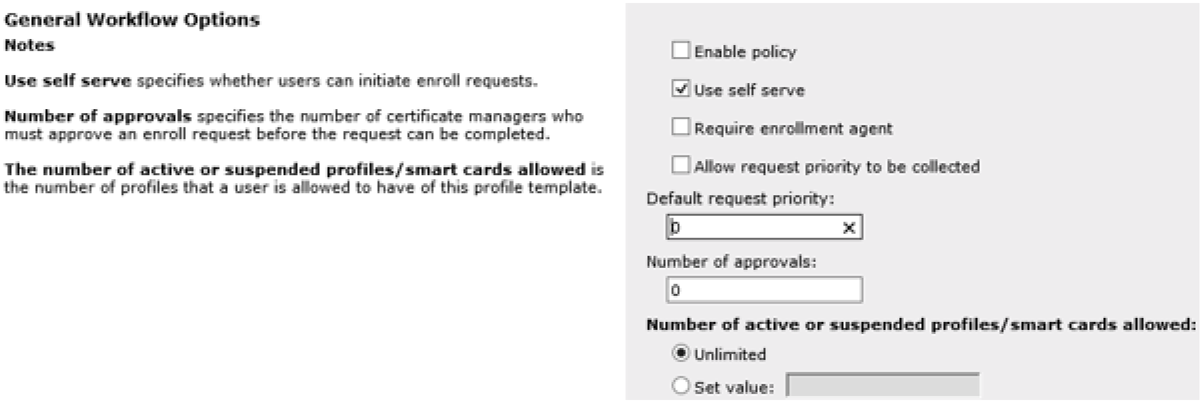
General | Members | Member Of | Managed By
Object | Security | Attribute Editor

Group or user names:

- Exchange Windows Permissions (TFC\Exchange Windows Per...
- MSOL_dba17b6d499c
- MIMCM-Managers (TFC\MIMCM-Managers)
- MIMCM-HelpDesk (TFC\MIMCM-HelpDesk)
- Domain Admins (TFC\Domain Admins)
- Enterprise Admins (TFC\Enterprise Admins)

Permissions for MIMCM-Managers	Allow	Deny
FIM CM Request Enroll	☑	☐
FIM CM Request Recover	☑	☐
FIM CM Request Renew	☑	☐
FIM CM Request Revoke	☑	☐
FIM CM Request Unblock Smart Card	☑	☐

For special permissions or advanced settings, click Advanced.



General Workflow Options

Notes

Use self serve specifies whether users can initiate enroll requests.

Number of approvals specifies the number of certificate managers who must approve an enroll request before the request can be completed.

The number of active or suspended profiles/smart cards allowed is the number of profiles that a user is allowed to have of this profile template.

☐ Enable policy

☑ Use self serve

☐ Require enrollment agent

☐ Allow request priority to be collected

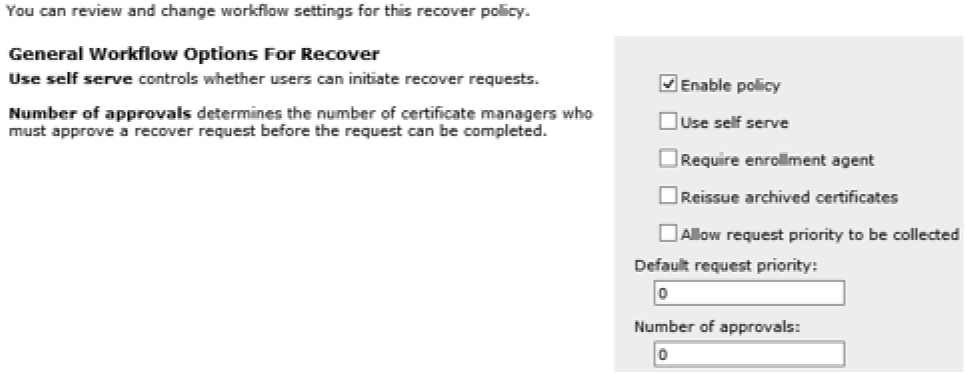
Default request priority: 0

Number of approvals: 0

Number of active or suspended profiles/smart cards allowed:

● Unlimited

○ Set value:



You can review and change workflow settings for this recover policy.

General Workflow Options For Recover

Use self serve controls whether users can initiate recover requests.

Number of approvals determines the number of certificate managers who must approve a recover request before the request can be completed.

☑ Enable policy

☐ Use self serve

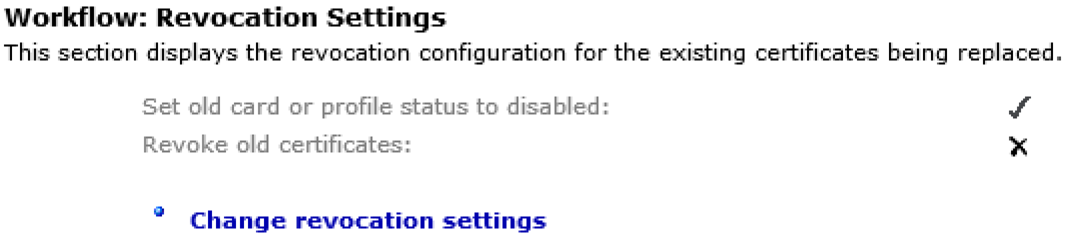
☐ Require enrollment agent

☐ Reissue archived certificates

☐ Allow request priority to be collected

Default request priority: 0

Number of approvals: 0

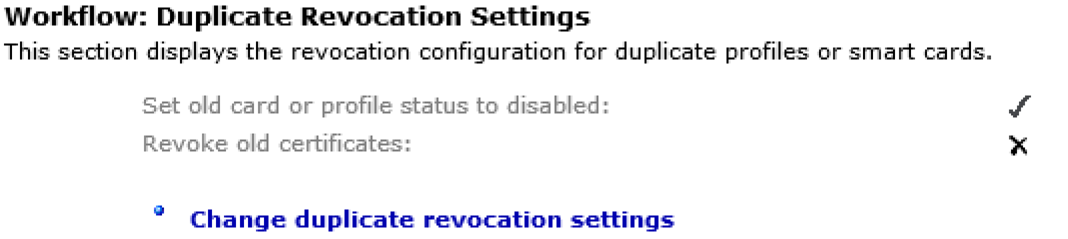


Workflow: Revocation Settings

This section displays the revocation configuration for the existing certificates being replaced.

Set old card or profile status to disabled:	✓
Revoke old certificates:	✗

- Change revocation settings

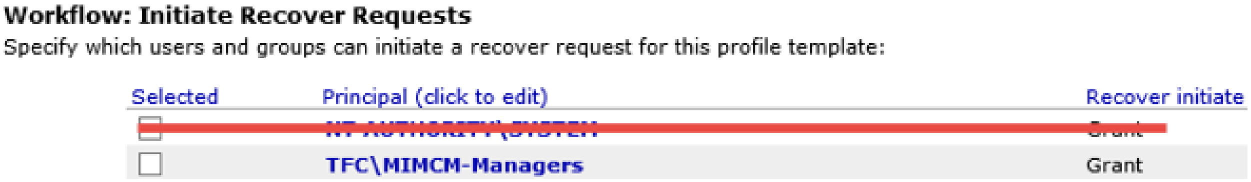


Workflow: Duplicate Revocation Settings

This section displays the revocation configuration for duplicate profiles or smart cards.

Set old card or profile status to disabled:	✓
Revoke old certificates:	✗

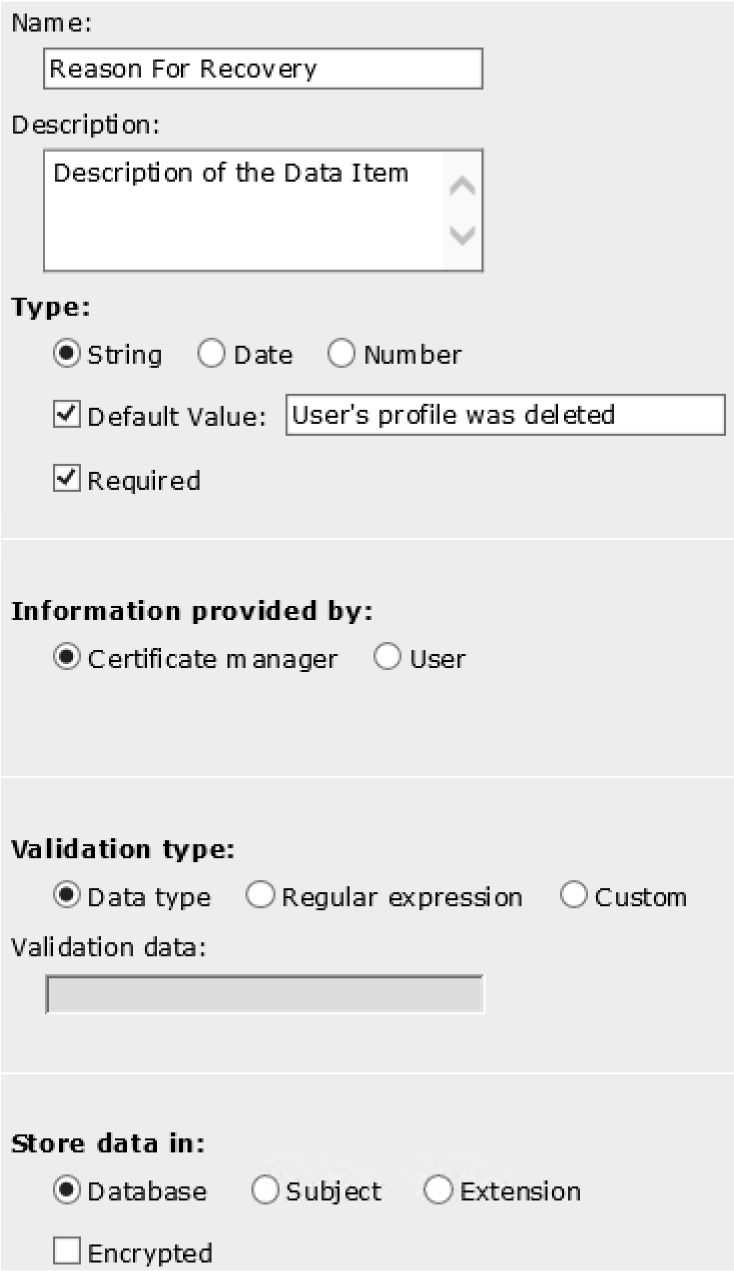
- Change duplicate revocation settings



Workflow: Initiate Recover Requests

Specify which users and groups can initiate a recover request for this profile template:

Selected	Principal (click to edit)	Recover initiate
☐	~~NT AUTHORITY\SYSTEM~~	~~Grant~~
☐	TFC\MIMCM-Managers	Grant



Name:

Reason For Recovery

Description:

Description of the Data Item

Type:

● String ○ Date ○ Number

☑ Default Value: User's profile was deleted

☑ Required

Information provided by:

● Certificate manager ○ User

Validation type:

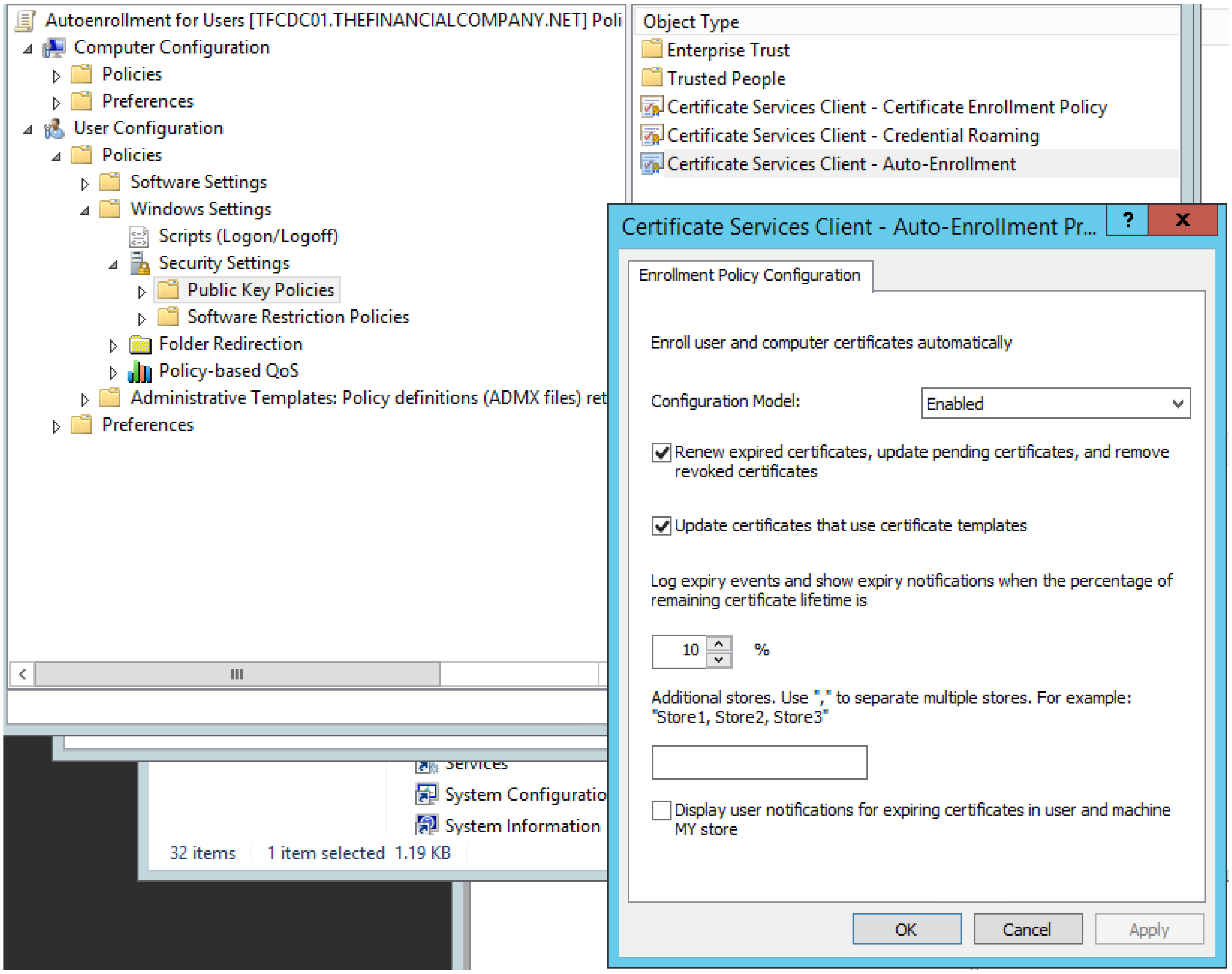
● Data type ○ Regular expression ○ Custom

Validation data:

Store data in:

● Database ○ Subject ○ Extension

□ Encrypted


Autoenrollment for Users [TFCDC01.THEFINANCIALCOMPANY.NET] Poli
Computer Configuration
Policies
Preferences
User Configuration
Policies
Software Settings
Windows Settings
Scripts (Logon/Logoff)
Security Settings
Public Key Policies
Software Restriction Policies
Folder Redirection
Policy-based QoS
Administrative Templates: Policy definitions (ADMX files) ret
Preferences
Object Type
Enterprise Trust
Trusted People
Certificate Services Client - Certificate Enrollment Policy
Certificate Services Client - Credential Roaming
Certificate Services Client - Auto-Enrollment
Services
System Configuratio
System Information
32 items 1 item selected 1.19 KB

Certificate Services Client - Auto-Enrollment Pr...

Enrollment Policy Configuration

Enroll user and computer certificates automatically

Configuration Model: Enabled

☑ Renew expired certificates, update pending certificates, and remove revoked certificates

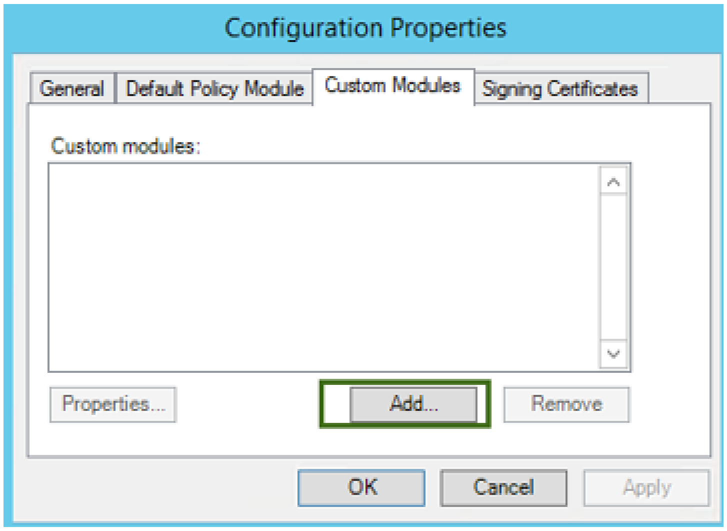
☑ Update certificates that use certificate templates

Log expiry events and show expiry notifications when the percentage of remaining certificate lifetime is

10 %

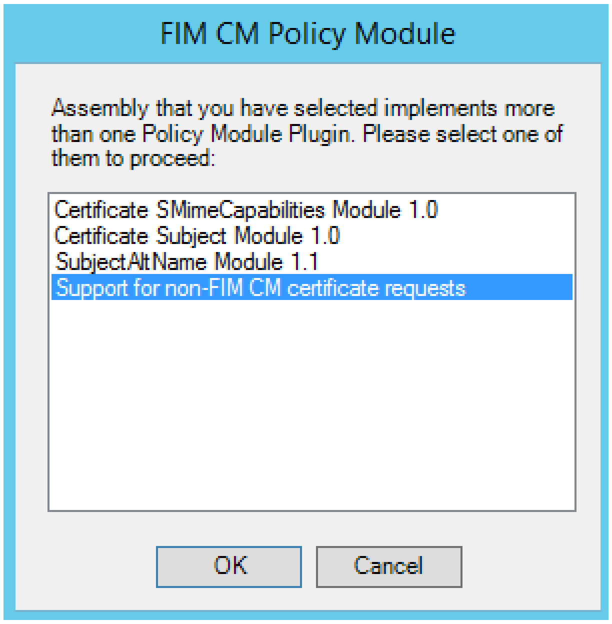
Additional stores. Use "," to separate multiple stores. For example: "Store1, Store2, Store3"

□ Display user notifications for expiring certificates in user and machine MY store



Configuration Properties

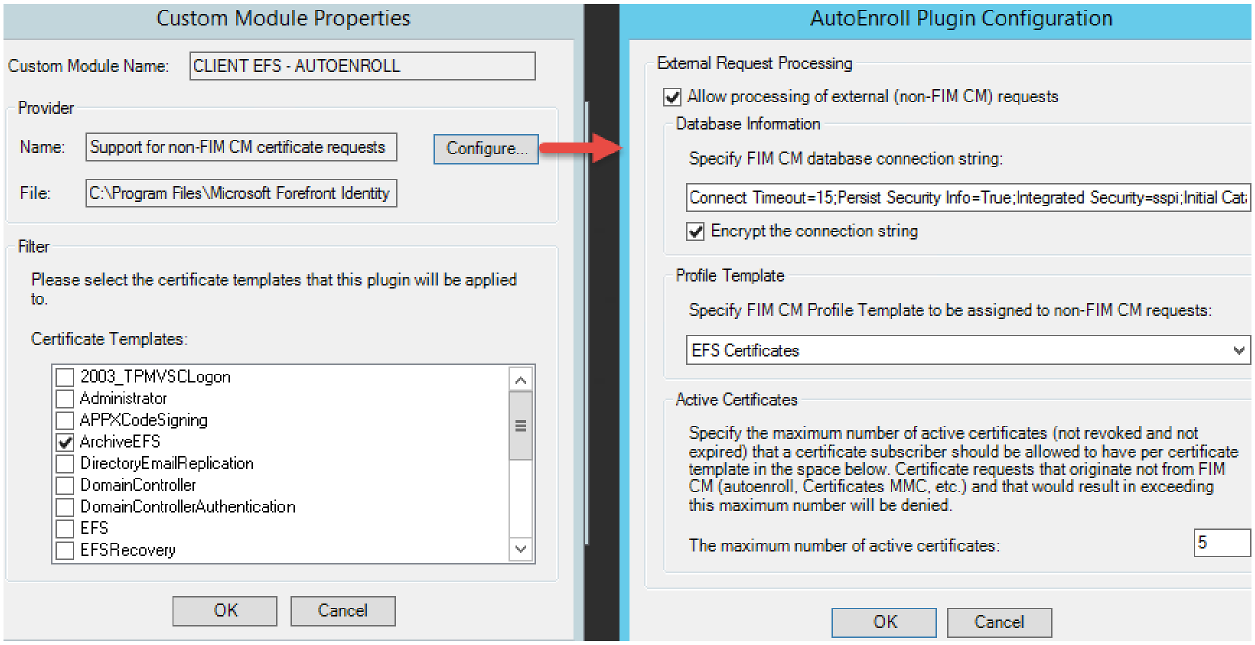
Custom modules:



FIM CM Policy Module

Assembly that you have selected implements more than one Policy Module Plugin. Please select one of them to proceed:

- Certificate SMimeCapabilities Module 1.0
- Certificate Subject Module 1.0
- SubjectAltName Module 1.1
- Support for non-FIM CM certificate requests



Custom Module Properties

Custom Module Name: CLIENT EFS - AUTOENROLL

Provider

Name: Support for non-FIM CM certificate requests

File: C:\Program Files\Microsoft Forefront Identity

Filter

Please select the certificate templates that this plugin will be applied to.

Certificate Templates:

- □ 2003_TPMVSCLogon
- □ Administrator
- □ APPXCodeSigning
- ☑ ArchiveEFS
- □ DirectoryEmailReplication
- □ DomainController
- □ DomainControllerAuthentication
- □ EFS
- □ EFSRecovery

AutoEnroll Plugin Configuration

External Request Processing

☑ Allow processing of external (non-FIM CM) requests

Database Information

Specify FIM CM database connection string:

Connect Timeout=15;Persist Security Info=True;Integrated Security=sspi;Initial Cat

☑ Encrypt the connection string

Profile Template

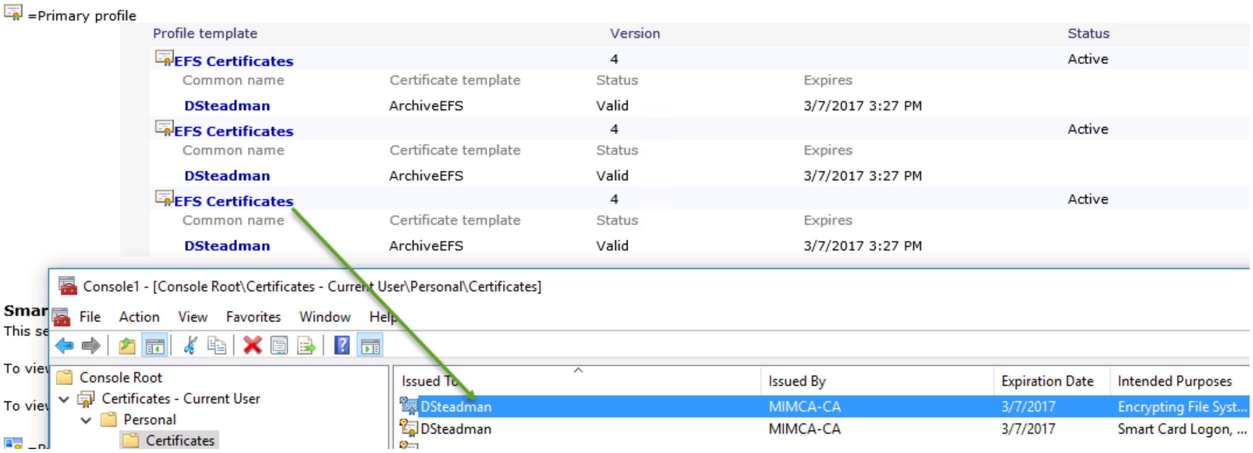
Specify FIM CM Profile Template to be assigned to non-FIM CM requests:

EFS Certificates

Active Certificates

Specify the maximum number of active certificates (not revoked and not expired) that a certificate subscriber should be allowed to have per certificate template in the space below. Certificate requests that originate not from FIM CM (autoenroll, Certificates MMC, etc.) and that would result in exceeding this maximum number will be denied.

The maximum number of active certificates: 5



=Primary profile

Profile template		Version		Status
EFS Certificates		4		Active
Common name	Certificate template	Status	Expires	
DSteadman	ArchiveEFS	Valid	3/7/2017 3:27 PM	
EFS Certificates		4		Active
Common name	Certificate template	Status	Expires	
DSteadman	ArchiveEFS	Valid	3/7/2017 3:27 PM	
EFS Certificates		4		Active
Common name	Certificate template	Status	Expires	
DSteadman	ArchiveEFS	Valid	3/7/2017 3:27 PM	

Smar

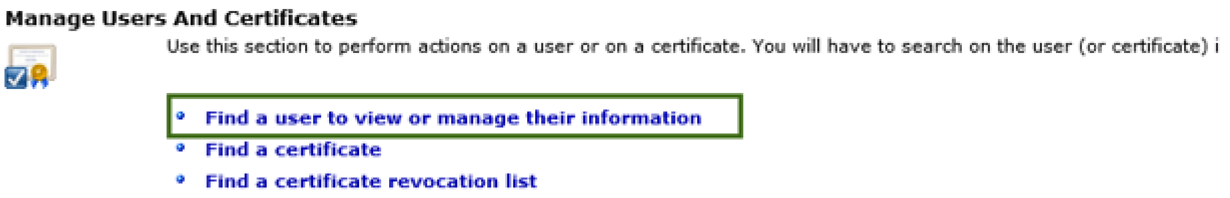
This se

To viev

To viev

Console1 - [Console Root\Certificates - Current User\Personal\Certificates]

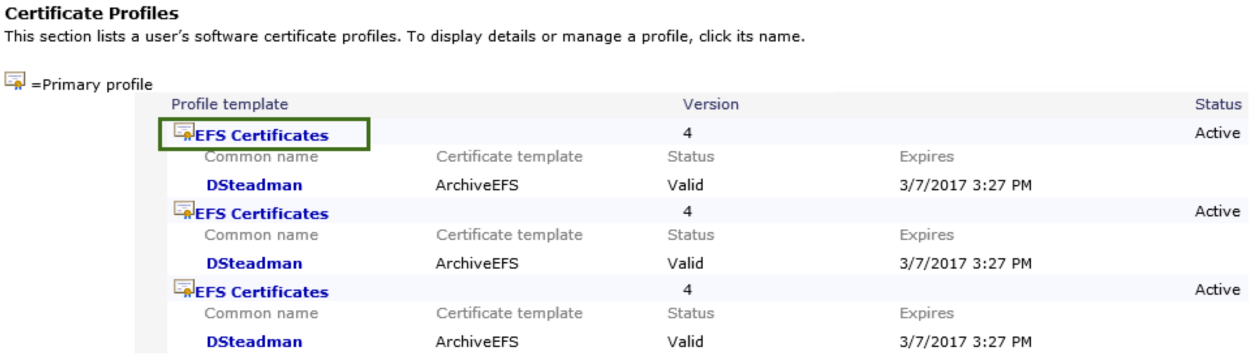
Issued To	Issued By	Expiration Date	Intended Purposes
DSteadman	MIMCA-CA	3/7/2017	Encrypting File Syst...
DSteadman	MIMCA-CA	3/7/2017	Smart Card Logon, ...



Manage Users And Certificates

Use this section to perform actions on a user or on a certificate. You will have to search on the user (or certificate) i

- Find a user to view or manage their information
- Find a certificate
- Find a certificate revocation list

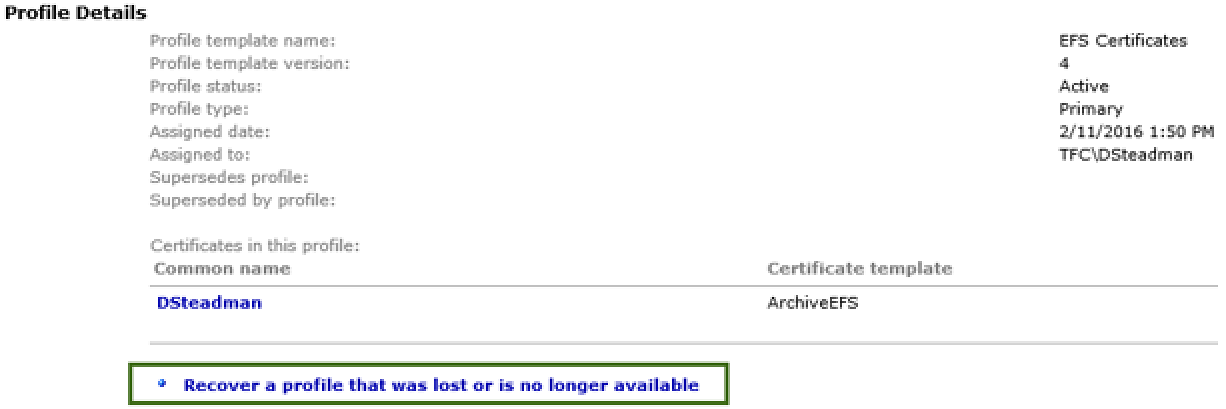


Certificate Profiles

This section lists a user's software certificate profiles. To display details or manage a profile, click its name.

=Primary profile

Profile template		Version		Status
EFS Certificates		4		Active
Common name	Certificate template	Status	Expires	
DSteadman	ArchiveEFS	Valid	3/7/2017 3:27 PM	
EFS Certificates		4		Active
Common name	Certificate template	Status	Expires	
DSteadman	ArchiveEFS	Valid	3/7/2017 3:27 PM	
EFS Certificates		4		Active
Common name	Certificate template	Status	Expires	
DSteadman	ArchiveEFS	Valid	3/7/2017 3:27 PM	



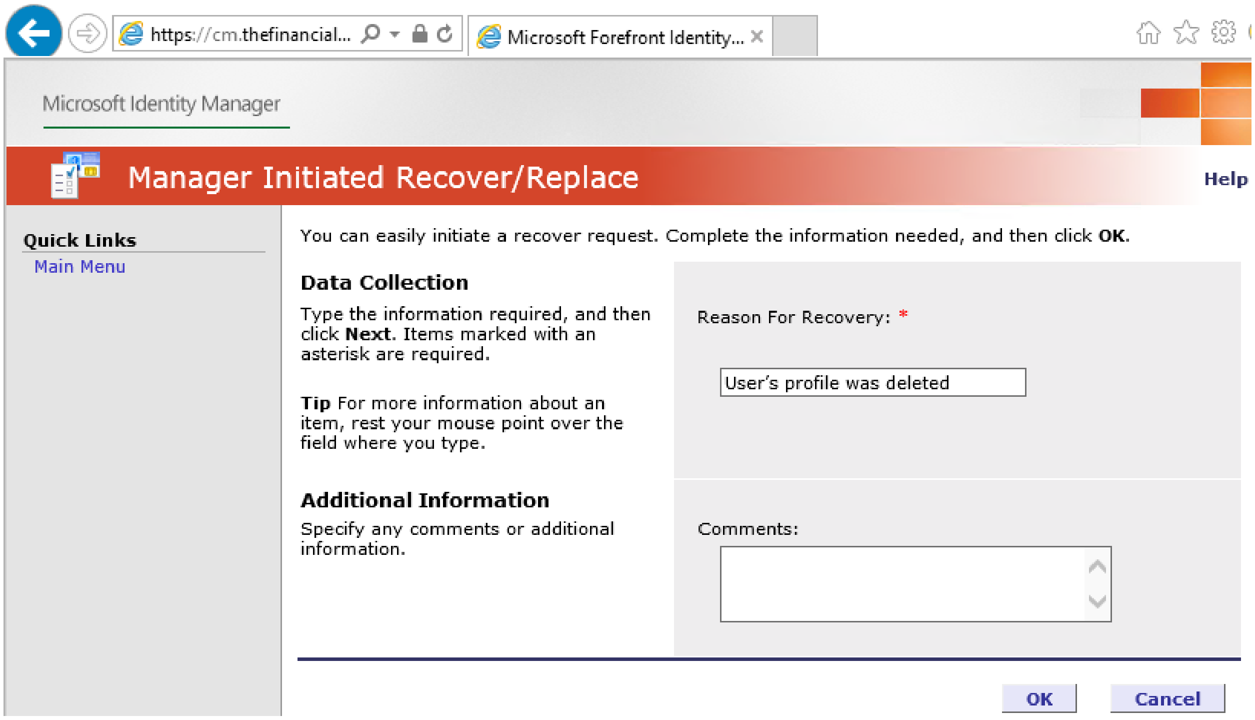
Profile Details

Profile template name:	EFS Certificates
Profile template version:	4
Profile status:	Active
Profile type:	Primary
Assigned date:	2/11/2016 1:50 PM
Assigned to:	TFC\DSteadman
Supersedes profile:	
Superseded by profile:	

Certificates in this profile:

Common name	Certificate template
DSteadman	ArchiveEFS

- Recover a profile that was lost or is no longer available


https://cm.thefinancial...
Microsoft Forefront Identity...
Microsoft Identity Manager

Manager Initiated Recover/Replace

Help

Quick Links

Main Menu

You can easily initiate a recover request. Complete the information needed, and then click **OK**.

Data Collection

Type the information required, and then click **Next**. Items marked with an asterisk are required.

Tip For more information about an item, rest your mouse point over the field where you type.

Reason For Recovery: *

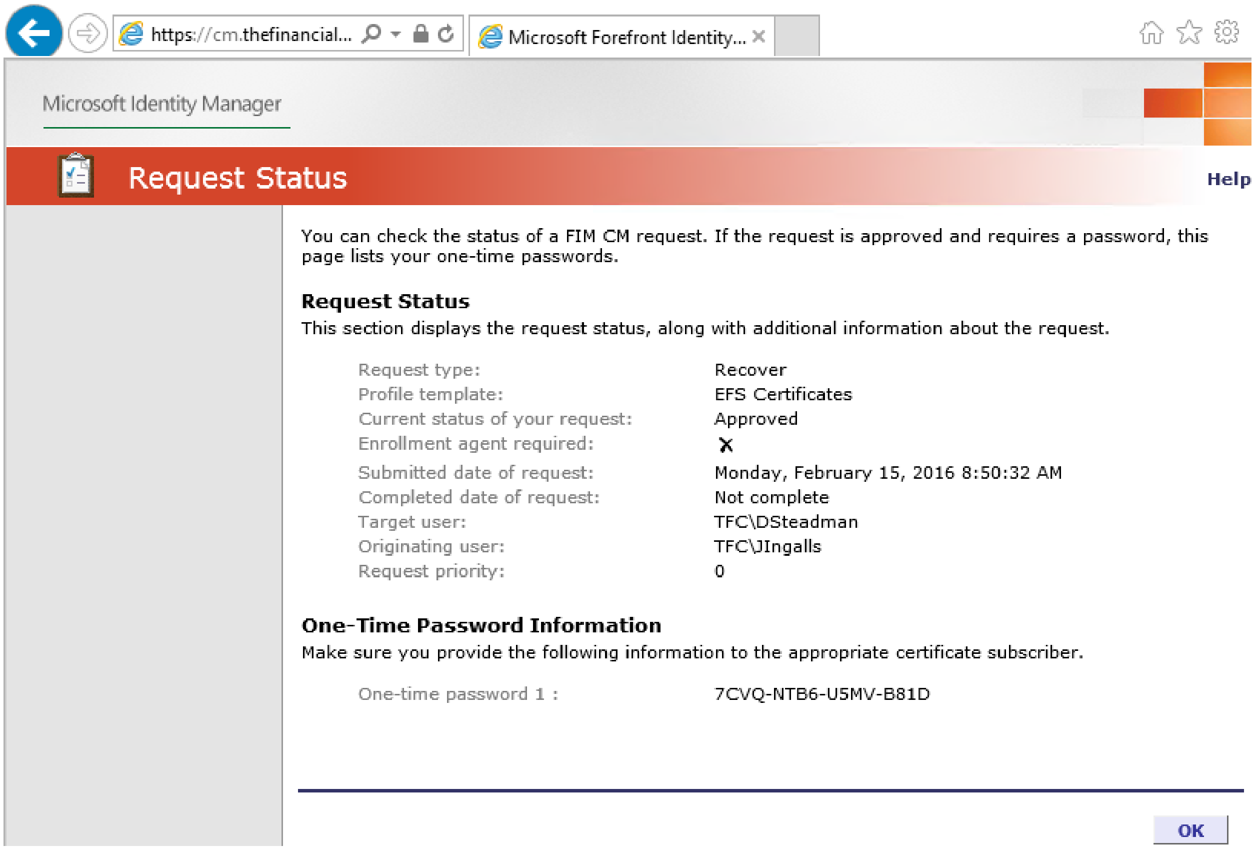
User's profile was deleted

Additional Information

Specify any comments or additional information.

Comments:

OK Cancel


https://cm.thefinancial...
Microsoft Forefront Identity...
Microsoft Identity Manager

Request Status

Help

You can check the status of a FIM CM request. If the request is approved and requires a password, this page lists your one-time passwords.

Request Status

This section displays the request status, along with additional information about the request.

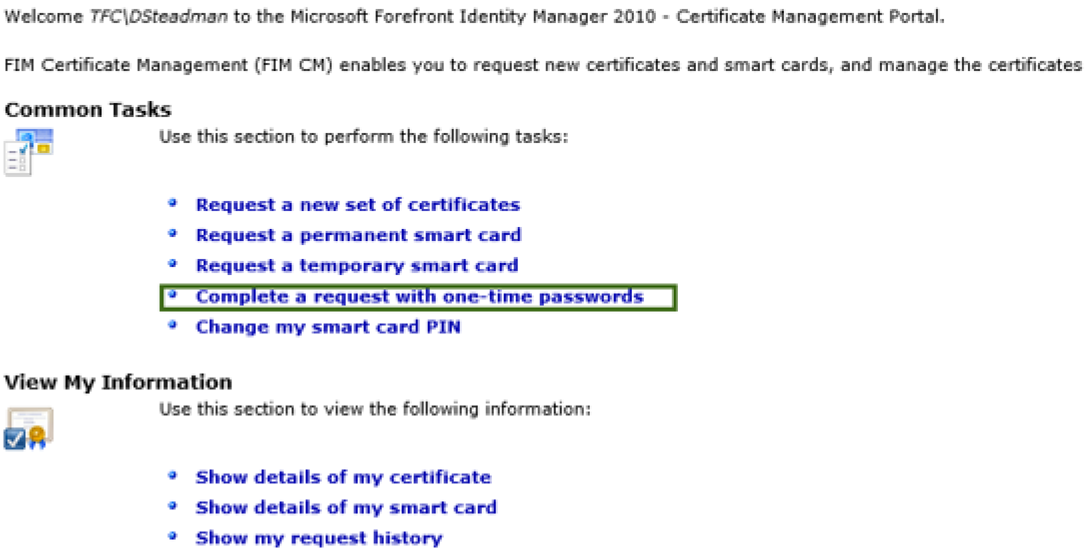
Request type:	Recover
Profile template:	EFS Certificates
Current status of your request:	Approved
Enrollment agent required:	✗
Submitted date of request:	Monday, February 15, 2016 8:50:32 AM
Completed date of request:	Not complete
Target user:	TFC\DSteadman
Originating user:	TFC\JIngalls
Request priority:	0

One-Time Password Information

Make sure you provide the following information to the appropriate certificate subscriber.

One-time password 1 :	7CVQ-NTB6-U5MV-B81D

OK



Welcome *TFC\DSteadman* to the Microsoft Forefront Identity Manager 2010 - Certificate Management Portal.

FIM Certificate Management (FIM CM) enables you to request new certificates and smart cards, and manage the certificates

Common Tasks

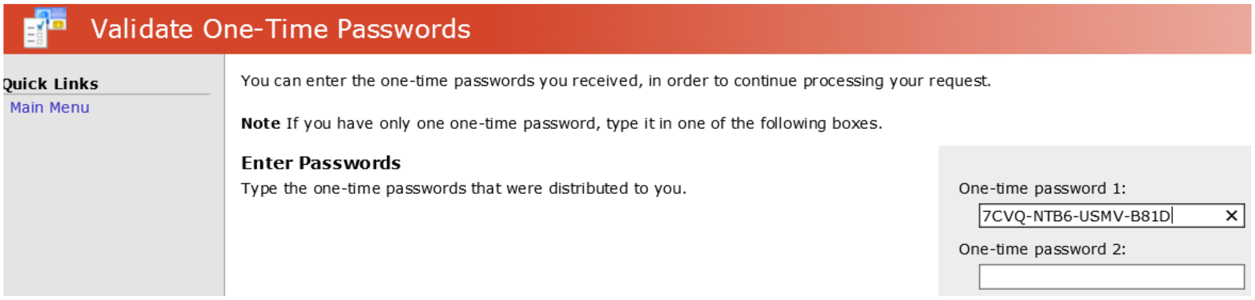
Use this section to perform the following tasks:

- Request a new set of certificates
- Request a permanent smart card
- Request a temporary smart card
- Complete a request with one-time passwords
- Change my smart card PIN

View My Information

Use this section to view the following information:

- Show details of my certificate
- Show details of my smart card
- Show my request history



Validate One-Time Passwords

You can enter the one-time passwords you received, in order to continue processing your request.

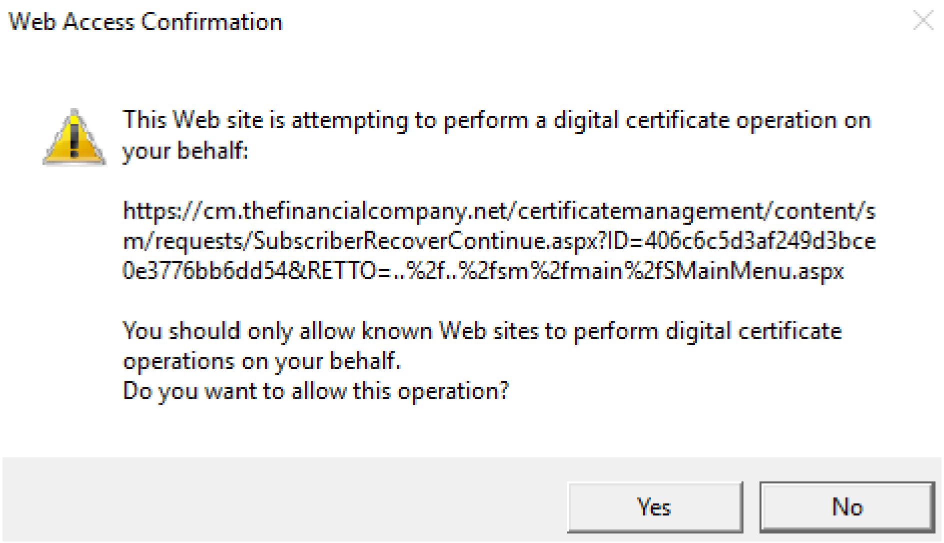
Note If you have only one one-time password, type it in one of the following boxes.

Enter Passwords

Type the one-time passwords that were distributed to you.

One-time password 1: 7CVQ-NTB6-USMV-B81D

One-time password 2:

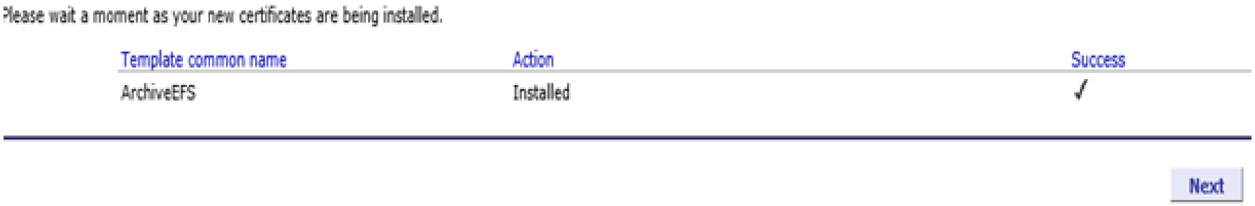


Web Access Confirmation

This Web site is attempting to perform a digital certificate operation on your behalf:

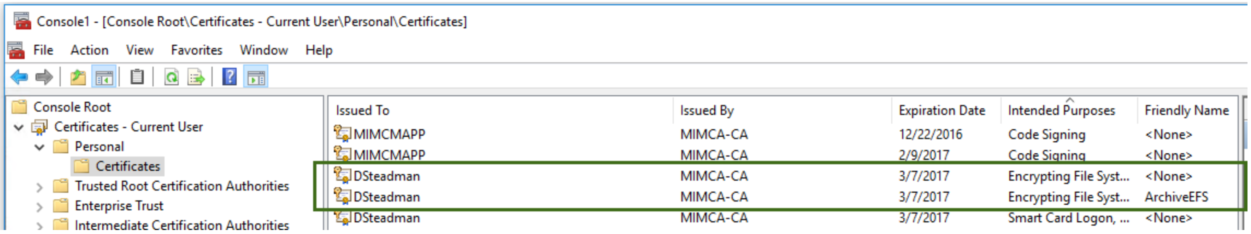
https://cm.thefinancialcompany.net/certificatemanagement/content/sm/requests/SubscriberRecoverContinue.aspx?ID=406c6c5d3af249d3bce0e3776bb6dd54&RETTO=..%2f..%2fsm%2fmain%2fSMainMenu.aspx

You should only allow known Web sites to perform digital certificate operations on your behalf.
Do you want to allow this operation?

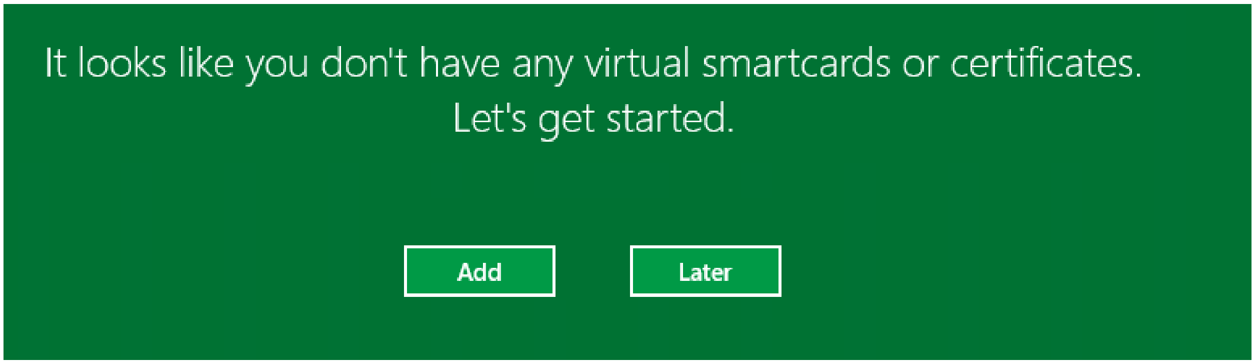


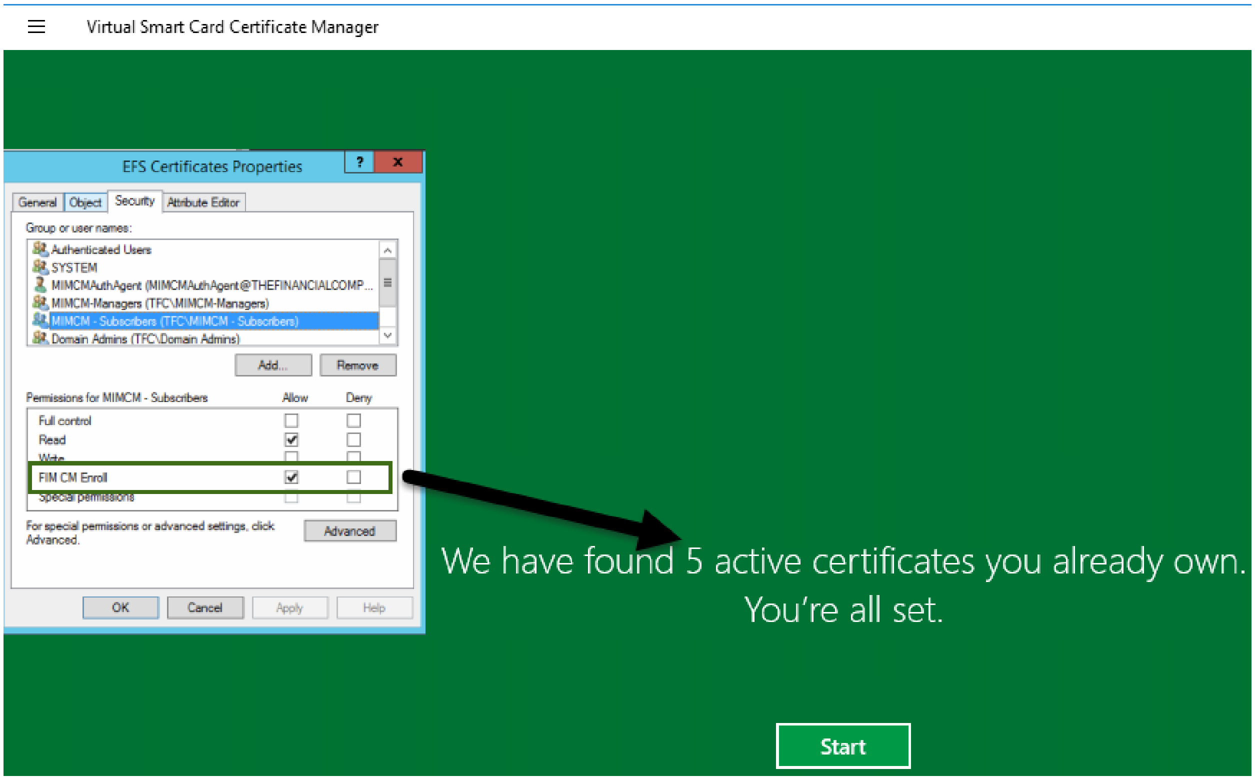
Please wait a moment as your new certificates are being installed.

Template common name	Action	Success
ArchiveEFS	Installed	✓


Console1 - [Console Root\Certificates - Current User\Personal\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
MIMCMAPP	MIMCA-CA	12/22/2016	Code Signing	<None>
MIMCMAPP	MIMCA-CA	2/9/2017	Code Signing	<None>
DSteadman	MIMCA-CA	3/7/2017	Encrypting File Syst...	<None>
DSteadman	MIMCA-CA	3/7/2017	Encrypting File Syst...	ArchiveEFS
DSteadman	MIMCA-CA	3/7/2017	Smart Card Logon, ...	<None>


It looks like you don't have any virtual smartcards or certificates. Let's get started.


Virtual Smart Card Certificate Manager
EFS Certificates Properties
General
Object
Security
Attribute Editor

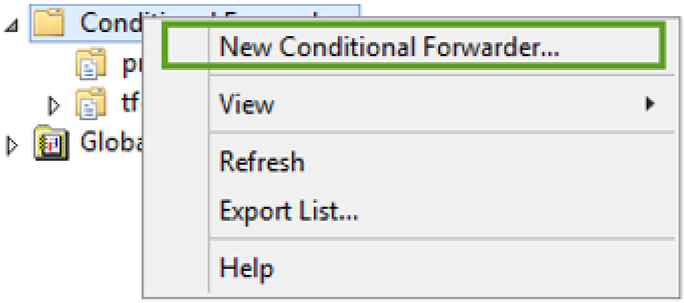
Group or user names:

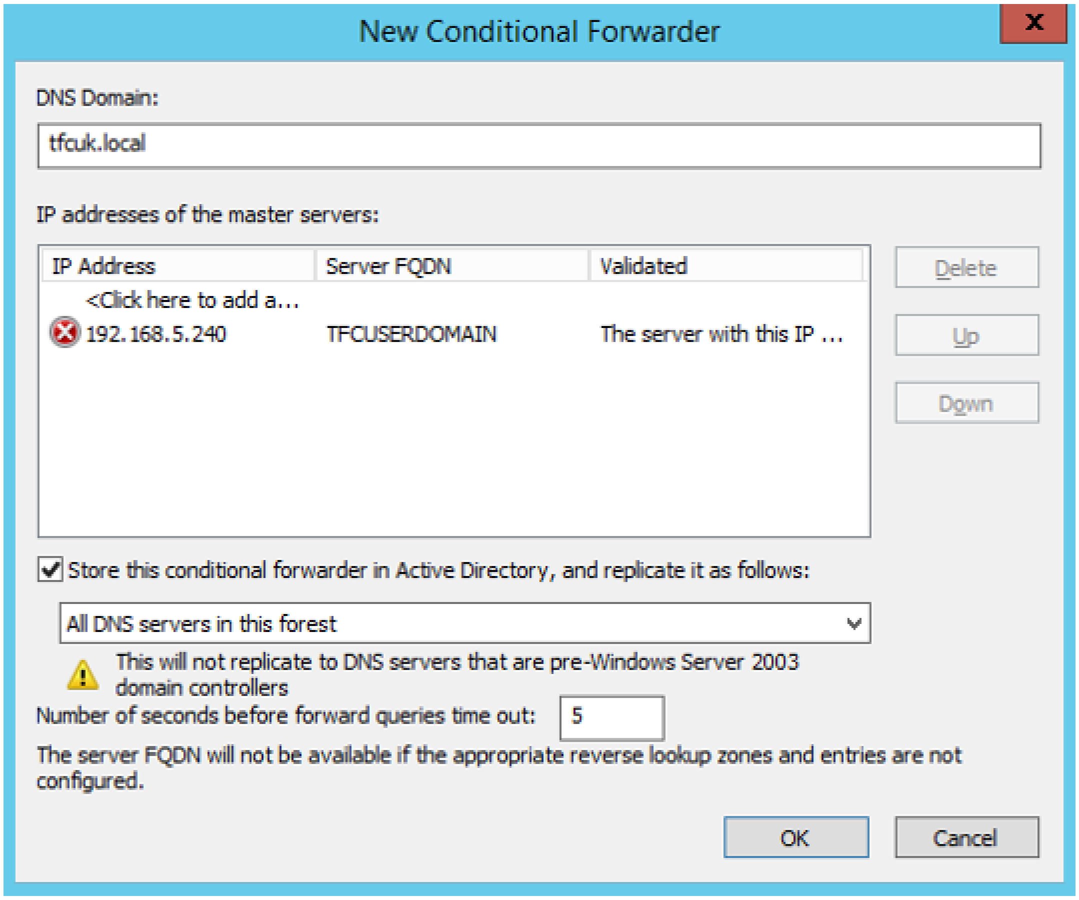
- Authenticated Users
- SYSTEM
- MIMCMAuthAgent (MIMCMAuthAgent@THEFINANCIALCOMP...
- MIMCM-Managers (TFC\MIMCM-Managers)
- MIMCM - Subscribers (TFC\MIMCM - Subscribers)
- Domain Admins (TFC\Domain Admins)

Permissions for MIMCM - Subscribers	Allow	Deny
Full control	□	□
Read	☑	□
Write	□	□
FIM CM Enroll	☑	□
Special permissions	□	□

For special permissions or advanced settings, click Advanced.

We have found 5 active certificates you already own. You're all set.




New Conditional Forwarder

DNS Domain:

tfcuk.local

IP addresses of the master servers:

IP Address	Server FQDN	Validated
<Click here to add a...		
☒ 192.168.5.240	TFCUSERDOMAIN	The server with this IP ...

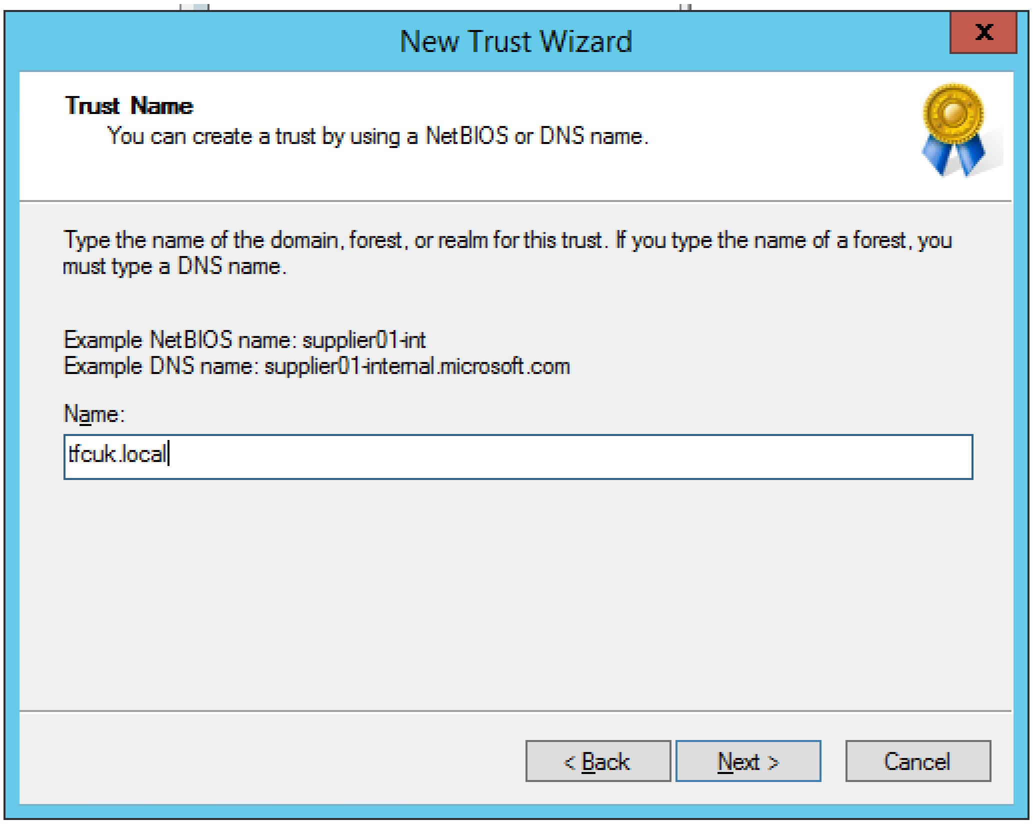
☑ Store this conditional forwarder in Active Directory, and replicate it as follows:

All DNS servers in this forest

⚠ This will not replicate to DNS servers that are pre-Windows Server 2003 domain controllers

Number of seconds before forward queries time out: 5

The server FQDN will not be available if the appropriate reverse lookup zones and entries are not configured.



New Trust Wizard

Trust Name

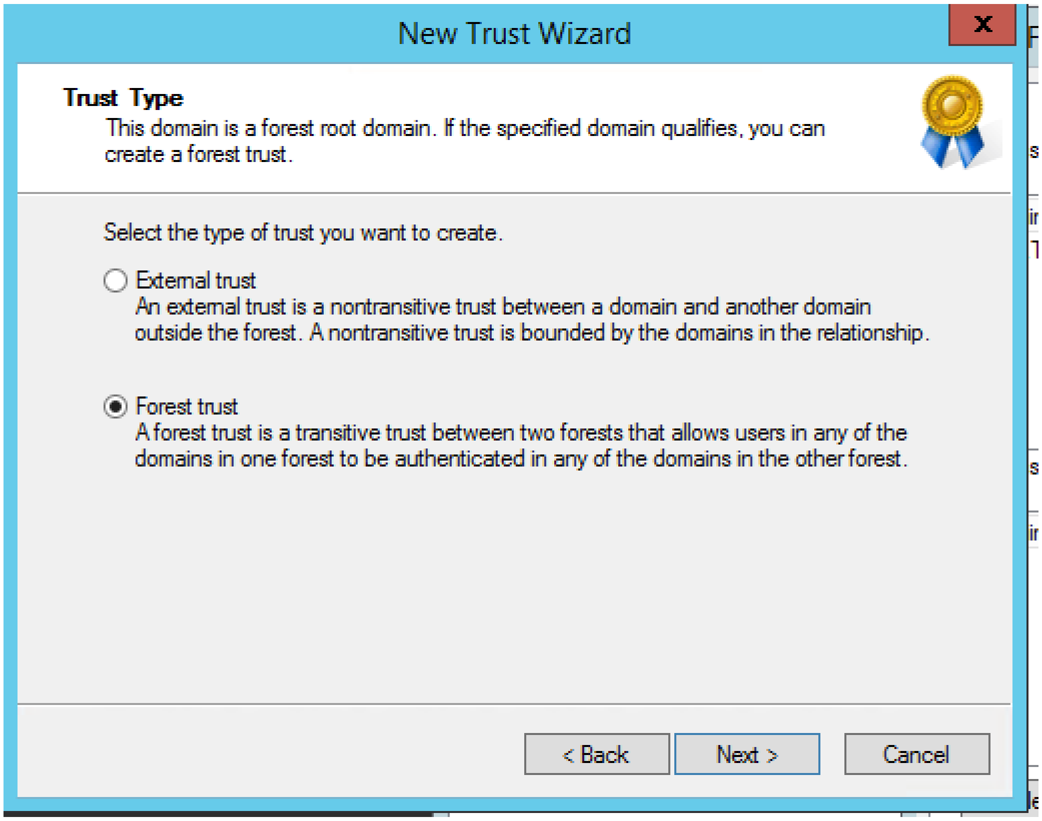
You can create a trust by using a NetBIOS or DNS name.

Type the name of the domain, forest, or realm for this trust. If you type the name of a forest, you must type a DNS name.

Example NetBIOS name: supplier01-int
Example DNS name: supplier01-internal.microsoft.com

Name:

tfcuk.local



New Trust Wizard

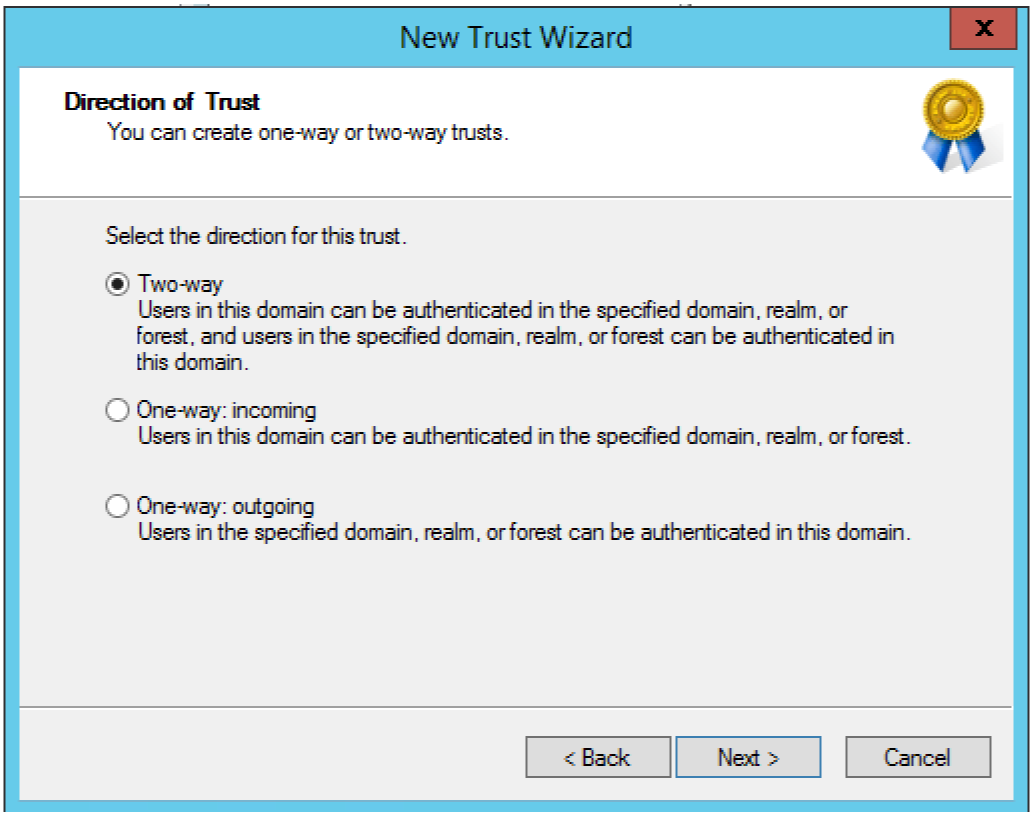
Trust Type

This domain is a forest root domain. If the specified domain qualifies, you can create a forest trust.

Select the type of trust you want to create.

○ External trust
An external trust is a nontransitive trust between a domain and another domain outside the forest. A nontransitive trust is bounded by the domains in the relationship.

● Forest trust
A forest trust is a transitive trust between two forests that allows users in any of the domains in one forest to be authenticated in any of the domains in the other forest.



Direction of Trust

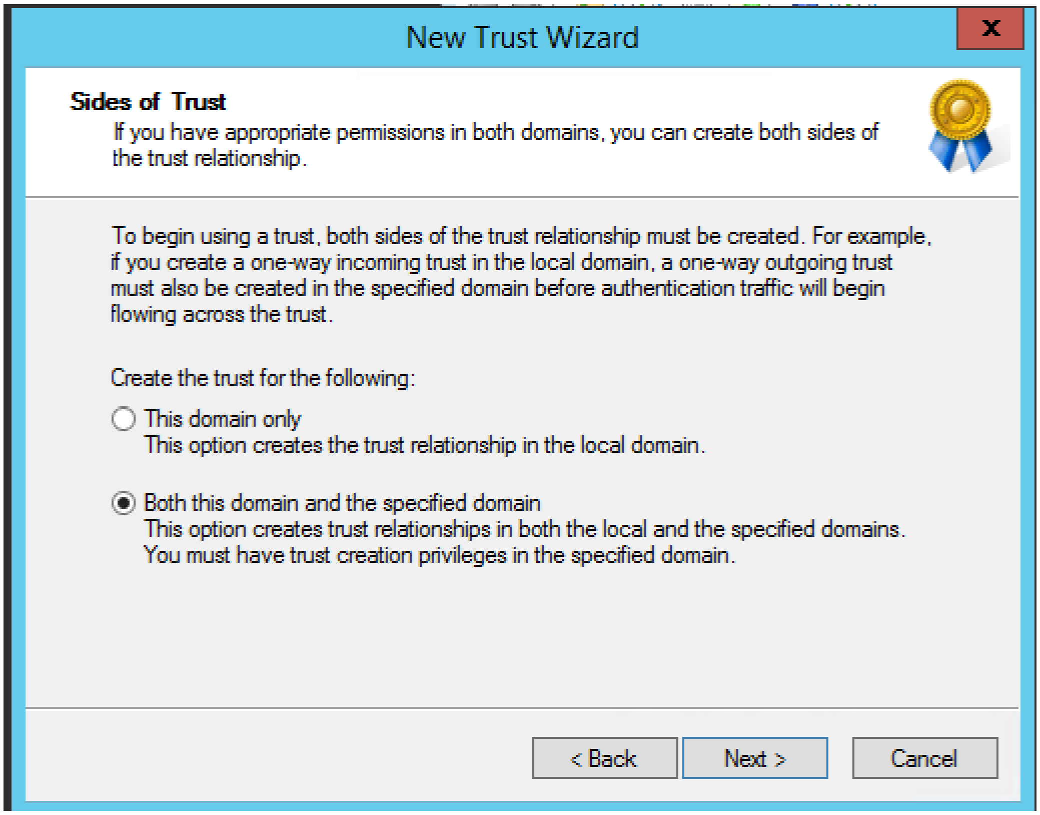
You can create one-way or two-way trusts.

Select the direction for this trust.

● Two-way
Users in this domain can be authenticated in the specified domain, realm, or forest, and users in the specified domain, realm, or forest can be authenticated in this domain.

○ One-way: incoming
Users in this domain can be authenticated in the specified domain, realm, or forest.

○ One-way: outgoing
Users in the specified domain, realm, or forest can be authenticated in this domain.



Sides of Trust

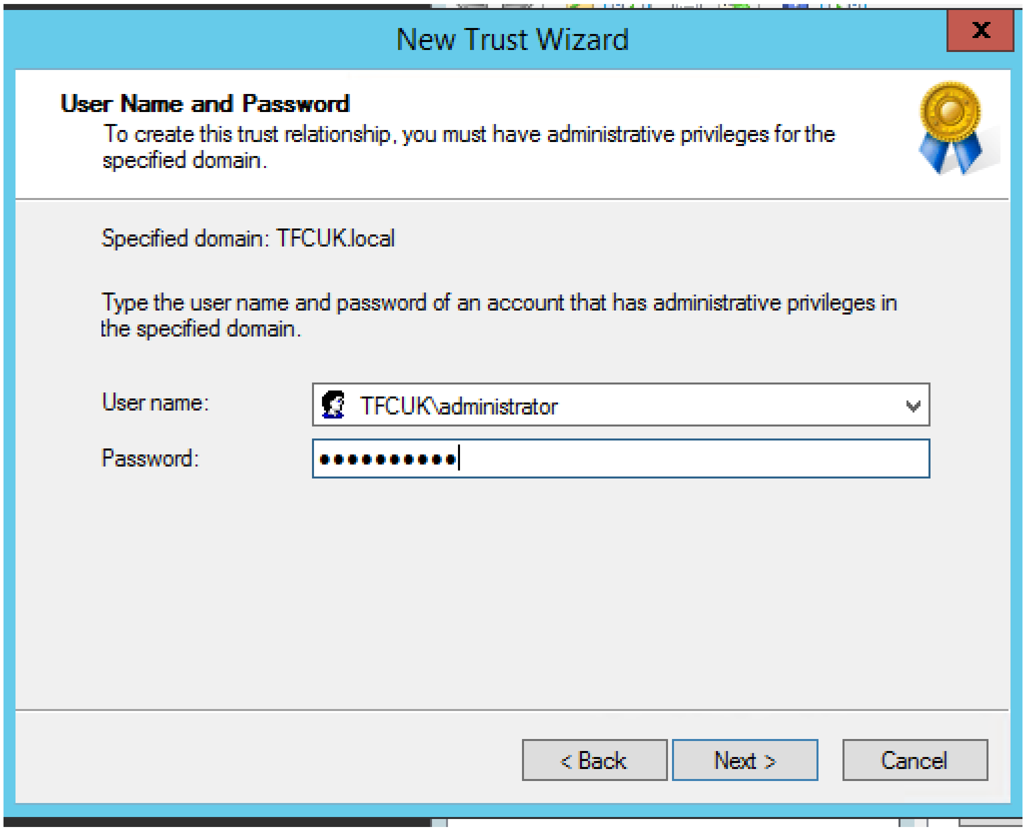
If you have appropriate permissions in both domains, you can create both sides of the trust relationship.

To begin using a trust, both sides of the trust relationship must be created. For example, if you create a one-way incoming trust in the local domain, a one-way outgoing trust must also be created in the specified domain before authentication traffic will begin flowing across the trust.

Create the trust for the following:

○ This domain only
This option creates the trust relationship in the local domain.

● Both this domain and the specified domain
This option creates trust relationships in both the local and the specified domains. You must have trust creation privileges in the specified domain.



User Name and Password

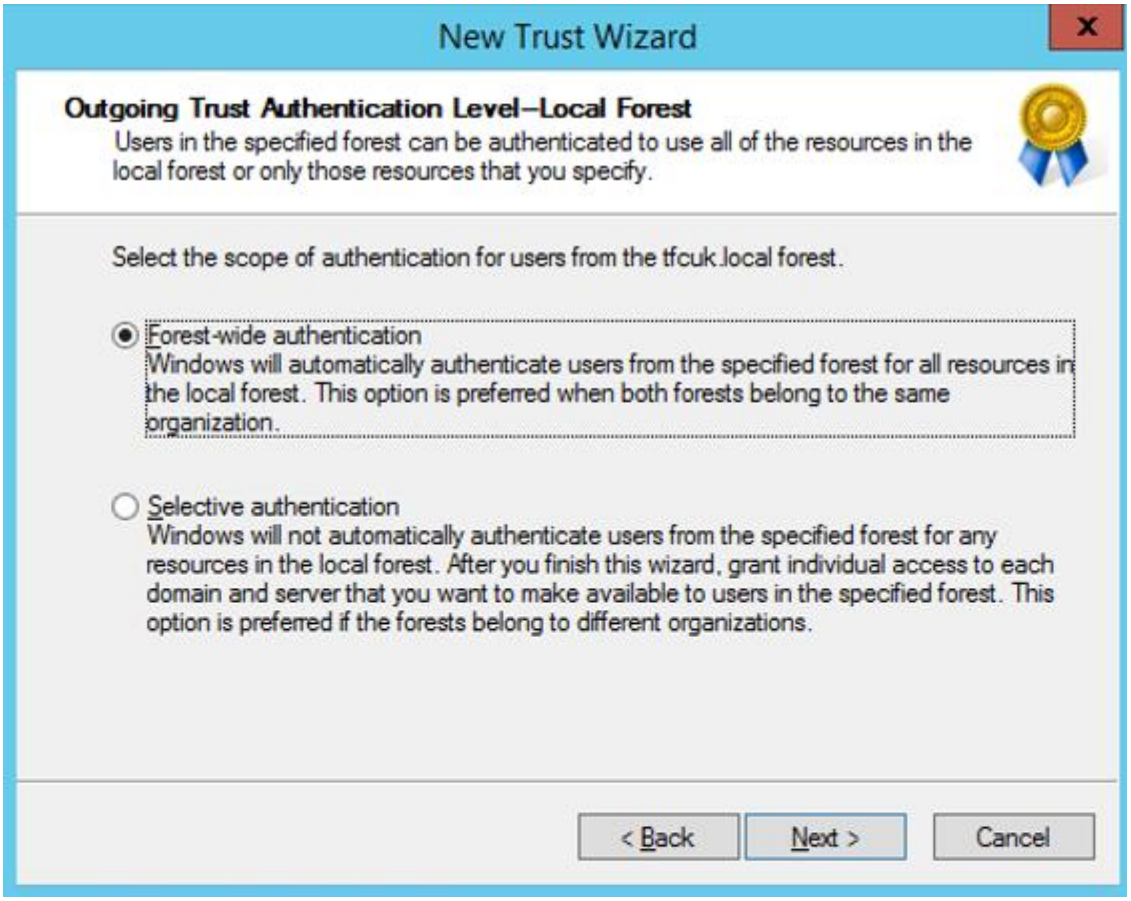
To create this trust relationship, you must have administrative privileges for the specified domain.

Specified domain: TFCUK.local

Type the user name and password of an account that has administrative privileges in the specified domain.

User name: TFCUK\administrator

Password: ●●●●●●●●●●●



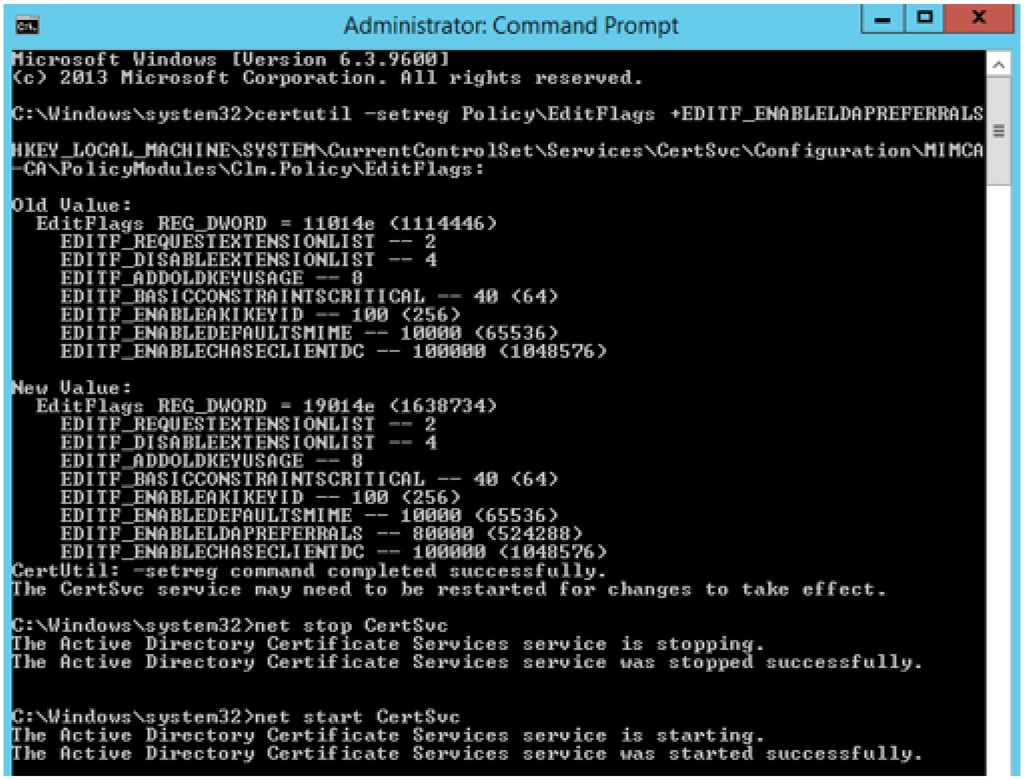
Outgoing Trust Authentication Level—Local Forest

Users in the specified forest can be authenticated to use all of the resources in the local forest or only those resources that you specify.

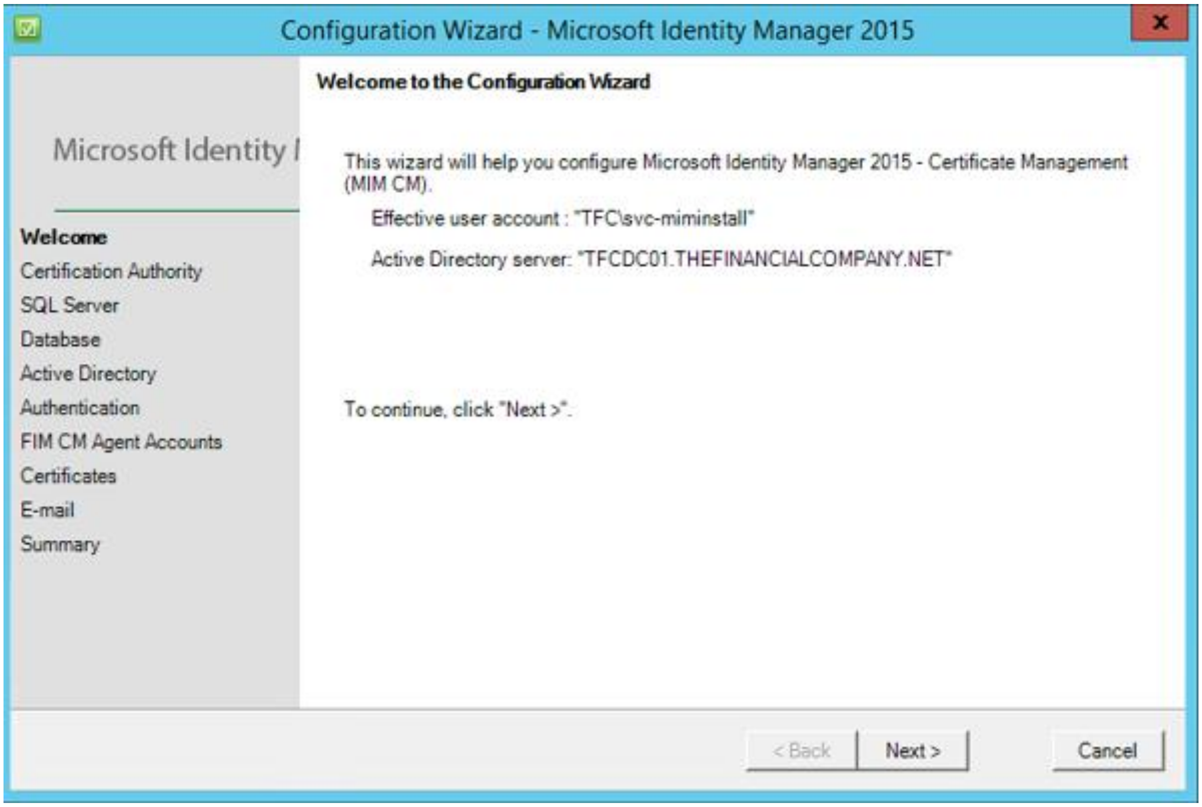
Select the scope of authentication for users from the tfcuk.local forest.

● Forest-wide authentication
Windows will automatically authenticate users from the specified forest for all resources in the local forest. This option is preferred when both forests belong to the same organization.

○ Selective authentication
Windows will not automatically authenticate users from the specified forest for any resources in the local forest. After you finish this wizard, grant individual access to each domain and server that you want to make available to users in the specified forest. This option is preferred if the forests belong to different organizations.



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>certutil -setreg Policy\EditFlags +EDITF_ENABLELDAPREFERRALS

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\MIMCA
-CA\PolicyModules\Clm.Policy\EditFlags:

Old Value:
  EditFlags REG_DWORD = 11014e (1114446)
    EDITF_REQUESTEXTENSIONLIST -- 2
    EDITF_DISABLEEXTENSIONLIST -- 4
    EDITF_ADDOLDKEYUSAGE -- 8
    EDITF_BASICCONSTRAINTSCRITICAL -- 40 (64)
    EDITF_ENABLEAKIKEYID -- 100 (256)
    EDITF_ENABLEDEFAULTSMIME -- 10000 (65536)
    EDITF_ENABLECHASECLIENTDC -- 100000 (1048576)

New Value:
  EditFlags REG_DWORD = 19014e (1638734)
    EDITF_REQUESTEXTENSIONLIST -- 2
    EDITF_DISABLEEXTENSIONLIST -- 4
    EDITF_ADDOLDKEYUSAGE -- 8
    EDITF_BASICCONSTRAINTSCRITICAL -- 40 (64)
    EDITF_ENABLEAKIKEYID -- 100 (256)
    EDITF_ENABLEDEFAULTSMIME -- 10000 (65536)
    EDITF_ENABLELDAPREFERRALS -- 80000 (524288)
    EDITF_ENABLECHASECLIENTDC -- 100000 (1048576)
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.

C:\Windows\system32>net stop CertSvc
The Active Directory Certificate Services service is stopping.
The Active Directory Certificate Services service was stopped successfully.


C:\Windows\system32>net start CertSvc
The Active Directory Certificate Services service is starting.
The Active Directory Certificate Services service was started successfully.
```



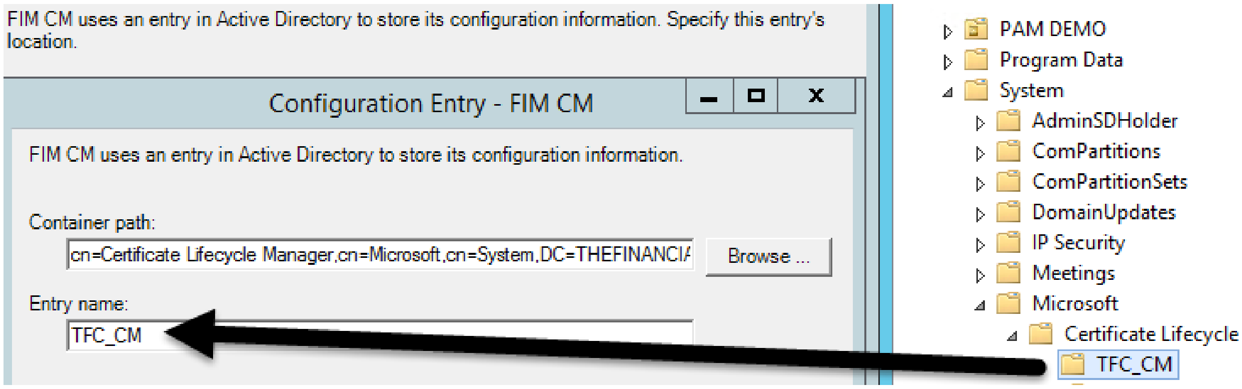
Welcome to the Configuration Wizard

This wizard will help you configure Microsoft Identity Manager 2015 - Certificate Management (MIM CM).

Effective user account : "TFC\svc-miminstall"

Active Directory server: "TFCDC01.THEFINANCIALCOMPANY.NET"

To continue, click "Next >".



FIM CM uses an entry in Active Directory to store its configuration information. Specify this entry's location.

Configuration Entry - FIM CM

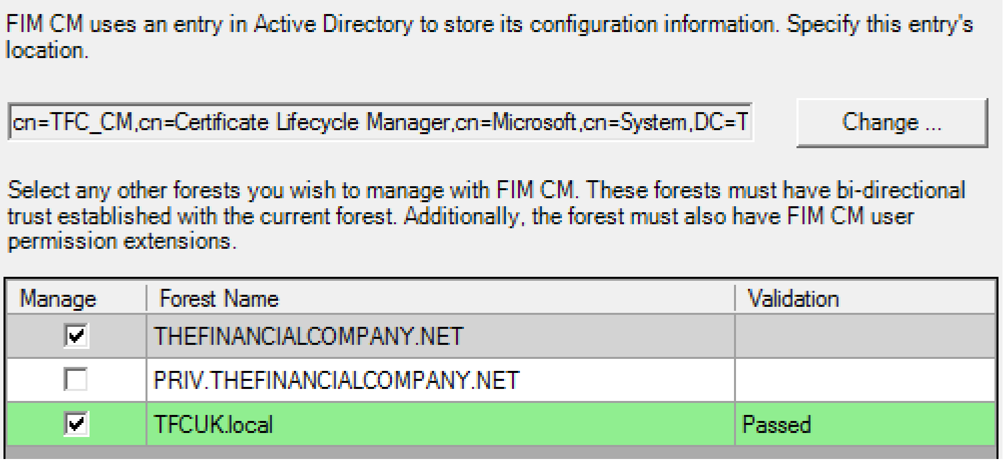
FIM CM uses an entry in Active Directory to store its configuration information.

Container path:

cn=Certificate Lifecycle Manager,cn=Microsoft,cn=System,DC=THEFINANCIA

Entry name:

TFC_CM

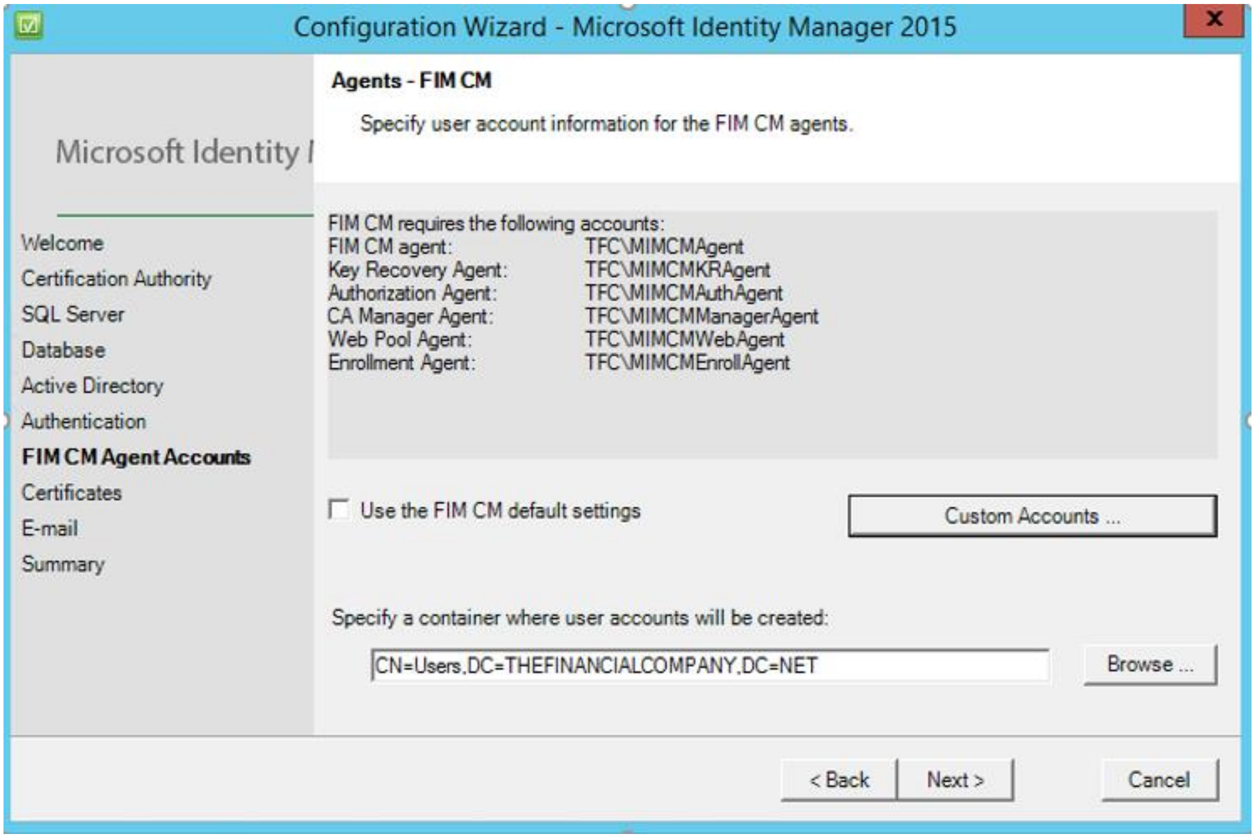


FIM CM uses an entry in Active Directory to store its configuration information. Specify this entry's location.

cn=TFC_CM,cn=Certificate Lifecycle Manager,cn=Microsoft,cn=System,DC=T

Select any other forests you wish to manage with FIM CM. These forests must have bi-directional trust established with the current forest. Additionally, the forest must also have FIM CM user permission extensions.

Manage	Forest Name	Validation
☑	THEFINANCIALCOMPANY.NET	
□	PRIV.THEFINANCIALCOMPANY.NET	
☑	TFCUK.local	Passed



Configuration Wizard - Microsoft Identity Manager 2015

Agents - FIM CM

Specify user account information for the FIM CM agents.

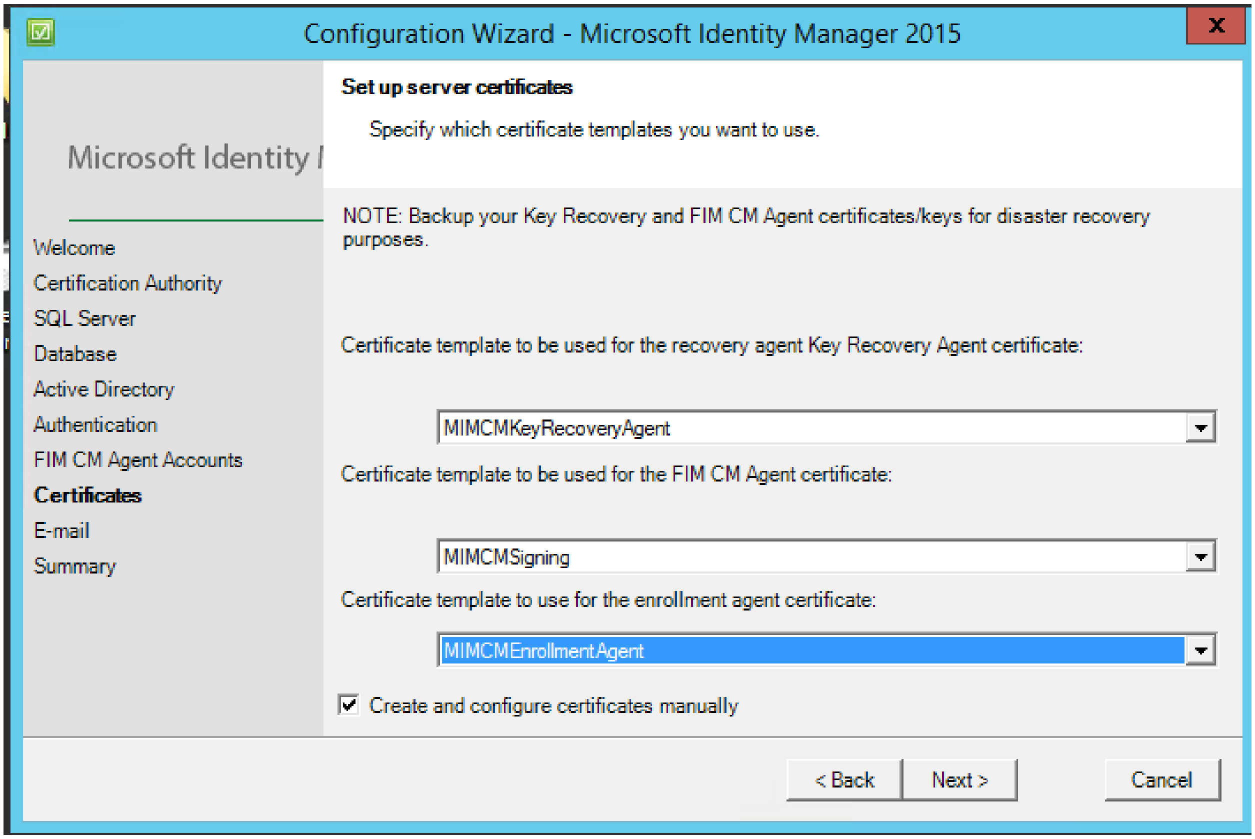
FIM CM requires the following accounts:

FIM CM agent:	TFC\MIMCMAgent
Key Recovery Agent:	TFC\MIMCMKRAgent
Authorization Agent:	TFC\MIMCMAuthAgent
CA Manager Agent:	TFC\MIMCMManagerAgent
Web Pool Agent:	TFC\MIMCMWebAgent
Enrollment Agent:	TFC\MIMCMEnrollAgent

☐ Use the FIM CM default settings

Specify a container where user accounts will be created:

CN=Users,DC=THEFINANCIALCOMPANY,DC=NET



Configuration Wizard - Microsoft Identity Manager 2015

Set up server certificates

Specify which certificate templates you want to use.

NOTE: Backup your Key Recovery and FIM CM Agent certificates/keys for disaster recovery purposes.

Certificate template to be used for the recovery agent Key Recovery Agent certificate:

MIMCMKeyRecoveryAgent

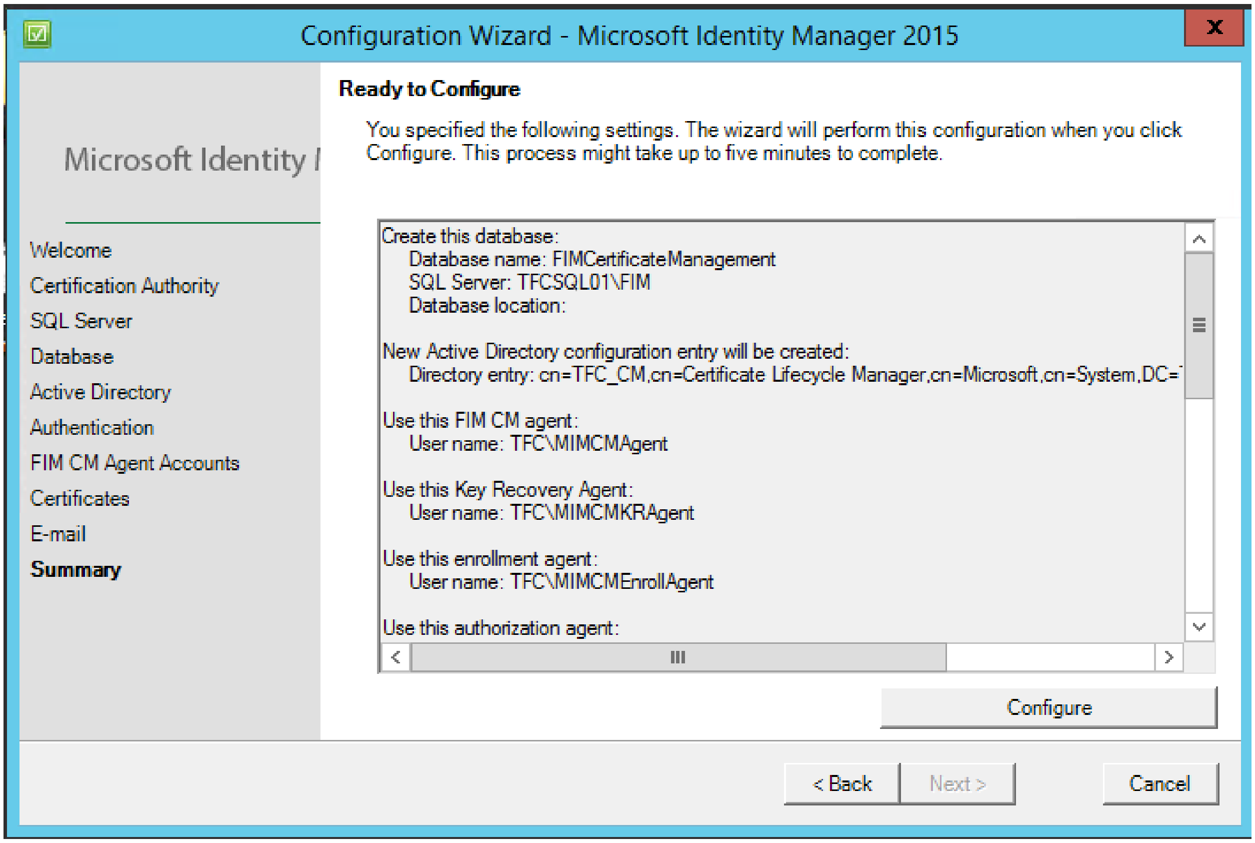
Certificate template to be used for the FIM CM Agent certificate:

MIMCMSigning

Certificate template to use for the enrollment agent certificate:

MIMCMEnrollmentAgent

☑ Create and configure certificates manually

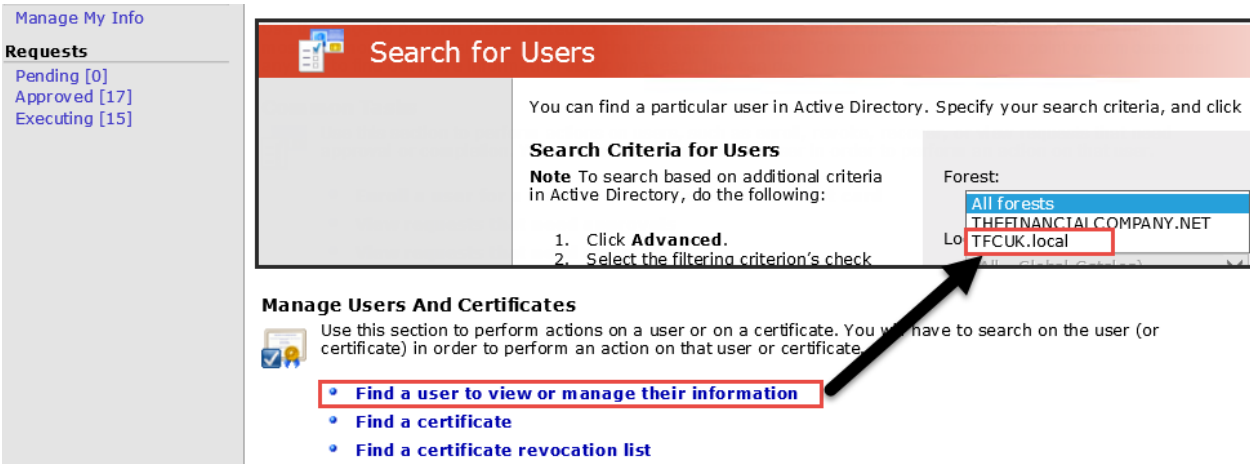


Configuration Wizard - Microsoft Identity Manager 2015

Ready to Configure

You specified the following settings. The wizard will perform this configuration when you click Configure. This process might take up to five minutes to complete.

```
Create this database:
    Database name: FIMCertificateManagement
    SQL Server: TFCSQL01\FIM
    Database location:

New Active Directory configuration entry will be created:
    Directory entry: cn=TFC_CM,cn=Certificate Lifecycle Manager,cn=Microsoft,cn=System,DC=

Use this FIM CM agent:
    User name: TFC\MIMCMAgent

Use this Key Recovery Agent:
    User name: TFC\MIMCMKRAgent

Use this enrollment agent:
    User name: TFC\MIMCMEnrollAgent

Use this authorization agent:
```



Search for Users

You can find a particular user in Active Directory. Specify your search criteria, and click

Search Criteria for Users

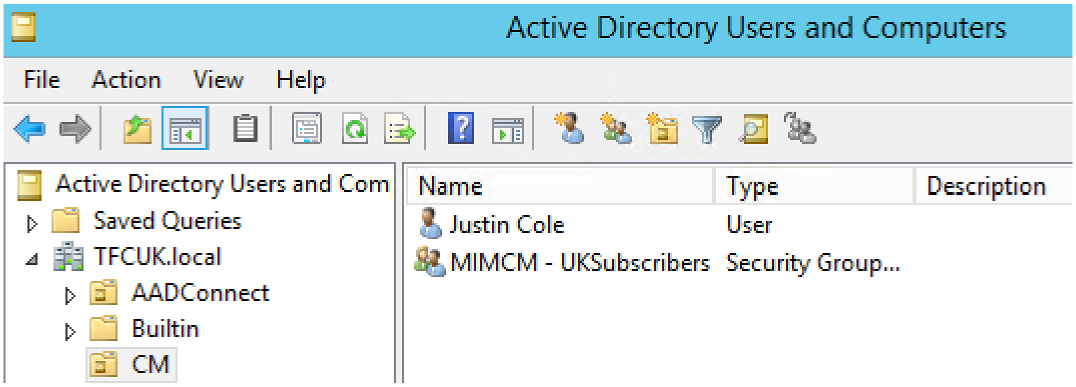
Note To search based on additional criteria in Active Directory, do the following:

1. Click **Advanced**.
2. Select the filtering criterion's check

Manage Users And Certificates

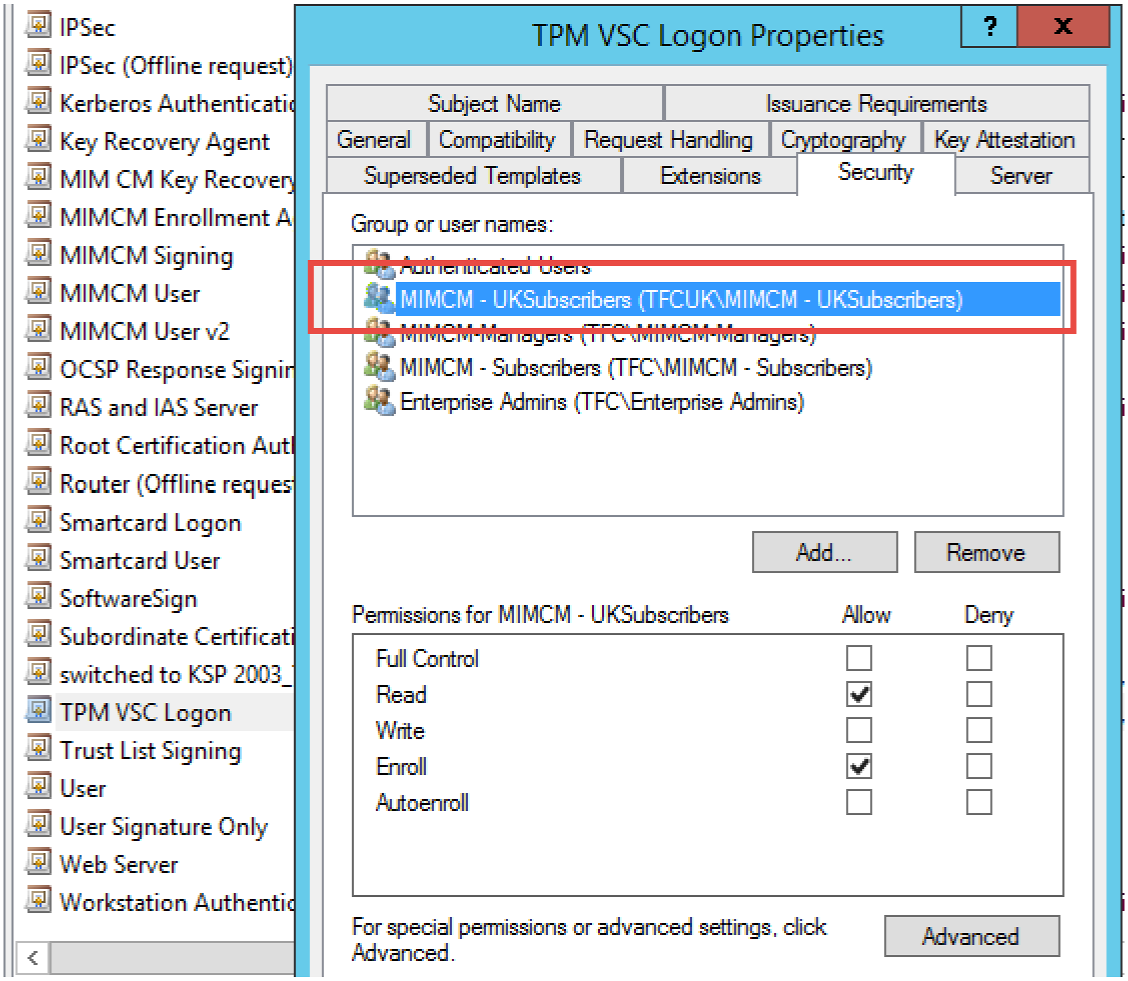
Use this section to perform actions on a user or on a certificate. You will have to search on the user (or certificate) in order to perform an action on that user or certificate.

- Find a user to view or manage their information
- Find a certificate
- Find a certificate revocation list



- Active Directory Users and Com
  - Saved Queries
  - TFCUK.local
    - AADConnect
    - Builtin
    - CM

Name	Type	Description
Justin Cole	User	
MIMCM - UKSubscribers	Security Group...	



- IPSec
- IPSec (Offline request)
- Kerberos Authenticatio
- Key Recovery Agent
- MIM CM Key Recovery
- MIMCM Enrollment A
- MIMCM Signing
- MIMCM User
- MIMCM User v2
- OCSP Response Signin
- RAS and IAS Server
- Root Certification Autl
- Router (Offline reques
- Smartcard Logon
- Smartcard User
- SoftwareSign
- Subordinate Certificati
- switched to KSP 2003_
- TPM VSC Logon
- Trust List Signing
- User
- User Signature Only
- Web Server
- Workstation Authentic

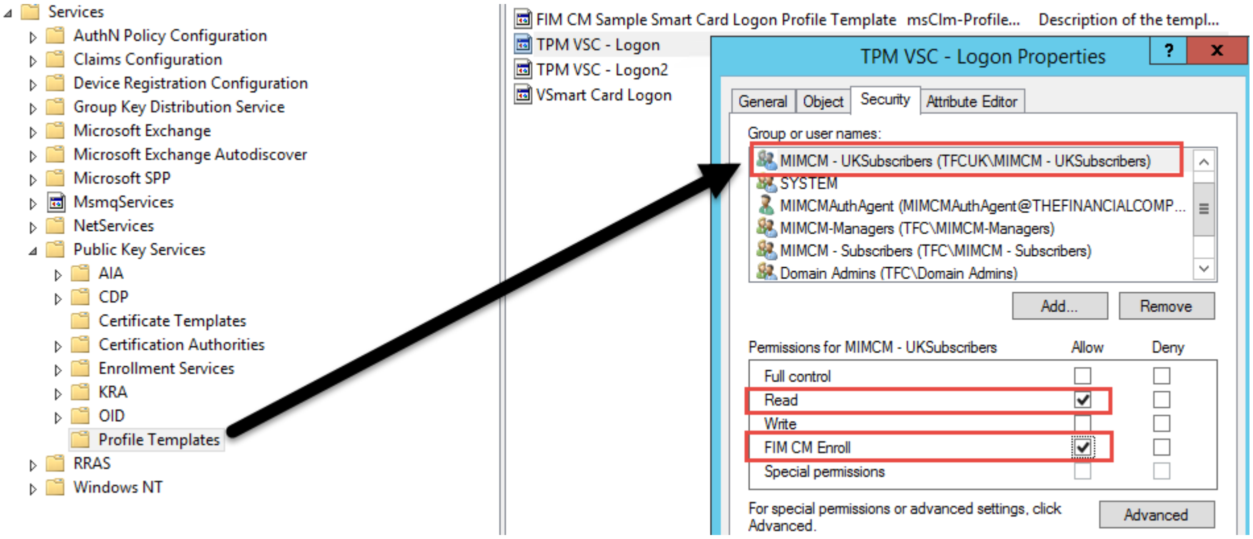
TPM VSC Logon Properties

Group or user names:

- Authenticated Users
- MIMCM - UKSubscribers (TFCUK\MIMCM - UKSubscribers)
- MIMCM-Managers (TFC\MIMCM-Managers)
- MIMCM - Subscribers (TFC\MIMCM - Subscribers)
- Enterprise Admins (TFC\Enterprise Admins)

Permissions for MIMCM - UKSubscribers	Allow	Deny
Full Control	□	□
Read	☑	□
Write	□	□
Enroll	☑	□
Autoenroll	□	□

For special permissions or advanced settings, click Advanced.

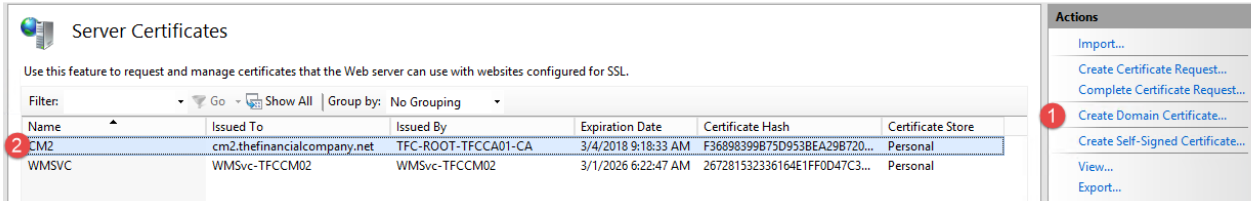


Group or user names:

- MIMCM - UKSubscribers (TFCUK\MIMCM - UKSubscribers)
- SYSTEM
- MIMCMAuthAgent (MIMCMAuthAgent@THEFINANCIALCOMP...
- MIMCM-Managers (TFC\MIMCM-Managers)
- MIMCM - Subscribers (TFC\MIMCM - Subscribers)
- Domain Admins (TFC\Domain Admins)

Permissions for MIMCM - UKSubscribers	Allow	Deny
Full control	□	□
Read	☑	□
Write	□	□
FIM CM Enroll	☑	□
Special permissions	□	□

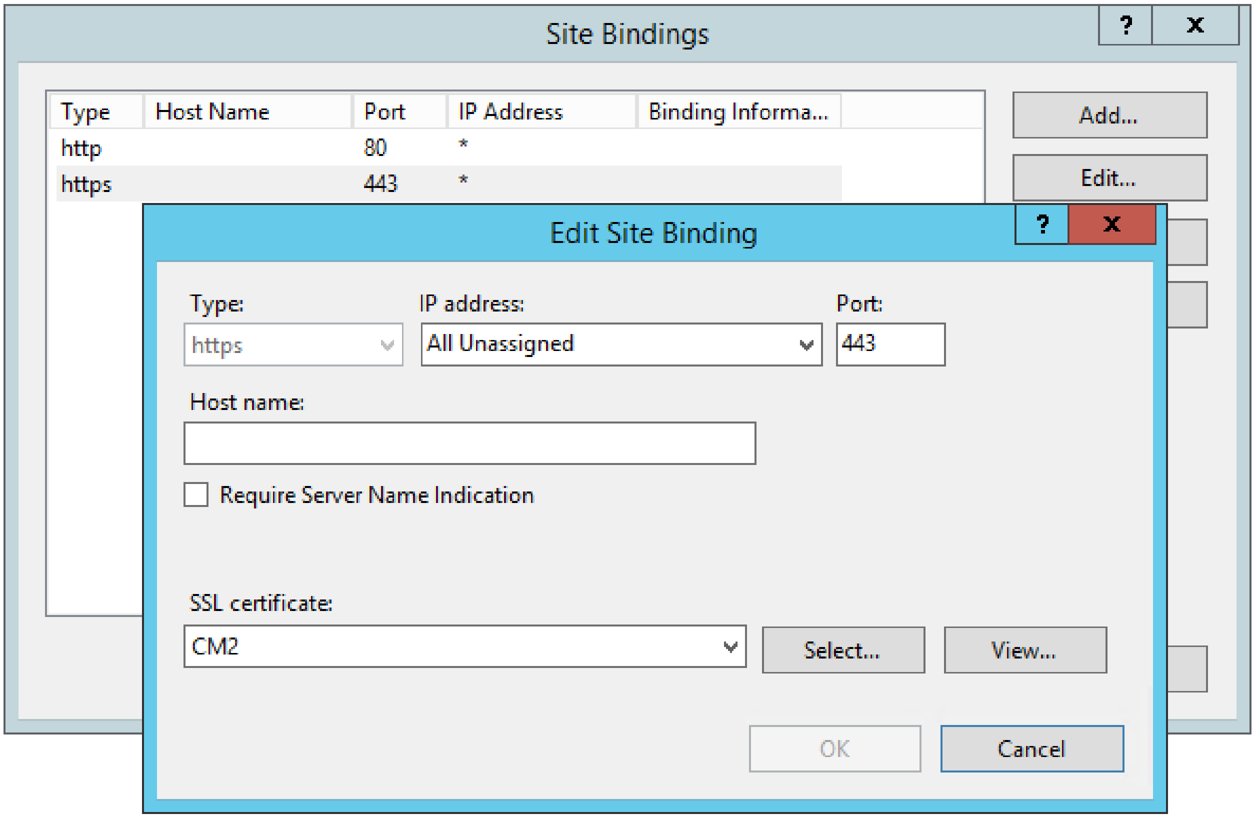
For special permissions or advanced settings, click Advanced.


Server Certificates
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
1
Create Domain Certificate...
Create Self-Signed Certificate...
View...
Export...
2

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Filter: Go Show All | Group by: No Grouping

Name	Issued To	Issued By	Expiration Date	Certificate Hash	Certificate Store
CM2	cm2.thefinancialcompany.net	TFC-ROOT-TFCCA01-CA	3/4/2018 9:18:33 AM	F36898399B75D953BEA29B720...	Personal
WMSVC	WMSvc-TFCCM02	WMSvc-TFCCM02	3/1/2026 6:22:47 AM	267281532336164E1FF0D47C3...	Personal



Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	
https		443	*	

Type: https

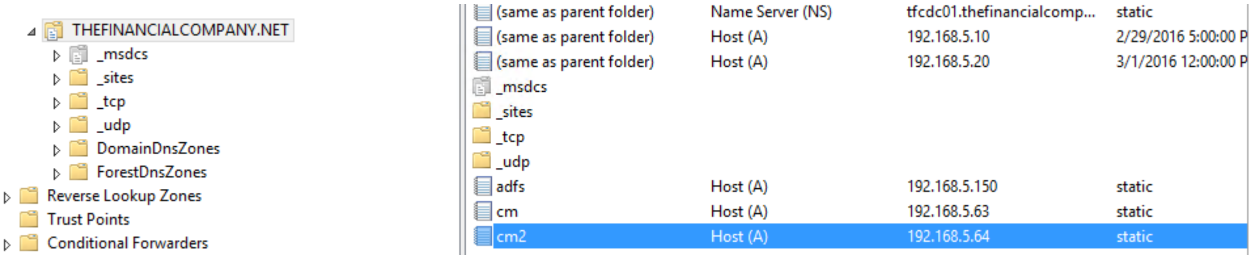
IP address: All Unassigned

Port: 443

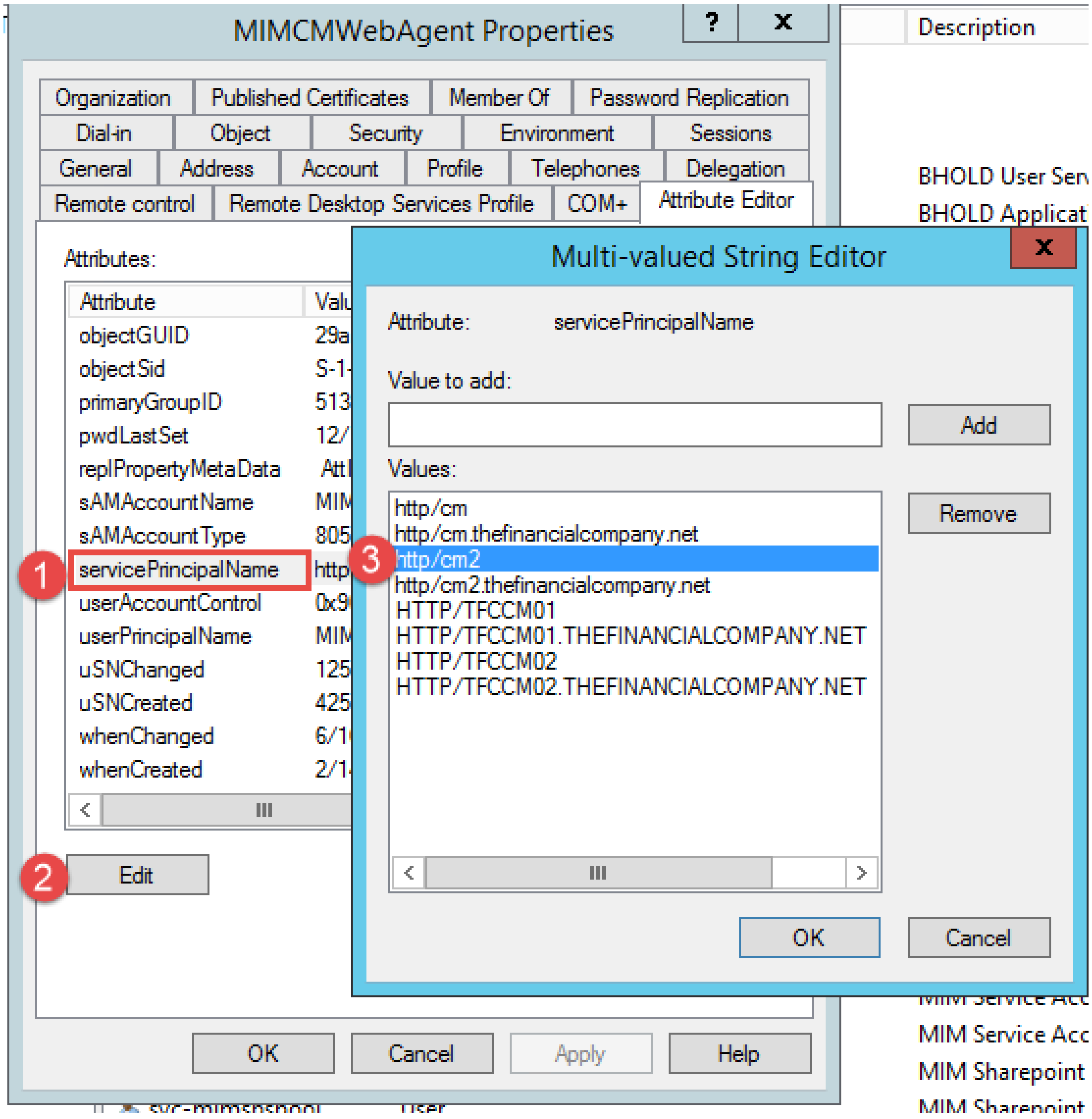
Host name:

□ Require Server Name Indication

SSL certificate: CM2



(same as parent folder)	Name Server (NS)	tfcdc01.thefinancialcomp...	static
(same as parent folder)	Host (A)	192.168.5.10	2/29/2016 5:00:00 P
(same as parent folder)	Host (A)	192.168.5.20	3/1/2016 12:00:00 P
_msdcs			
_sites			
_tcp			
_udp			
adfs	Host (A)	192.168.5.150	static
cm	Host (A)	192.168.5.63	static
cm2	Host (A)	192.168.5.64	static



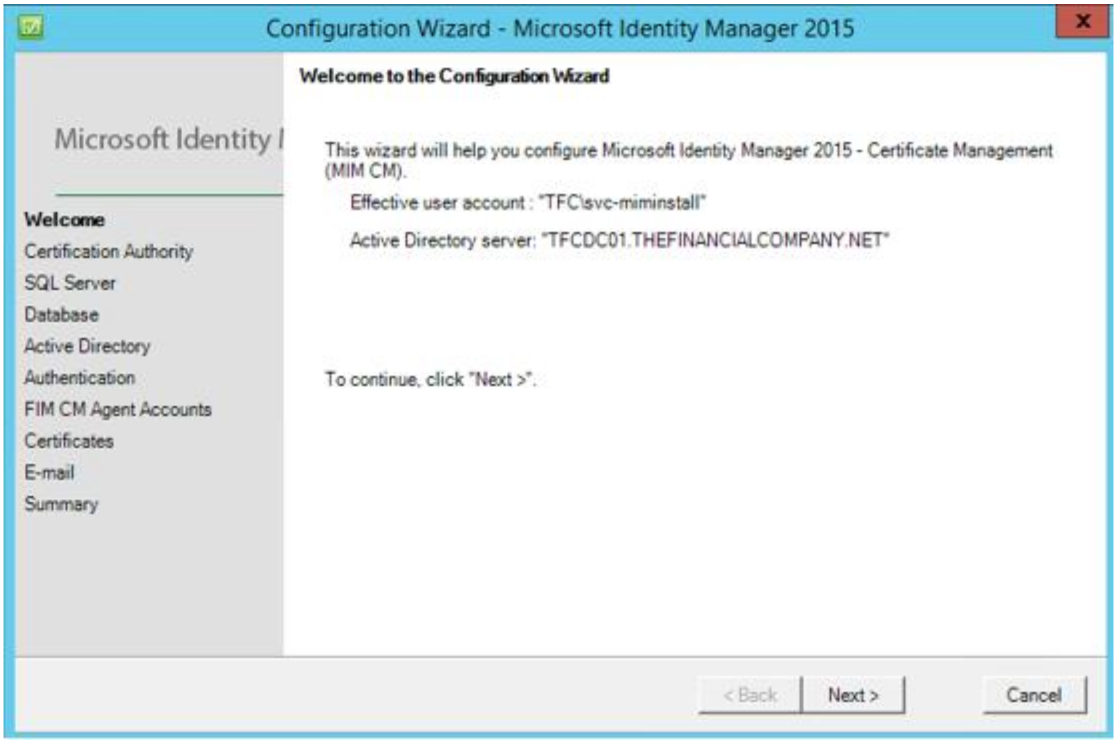
Attribute	Valu
objectGUID	29a
objectSid	S-1-
primaryGroupID	513
pwdLastSet	12/
replPropertyMetaData	Att
sAMAccountName	MIM
sAMAccountType	805
servicePrincipalName	http
userAccountControl	0x9
userPrincipalName	MIM
uSNChanged	125
uSNCreated	425
whenChanged	6/1
whenCreated	2/1

Attribute: servicePrincipalName

Value to add:

Values:

http/cm
http/cm.thefinancialcompany.net
http/cm2
http/cm2.thefinancialcompany.net
HTTP/TFCCM01
HTTP/TFCCM01.THEFINANCIALCOMPANY.NET
HTTP/TFCCM02
HTTP/TFCCM02.THEFINANCIALCOMPANY.NET



Configuration Wizard - Microsoft Identity Manager 2015

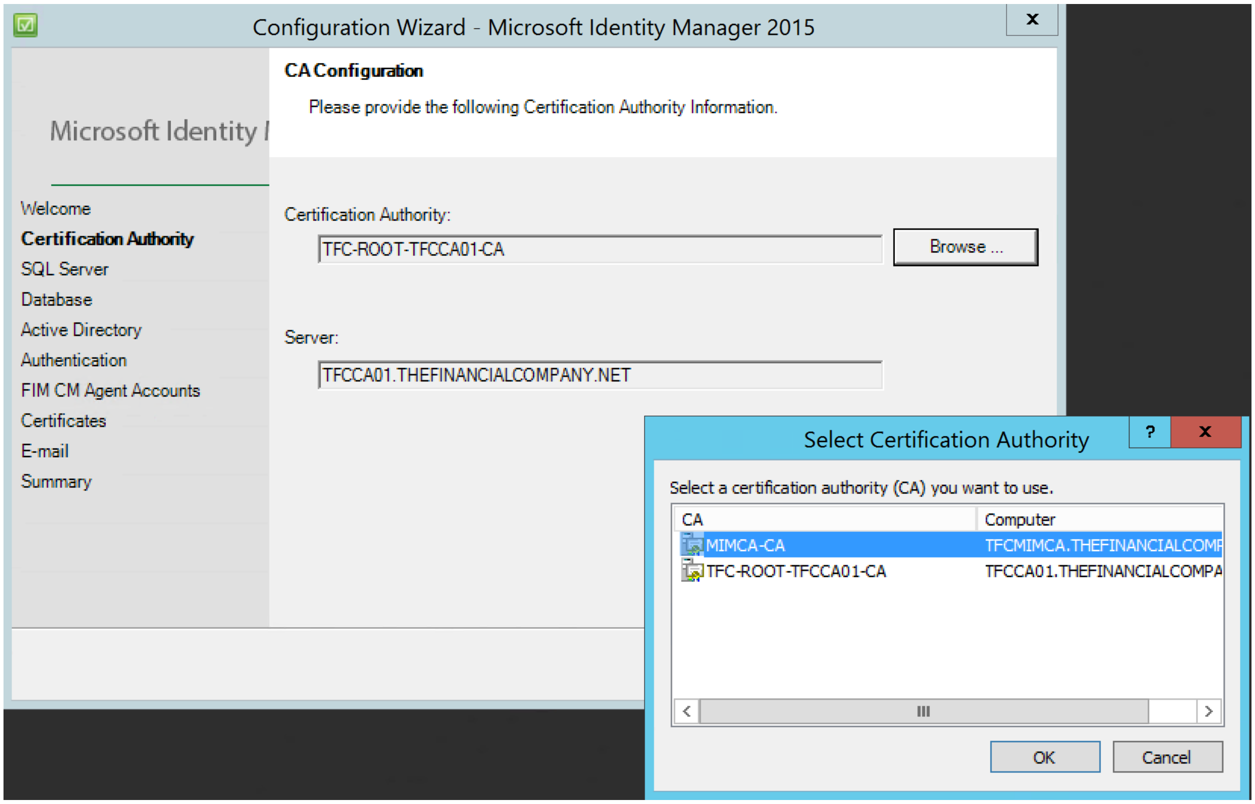
Welcome to the Configuration Wizard

This wizard will help you configure Microsoft Identity Manager 2015 - Certificate Management (MIM CM).

Effective user account : "TFC\svc-miminstall"

Active Directory server: "TFCDC01.THEFINANCIALCOMPANY.NET"

To continue, click "Next >".



Configuration Wizard - Microsoft Identity Manager 2015

CA Configuration

Please provide the following Certification Authority Information.

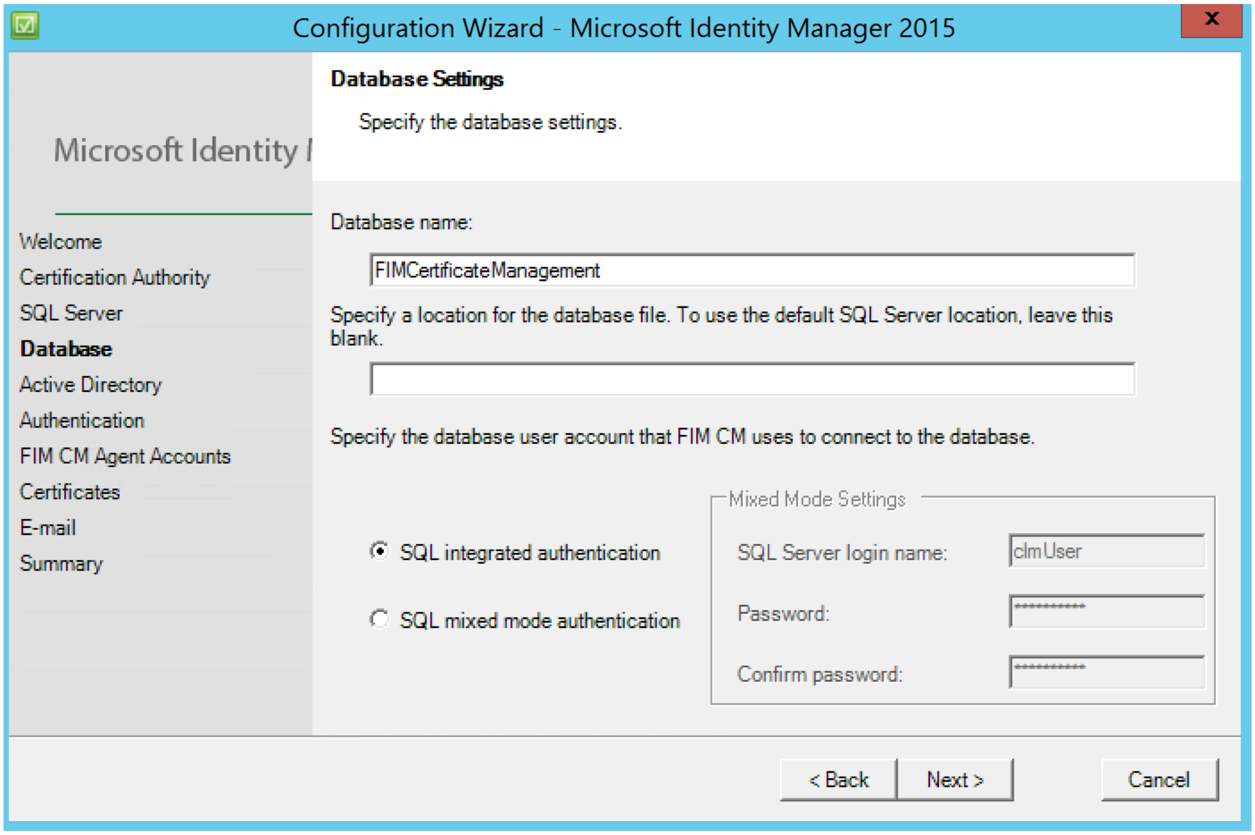
Certification Authority: TFC-ROOT-TFCCA01-CA

Server: TFCCA01.THEFINANCIALCOMPANY.NET

Select Certification Authority

Select a certification authority (CA) you want to use.

CA	Computer
MIMCA-CA	TFCMIMCA.THEFINANCIALCOMP
TFC-ROOT-TFCCA01-CA	TFCCA01.THEFINANCIALCOMPA



Database Settings

Specify the database settings.

Database name: FIMCertificateManagement

Specify a location for the database file. To use the default SQL Server location, leave this blank.

Specify the database user account that FIM CM uses to connect to the database.

● SQL integrated authentication

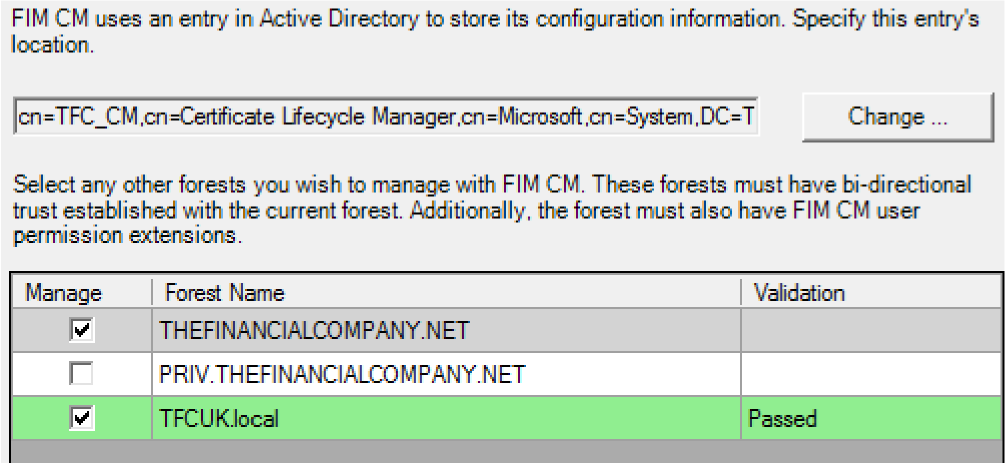
○ SQL mixed mode authentication

Mixed Mode Settings

SQL Server login name: clmUser

Password: ************

Confirm password: ************

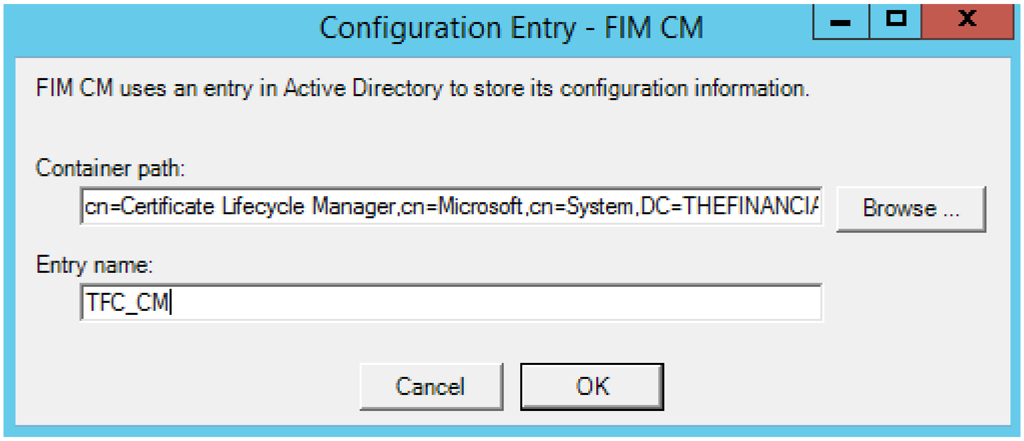


FIM CM uses an entry in Active Directory to store its configuration information. Specify this entry's location.

cn=TFC_CM,cn=Certificate Lifecycle Manager,cn=Microsoft,cn=System,DC=T

Select any other forests you wish to manage with FIM CM. These forests must have bi-directional trust established with the current forest. Additionally, the forest must also have FIM CM user permission extensions.

Manage	Forest Name	Validation
☑	THEFINANCIALCOMPANY.NET	
☐	PRIV.THEFINANCIALCOMPANY.NET	
☑	TFCUK.local	Passed

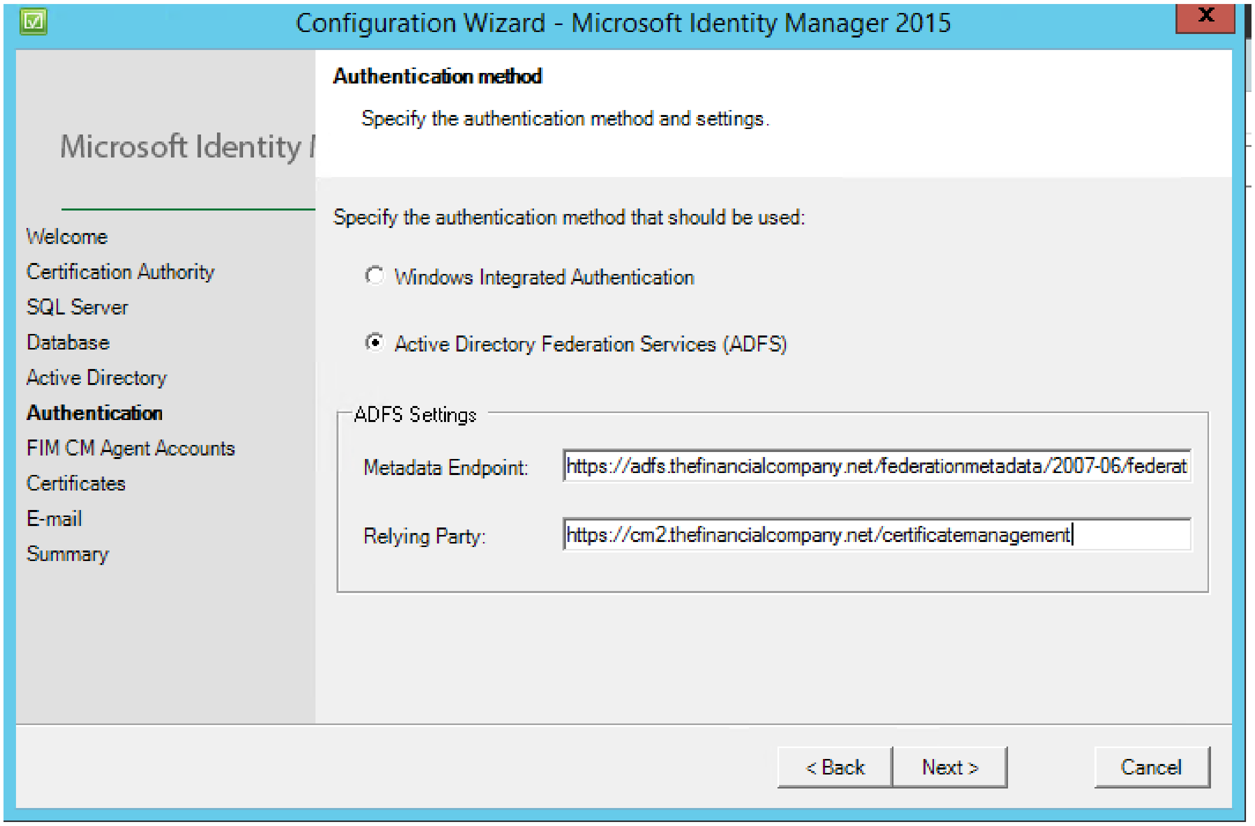


Configuration Entry - FIM CM

FIM CM uses an entry in Active Directory to store its configuration information.

Container path: cn=Certificate Lifecycle Manager,cn=Microsoft,cn=System,DC=THEFINANCIA

Entry name: TFC_CM



Configuration Wizard - Microsoft Identity Manager 2015

Authentication method

Specify the authentication method and settings.

Specify the authentication method that should be used:

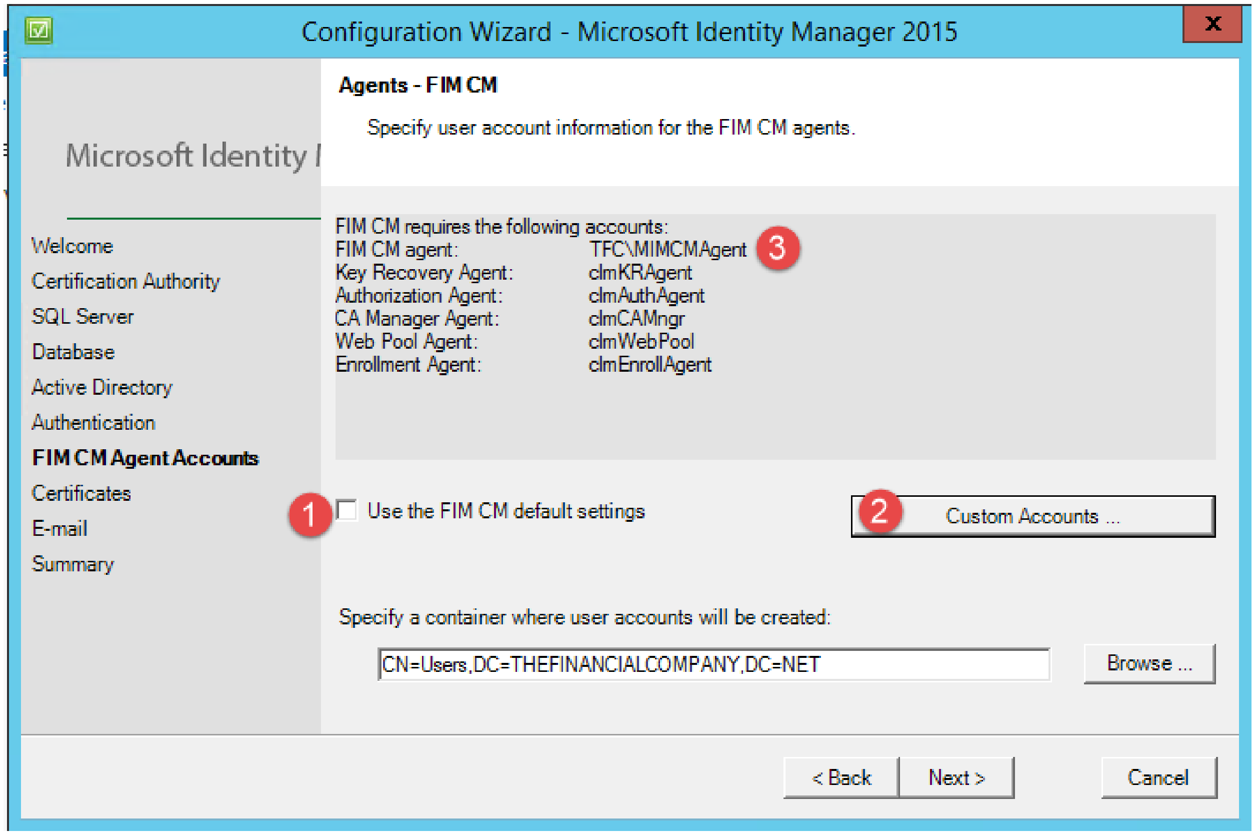
○ Windows Integrated Authentication

● Active Directory Federation Services (ADFS)

ADFS Settings

Metadata Endpoint: https://adfs.thefinancialcompany.net/federationmetadata/2007-06/federat

Relying Party: https://cm2.thefinancialcompany.net/certificatemanagement



Agents - FIM CM

Specify user account information for the FIM CM agents.

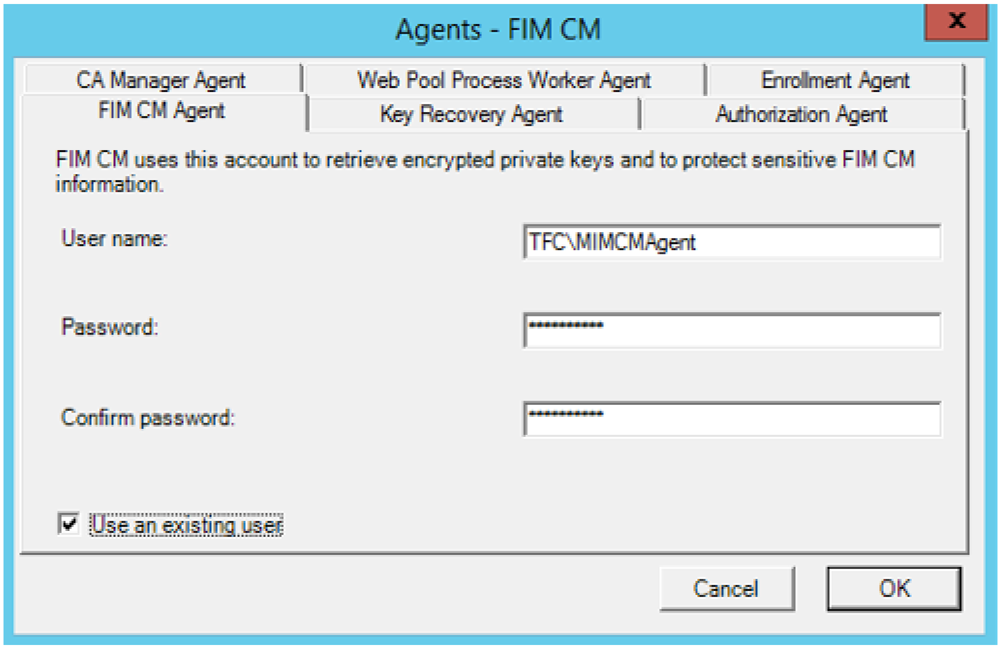
FIM CM requires the following accounts:

FIM CM agent:	TFC\MIMCMAgent
Key Recovery Agent:	clmKRAgent
Authorization Agent:	clmAuthAgent
CA Manager Agent:	clmCAMngr
Web Pool Agent:	clmWebPool
Enrollment Agent:	clmEnrollAgent

□ Use the FIM CM default settings

Specify a container where user accounts will be created:

CN=Users,DC=THEFINANCIALCOMPANY,DC=NET



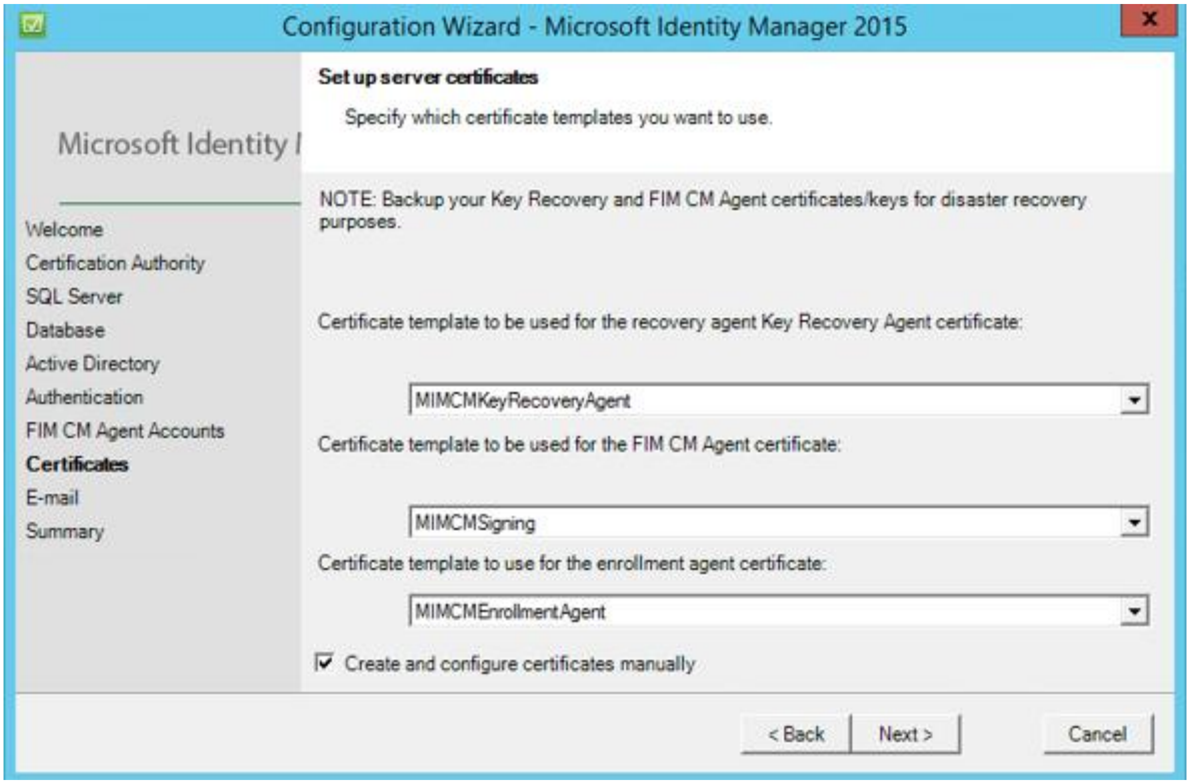
FIM CM uses this account to retrieve encrypted private keys and to protect sensitive FIM CM information.

User name: TFC\MIMCMAgent

Password: ***********

Confirm password: ***********

☑ Use an existing user



Set up server certificates

Specify which certificate templates you want to use.

NOTE: Backup your Key Recovery and FIM CM Agent certificates/keys for disaster recovery purposes.

Certificate template to be used for the recovery agent Key Recovery Agent certificate:

MIMCMKeyRecoveryAgent

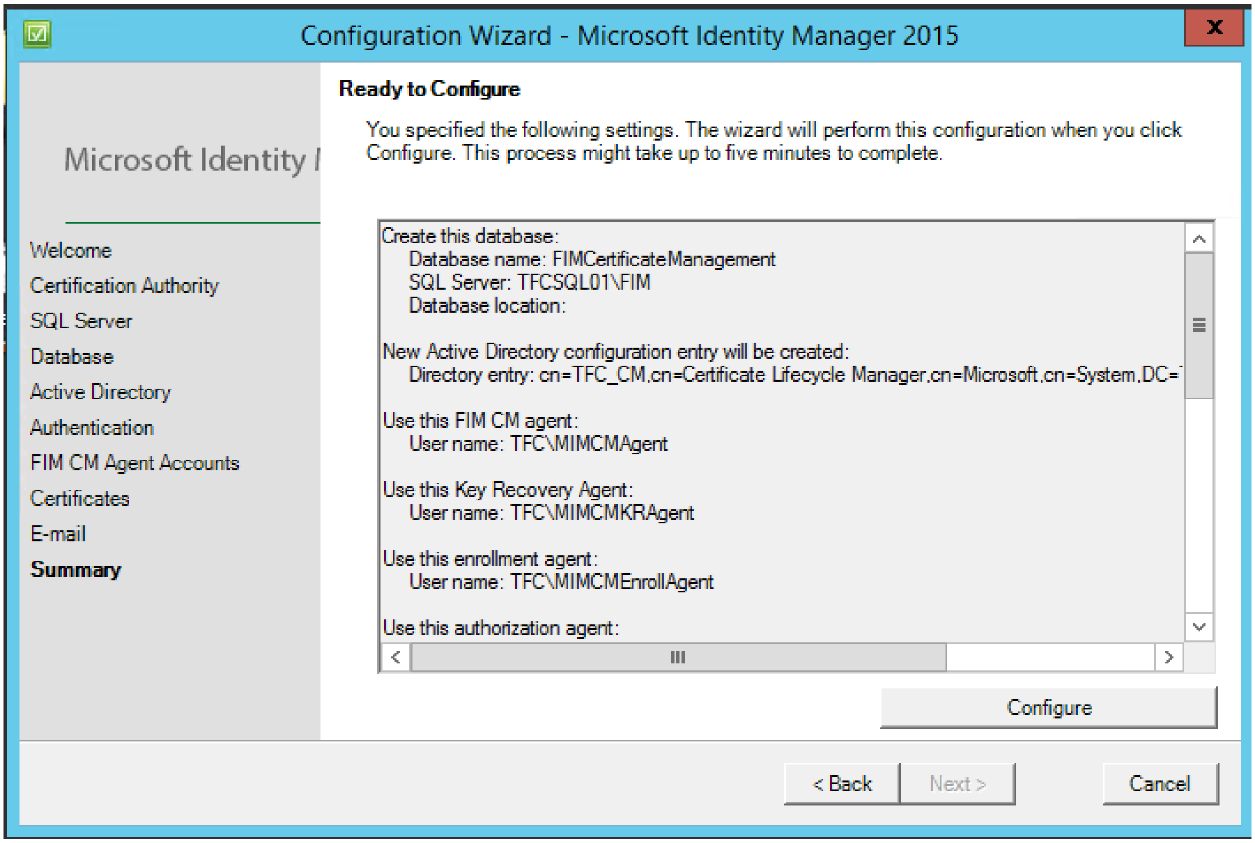
Certificate template to be used for the FIM CM Agent certificate:

MIMCMSigning

Certificate template to use for the enrollment agent certificate:

MIMCMEnrollmentAgent

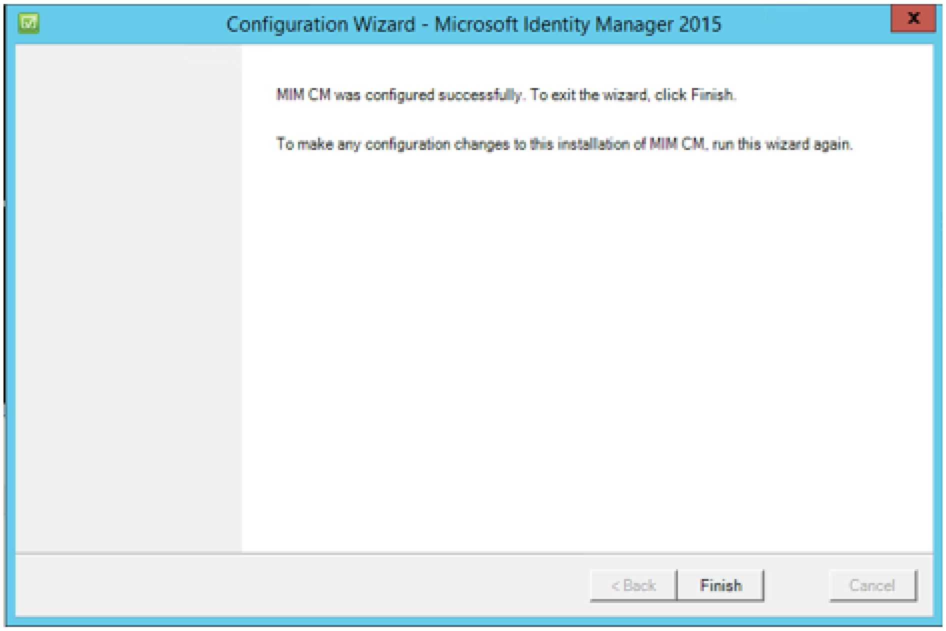
☑ Create and configure certificates manually



Ready to Configure

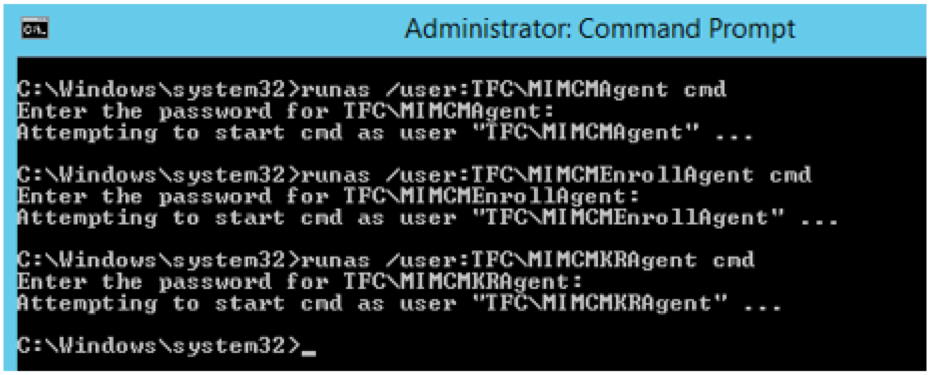
You specified the following settings. The wizard will perform this configuration when you click Configure. This process might take up to five minutes to complete.

```
Create this database:
    Database name: FIMCertificateManagement
    SQL Server: TFCSQL01\FIM
    Database location:

New Active Directory configuration entry will be created:
    Directory entry: cn=TFC_CM,cn=Certificate Lifecycle Manager,cn=Microsoft,cn=System,DC=

Use this FIM CM agent:
    User name: TFC\MIMCMAgent

Use this Key Recovery Agent:
    User name: TFC\MIMCMKRAgent

Use this enrollment agent:
    User name: TFC\MIMCMEnrollAgent

Use this authorization agent:
```

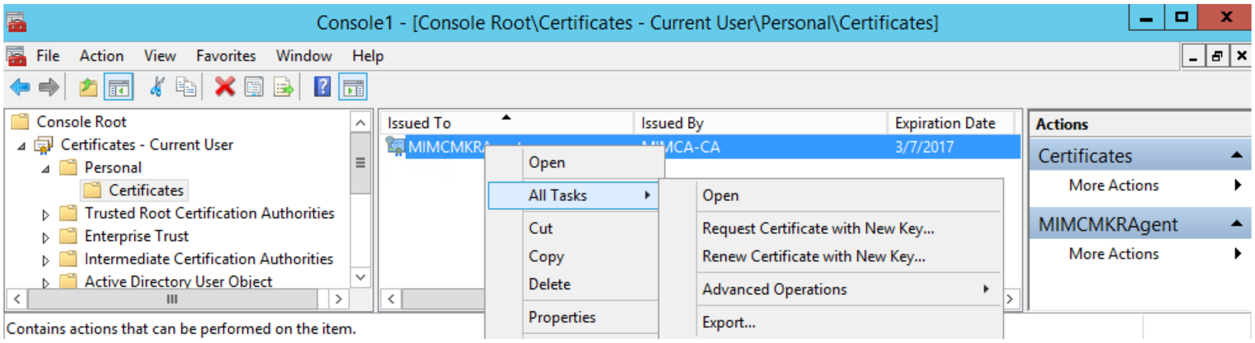


MIM CM was configured successfully. To exit the wizard, click Finish.

To make any configuration changes to this installation of MIM CM, run this wizard again.

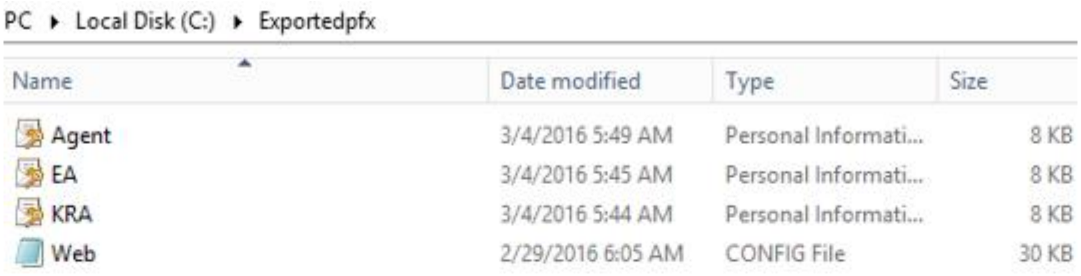


```
C:\Windows\system32>runas /user:TFC\MIMCMAgent cmd
Enter the password for TFC\MIMCMAgent:
Attempting to start cmd as user "TFC\MIMCMAgent" ...

C:\Windows\system32>runas /user:TFC\MIMCMEnrollAgent cmd
Enter the password for TFC\MIMCMEnrollAgent:
Attempting to start cmd as user "TFC\MIMCMEnrollAgent" ...

C:\Windows\system32>runas /user:TFC\MIMCMKRAgent cmd
Enter the password for TFC\MIMCMKRAgent:
Attempting to start cmd as user "TFC\MIMCMKRAgent" ...

C:\Windows\system32>_
```

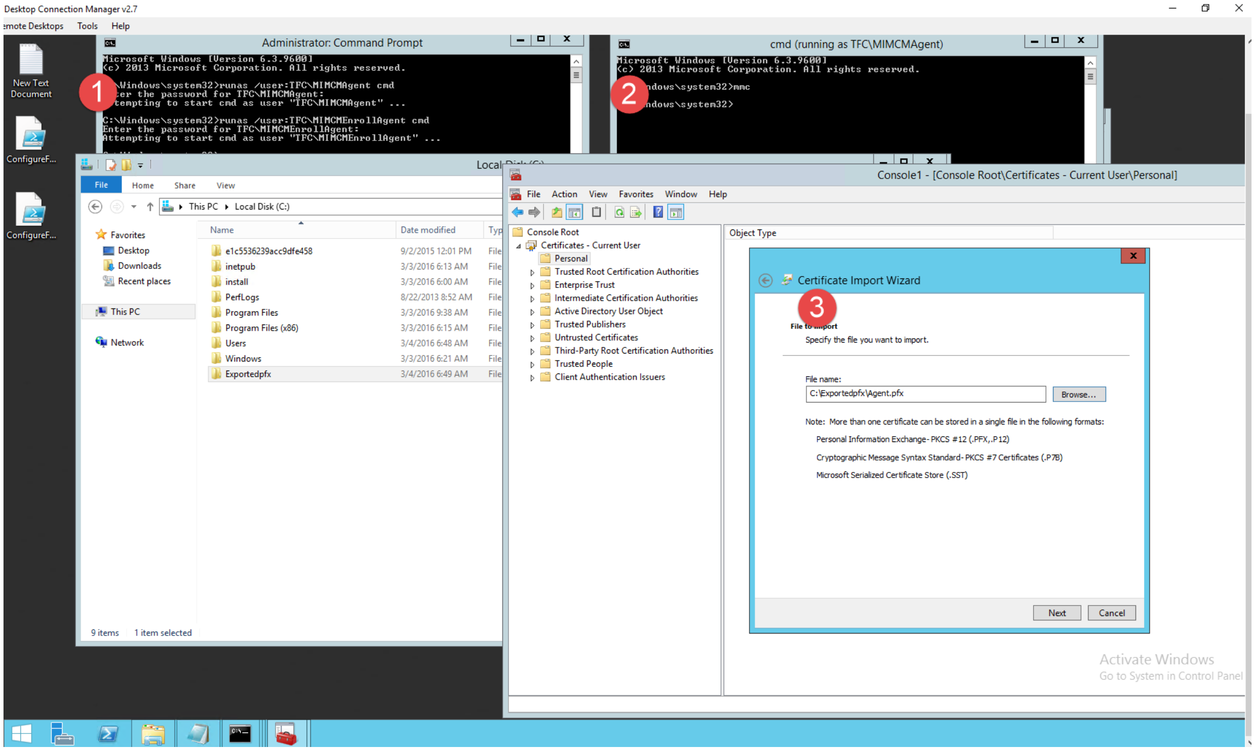

Console1 - [Console Root\Certificates - Current User\Personal\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Open
All Tasks
Cut
Copy
Delete
Properties
Open
Request Certificate with New Key...
Renew Certificate with New Key...
Advanced Operations
Export...
Actions
Certificates
More Actions
MIMCMKRAgent
More Actions

Issued To	Issued By	Expiration Date
MIMCMKRA	MIMCA-CA	3/7/2017

Contains actions that can be performed on the item.



Name	Date modified	Type	Size
Agent	3/4/2016 5:49 AM	Personal Informati...	8 KB
EA	3/4/2016 5:45 AM	Personal Informati...	8 KB
KRA	3/4/2016 5:44 AM	Personal Informati...	8 KB
Web	2/29/2016 6:05 AM	CONFIG File	30 KB


Desktop Connection Manager v2.7
emote Desktops Tools Help
New Text Document
ConfigureF...
ConfigureF...
1
2
3
Local Disk (C:)
File Home Share View
This PC ▸ Local Disk (C:)
Favorites
Desktop
Downloads
Recent places
This PC
Network
9 items 1 item selected
Console1 - [Console Root\Certificates - Current User\Personal]
File Action View Favorites Window Help
Object Type
Activate Windows
Go to System in Control Panel

Administrator: Command Prompt

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

 \Windows\system32>runas /user:TFC\MIMCMAgent cmd
 ter the password for TFC\MIMCMAgent:
 tempting to start cmd as user "TFC\MIMCMAgent" ...

C:\Windows\system32>runas /user:TFC\MIMCMEnrollAgent cmd
Enter the password for TFC\MIMCMEnrollAgent:
Attempting to start cmd as user "TFC\MIMCMEnrollAgent" ...
```

cmd (running as TFC\MIMCMAgent)

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

 ndows\system32>mmc

 ndows\system32>
```

Name	Date modified	Typ
e1c5536239acc9dfe458	9/2/2015 12:01 PM	File
inetpub	3/3/2016 6:13 AM	File
install	3/3/2016 6:00 AM	File
PerfLogs	8/22/2013 8:52 AM	File
Program Files	3/3/2016 9:38 AM	File
Program Files (x86)	3/3/2016 6:15 AM	File
Users	3/4/2016 6:48 AM	File
Windows	3/3/2016 6:21 AM	File
Exportedpfx	3/4/2016 6:49 AM	File

- Console Root
  - Certificates - Current User
    - Personal
    - Trusted Root Certification Authorities
    - Enterprise Trust
    - Intermediate Certification Authorities
    - Active Directory User Object
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authorities
    - Trusted People
    - Client Authentication Issuers

Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:
C:\Exportedpfx\Agent.pfx Browse...

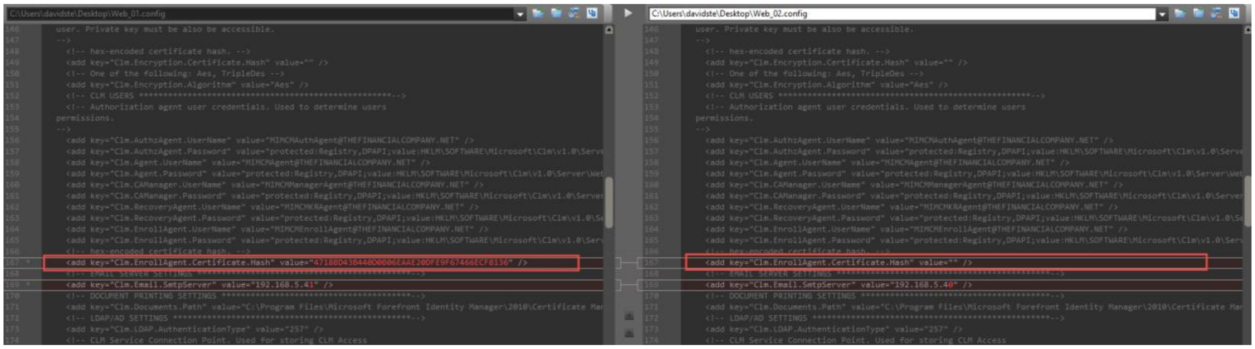
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Next Cancel

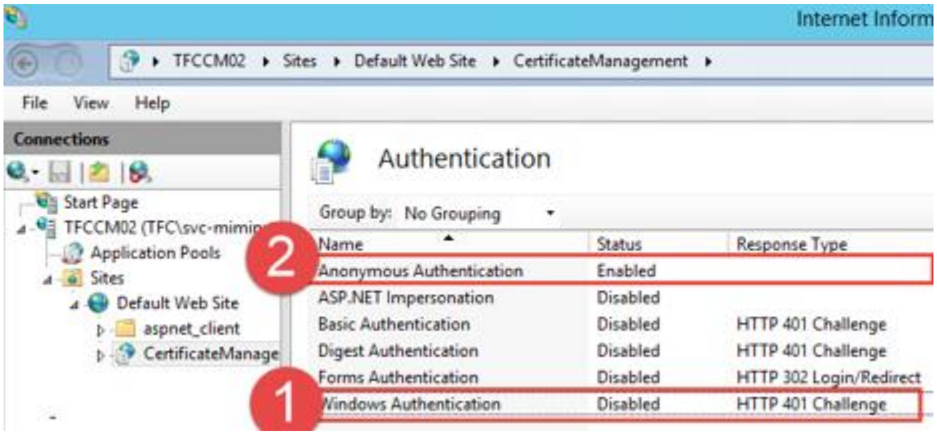


C:\Users\davidste\Desktop\Web_01.config

```
user. Private key must be also be accessible.
-->
  <!-- hex-encoded certificate hash. -->
  <add key="Clm.Encryption.Certificate.Hash" value="" />
  <!-- One of the following: Aes, TripleDes -->
  <add key="Clm.Encryption.Algoritnm" value="Aes" />
  <!-- CLM USERS ****************************************************-->
  <!-- Authorization agent user credentials. Used to determine users
permissions.
-->
  <add key="Clm.AuthzAgent.UserName" value="MIMCMAuthAgent@THEFINANCIALCOMPANY.NET" />
  <add key="Clm.AuthzAgent.Password" value="protected:Registry,DPAPI;value:HKLM\SOFTWARE\Microsoft\Clm\v1.0\Serv
  <add key="Clm.Agent.UserName" value="MIMCMAgent@THEFINANCIALCOMPANY.NET" />
  <add key="Clm.Agent.Password" value="protected:Registry,DPAPI;value:HKLM\SOFTWARE\Microsoft\Clm\v1.0\Server\Wel
  <add key="Clm.CAManager.UserName" value="MIMCMManagerAgent@THEFINANCIALCOMPANY.NET" />
  <add key="Clm.CAManager.Password" value="protected:Registry,DPAPI;value:HKLM\SOFTWARE\Microsoft\Clm\v1.0\Server
  <add key="Clm.RecoveryAgent.UserName" value="MIMCMKRAgent@THEFINANCIALCOMPANY.NET" />
  <add key="Clm.RecoveryAgent.Password" value="protected:Registry,DPAPI;value:HKLM\SOFTWARE\Microsoft\Clm\v1.0\Se
  <add key="Clm.EnrollAgent.UserName" value="MIMCMEnrollAgent@THEFINANCIALCOMPANY.NET" />
  <add key="Clm.EnrollAgent.Password" value="protected:Registry,DPAPI;value:HKLM\SOFTWARE\Microsoft\Clm\v1.0\Serv
  <!-- hex-encoded certificate hash. -->
  <add key="Clm.EnrollAgent.Certificate.Hash" value="47188D438440D0D06EAAE20DFE9F67466ECF8136" />
  <!-- EMAIL SERVER SETTINGS ********************************************-->
  <add key="Clm.Email.SmtpServer" value="192.168.5.41" />
  <!-- DOCUMENT PRINTING SETTINGS ***************************************-->
  <add key="Clm.Documents.Path" value="C:\Program Files\Microsoft Forefront Identity Manager\2010\Certificate Mar
  <!-- LDAP/AD SETTINGS ************************************************-->
  <add key="Clm.LDAP.AuthenticationType" value="257" />
  <!-- CLM Service Connection Point. Used for storing CLM Access
```

C:\Users\davidste\Desktop\Web_02.config

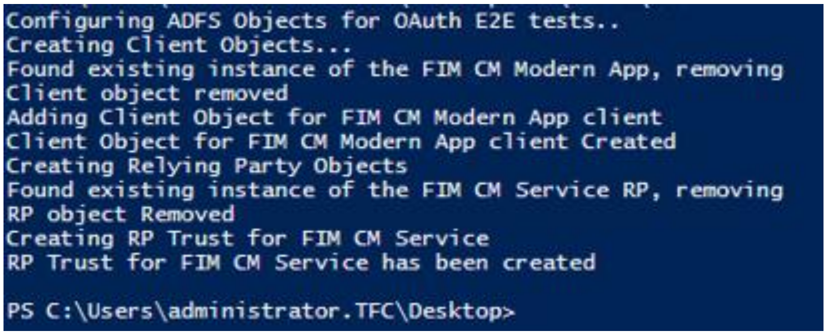
```
user. Private key must be also be accessible.
-->
  <!-- hex-encoded certificate hash. -->
  <add key="Clm.Encryption.Certificate.Hash" value="" />
  <!-- One of the following: Aes, TripleDes -->
  <add key="Clm.Encryption.Algoritnm" value="Aes" />
  <!-- CLM USERS ****************************************************-->
  <!-- Authorization agent user credentials. Used to determine users
permissions.
-->
  <add key="Clm.AuthzAgent.UserName" value="MIMCMAuthAgent@THEFINANCIALCOMPANY.NET" />
  <add key="Clm.AuthzAgent.Password" value="protected:Registry,DPAPI;value:HKLM\SOFTWARE\Microsoft\Clm\v1.0\Serv
  <add key="Clm.Agent.UserName" value="MIMCMAgent@THEFINANCIALCOMPANY.NET" />
  <add key="Clm.Agent.Password" value="protected:Registry,DPAPI;value:HKLM\SOFTWARE\Microsoft\Clm\v1.0\Server\Wel
  <add key="Clm.CAManager.UserName" value="MIMCMManagerAgent@THEFINANCIALCOMPANY.NET" />
  <add key="Clm.CAManager.Password" value="protected:Registry,DPAPI;value:HKLM\SOFTWARE\Microsoft\Clm\v1.0\Server
  <add key="Clm.RecoveryAgent.UserName" value="MIMCMKRAgent@THEFINANCIALCOMPANY.NET" />
  <add key="Clm.RecoveryAgent.Password" value="protected:Registry,DPAPI;value:HKLM\SOFTWARE\Microsoft\Clm\v1.0\Se
  <add key="Clm.EnrollAgent.UserName" value="MIMCMEnrollAgent@THEFINANCIALCOMPANY.NET" />
  <add key="Clm.EnrollAgent.Password" value="protected:Registry,DPAPI;value:HKLM\SOFTWARE\Microsoft\Clm\v1.0\Serv
  <!-- hex-encoded certificate hash. -->
  <add key="Clm.EnrollAgent.Certificate.Hash" value="" />
  <!-- EMAIL SERVER SETTINGS ********************************************-->
  <add key="Clm.Email.SmtpServer" value="192.168.5.40" />
  <!-- DOCUMENT PRINTING SETTINGS ***************************************-->
  <add key="Clm.Documents.Path" value="C:\Program Files\Microsoft Forefront Identity Manager\2010\Certificate Mar
  <!-- LDAP/AD SETTINGS ************************************************-->
  <add key="Clm.LDAP.AuthenticationType" value="257" />
  <!-- CLM Service Connection Point. Used for storing CLM Access
```



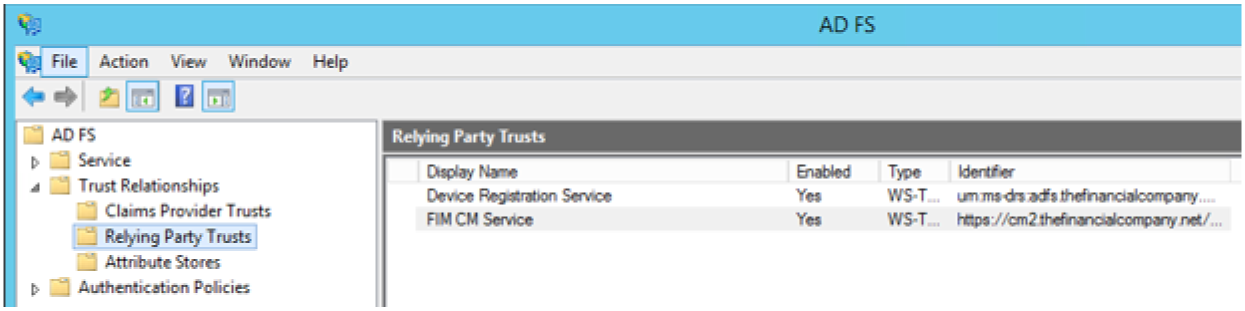
Authentication

Group by: No Grouping

Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Disabled	HTTP 401 Challenge

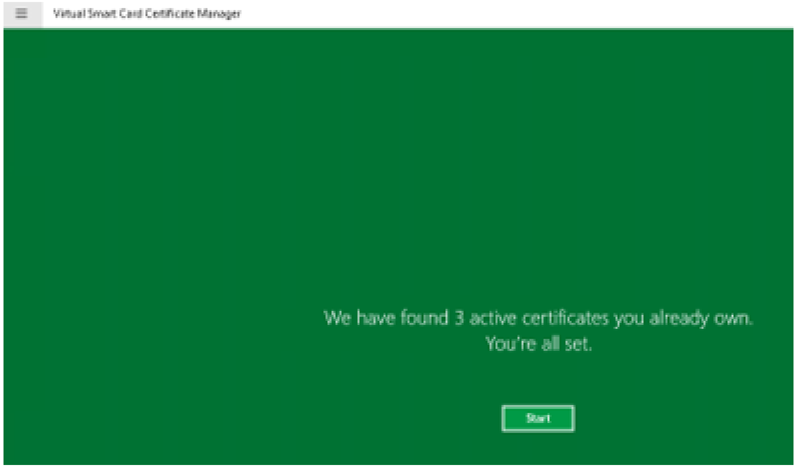


```
Configuring ADFS Objects for OAuth E2E tests..
Creating Client Objects...
Found existing instance of the FIM CM Modern App, removing
Client object removed
Adding Client Object for FIM CM Modern App client
Client Object for FIM CM Modern App client Created
Creating Relying Party Objects
Found existing instance of the FIM CM Service RP, removing
RP object Removed
Creating RP Trust for FIM CM Service
RP Trust for FIM CM Service has been created

PS C:\Users\administrator.TFC\Desktop>
```

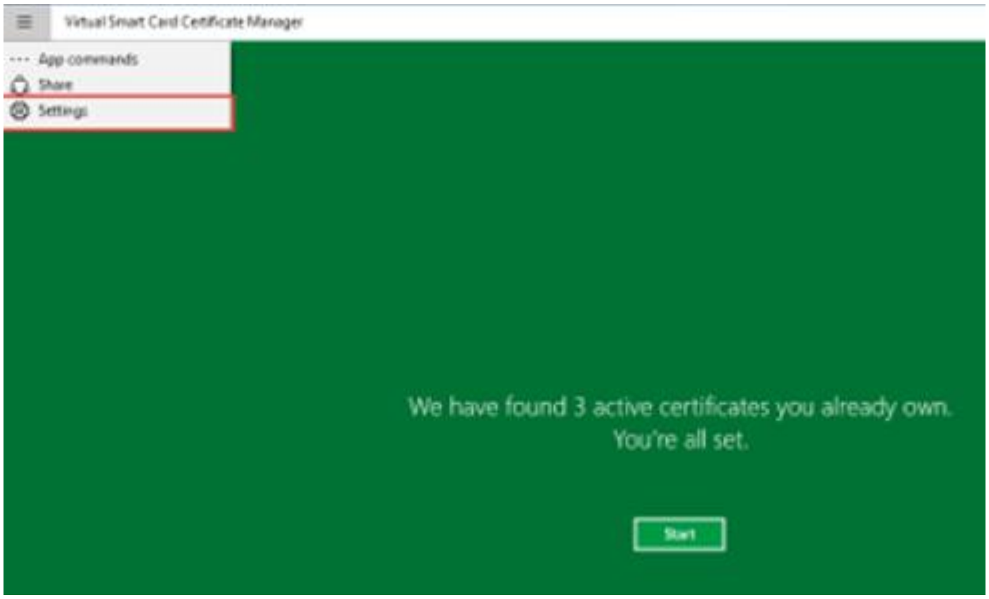


Relying Party Trusts

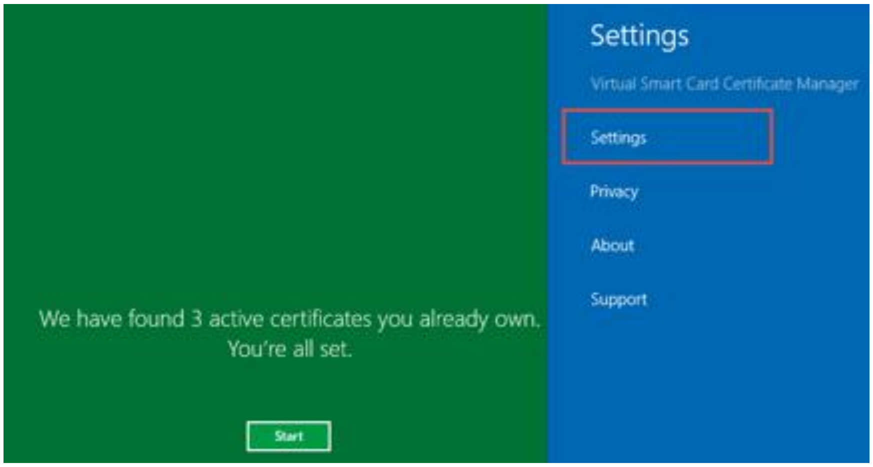
Display Name	Enabled	Type	Identifier
Device Registration Service	Yes	WS-T...	urn:ms-drs:adfs.thefinancialcompany....
FIM CM Service	Yes	WS-T...	https://cm2.thefinancialcompany.net/...



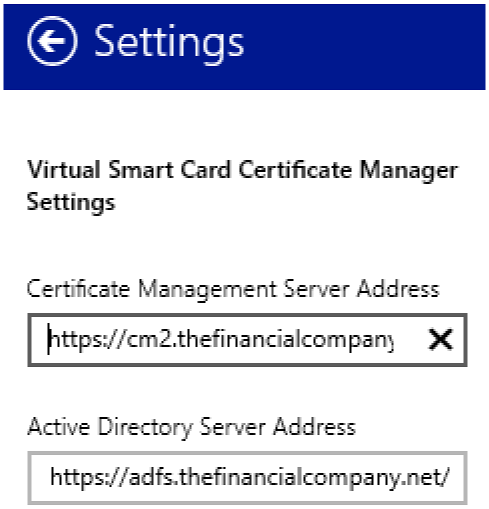
We have found 3 active certificates you already own.
You're all set.



We have found 3 active certificates you already own. You're all set.



We have found 3 active certificates you already own. You're all set.



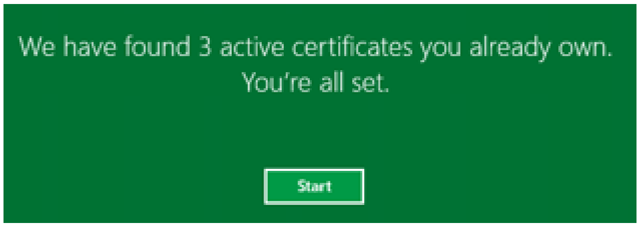
Virtual Smart Card Certificate Manager Settings

Certificate Management Server Address

https://cm2.thefinancialcompany

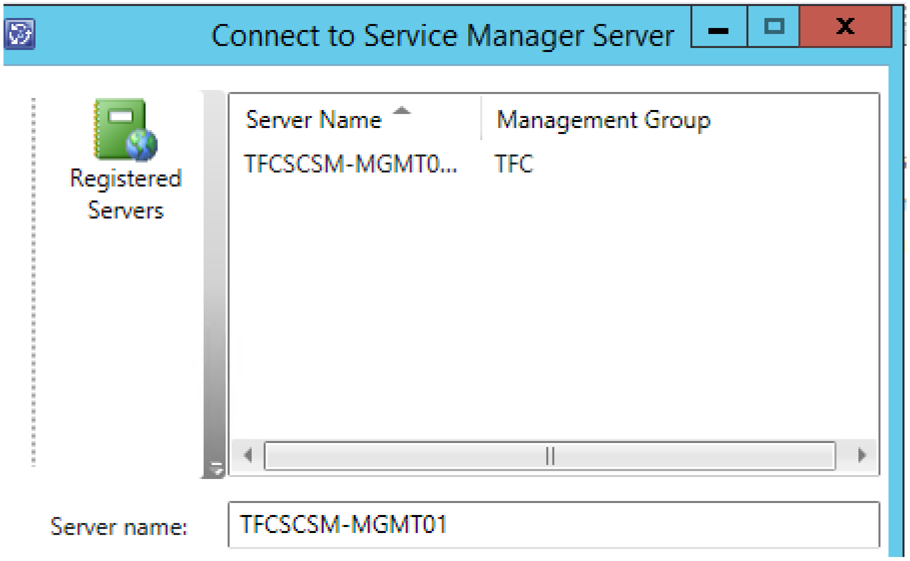
Active Directory Server Address

https://adfs.thefinancialcompany.net/



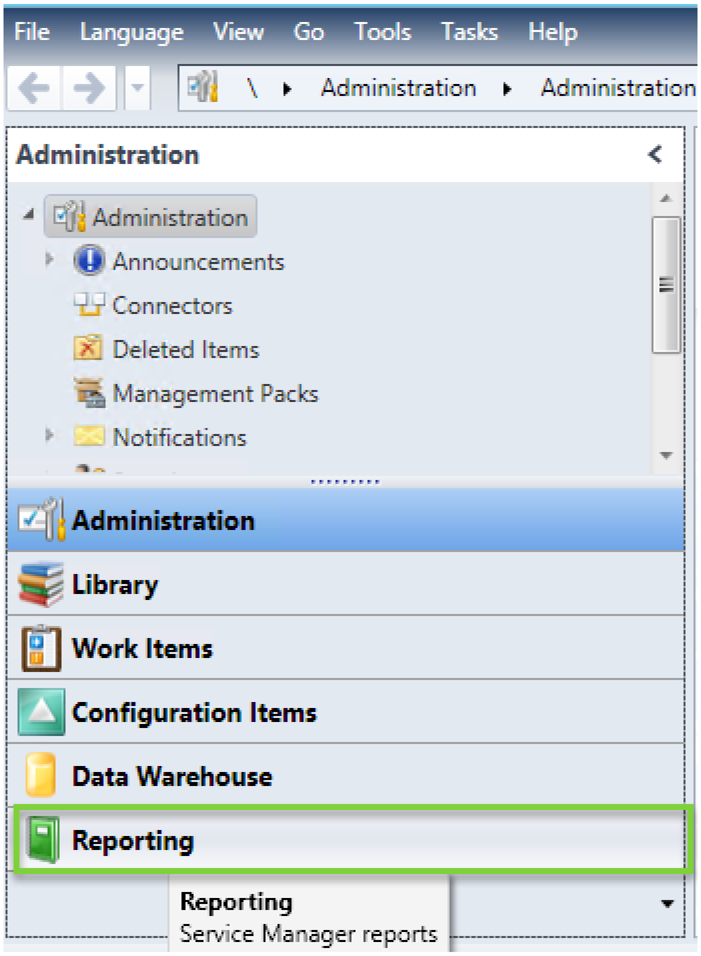
We have found 3 active certificates you already own.
You're all set.

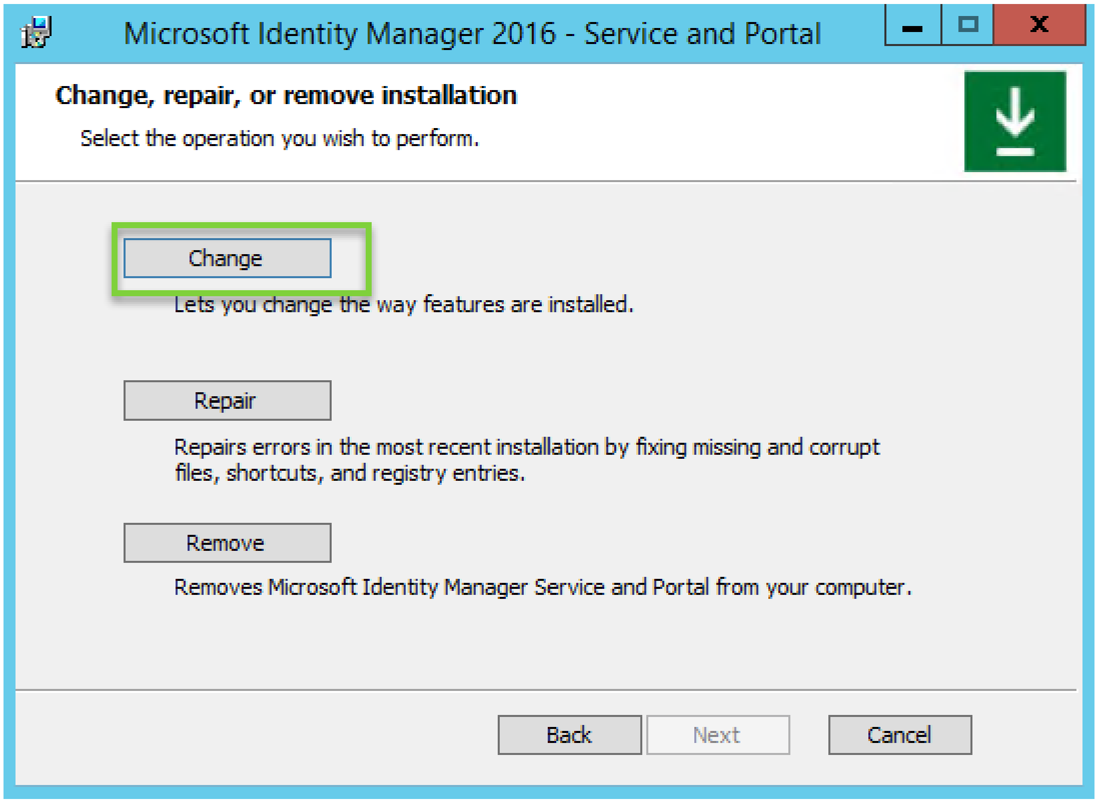
Chapter 13: Reporting



Server Name	Management Group
TFCSCSM-MGMT0...	TFC

Server name: TFCSCSM-MGMT01





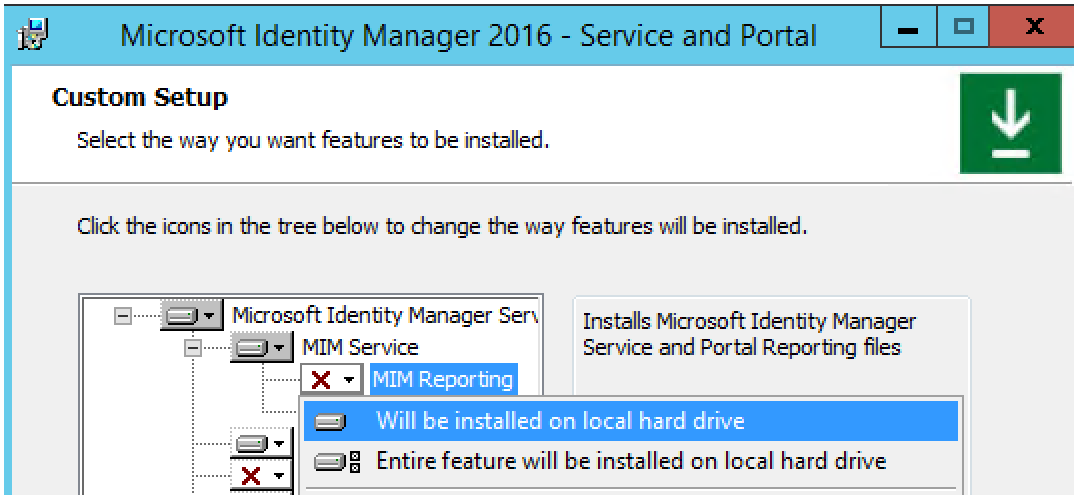
Change, repair, or remove installation

Select the operation you wish to perform.

Lets you change the way features are installed.

Repairs errors in the most recent installation by fixing missing and corrupt files, shortcuts, and registry entries.

Removes Microsoft Identity Manager Service and Portal from your computer.

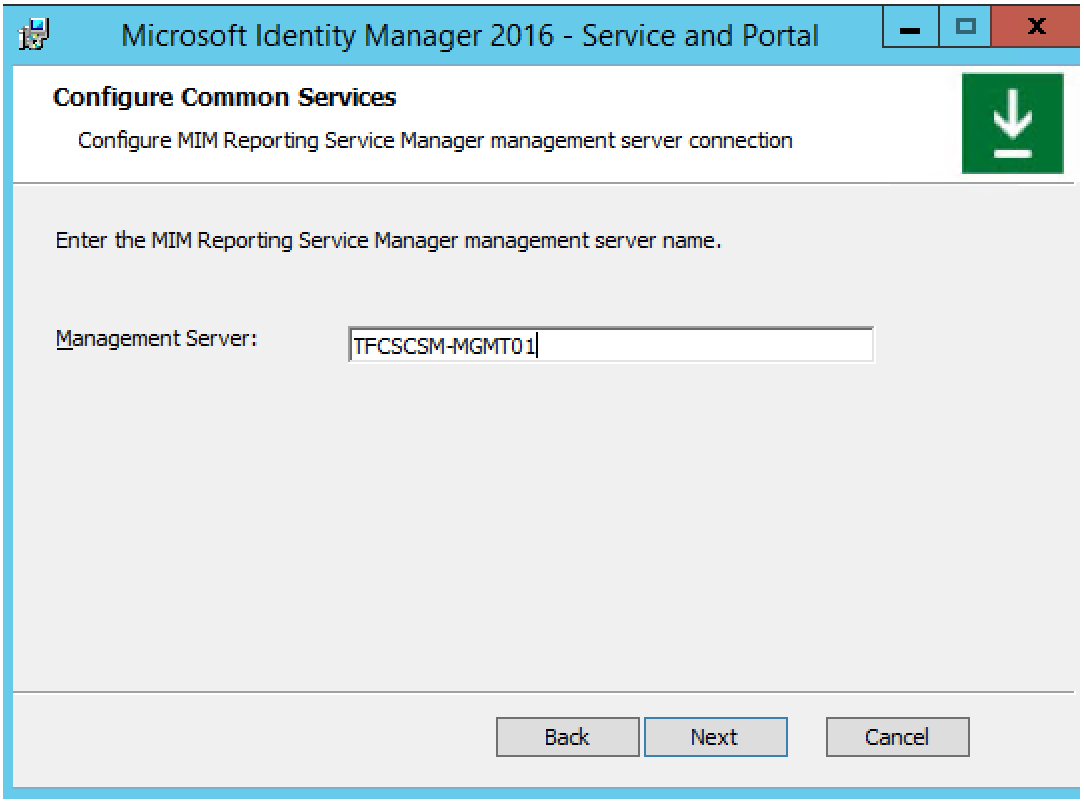

Microsoft Identity Manager 2016 - Service and Portal
Microsoft Identity Manager Serv
MIM Service
MIM Reporting
Will be installed on local hard drive
Entire feature will be installed on local hard drive

Custom Setup

Select the way you want features to be installed.

Click the icons in the tree below to change the way features will be installed.

Installs Microsoft Identity Manager Service and Portal Reporting files



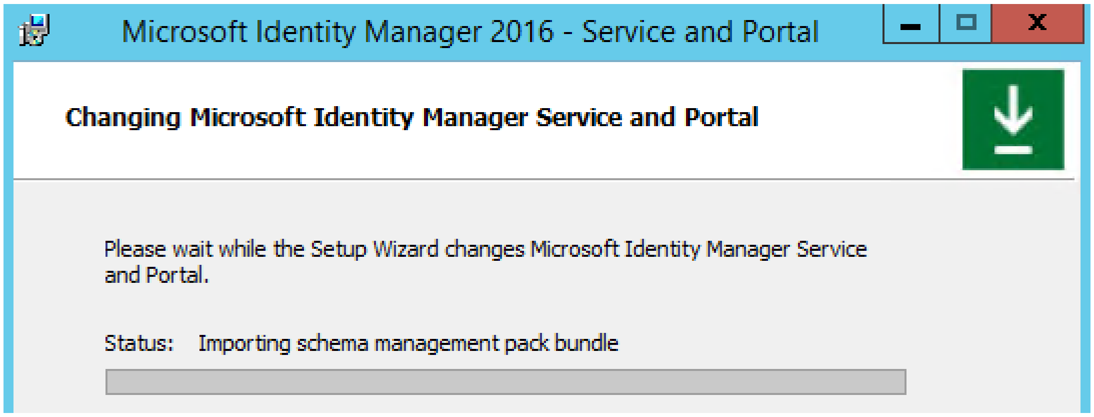
Microsoft Identity Manager 2016 - Service and Portal

Configure Common Services

Configure MIM Reporting Service Manager management server connection

Enter the MIM Reporting Service Manager management server name.

Management Server: TFCSCSM-MGMT01

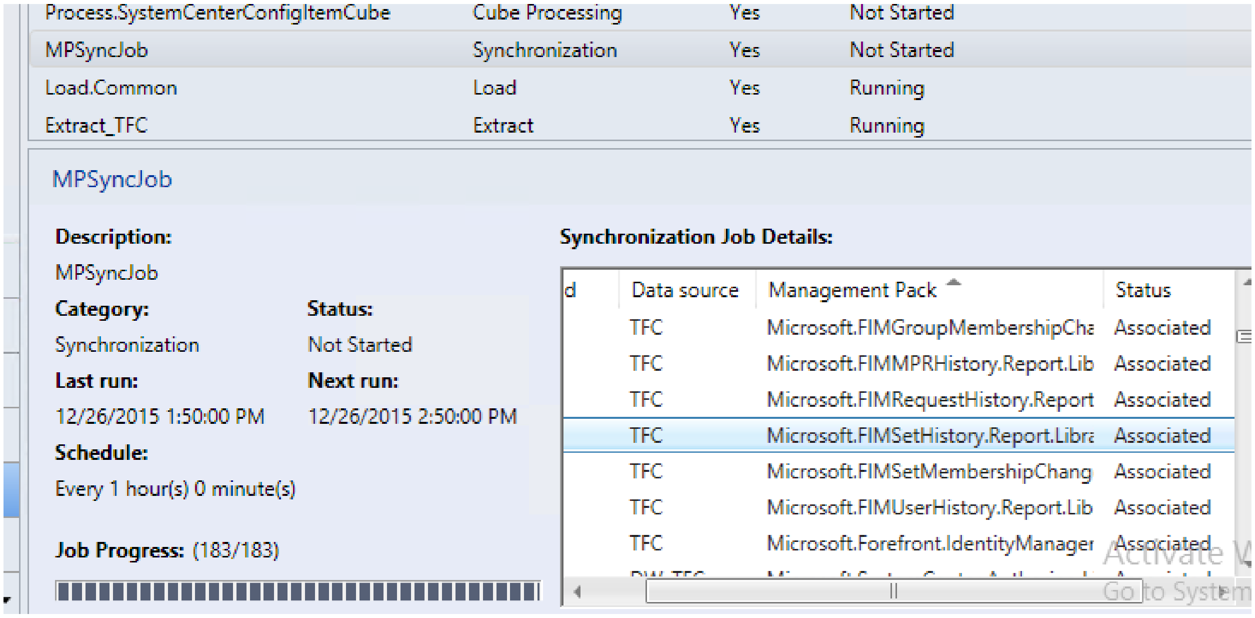


Microsoft Identity Manager 2016 - Service and Portal

Changing Microsoft Identity Manager Service and Portal

Please wait while the Setup Wizard changes Microsoft Identity Manager Service and Portal.

Status: Importing schema management pack bundle



Process.SystemCenterConfigItemCube	Cube Processing	Yes	Not Started
MPSyncJob	Synchronization	Yes	Not Started
Load.Common	Load	Yes	Running
Extract_TFC	Extract	Yes	Running

MPSyncJob

Description:
MPSyncJob

Category: Synchronization

Status: Not Started

Last run: 12/26/2015 1:50:00 PM

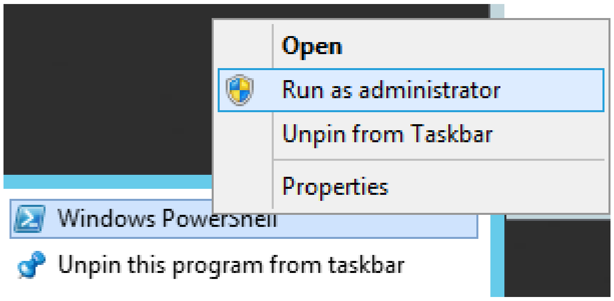
Next run: 12/26/2015 2:50:00 PM

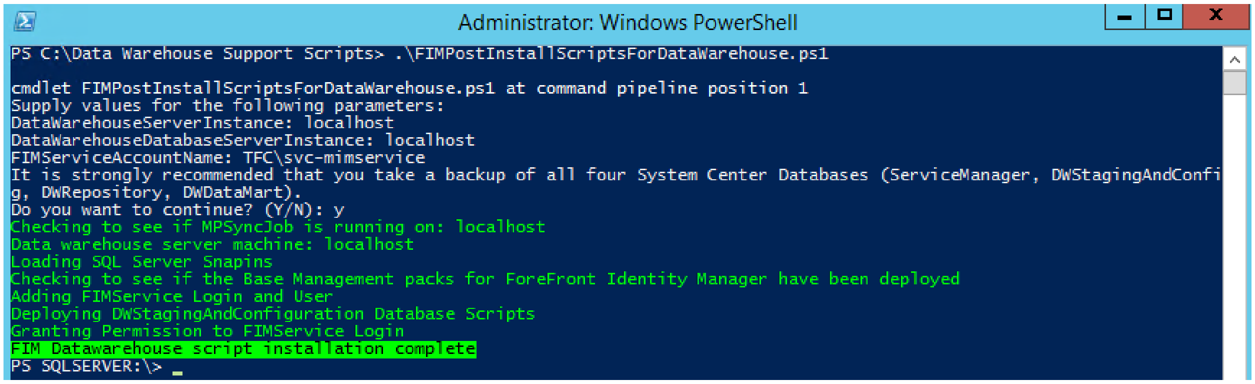
Schedule:
Every 1 hour(s) 0 minute(s)

Job Progress: (183/183)

Synchronization Job Details:

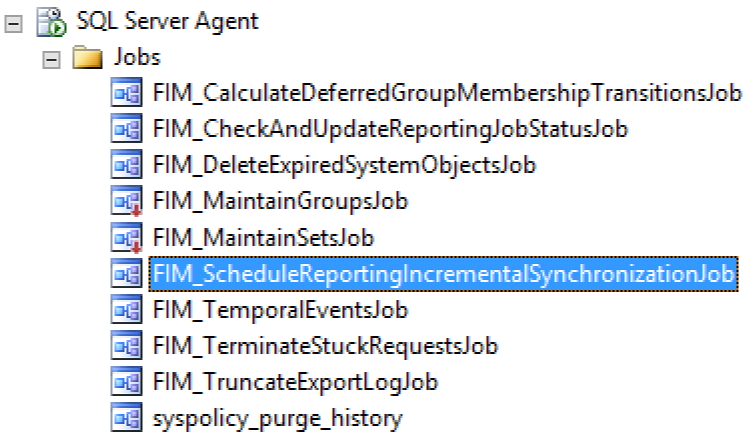
d	Data source	Management Pack	Status
	TFC	Microsoft.FIMGroupMembershipCha	Associated
	TFC	Microsoft.FIMMPRHistory.Report.Lib	Associated
	TFC	Microsoft.FIMRequestHistory.Report	Associated
	TFC	Microsoft.FIMSetHistory.Report.Libra	Associated
	TFC	Microsoft.FIMSetMembershipChang	Associated
	TFC	Microsoft.FIMUserHistory.Report.Lib	Associated
	TFC	Microsoft.Forefront.IdentityManager	Associated



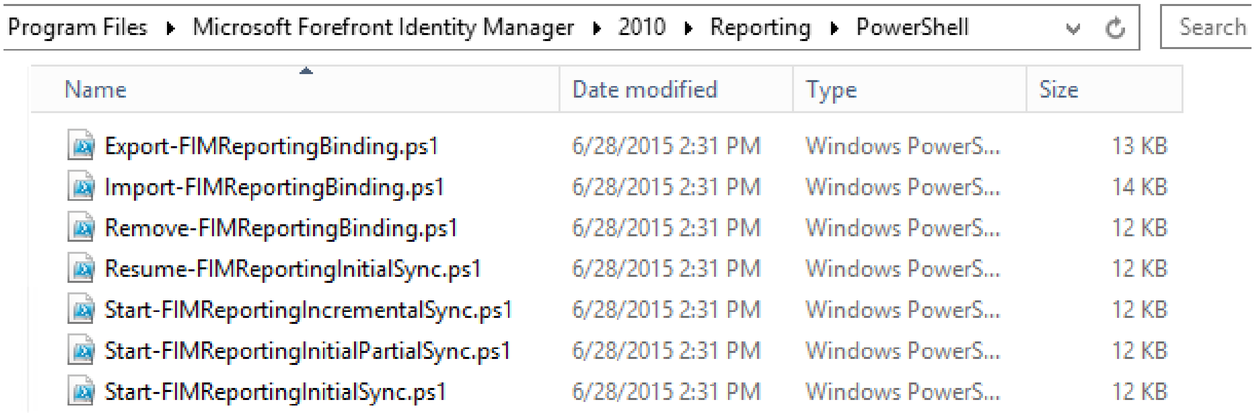


Administrator: Windows PowerShell

```
PS C:\Data Warehouse Support Scripts> .\FIMPostInstallScriptsForDataWarehouse.ps1

cmdlet FIMPostInstallScriptsForDataWarehouse.ps1 at command pipeline position 1
Supply values for the following parameters:
DataWarehouseServerInstance: localhost
DataWarehouseDatabaseServerInstance: localhost
FIMServiceAccountName: TFC\svc-mimservice
It is strongly recommended that you take a backup of all four System Center Databases (ServiceManager, DWStagingAndConfi
g, DWRepository, DWDataMart).
Do you want to continue? (Y/N): y
Checking to see if MPSyncJob is running on: localhost
Data warehouse server machine: localhost
Loading SQL Server Snapins
Checking to see if the Base Management packs for ForeFront Identity Manager have been deployed
Adding FIMService Login and User
Deploying DWStagingAndConfiguration Database Scripts
Granting Permission to FIMService Login
FIM Datawarehouse script installation complete
PS SQLSERVER:\> _
```

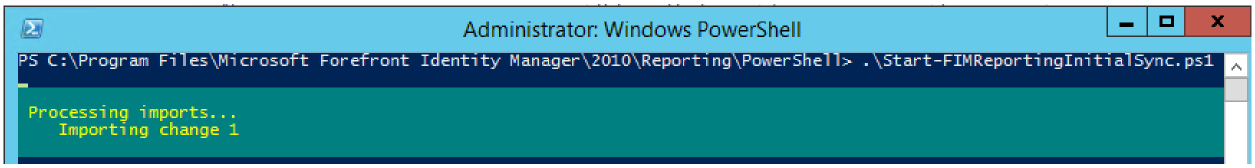


SQL Server Agent
- Jobs
  - FIM_CalculateDeferredGroupMembershipTransitionsJob
  - FIM_CheckAndUpdateReportingJobStatusJob
  - FIM_DeleteExpiredSystemObjectsJob
  - FIM_MaintainGroupsJob
  - FIM_MaintainSetsJob
  - FIM_ScheduleReportingIncrementalSynchronizationJob
  - FIM_TemporalEventsJob
  - FIM_TerminateStuckRequestsJob
  - FIM_TruncateExportLogJob
  - syspolicy_purge_history

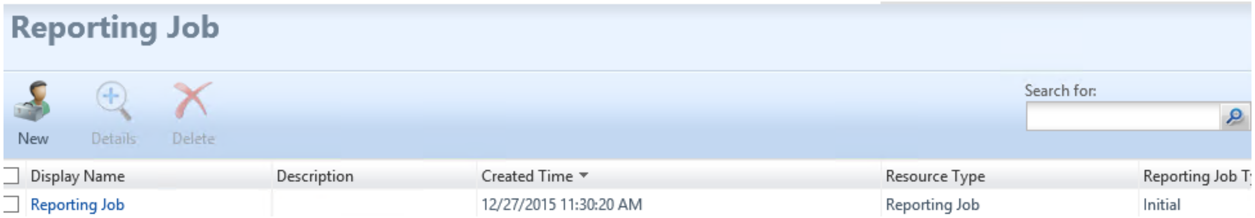


Program Files ▸ Microsoft Forefront Identity Manager ▸ 2010 ▸ Reporting ▸ PowerShell
Search

Name	Date modified	Type	Size
Export-FIMReportingBinding.ps1	6/28/2015 2:31 PM	Windows PowerS...	13 KB
Import-FIMReportingBinding.ps1	6/28/2015 2:31 PM	Windows PowerS...	14 KB
Remove-FIMReportingBinding.ps1	6/28/2015 2:31 PM	Windows PowerS...	12 KB
Resume-FIMReportingInitialSync.ps1	6/28/2015 2:31 PM	Windows PowerS...	12 KB
Start-FIMReportingIncrementalSync.ps1	6/28/2015 2:31 PM	Windows PowerS...	12 KB
Start-FIMReportingInitialPartialSync.ps1	6/28/2015 2:31 PM	Windows PowerS...	12 KB
Start-FIMReportingInitialSync.ps1	6/28/2015 2:31 PM	Windows PowerS...	12 KB

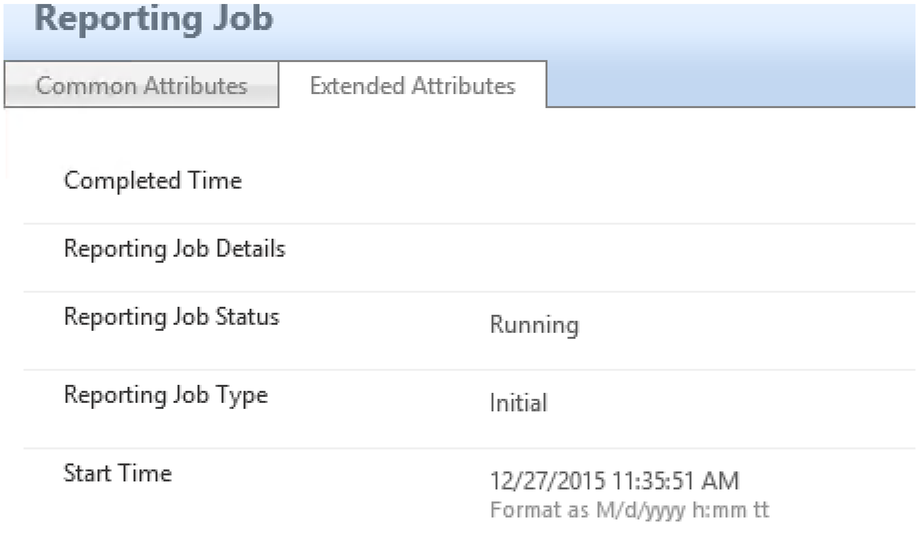


```
PS C:\Program Files\Microsoft Forefront Identity Manager\2010\Reporting\PowerShell> .\Start-FIMReportingInitialSync.ps1

 Processing imports...
    Importing change 1
```

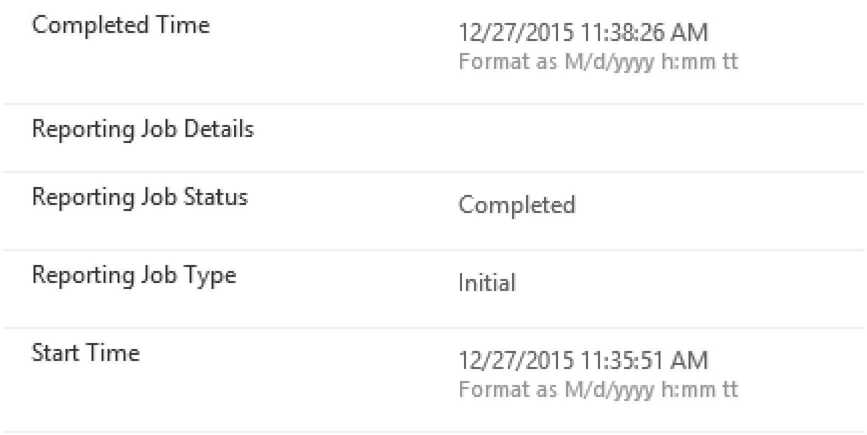


Reporting Job

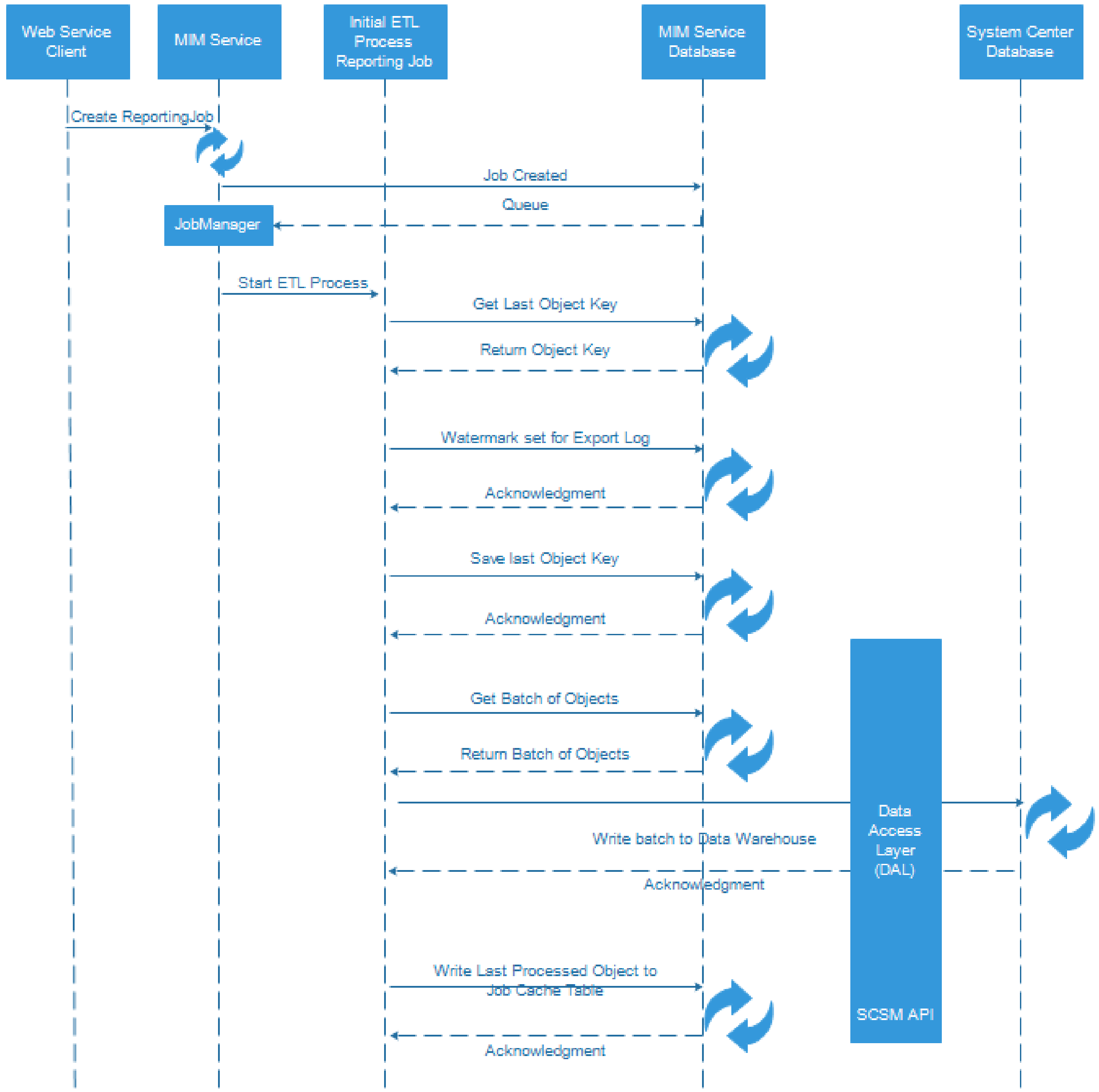
□	Display Name	Description	Created Time ▾	Resource Type	Reporting Job T
□	Reporting Job		12/27/2015 11:30:20 AM	Reporting Job	Initial

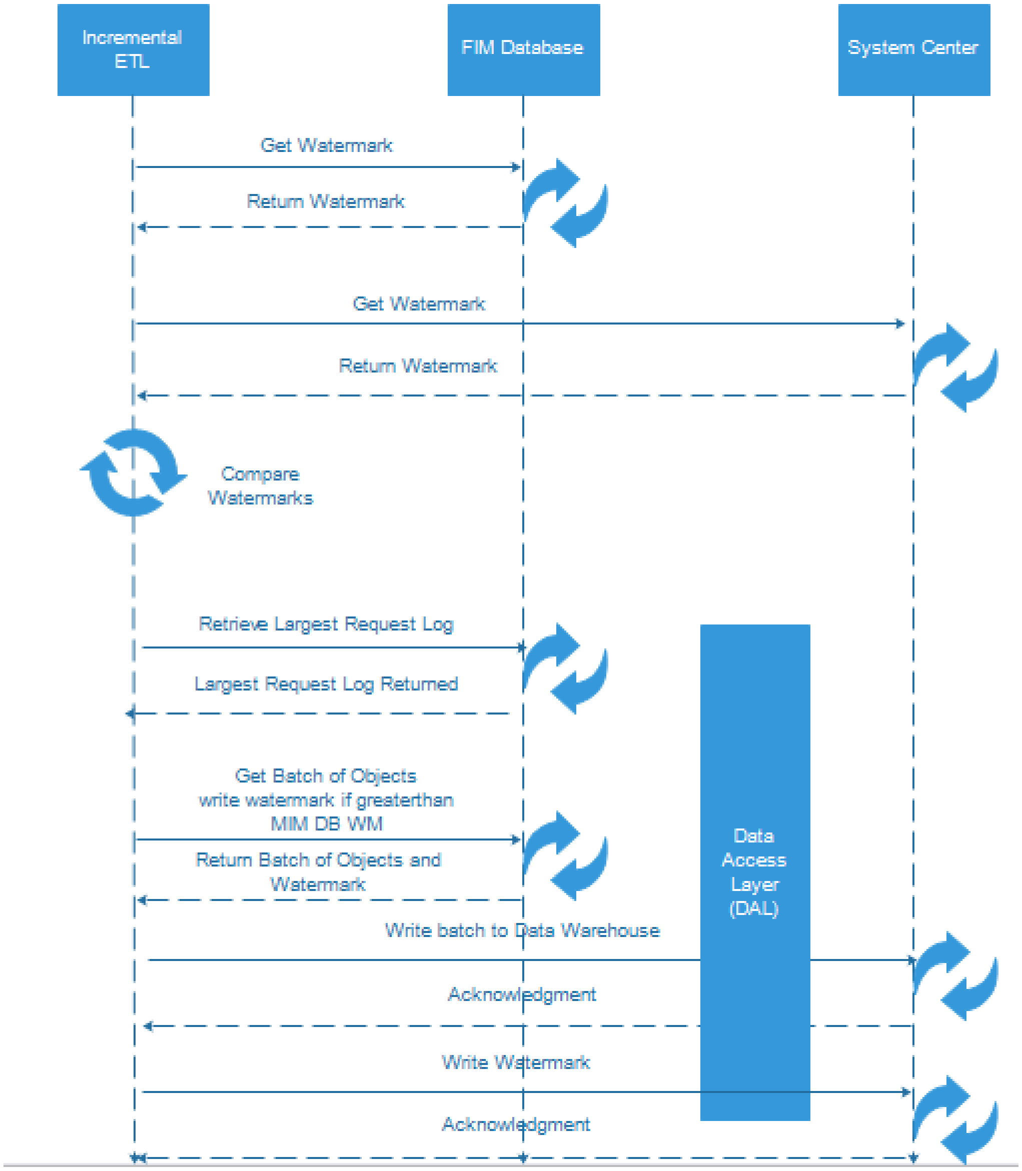


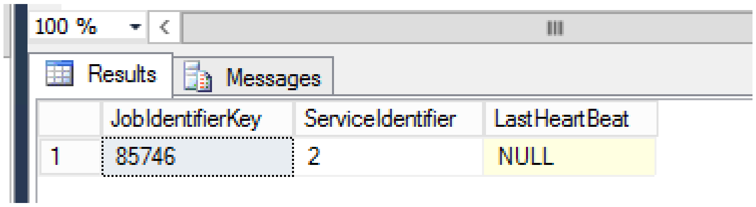
Completed Time	
Reporting Job Details	
Reporting Job Status	Running
Reporting Job Type	Initial
Start Time	12/27/2015 11:35:51 AM Format as M/d/yyyy h:mm tt



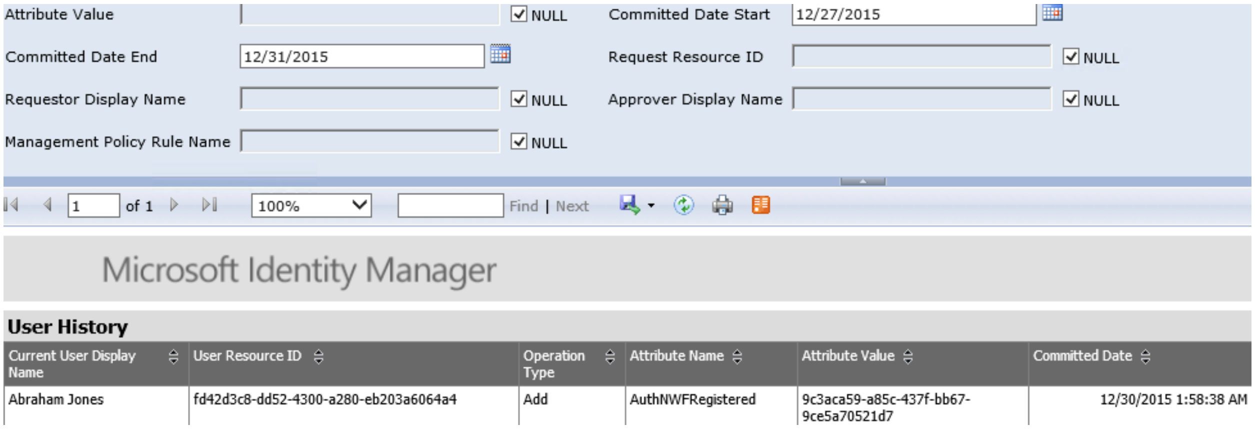
Completed Time	12/27/2015 11:38:26 AM Format as M/d/yyyy h:mm tt
Reporting Job Details	
Reporting Job Status	Completed
Reporting Job Type	Initial
Start Time	12/27/2015 11:35:51 AM Format as M/d/yyyy h:mm tt


Web Service Client
MIM Service
Initial ETL Process Reporting Job
MIM Service Database
System Center Database
Create ReportingJob
Job Created
Queue
JobManager
Start ETL Process
Get Last Object Key
Return Object Key
Watermark set for Export Log
Acknowledgment
Save last Object Key
Acknowledgment
Get Batch of Objects
Return Batch of Objects
Data Access Layer (DAL)
Write batch to Data Warehouse
Acknowledgment
SCSM API
Write Last Processed Object to Job Cache Table
Acknowledgment


Incremental ETL
FIM Database
System Center
Get Watermark
Return Watermark
Get Watermark
Return Watermark
Compare Watermarks
Retrieve Largest Request Log
Largest Request Log Returned
Get Batch of Objects write watermark if greaterthan MIM DB WM
Return Batch of Objects and Watermark
Data Access Layer (DAL)
Write batch to Data Warehouse
Acknowledgment
Write Watermark
Acknowledgment



	JobIdentifierKey	ServiceIdentifier	LastHeartBeat
1	85746	2	NULL

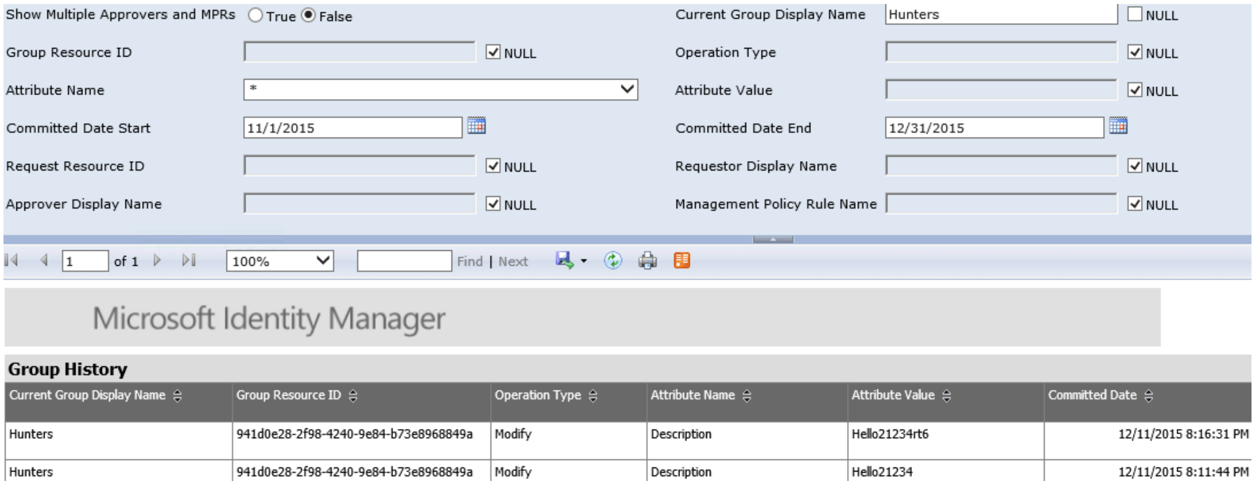


Attribute Value	☑ NULL	Committed Date Start	12/27/2015
Committed Date End	12/31/2015	Request Resource ID	☑ NULL
Requestor Display Name	☑ NULL	Approver Display Name	☑ NULL
Management Policy Rule Name	☑ NULL		

Microsoft Identity Manager

User History

Current User Display Name	User Resource ID	Operation Type	Attribute Name	Attribute Value	Committed Date
Abraham Jones	fd42d3c8-dd52-4300-a280-eb203a6064a4	Add	AuthNWFRegistered	9c3aca59-a85c-437f-bb67-9ce5a70521d7	12/30/2015 1:58:38 AM

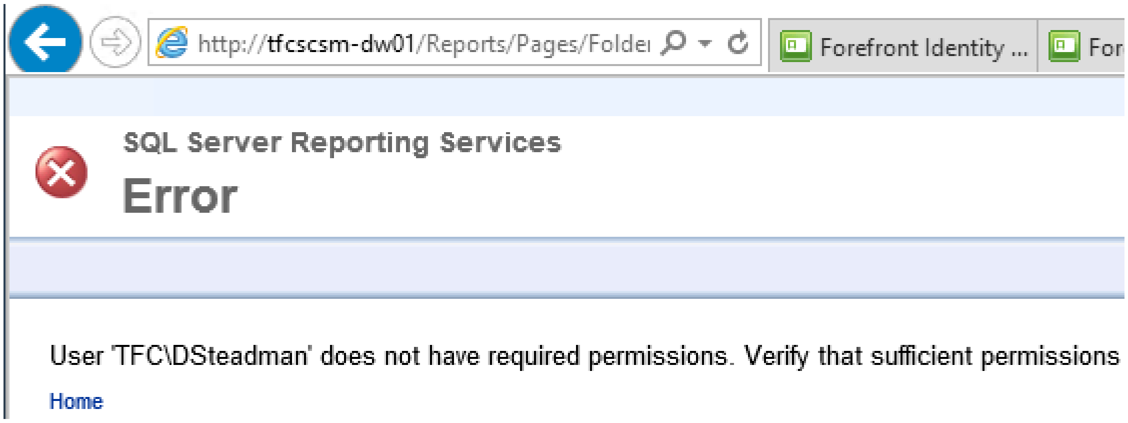


Show Multiple Approvers and MPRs	○ True ● False	Current Group Display Name	Hunters □ NULL
Group Resource ID	☑ NULL	Operation Type	☑ NULL
Attribute Name	*	Attribute Value	☑ NULL
Committed Date Start	11/1/2015	Committed Date End	12/31/2015
Request Resource ID	☑ NULL	Requestor Display Name	☑ NULL
Approver Display Name	☑ NULL	Management Policy Rule Name	☑ NULL

Microsoft Identity Manager

Group History

Current Group Display Name	Group Resource ID	Operation Type	Attribute Name	Attribute Value	Committed Date
Hunters	941d0e28-2f98-4240-9e84-b73e8968849a	Modify	Description	Hello21234rt6	12/11/2015 8:16:31 PM
Hunters	941d0e28-2f98-4240-9e84-b73e8968849a	Modify	Description	Hello21234	12/11/2015 8:11:44 PM

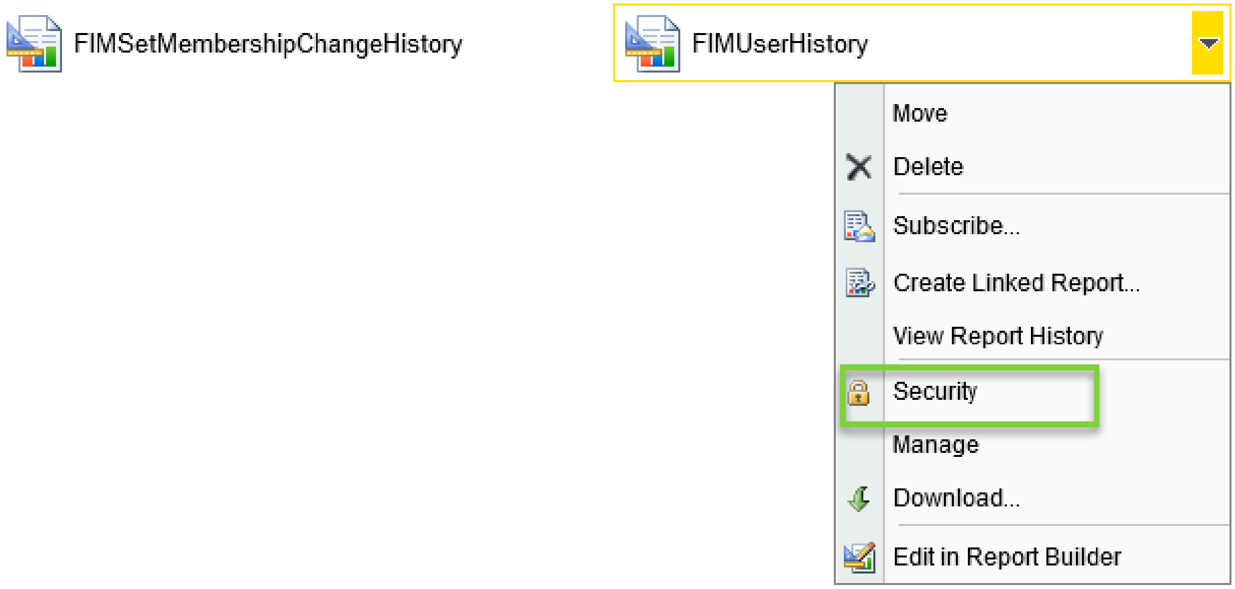


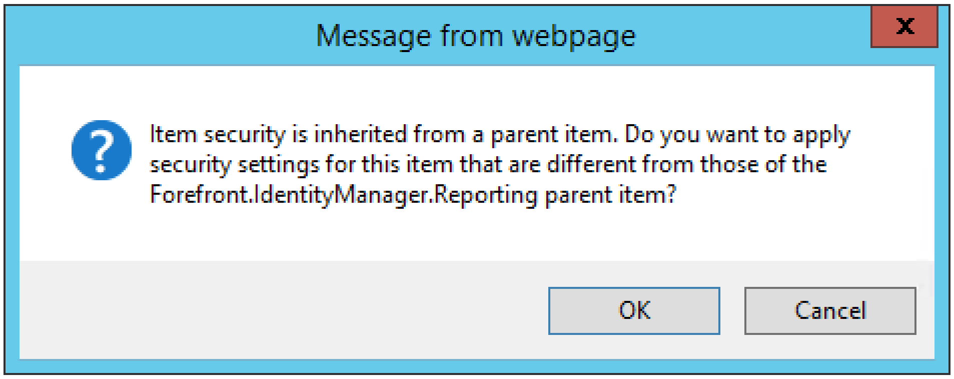
SQL Server Reporting Services

Error

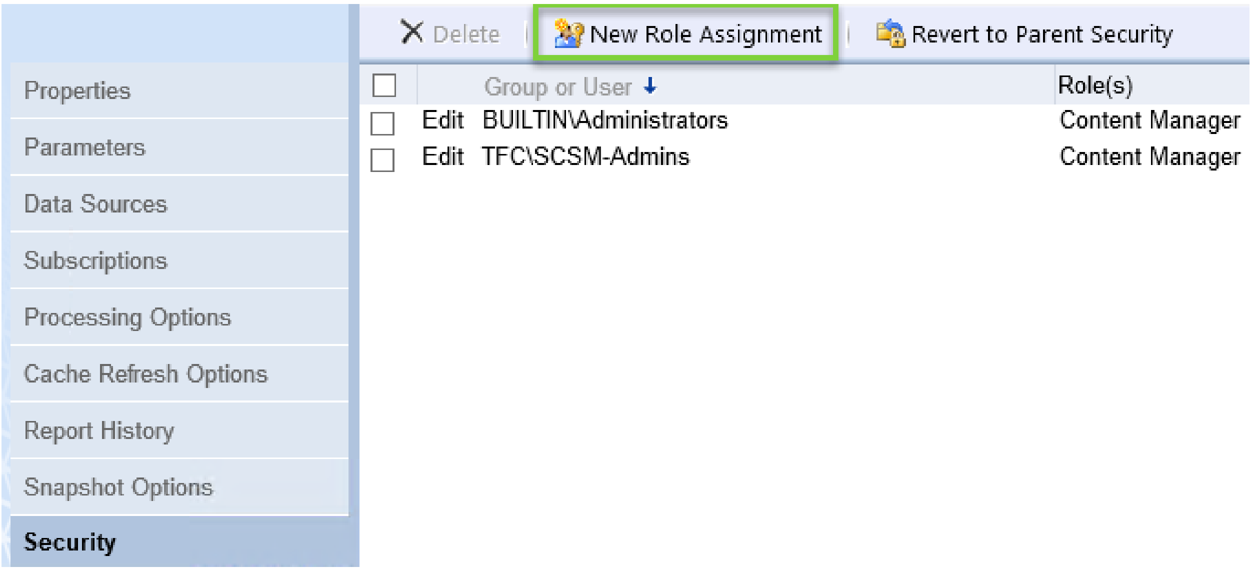
User 'TFC\DSteadman' does not have required permissions. Verify that sufficient permissions

Home

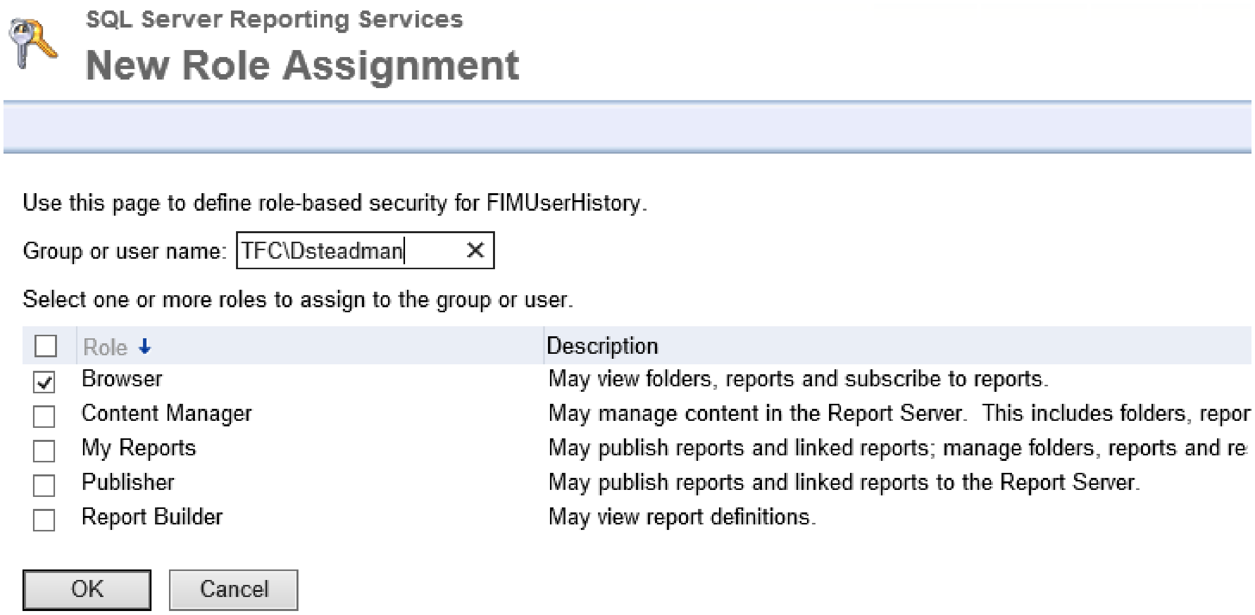




Item security is inherited from a parent item. Do you want to apply security settings for this item that are different from those of the Forefront.IdentityManager.Reporting parent item?



□		Group or User ↓	Role(s)
□	Edit	BUILTIN\Administrators	Content Manager
□	Edit	TFC\SCSM-Admins	Content Manager



SQL Server Reporting Services

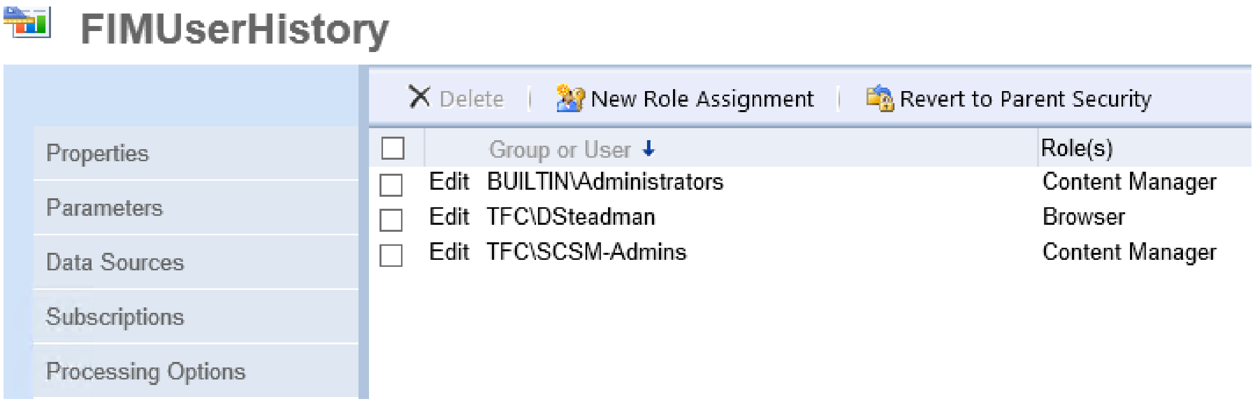
New Role Assignment

Use this page to define role-based security for FIMUserHistory.

Group or user name: TFC\Dsteadman

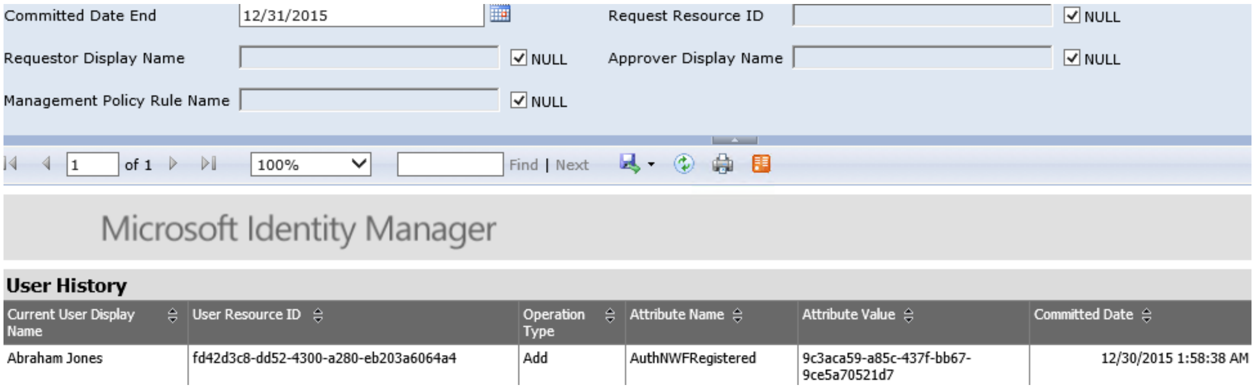
Select one or more roles to assign to the group or user.

□	Role	Description
☑	Browser	May view folders, reports and subscribe to reports.
□	Content Manager	May manage content in the Report Server. This includes folders, repor
□	My Reports	May publish reports and linked reports; manage folders, reports and re
□	Publisher	May publish reports and linked reports to the Report Server.
□	Report Builder	May view report definitions.



FIMUserHistory

□		Group or User	Role(s)
□	Edit	BUILTIN\Administrators	Content Manager
□	Edit	TFC\DSteadman	Browser
□	Edit	TFC\SCSM-Admins	Content Manager

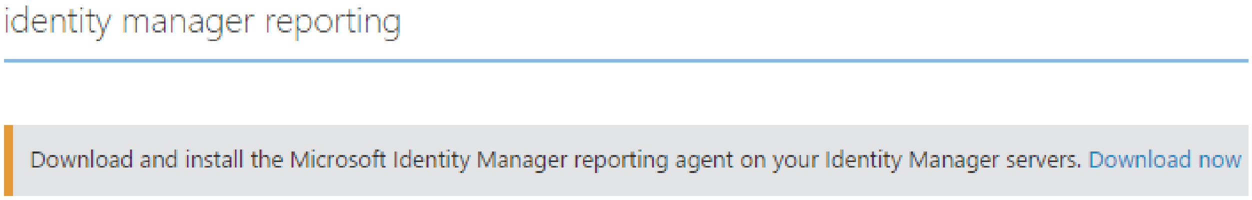


Committed Date End	12/31/2015		Request Resource ID		☑ NULL
Requestor Display Name		☑ NULL	Approver Display Name		☑ NULL
Management Policy Rule Name		☑ NULL			

Microsoft Identity Manager

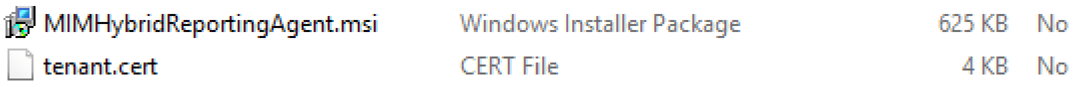
User History

Current User Display Name	User Resource ID	Operation Type	Attribute Name	Attribute Value	Committed Date
Abraham Jones	fd42d3c8-dd52-4300-a280-eb203a6064a4	Add	AuthNWFRegistered	9c3aca59-a85c-437f-bb67-9ce5a70521d7	12/30/2015 1:58:38 AM

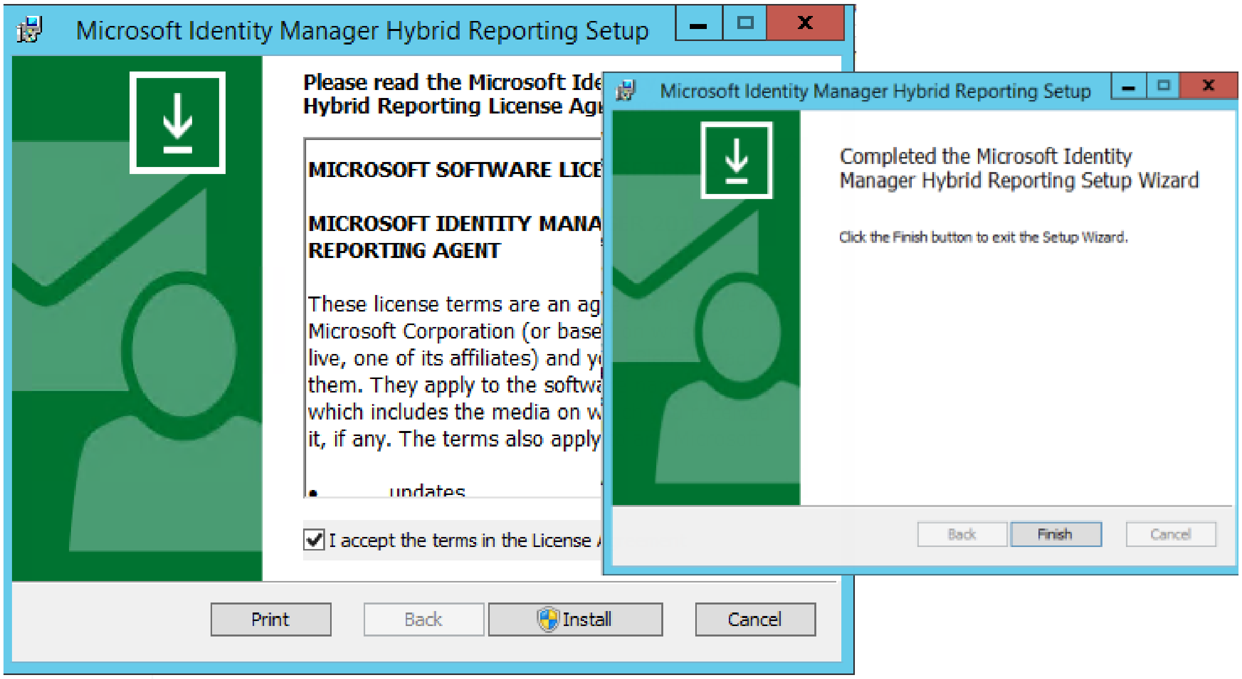


identity manager reporting

Download and install the Microsoft Identity Manager reporting agent on your Identity Manager servers. Download now



MIMHybridReportingAgent.msi	Windows Installer Package	625 KB	No
tenant.cert	CERT File	4 KB	No



Microsoft Identity Manager Hybrid Reporting Setup

**Please read the Microsoft Ide
Hybrid Reporting License Ag**

MICROSOFT SOFTWARE LICE

**MICROSOFT IDENTITY MANA
REPORTING AGENT**

These license terms are an ag
Microsoft Corporation (or base
live, one of its affiliates) and y
them. They apply to the softw
which includes the media on w
it, if any. The terms also apply

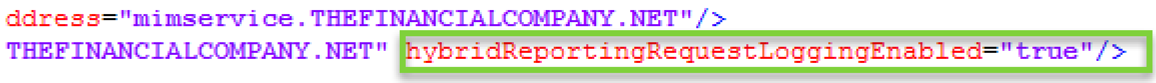
- updates

☑ I accept the terms in the License

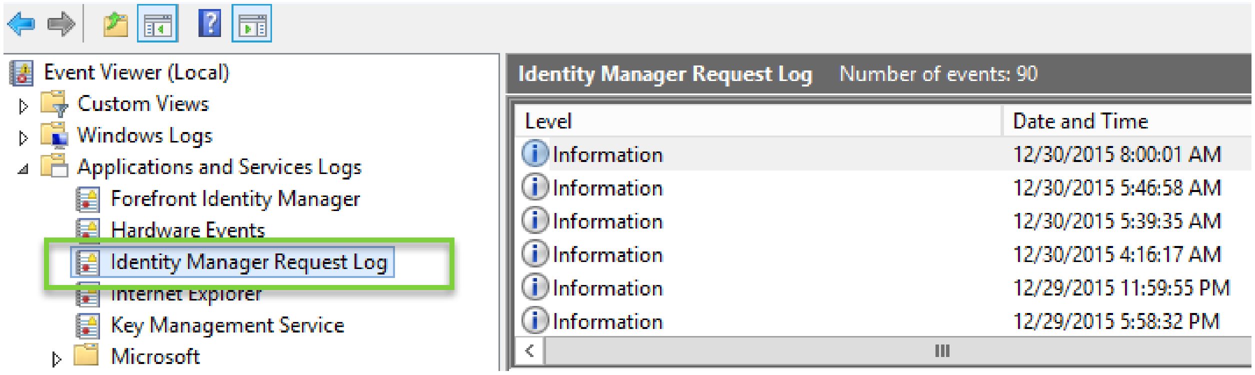
Print
Back
Install
Cancel
Microsoft Identity Manager Hybrid Reporting Setup

Completed the Microsoft Identity Manager Hybrid Reporting Setup Wizard

Click the Finish button to exit the Setup Wizard.

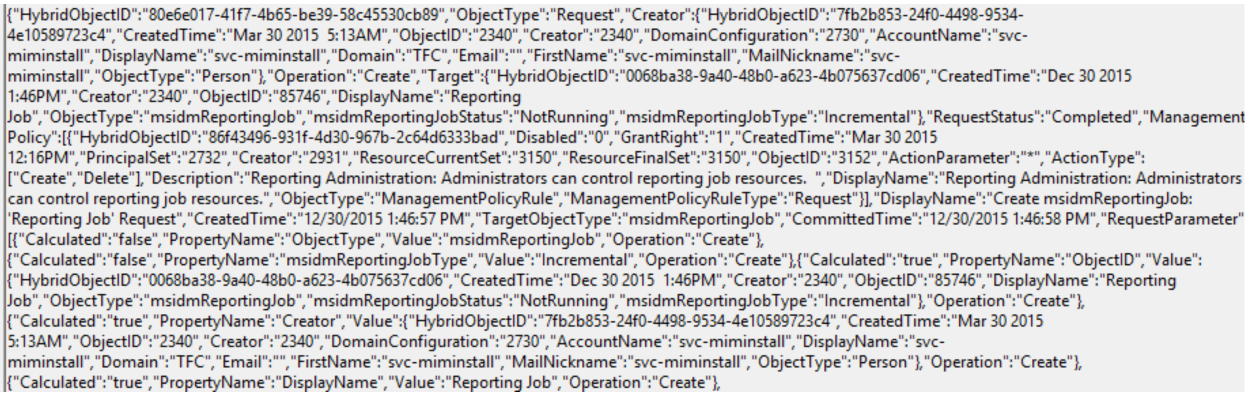


```
ddress="mimservice.THEFINANCIALCOMPANY.NET"/>
THEFINANCIALCOMPANY.NET" hybridReportingRequestLoggingEnabled="true"/>
```

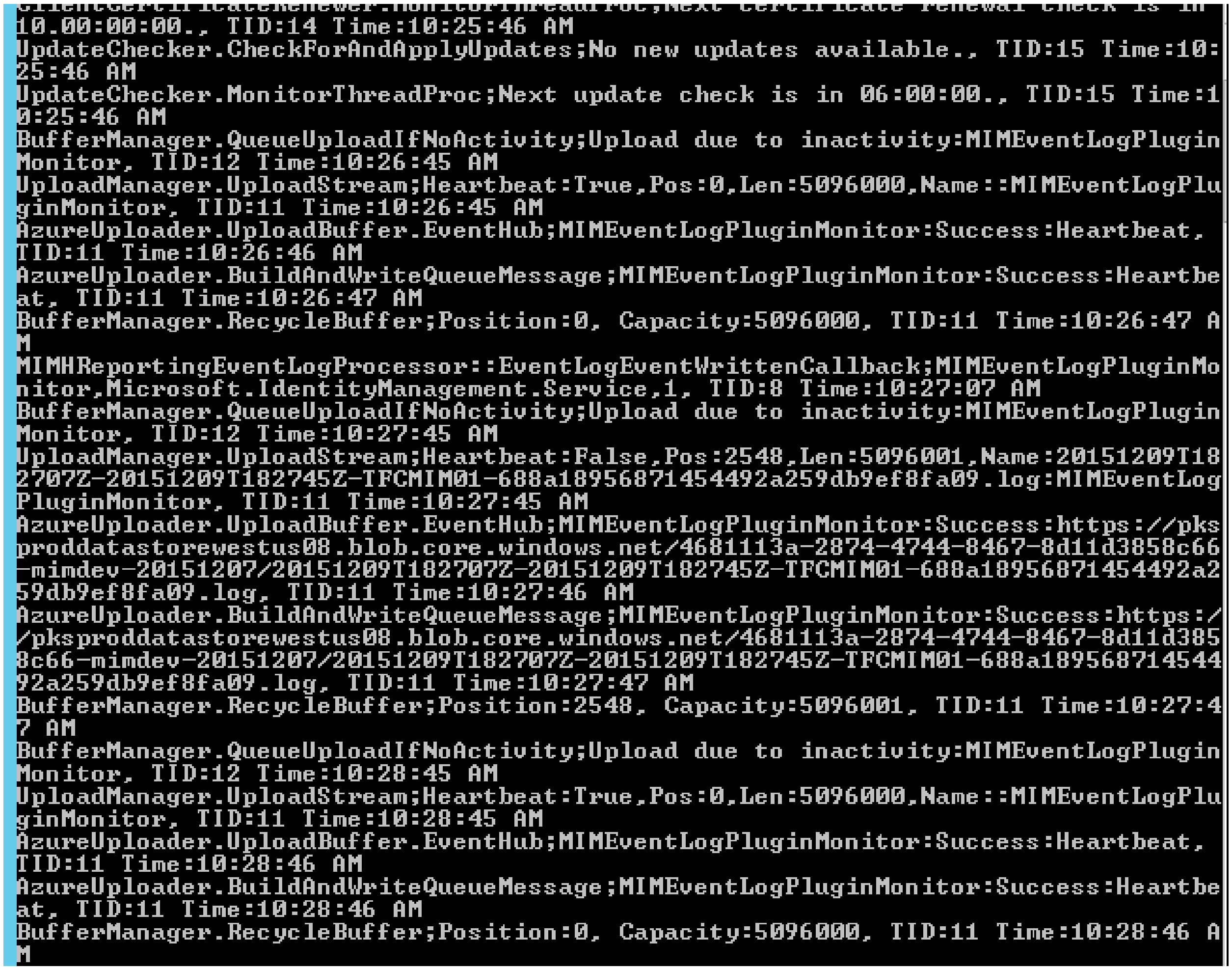


Identity Manager Request Log   Number of events: 90

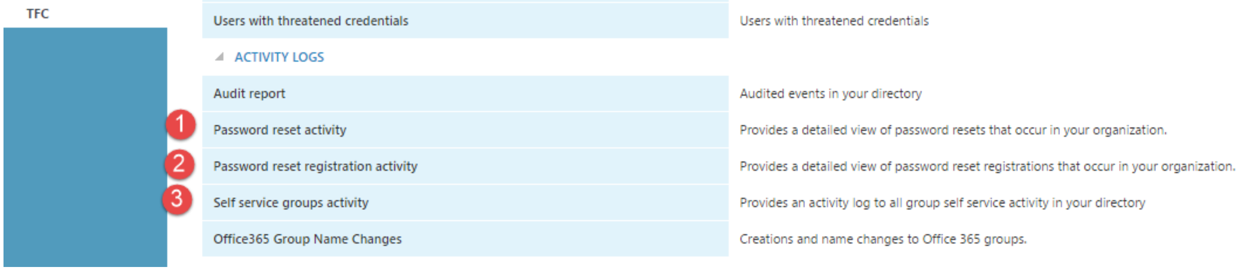
Level	Date and Time
Information	12/30/2015 8:00:01 AM
Information	12/30/2015 5:46:58 AM
Information	12/30/2015 5:39:35 AM
Information	12/30/2015 4:16:17 AM
Information	12/29/2015 11:59:55 PM
Information	12/29/2015 5:58:32 PM



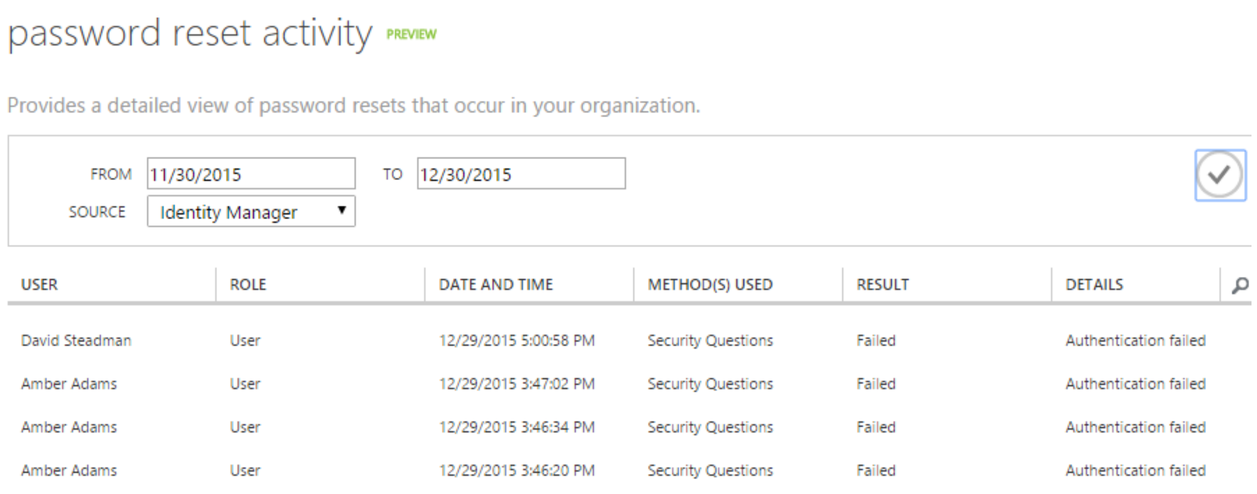
```
{"HybridObjectID":"80e6e017-41f7-4b65-be39-58c45530cb89","ObjectType":"Request","Creator":{"HybridObjectID":"7fb2b853-24f0-4498-9534-
4e10589723c4","CreatedTime":"Mar 30 2015  5:13AM","ObjectID":"2340","Creator":"2340","DomainConfiguration":"2730","AccountName":"svc-
miminstall","DisplayName":"svc-miminstall","Domain":"TFC","Email":"","FirstName":"svc-miminstall","MailNickname":"svc-
miminstall","ObjectType":"Person"},"Operation":"Create","Target":{"HybridObjectID":"0068ba38-9a40-48b0-a623-4b075637cd06","CreatedTime":"Dec 30 2015
1:46PM","Creator":"2340","ObjectID":"85746","DisplayName":"Reporting
Job","ObjectType":"msidmReportingJob","msidmReportingJobStatus":"NotRunning","msidmReportingJobType":"Incremental"},"RequestStatus":"Completed","Management
Policy":[{"HybridObjectID":"86f43496-931f-4d30-967b-2c64d6333bad","Disabled":"0","GrantRight":"1","CreatedTime":"Mar 30 2015
12:16PM","PrincipalSet":"2732","Creator":"2931","ResourceCurrentSet":"3150","ResourceFinalSet":"3150","ObjectID":"3152","ActionParameter":"*","ActionType":
["Create","Delete"],"Description":"Reporting Administration: Administrators can control reporting job resources.  ","DisplayName":"Reporting Administration: Administrators
can control reporting job resources.","ObjectType":"ManagementPolicyRule","ManagementPolicyRuleType":"Request"}],"DisplayName":"Create msidmReportingJob:
'Reporting Job' Request","CreatedTime":"12/30/2015 1:46:57 PM","TargetObjectType":"msidmReportingJob","CommittedTime":"12/30/2015 1:46:58 PM","RequestParameter"
[{"Calculated":"false","PropertyName":"ObjectType","Value":"msidmReportingJob","Operation":"Create"},
{"Calculated":"false","PropertyName":"msidmReportingJobType","Value":"Incremental","Operation":"Create"},{"Calculated":"true","PropertyName":"ObjectID","Value":
{"HybridObjectID":"0068ba38-9a40-48b0-a623-4b075637cd06","CreatedTime":"Dec 30 2015  1:46PM","Creator":"2340","ObjectID":"85746","DisplayName":"Reporting
Job","ObjectType":"msidmReportingJob","msidmReportingJobStatus":"NotRunning","msidmReportingJobType":"Incremental"},"Operation":"Create"},
{"Calculated":"true","PropertyName":"Creator","Value":{"HybridObjectID":"7fb2b853-24f0-4498-9534-4e10589723c4","CreatedTime":"Mar 30 2015
5:13AM","ObjectID":"2340","Creator":"2340","DomainConfiguration":"2730","AccountName":"svc-miminstall","DisplayName":"svc-
miminstall","Domain":"TFC","Email":"","FirstName":"svc-miminstall","MailNickname":"svc-miminstall","ObjectType":"Person"},"Operation":"Create"},
{"Calculated":"true","PropertyName":"DisplayName","Value":"Reporting Job","Operation":"Create"},
```



```
ClientCertificateRenewer.MonitorThreadProc;Next certificate renewal check is in
10.00:00:00., TID:14 Time:10:25:46 AM
UpdateChecker.CheckForAndApplyUpdates;No new updates available., TID:15 Time:10:
25:46 AM
UpdateChecker.MonitorThreadProc;Next update check is in 06:00:00., TID:15 Time:1
0:25:46 AM
BufferManager.QueueUploadIfNoActivity;Upload due to inactivity:MIMEventLogPlugin
Monitor, TID:12 Time:10:26:45 AM
UploadManager.UploadStream;Heartbeat:True,Pos:0,Len:5096000,Name::MIMEventLogPlu
ginMonitor, TID:11 Time:10:26:45 AM
AzureUploader.UploadBuffer.EventHub;MIMEventLogPluginMonitor:Success:Heartbeat,
TID:11 Time:10:26:46 AM
AzureUploader.BuildAndWriteQueueMessage;MIMEventLogPluginMonitor:Success:Heartbe
at, TID:11 Time:10:26:47 AM
BufferManager.RecycleBuffer;Position:0, Capacity:5096000, TID:11 Time:10:26:47 A
M
MIMHReportingEventLogProcessor::EventLogEventWrittenCallback;MIMEventLogPluginMo
nitor,Microsoft.IdentityManagement.Service,1, TID:8 Time:10:27:07 AM
BufferManager.QueueUploadIfNoActivity;Upload due to inactivity:MIMEventLogPlugin
Monitor, TID:12 Time:10:27:45 AM
UploadManager.UploadStream;Heartbeat:False,Pos:2548,Len:5096001,Name:20151209T18
2707Z-20151209T182745Z-TFCMIM01-688a18956871454492a259db9ef8fa09.log:MIMEventLog
PluginMonitor, TID:11 Time:10:27:45 AM
AzureUploader.UploadBuffer.EventHub;MIMEventLogPluginMonitor:Success:https://pks
proddatastorewestus08.blob.core.windows.net/4681113a-2874-4744-8467-8d11d3858c66
-mimdev-20151207/20151209T182707Z-20151209T182745Z-TFCMIM01-688a18956871454492a2
59db9ef8fa09.log, TID:11 Time:10:27:46 AM
AzureUploader.BuildAndWriteQueueMessage;MIMEventLogPluginMonitor:Success:https:/
/pksproddatastorewestus08.blob.core.windows.net/4681113a-2874-4744-8467-8d11d385
8c66-mimdev-20151207/20151209T182707Z-20151209T182745Z-TFCMIM01-688a189568714544
92a259db9ef8fa09.log, TID:11 Time:10:27:47 AM
BufferManager.RecycleBuffer;Position:2548, Capacity:5096001, TID:11 Time:10:27:4
7 AM
BufferManager.QueueUploadIfNoActivity;Upload due to inactivity:MIMEventLogPlugin
Monitor, TID:12 Time:10:28:45 AM
UploadManager.UploadStream;Heartbeat:True,Pos:0,Len:5096000,Name::MIMEventLogPlu
ginMonitor, TID:11 Time:10:28:45 AM
AzureUploader.UploadBuffer.EventHub;MIMEventLogPluginMonitor:Success:Heartbeat,
TID:11 Time:10:28:46 AM
AzureUploader.BuildAndWriteQueueMessage;MIMEventLogPluginMonitor:Success:Heartbe
at, TID:11 Time:10:28:46 AM
BufferManager.RecycleBuffer;Position:0, Capacity:5096000, TID:11 Time:10:28:46 A
M
```



Users with threatened credentials	Users with threatened credentials
◢ ACTIVITY LOGS	
Audit report	Audited events in your directory
1 Password reset activity	Provides a detailed view of password resets that occur in your organization.
2 Password reset registration activity	Provides a detailed view of password reset registrations that occur in your organization.
3 Self service groups activity	Provides an activity log to all group self service activity in your directory
Office365 Group Name Changes	Creations and name changes to Office 365 groups.



password reset activity

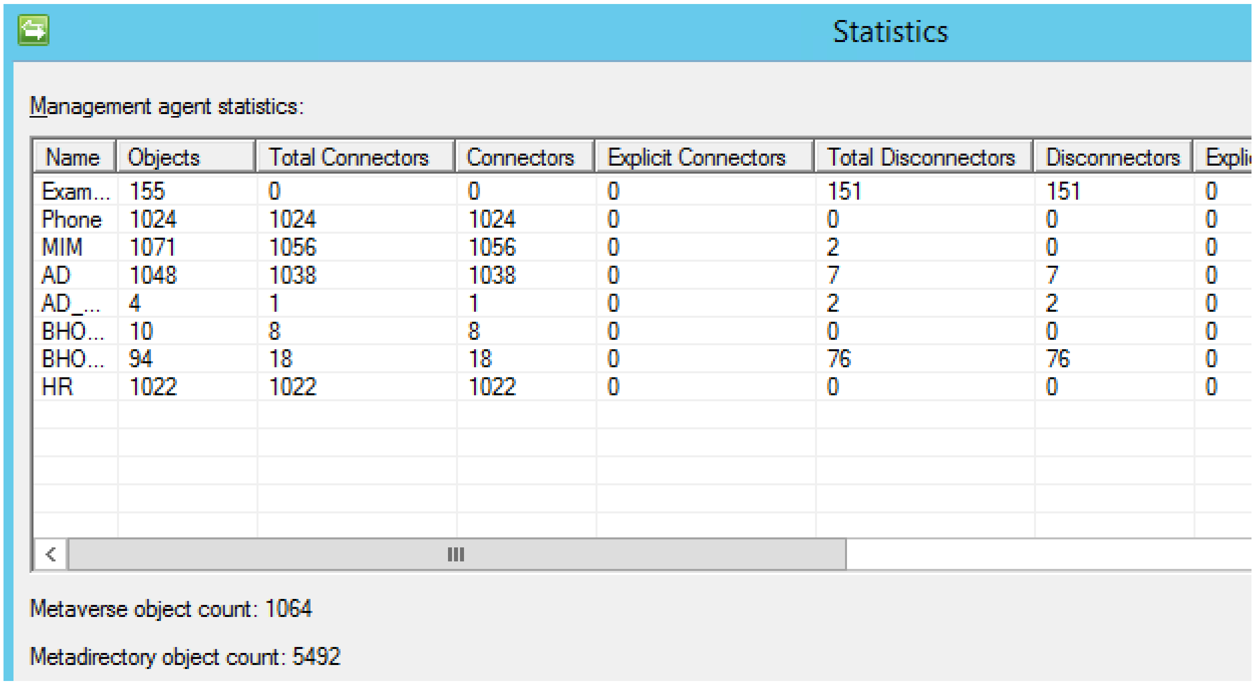
Provides a detailed view of password resets that occur in your organization.

FROM 11/30/2015 TO 12/30/2015

SOURCE Identity Manager ▾

USER	ROLE	DATE AND TIME	METHOD(S) USED	RESULT	DETAILS
David Steadman	User	12/29/2015 5:00:58 PM	Security Questions	Failed	Authentication failed
Amber Adams	User	12/29/2015 3:47:02 PM	Security Questions	Failed	Authentication failed
Amber Adams	User	12/29/2015 3:46:34 PM	Security Questions	Failed	Authentication failed
Amber Adams	User	12/29/2015 3:46:20 PM	Security Questions	Failed	Authentication failed

Chapter 14: Troubleshooting

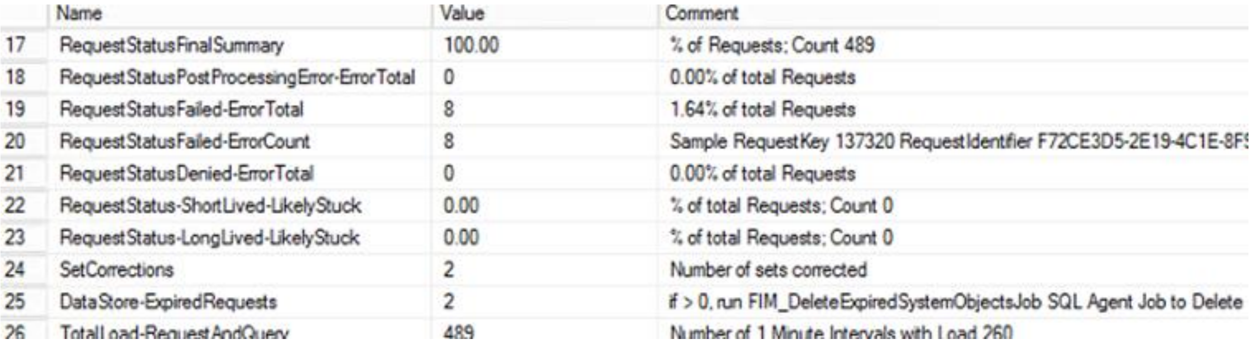


Management agent statistics:

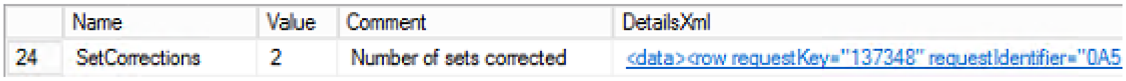
Name	Objects	Total Connectors	Connectors	Explicit Connectors	Total Disconnectors	Disconnectors	Expli
Exam...	155	0	0	0	151	151	0
Phone	1024	1024	1024	0	0	0	0
MIM	1071	1056	1056	0	2	0	0
AD	1048	1038	1038	0	7	7	0
AD_...	4	1	1	0	2	2	0
BHO...	10	8	8	0	0	0	0
BHO...	94	18	18	0	76	76	0
HR	1022	1022	1022	0	0	0	0

Metaverse object count: 1064

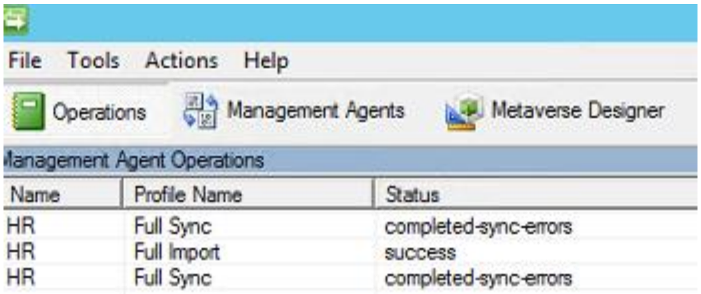
Metadirectory object count: 5492



	Name	Value	Comment
17	RequestStatusFinalSummary	100.00	% of Requests; Count 489
18	RequestStatusPostProcessingError-ErrorTotal	0	0.00% of total Requests
19	RequestStatusFailed-ErrorTotal	8	1.64% of total Requests
20	RequestStatusFailed-ErrorCount	8	Sample RequestKey 137320 RequestIdentifier F72CE3D5-2E19-4C1E-8F
21	RequestStatusDenied-ErrorTotal	0	0.00% of total Requests
22	RequestStatus-ShortLived-LikelyStuck	0.00	% of total Requests; Count 0
23	RequestStatus-LongLived-LikelyStuck	0.00	% of total Requests; Count 0
24	SetCorrections	2	Number of sets corrected
25	DataStore-ExpiredRequests	2	if > 0, run FIM_DeleteExpiredSystemObjectsJob SQL Agent Job to Delete
26	TotalLoad-RequestAndQuery	489	Number of 1 Minute Intervals with Load 260

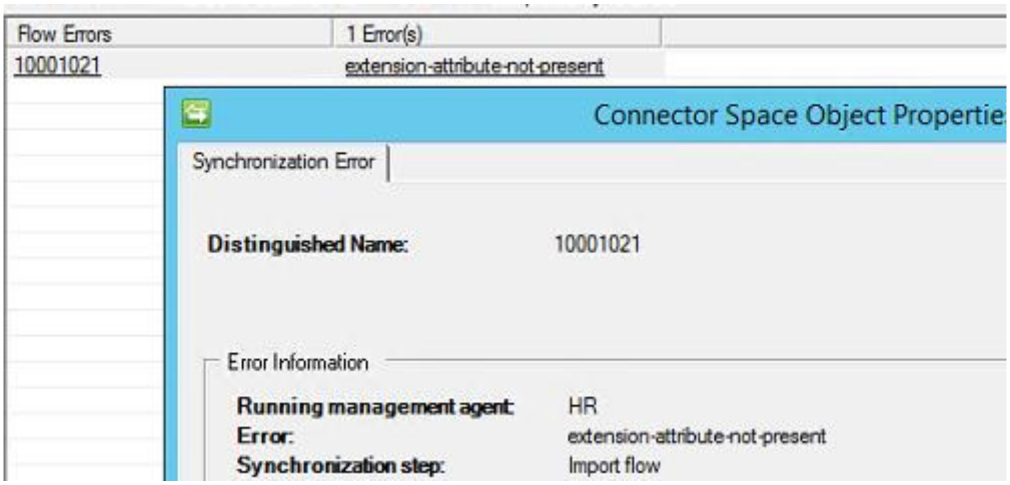


	Name	Value	Comment	DetailsXml
24	SetCorrections	2	Number of sets corrected	<data><row requestKey="137348" requestIdentifier="0A5



Management Agent Operations

Name	Profile Name	Status
HR	Full Sync	completed-sync-errors
HR	Full Import	success
HR	Full Sync	completed-sync-errors



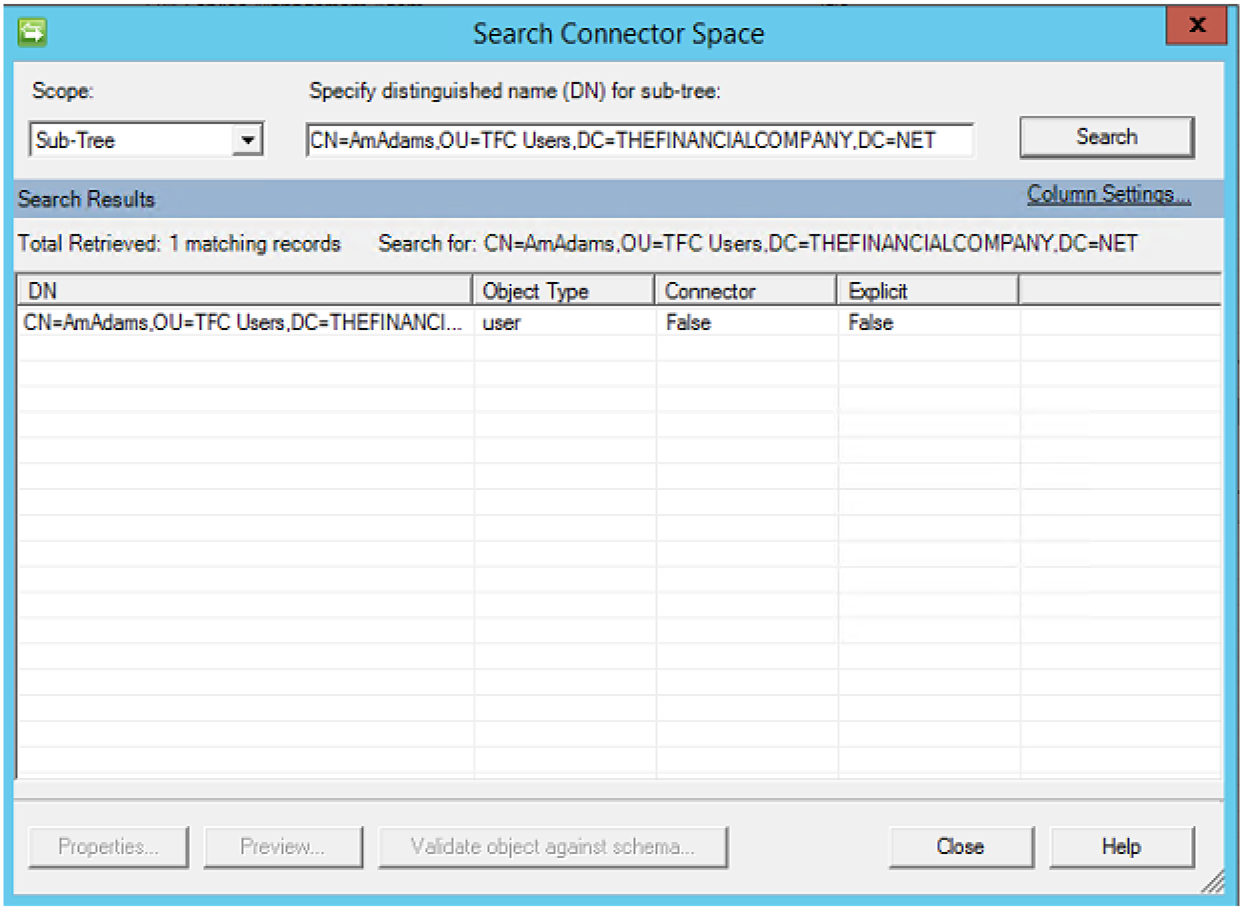
Flow Errors	1 Error(s)
10001021	extension-attribute-not-present

Connector Space Object Propertie

Distinguished Name: 10001021

Error Information

Running management agent: HR
Error: extension-attribute-not-present
Synchronization step: Import flow



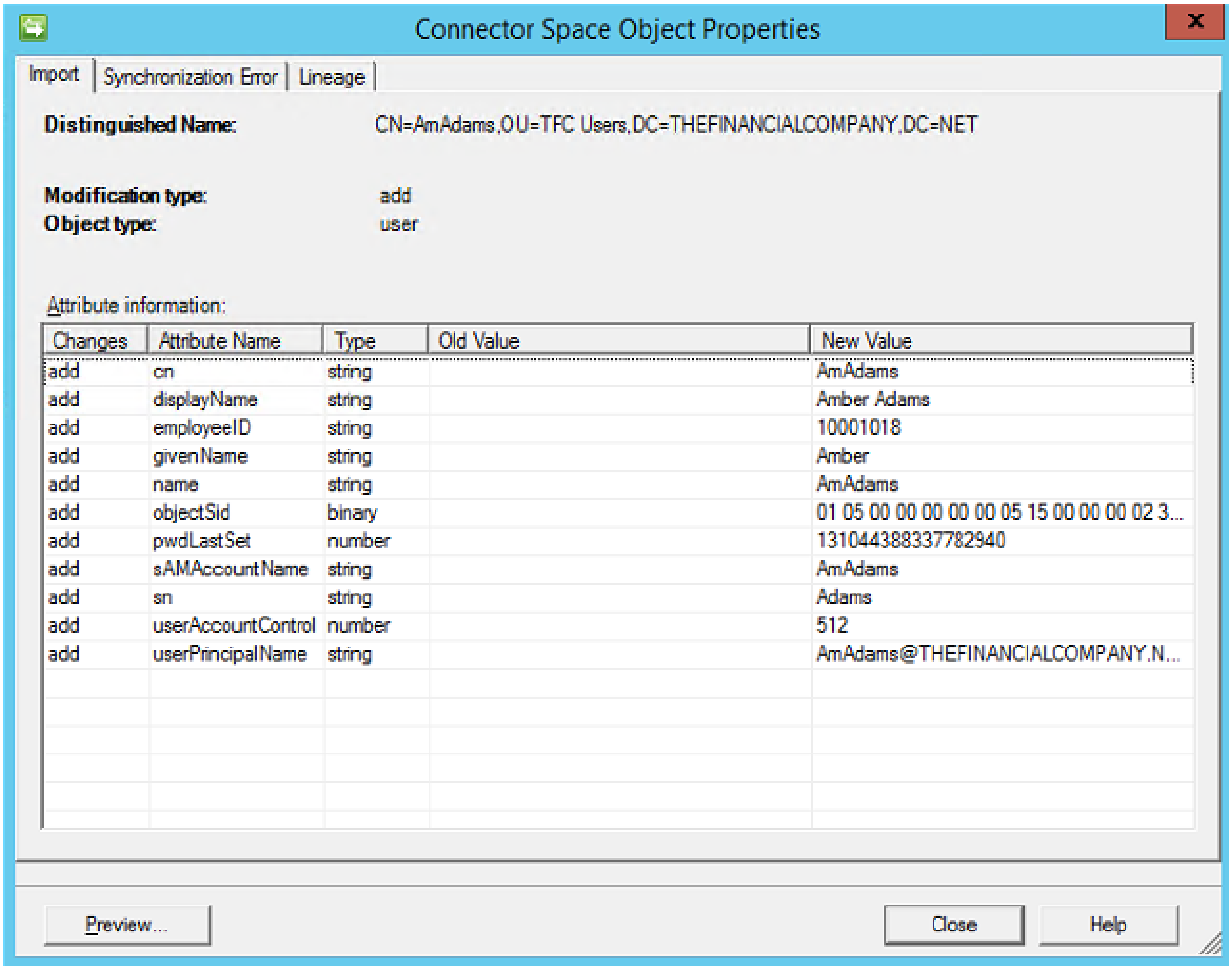
Search Connector Space

Scope: Sub-Tree

Specify distinguished name (DN) for sub-tree: CN=AmAdams,OU=TFC Users,DC=THEFINANCIALCOMPANY,DC=NET

Total Retrieved: 1 matching records   Search for: CN=AmAdams,OU=TFC Users,DC=THEFINANCIALCOMPANY,DC=NET

DN	Object Type	Connector	Explicit
CN=AmAdams,OU=TFC Users,DC=THEFINANCI...	user	False	False



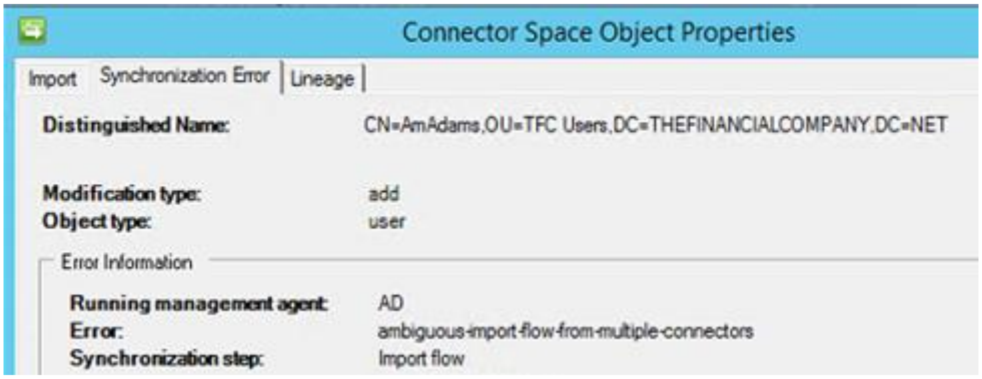
Distinguished Name: CN=AmAdams,OU=TFC Users,DC=THEFINANCIALCOMPANY,DC=NET

Modification type: add

Object type: user

Attribute information:

Changes	Attribute Name	Type	Old Value	New Value
add	cn	string		AmAdams
add	displayName	string		Amber Adams
add	employeeID	string		10001018
add	givenName	string		Amber
add	name	string		AmAdams
add	objectSid	binary		01 05 00 00 00 00 00 05 15 00 00 00 02 3...
add	pwdLastSet	number		131044388337782940
add	sAMAccountName	string		AmAdams
add	sn	string		Adams
add	userAccountControl	number		512
add	userPrincipalName	string		AmAdams@THEFINANCIALCOMPANY.N...



Distinguished Name: CN=AmAdams,OU=TFC Users,DC=THEFINANCIALCOMPANY,DC=NET

Modification type: add

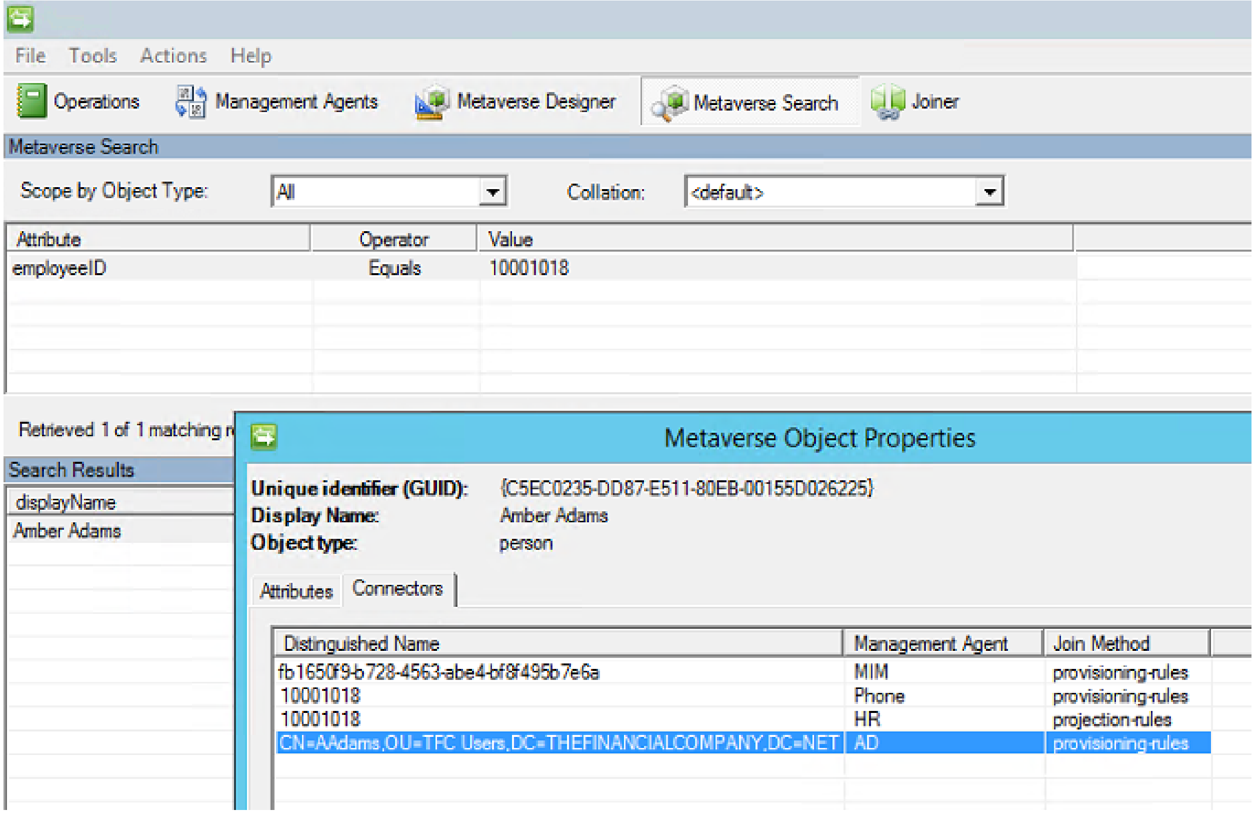
Object type: user

Error Information

Running management agent: AD

Error: ambiguous-import-flow-from-multiple-connectors

Synchronization step: Import flow



Metaverse Search

Scope by Object Type: All

Collation: <default>

Attribute	Operator	Value
employeeID	Equals	10001018

Retrieved 1 of 1 matching r

Search Results

displayName
Amber Adams

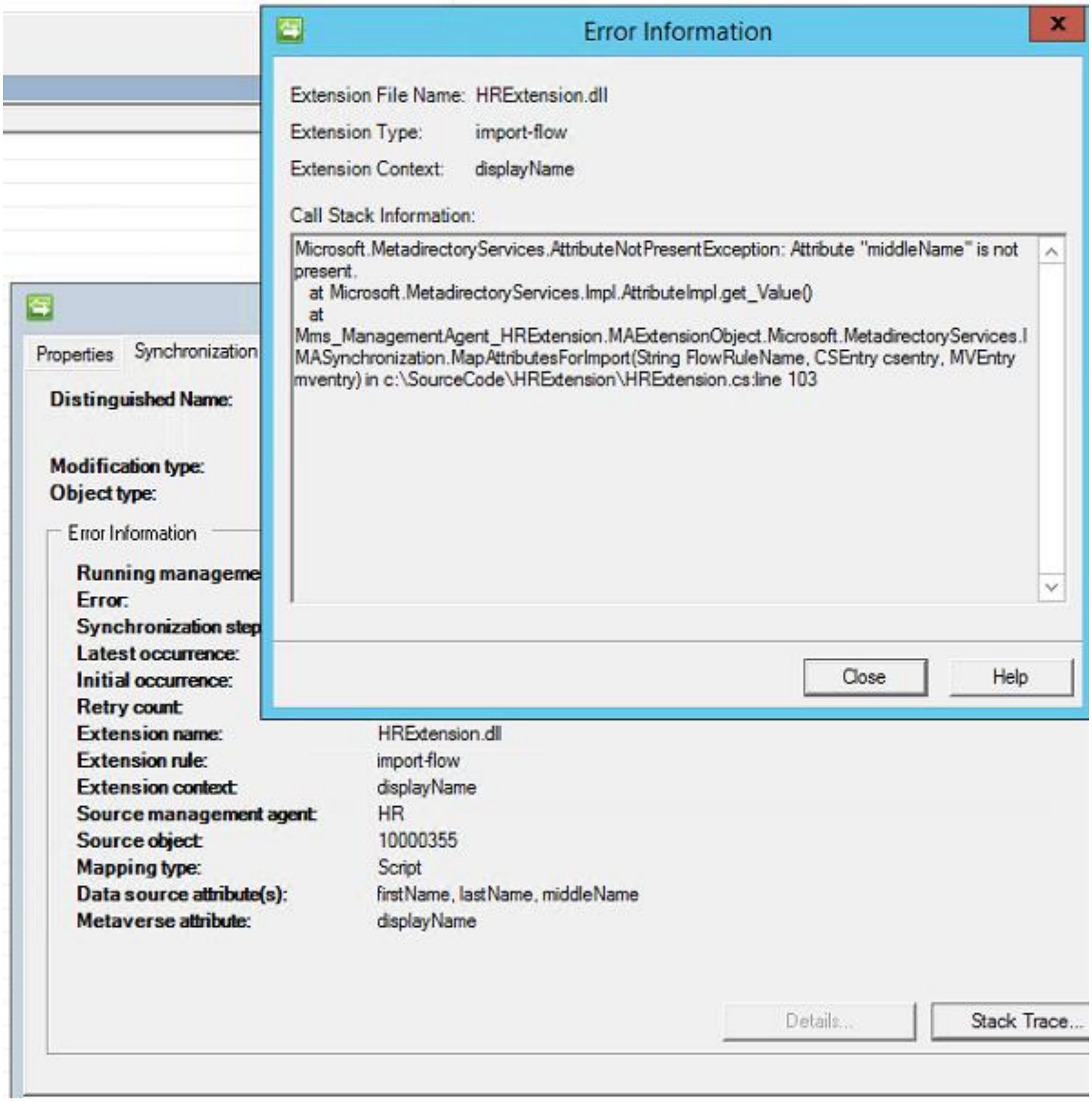
Metaverse Object Properties

Unique identifier (GUID): {C5EC0235-DD87-E511-80EB-00155D026225}

Display Name: Amber Adams

Object type: person

Distinguished Name	Management Agent	Join Method
fb1650f9-b728-4563-abe4-bf8f495b7e6a	MIM	provisioning-rules
10001018	Phone	provisioning-rules
10001018	HR	projection-rules
CN=AAdams,OU=TFC Users,DC=THEFINANCIALCOMPANY,DC=NET	AD	provisioning-rules



Error Information

Extension File Name: HRExtension.dll

Extension Type: import-flow

Extension Context: displayName

Call Stack Information:

```
Microsoft.MetadirectoryServices.AttributeNotPresentException: Attribute "middleName" is not present.
   at Microsoft.MetadirectoryServices.Impl.AttributeImpl.get_Value()
   at
Mms_ManagementAgent_HRExtension.MAExtensionObject.Microsoft.MetadirectoryServices.IMASynchronization.MapAttributesForImport(String FlowRuleName, CSEntry csentry, MVEntry mventry) in c:\SourceCode\HRExtension\HRExtension.cs:line 103
```

Distinguished Name:

Modification type:

Object type:

Error Information

Running manageme

Error:

Synchronization step

Latest occurrence:

Initial occurrence:

Retry count:

Extension name: HRExtension.dll

Extension rule: import-flow

Extension context: displayName

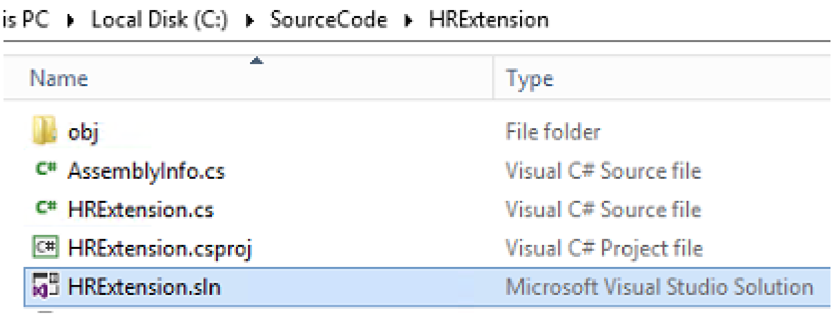
Source management agent: HR

Source object: 10000355

Mapping type: Script

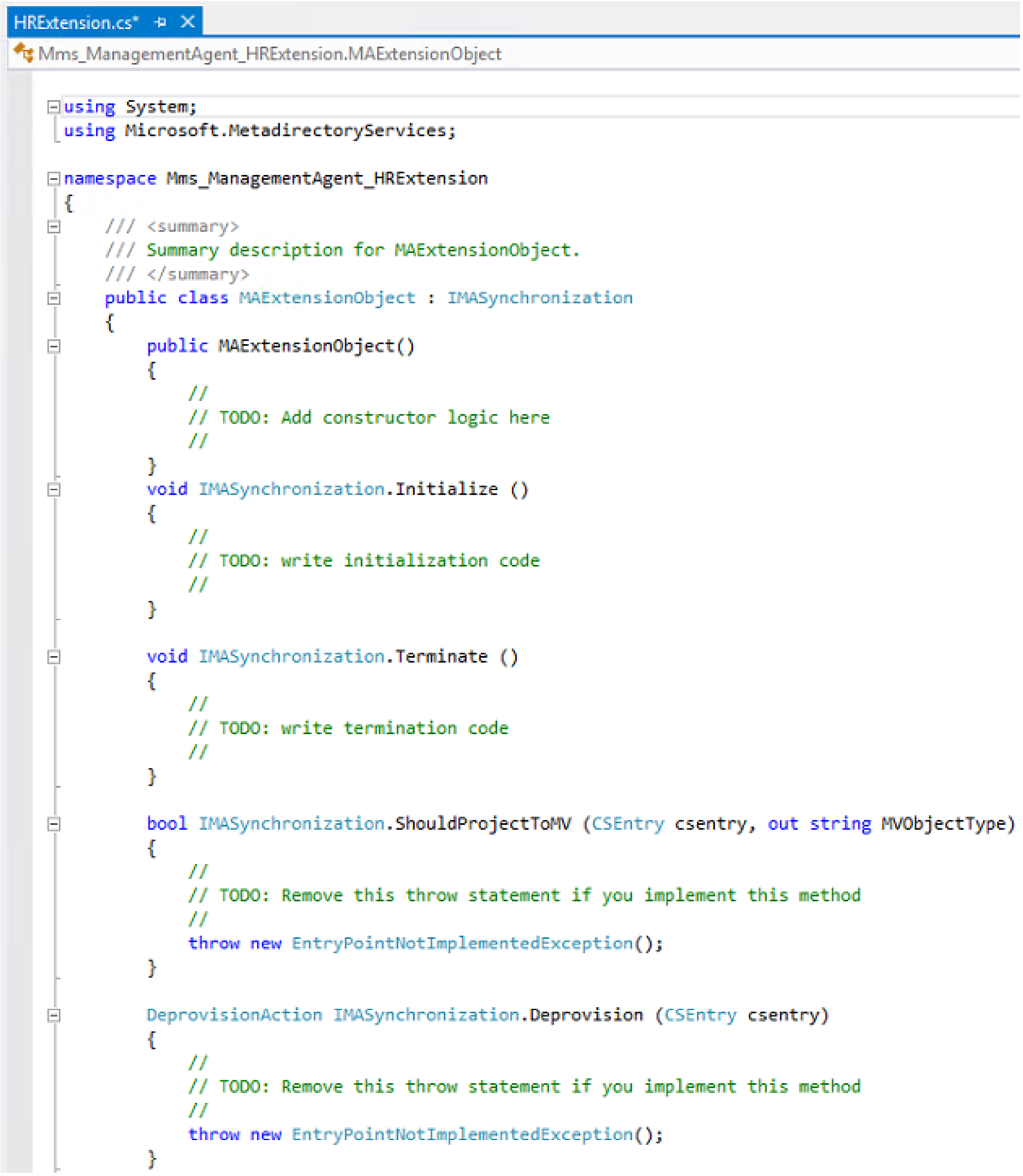
Data source attribute(s): firstName, lastName, middleName

Metaverse attribute: displayName

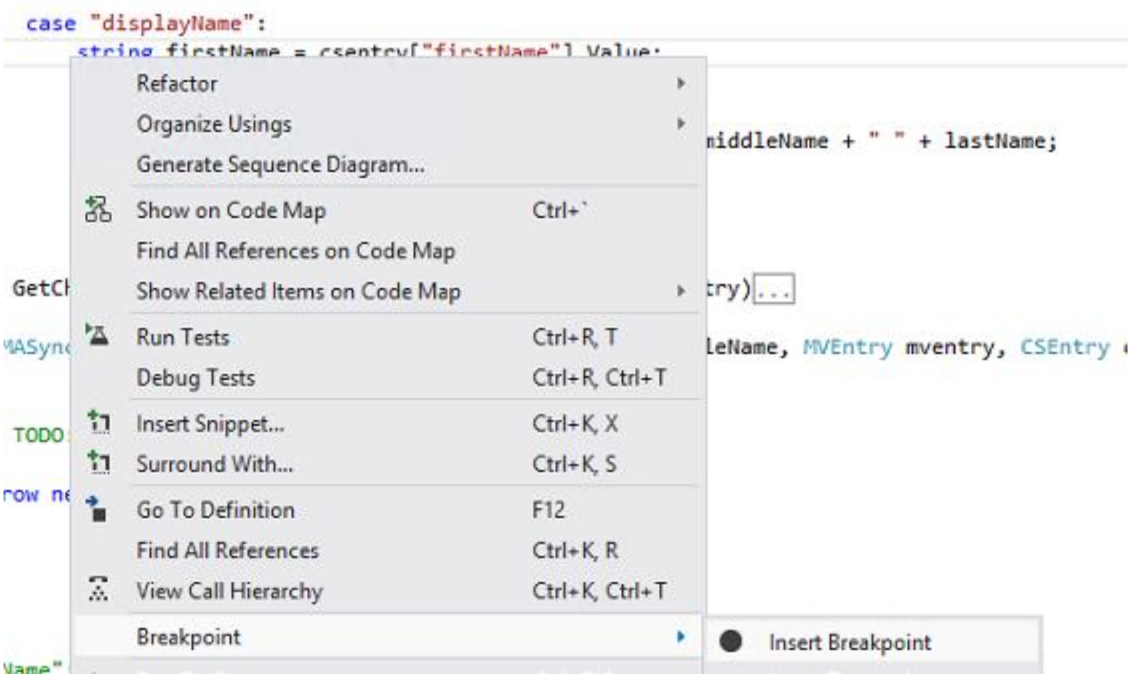


is PC ▸ Local Disk (C:) ▸ SourceCode ▸ HRExtension

Name	Type
obj	File folder
AssemblyInfo.cs	Visual C# Source file
HRExtension.cs	Visual C# Source file
HRExtension.csproj	Visual C# Project file
HRExtension.sln	Microsoft Visual Studio Solution

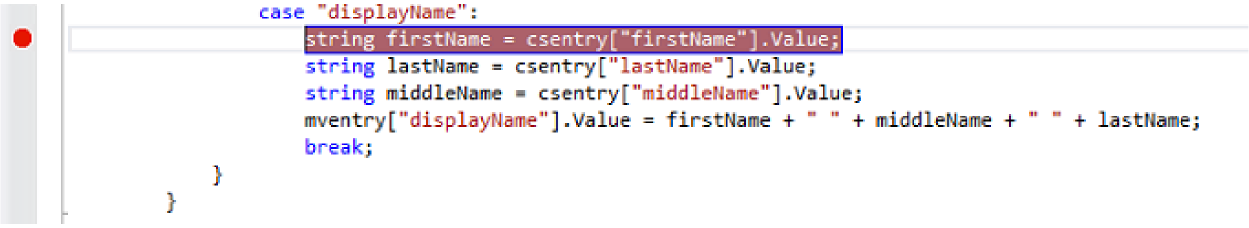


```
using System;
using Microsoft.MetadirectoryServices;

namespace Mms_ManagementAgent_HRExtension
{
    /// <summary>
    /// Summary description for MAExtensionObject.
    /// </summary>
    public class MAExtensionObject : IMASynchronization
    {
        public MAExtensionObject()
        {
            //
            // TODO: Add constructor logic here
            //
        }
        void IMASynchronization.Initialize ()
        {
            //
            // TODO: write initialization code
            //
        }

        void IMASynchronization.Terminate ()
        {
            //
            // TODO: write termination code
            //
        }

        bool IMASynchronization.ShouldProjectToMV (CSEntry csentry, out string MVObjectType)
        {
            //
            // TODO: Remove this throw statement if you implement this method
            //
            throw new EntryPointNotImplementedException();
        }

        DeprovisionAction IMASynchronization.Deprovision (CSEntry csentry)
        {
            //
            // TODO: Remove this throw statement if you implement this method
            //
            throw new EntryPointNotImplementedException();
        }
```

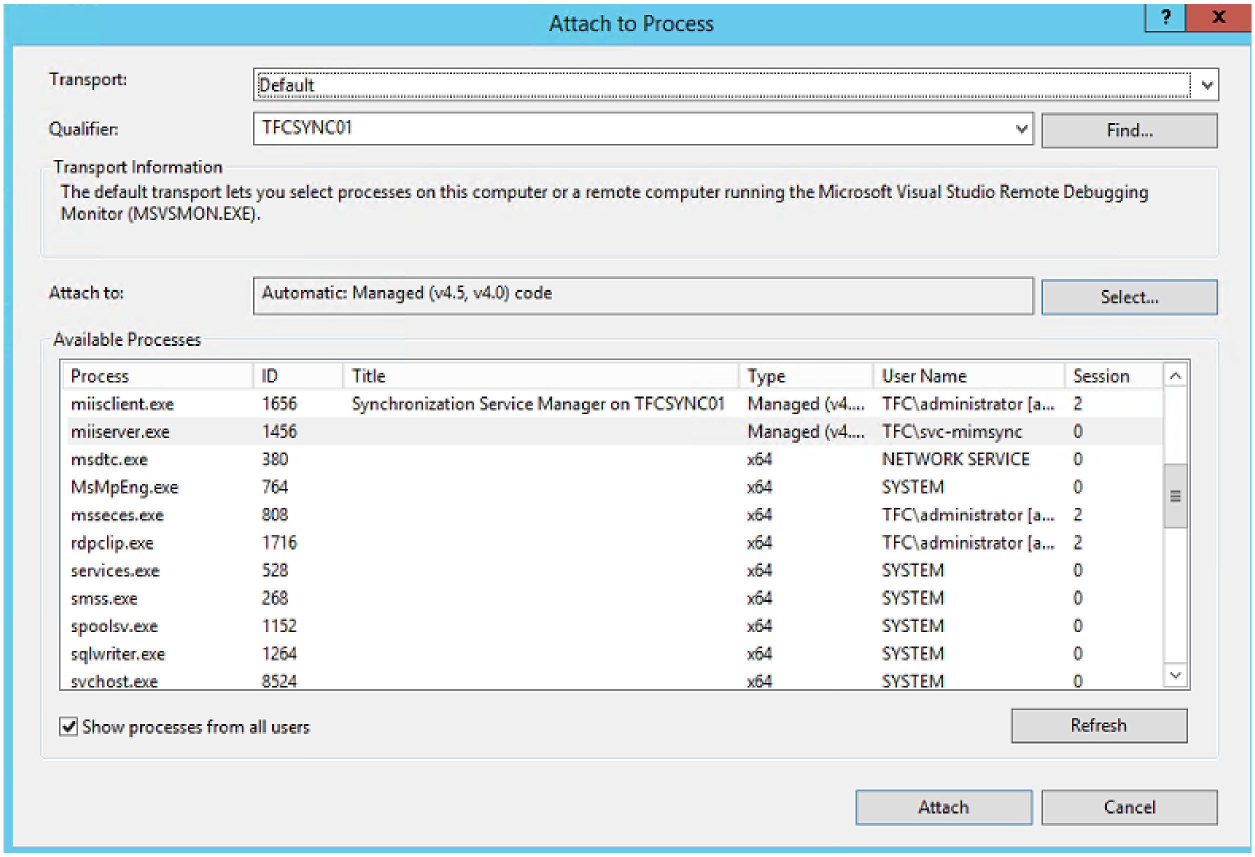


```
case "displayName":
    string firstName = csentry["firstName"].Value;
```

Refactor
Organize Usings
Generate Sequence Diagram...
Show on Code Map Ctrl+`
Find All References on Code Map
Show Related Items on Code Map
Run Tests Ctrl+R, T
Debug Tests Ctrl+R, Ctrl+T
Insert Snippet... Ctrl+K, X
Surround With... Ctrl+K, S
Go To Definition F12
Find All References Ctrl+K, R
View Call Hierarchy Ctrl+K, Ctrl+T
Breakpoint
Insert Breakpoint
iddleName + " " + lastName;
GetCl
try)
MASync
leName, MVEntry mventry, CSEntry
TODO
row ne
Name"



```
                case "displayName":
                    string firstName = csentry["firstName"].Value;
                    string lastName = csentry["lastName"].Value;
                    string middleName = csentry["middleName"].Value;
                    mventry["displayName"].Value = firstName + " " + middleName + " " + lastName;
                    break;
            }
        }
```



Attach to Process

Transport: Default

Qualifier: TFCSYNC01

Transport Information

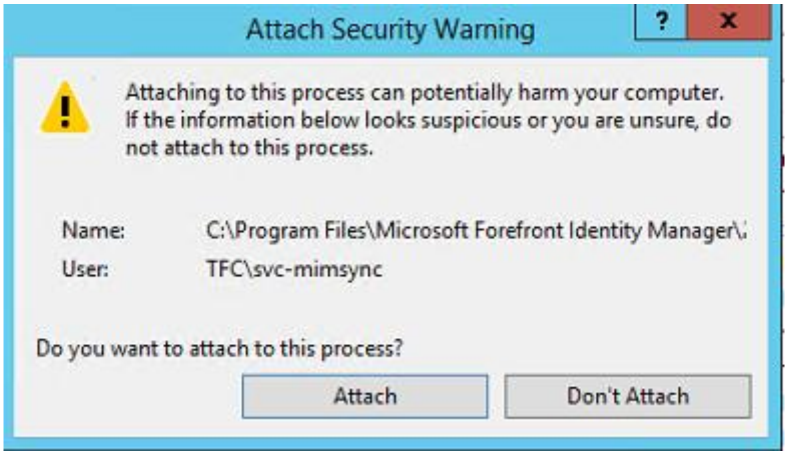
The default transport lets you select processes on this computer or a remote computer running the Microsoft Visual Studio Remote Debugging Monitor (MSVSMON.EXE).

Attach to: Automatic: Managed (v4.5, v4.0) code

Available Processes

Process	ID	Title	Type	User Name	Session
miisclient.exe	1656	Synchronization Service Manager on TFCSYNC01	Managed (v4....	TFC\administrator [a...	2
miiserver.exe	1456		Managed (v4....	TFC\svc-mimsync	0
msdtc.exe	380		x64	NETWORK SERVICE	0
MsMpEng.exe	764		x64	SYSTEM	0
msseces.exe	808		x64	TFC\administrator [a...	2
rdpclip.exe	1716		x64	TFC\administrator [a...	2
services.exe	528		x64	SYSTEM	0
smss.exe	268		x64	SYSTEM	0
spoolsv.exe	1152		x64	SYSTEM	0
sqlwriter.exe	1264		x64	SYSTEM	0
svchost.exe	8524		x64	SYSTEM	0

☑ Show processes from all users



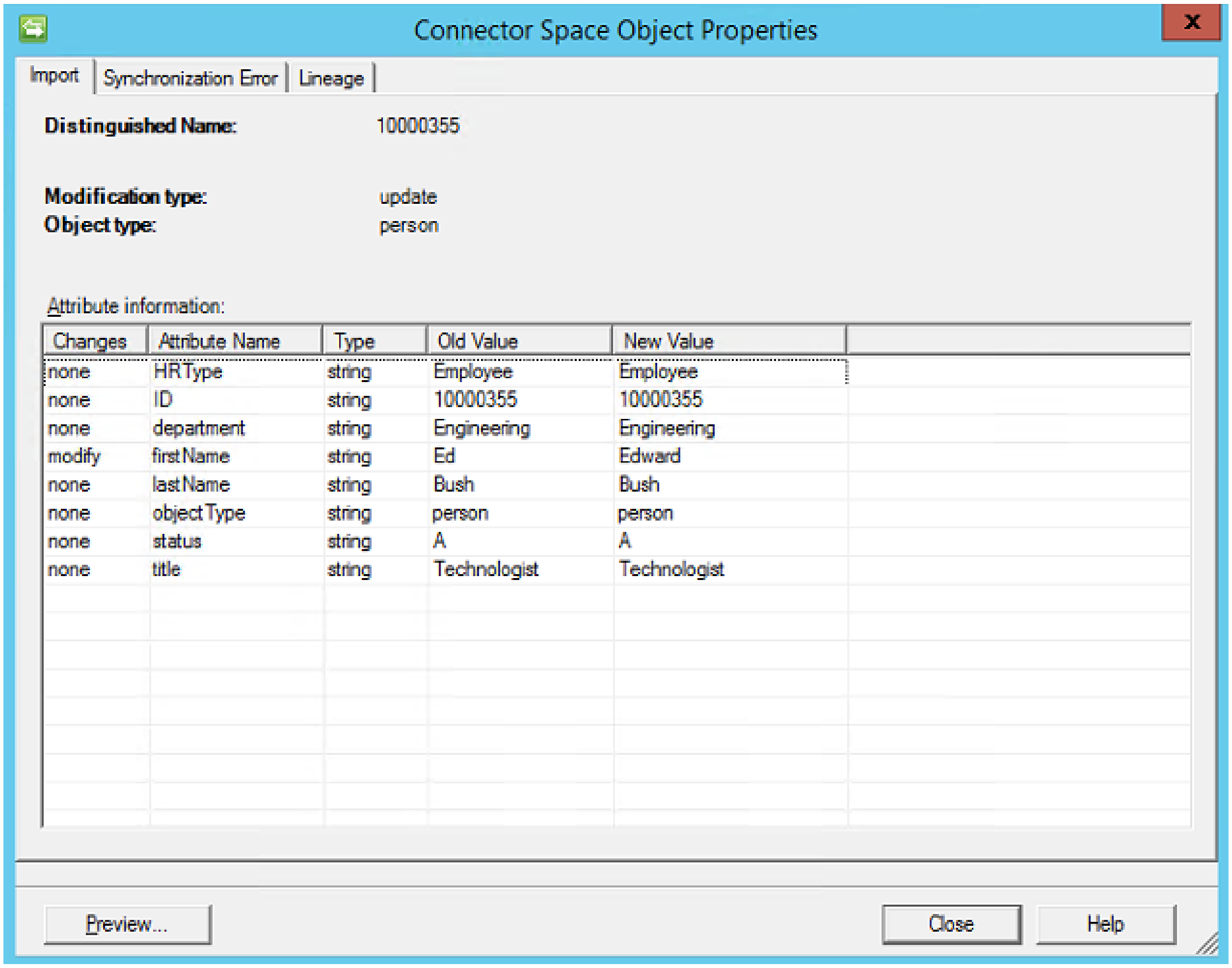
Attach Security Warning

Attaching to this process can potentially harm your computer. If the information below looks suspicious or you are unsure, do not attach to this process.

Name: C:\Program Files\Microsoft Forefront Identity Manager\

User: TFC\svc-mimsync

Do you want to attach to this process?

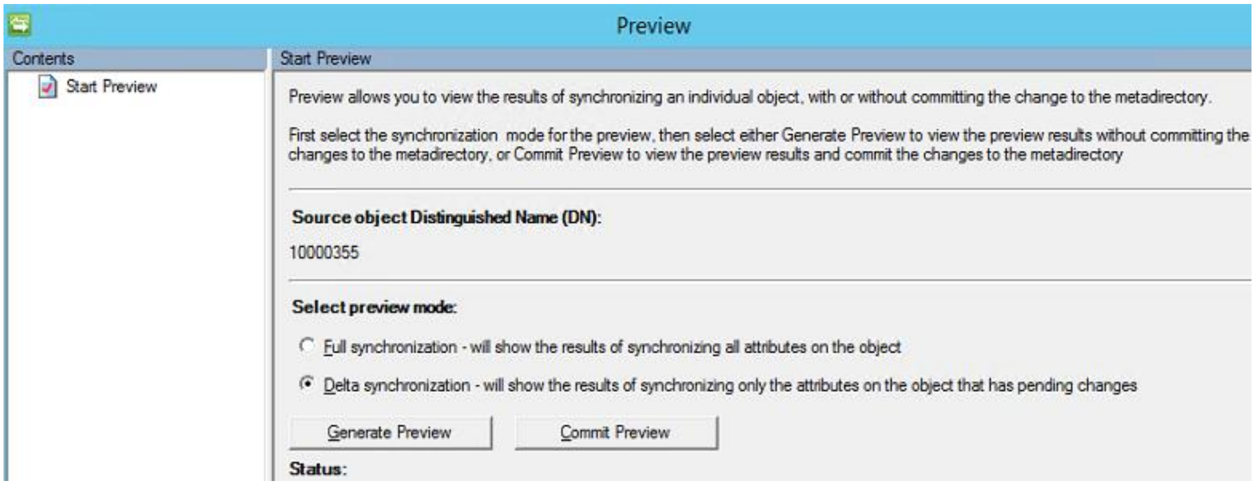


Distinguished Name: 10000355

Modification type: update
Object type: person

Attribute information:

Changes	Attribute Name	Type	Old Value	New Value
none	HRType	string	Employee	Employee
none	ID	string	10000355	10000355
none	department	string	Engineering	Engineering
modify	firstName	string	Ed	Edward
none	lastName	string	Bush	Bush
none	objectType	string	person	person
none	status	string	A	A
none	title	string	Technologist	Technologist



Preview allows you to view the results of synchronizing an individual object, with or without committing the change to the metadirectory.

First select the synchronization mode for the preview, then select either Generate Preview to view the preview results without committing the changes to the metadirectory, or Commit Preview to view the preview results and commit the changes to the metadirectory

Source object Distinguished Name (DN):

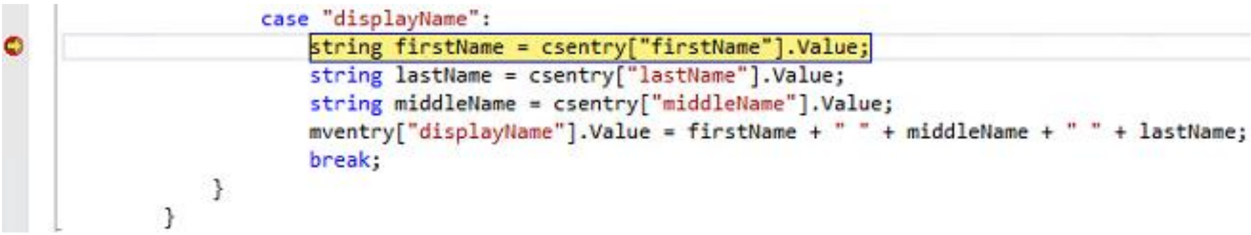
10000355

Select preview mode:

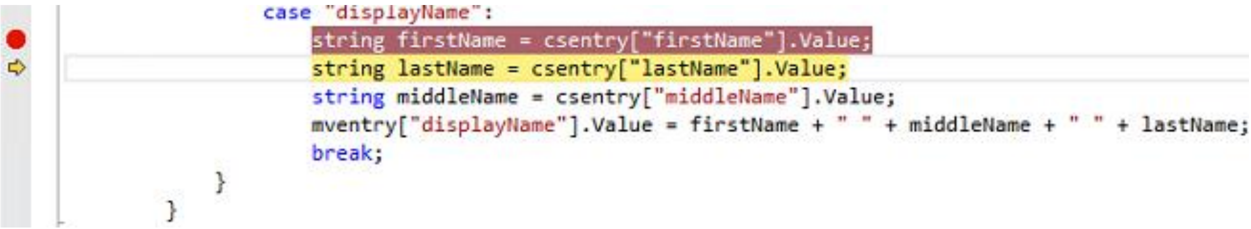
○ Full synchronization - will show the results of synchronizing all attributes on the object

● Delta synchronization - will show the results of synchronizing only the attributes on the object that has pending changes

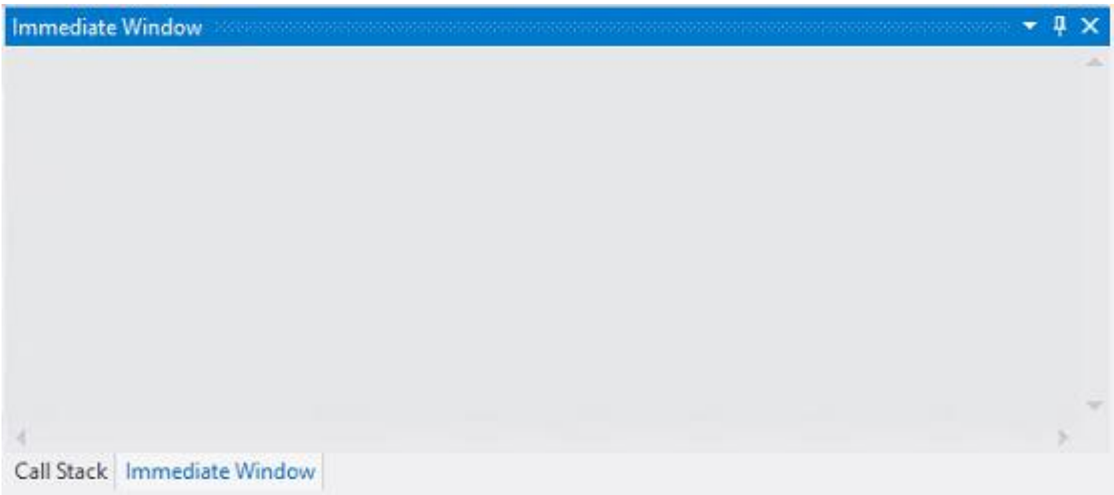
Status:

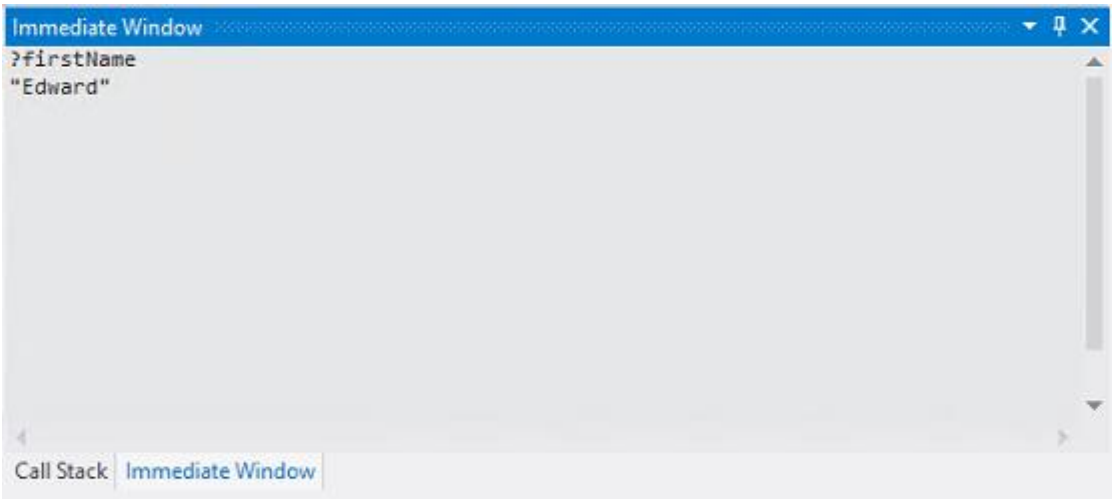


```
                    case "displayName":
                        string firstName = csentry["firstName"].Value;
                        string lastName = csentry["lastName"].Value;
                        string middleName = csentry["middleName"].Value;
                        mventry["displayName"].Value = firstName + " " + middleName + " " + lastName;
                        break;
                }
        }
```

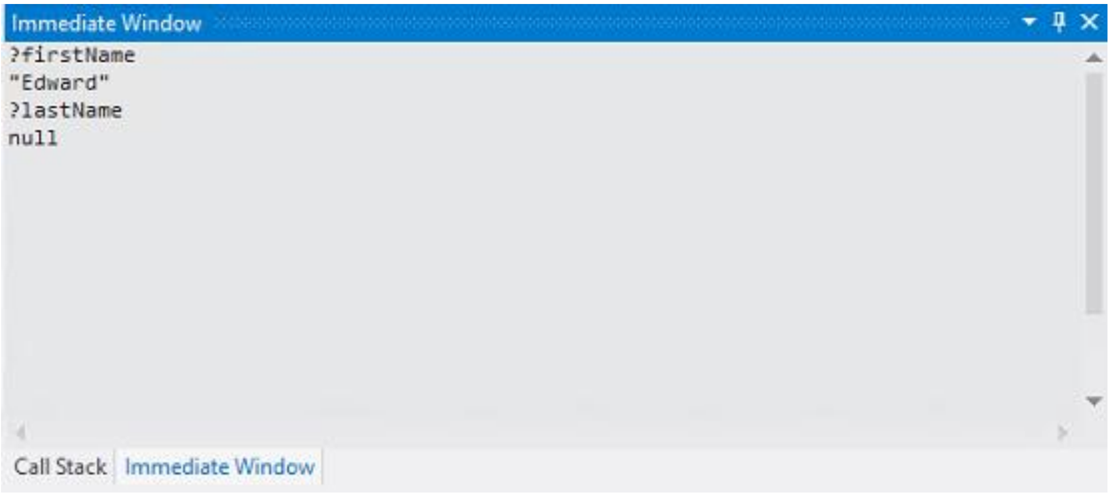


```
                    case "displayName":
                        string firstName = csentry["firstName"].Value;
                        string lastName = csentry["lastName"].Value;
                        string middleName = csentry["middleName"].Value;
                        mventry["displayName"].Value = firstName + " " + middleName + " " + lastName;
                        break;
                }
        }
```

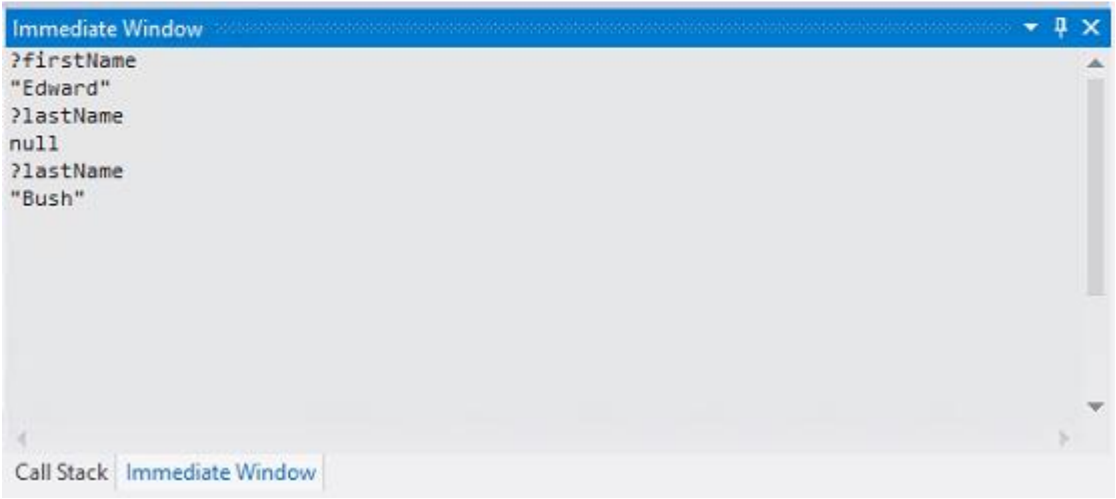




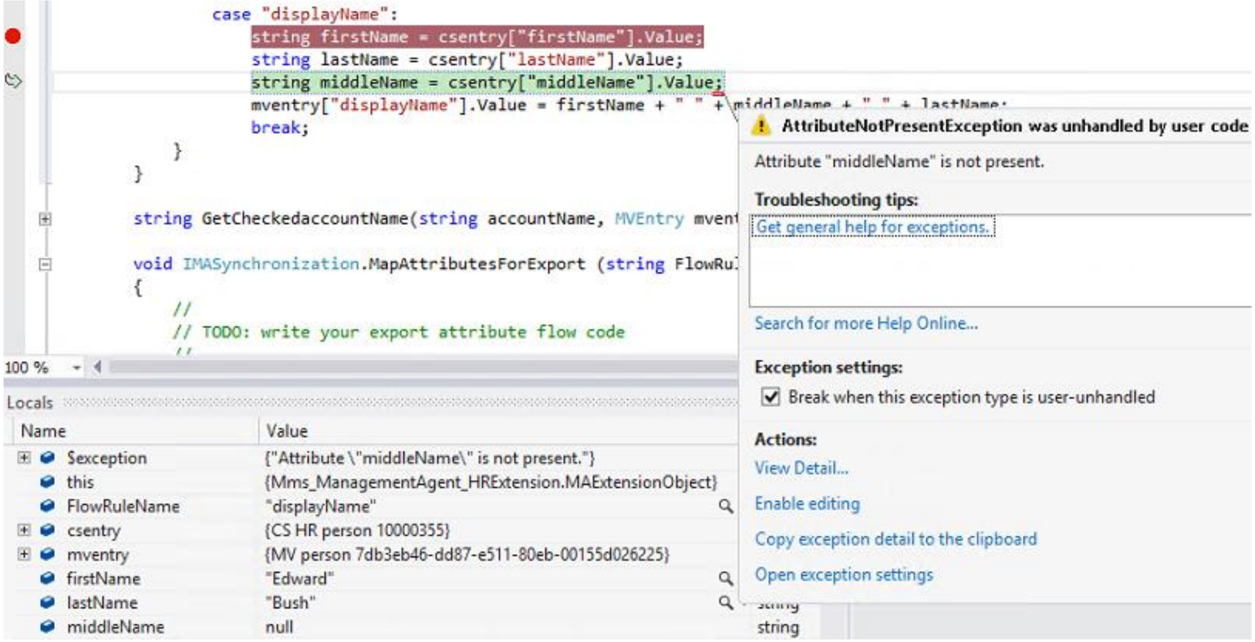
```
?firstName
"Edward"
```



```
?firstName
"Edward"
?lastName
null
```



```
?firstName
"Edward"
?lastName
null
?lastName
"Bush"
```



```
                case "displayName":
                    string firstName = csentry["firstName"].Value;
                    string lastName = csentry["lastName"].Value;
                    string middleName = csentry["middleName"].Value;
                    mventry["displayName"].Value = firstName + " " + middleName + " " + lastName;
                    break;

            }
        }

        string GetCheckedaccountName(string accountName, MVEntry mvent

        void IMASynchronization.MapAttributesForExport (string FlowRul
        {
            //
            // TODO: write your export attribute flow code
            //
```

AttributeNotPresentException was unhandled by user code

Attribute "middleName" is not present.

Troubleshooting tips:

Get general help for exceptions.

Search for more Help Online...

Exception settings:

☑ Break when this exception type is user-unhandled

Actions:

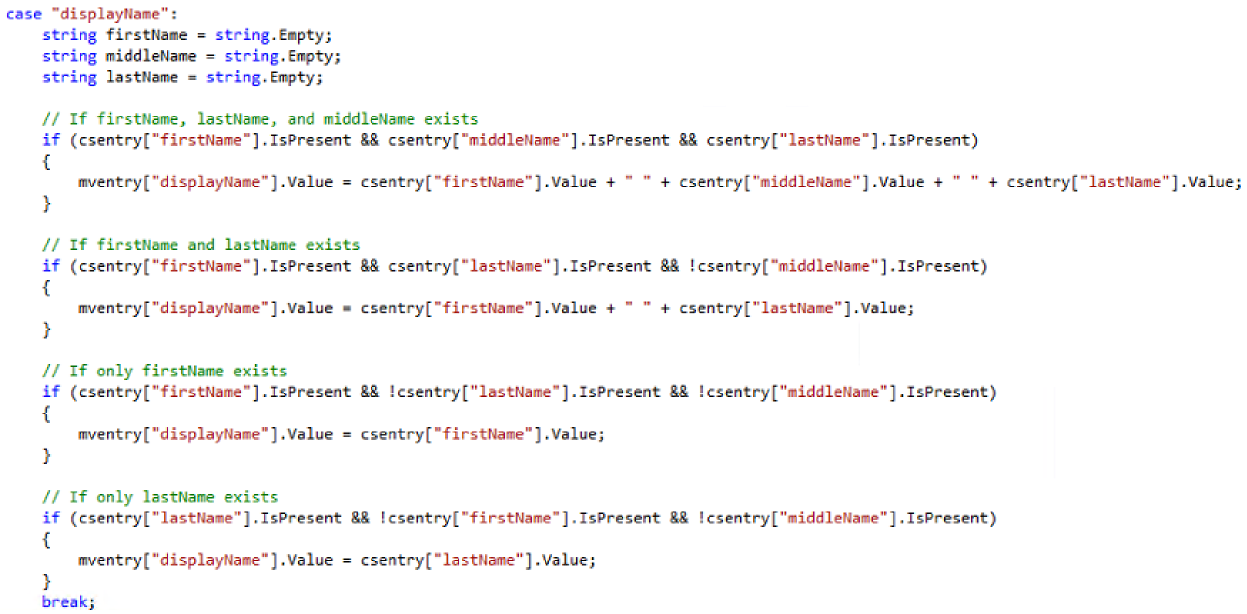
View Detail...

Enable editing

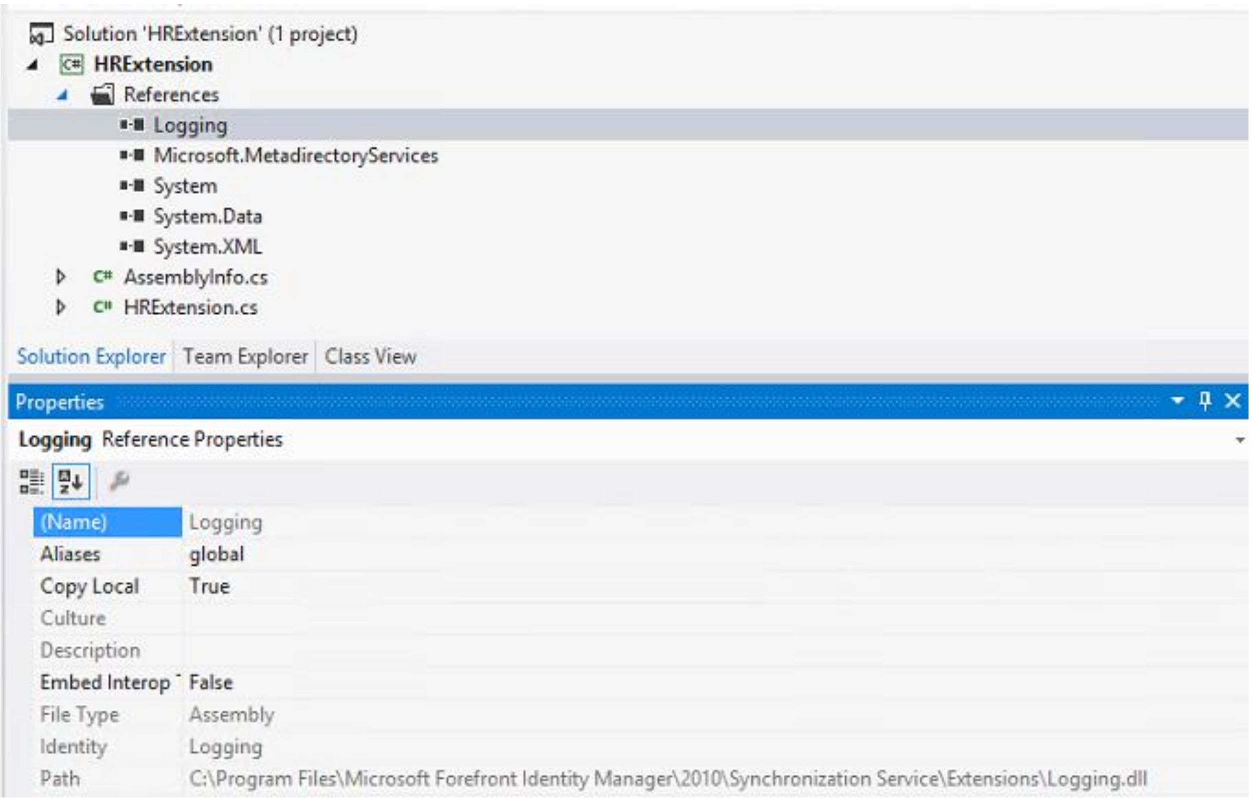
Copy exception detail to the clipboard

Open exception settings

Name	Value	
$exception	{"Attribute \"middleName\" is not present."}	
this	{Mms_ManagementAgent_HRExtension.MAExtensionObject}	
FlowRuleName	"displayName"	
csentry	{CS HR person 10000355}	
mventry	{MV person 7db3eb46-dd87-e511-80eb-00155d026225}	
firstName	"Edward"	
lastName	"Bush"	string
middleName	null	string

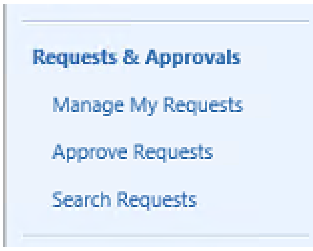


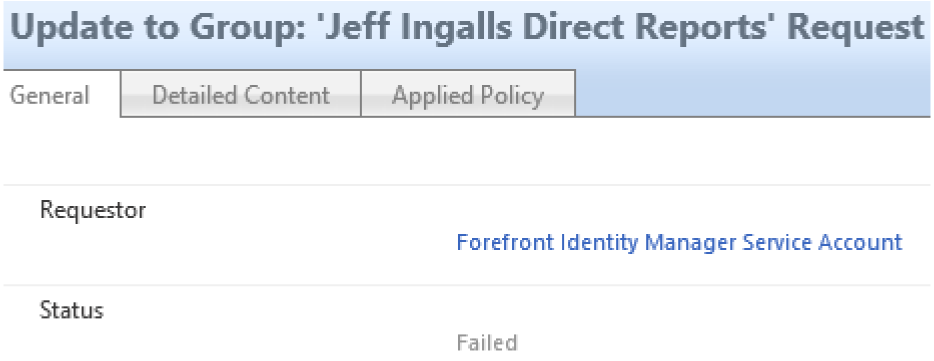
```
case "displayName":
    string firstName = string.Empty;
    string middleName = string.Empty;
    string lastName = string.Empty;

    // If firstName, lastName, and middleName exists
    if (csentry["firstName"].IsPresent && csentry["middleName"].IsPresent && csentry["lastName"].IsPresent)
    {
        mventry["displayName"].Value = csentry["firstName"].Value + " " + csentry["middleName"].Value + " " + csentry["lastName"].Value;
    }

    // If firstName and lastName exists
    if (csentry["firstName"].IsPresent && csentry["lastName"].IsPresent && !csentry["middleName"].IsPresent)
    {
        mventry["displayName"].Value = csentry["firstName"].Value + " " + csentry["lastName"].Value;
    }

    // If only firstName exists
    if (csentry["firstName"].IsPresent && !csentry["lastName"].IsPresent && !csentry["middleName"].IsPresent)
    {
        mventry["displayName"].Value = csentry["firstName"].Value;
    }

    // If only lastName exists
    if (csentry["lastName"].IsPresent && !csentry["firstName"].IsPresent && !csentry["middleName"].IsPresent)
    {
        mventry["displayName"].Value = csentry["lastName"].Value;
    }
    break;
```



Logging Reference Properties

(Name)	Logging
Aliases	global
Copy Local	True
Culture	
Description	
Embed Interop	False
File Type	Assembly
Identity	Logging
Path	C:\Program Files\Microsoft Forefront Identity Manager\2010\Synchronization Service\Extensions\Logging.dll





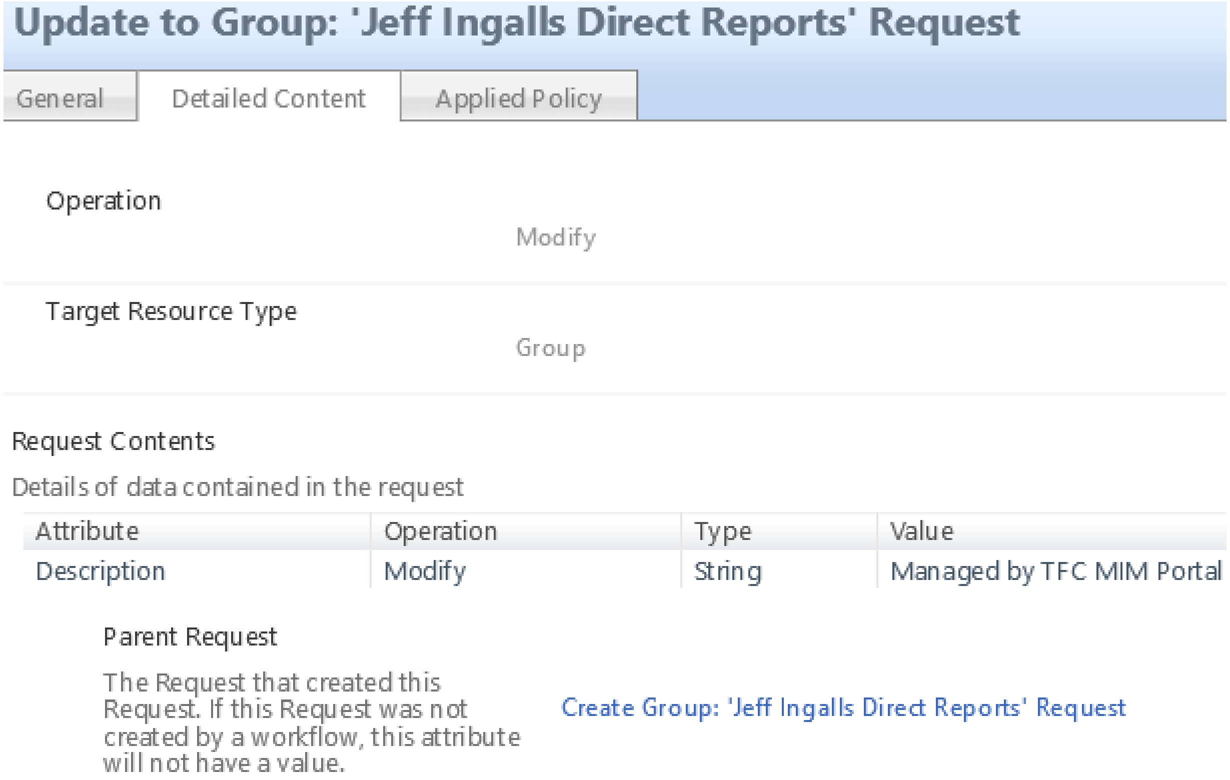
Update to Group: 'Jeff Ingalls Direct Reports' Request

Requestor

Forefront Identity Manager Service Account

Status

Failed



Update to Group: 'Jeff Ingalls Direct Reports' Request

Operation

Modify

Target Resource Type

Group

Request Contents

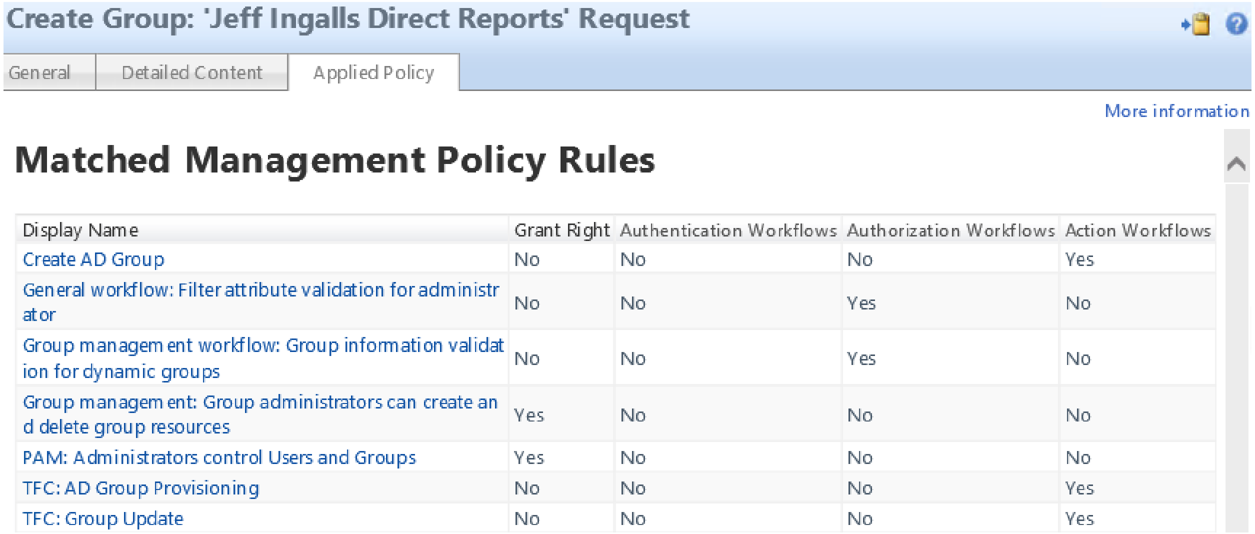
Details of data contained in the request

Attribute	Operation	Type	Value
Description	Modify	String	Managed by TFC MIM Portal

Parent Request

The Request that created this Request. If this Request was not created by a workflow, this attribute will not have a value.

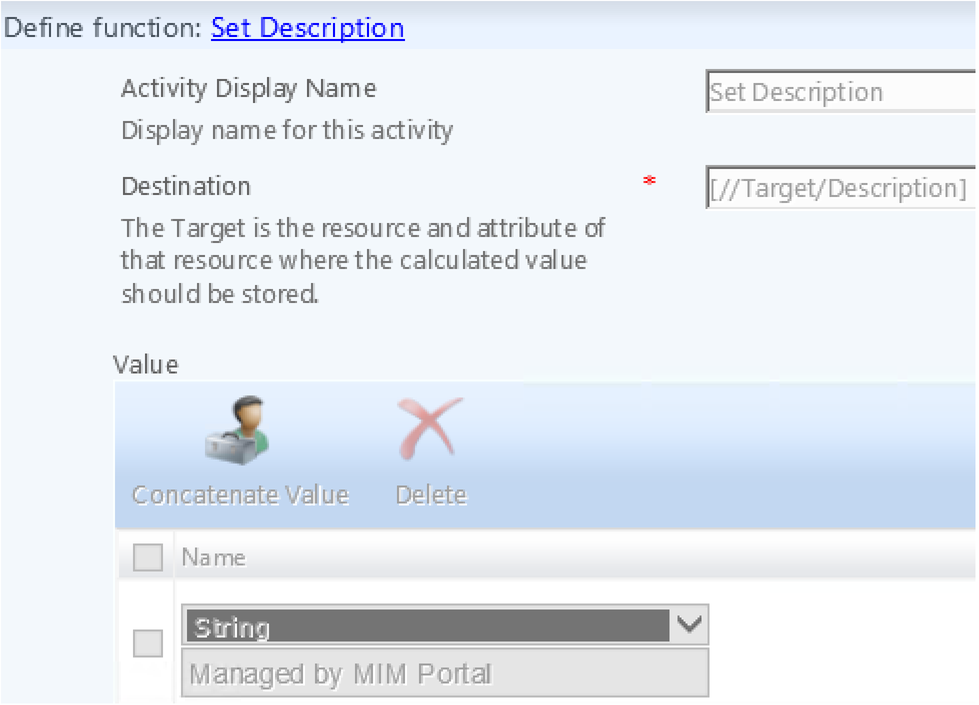
Create Group: 'Jeff Ingalls Direct Reports' Request



Create Group: 'Jeff Ingalls Direct Reports' Request

Matched Management Policy Rules

Display Name	Grant Right	Authentication Workflows	Authorization Workflows	Action Workflows
Create AD Group	No	No	No	Yes
General workflow: Filter attribute validation for administrator	No	No	Yes	No
Group management workflow: Group information validation for dynamic groups	No	No	Yes	No
Group management: Group administrators can create and delete group resources	Yes	No	No	No
PAM: Administrators control Users and Groups	Yes	No	No	No
TFC: AD Group Provisioning	No	No	No	Yes
TFC: Group Update	No	No	No	Yes



Define function: Set Description

Activity Display Name: Set Description

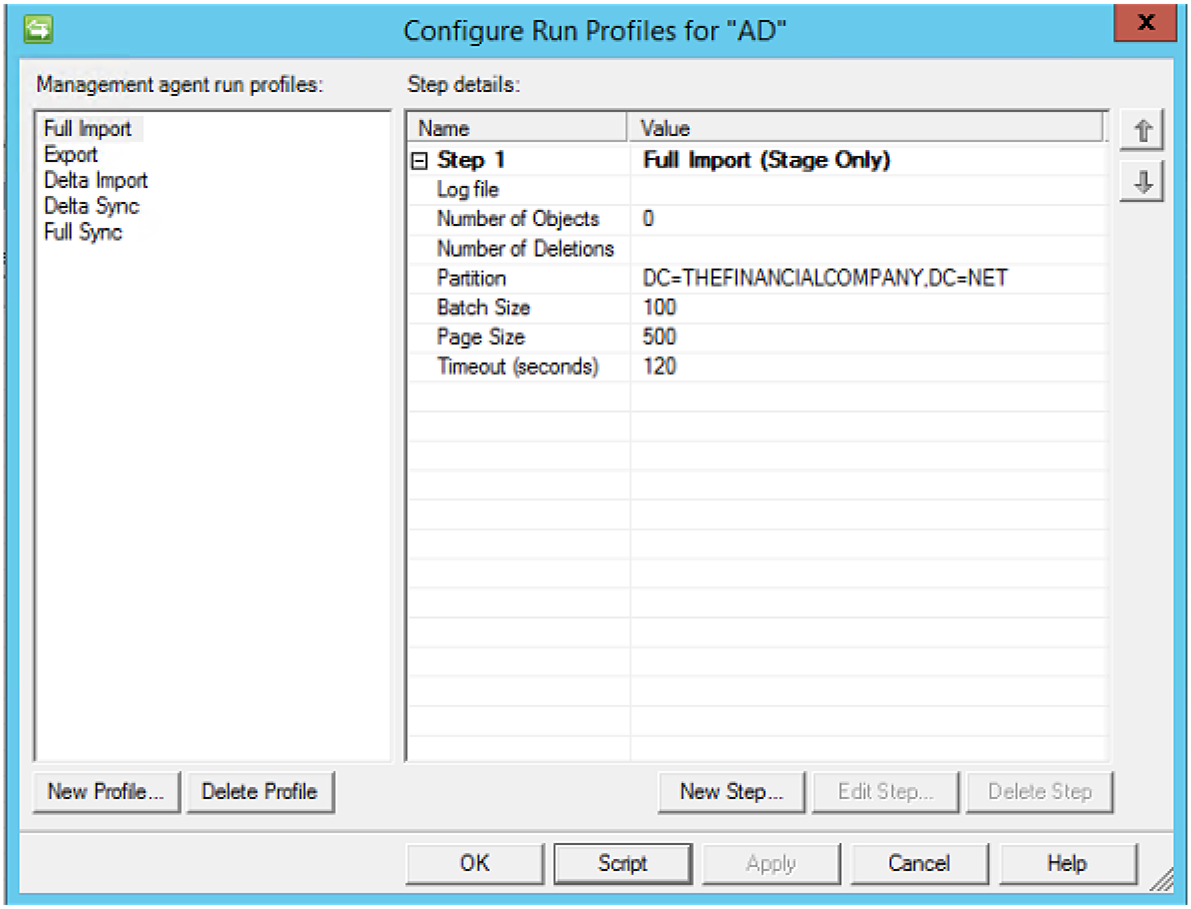
Display name for this activity

Destination * : [//Target/Description]

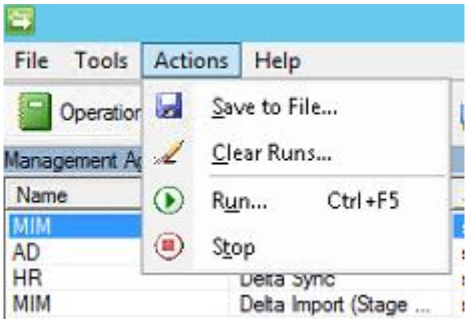
The Target is the resource and attribute of that resource where the calculated value should be stored.

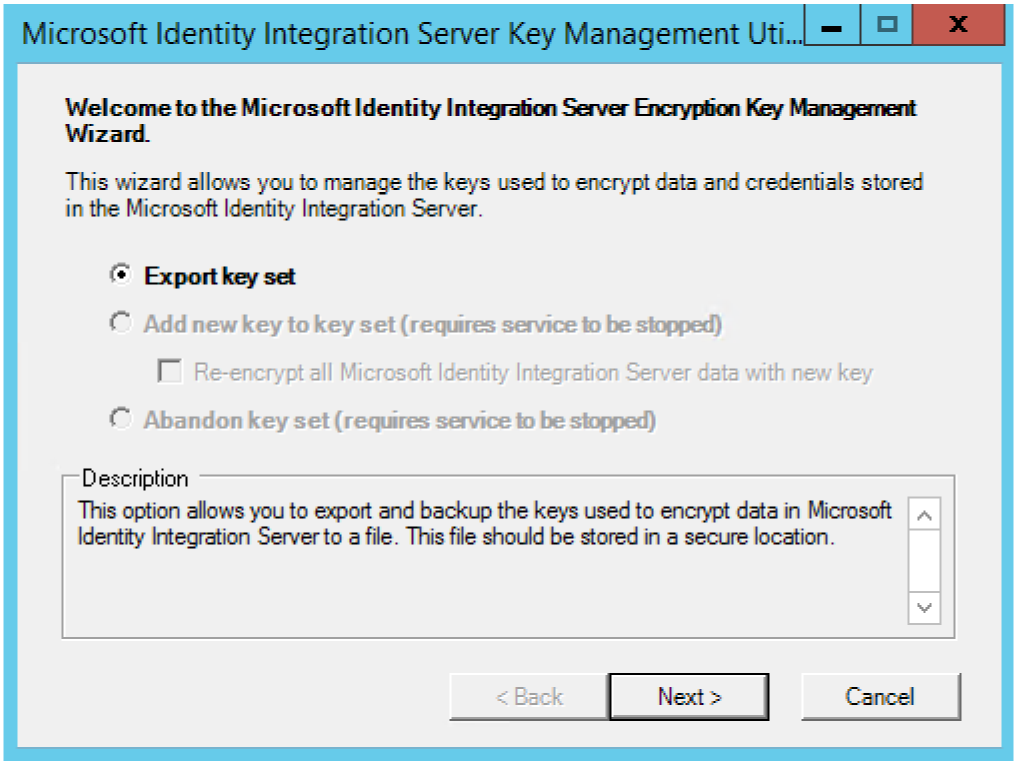
Value

□	Name
□	String Managed by MIM Portal



Name	Value
⊟ **Step 1**	**Full Import (Stage Only)**
Log file	
Number of Objects	0
Number of Deletions	
Partition	DC=THEFINANCIALCOMPANY,DC=NET
Batch Size	100
Page Size	500
Timeout (seconds)	120





Microsoft Identity Integration Server Key Management Uti...

Welcome to the Microsoft Identity Integration Server Encryption Key Management Wizard.

This wizard allows you to manage the keys used to encrypt data and credentials stored in the Microsoft Identity Integration Server.

● **Export key set**

○ **Add new key to key set (requires service to be stopped)**

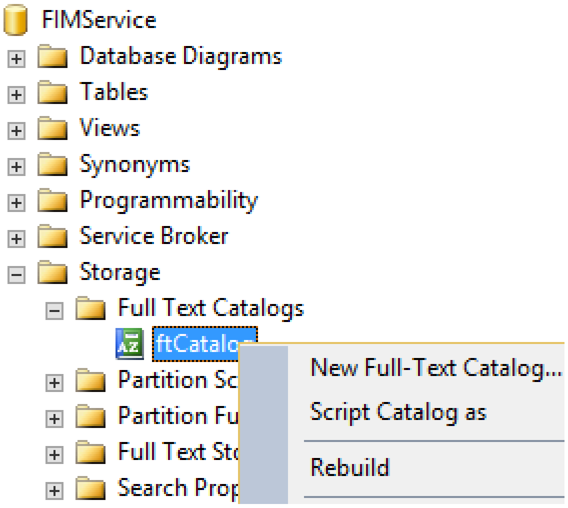
□ Re-encrypt all Microsoft Identity Integration Server data with new key

○ **Abandon key set (requires service to be stopped)**

Description

This option allows you to export and backup the keys used to encrypt data in Microsoft Identity Integration Server to a file. This file should be stored in a secure location.

< Back
Next >
Cancel



FIMService
Database Diagrams
Tables
Views
Synonyms
Programmability
Service Broker
Storage
Full Text Catalogs
ftCatalo
Partition Sc
Partition Fu
Full Text Sto
Search Prop
New Full-Text Catalog...
Script Catalog as
Rebuild