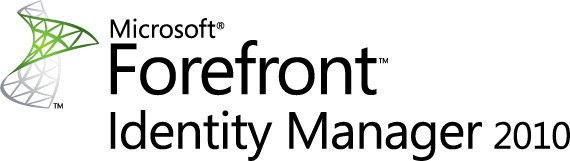
|  |  |  |
| --- | --- | --- |
| FIM-in-a-Box Prescriptive Guide | October 26  2011 | |
| This document provides a technical guide for implementing a standardized getting-started version of the Microsoft Forefront Identity Manager 2010 product. The document covers on core scenarios for setting up simple user and group management using out-of-the-box tools supplied with FIM 2010. The topics covered are declarative provisioning and de-provisioning of users and groups, user self-service management of passwords and policy based management. | | Forefront Identity Manager 2010 |



The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This guide is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2011 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Windows, Windows Server, SQL Server, Forefront Identity Manager, SharePoint, Visual Studio and Windows XP, Windows Vista, Windows 7 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.

Contents

[Document Overview 4](#_Toc307383639)

[Revision History 4](#_Toc307383640)

[December 23, 2010 | Version 0.8 4](#_Toc307383641)

[February 1, 2011 | Version 0.9 4](#_Toc307383642)

[March 22, 2011 | Version 1.0 4](#_Toc307383643)

[October 26, 2011 | Version 1.0 4](#_Toc307383644)

[Introduction to the FIM-in-a-Box guide 4](#_Toc307383645)

[Audience 4](#_Toc307383646)

[Benefits of Using This Guide 4](#_Toc307383647)

[Benefits for Customers Business Stakeholders/Decision Makers 5](#_Toc307383648)

[Benefits for Infrastructure Stakeholders/Decision Makers 5](#_Toc307383649)

[Benefits for Consultants or Partners 5](#_Toc307383650)

[Assumptions 5](#_Toc307383651)

[Feedback 5](#_Toc307383652)

[FIM-in-a-Box Prescriptive Guide 6](#_Toc307383653)

[Prerequisites 6](#_Toc307383654)

[Step-through guide 6](#_Toc307383655)

[How to use the steps 6](#_Toc307383656)

[Prepare the Active Directory 7](#_Toc307383657)

[Installing Forefront Identity Manager 2010 9](#_Toc307383658)

[Setting up the Synchronization Service 11](#_Toc307383659)

[Importing and configuring the Management Agents 11](#_Toc307383660)

[Configuring Run Profiles 12](#_Toc307383661)

[Configuring Deprovisioning 12](#_Toc307383662)

[Configuring the Metaverse Schema 13](#_Toc307383663)

[Configuring provisioning 14](#_Toc307383664)

[Loading existing users to the FIM Portal 14](#_Toc307383665)

[Configuring User Management through FIM portal 17](#_Toc307383666)

[Configuring Exchange mailbox creation for new users 23](#_Toc307383667)

[Importing the mail attribute 24](#_Toc307383668)

[Enabling the creation of Exchange 2003 mailbox for new users 25](#_Toc307383669)

[Enabling the creation of Exchange 2007 mailbox for new users 25](#_Toc307383670)

[Enabling the creation of Exchange 2010 mailbox for new users 26](#_Toc307383671)

[Configuring simple Group Management through FIM portal 27](#_Toc307383672)

[Configuring Password Reset through FIM portal 31](#_Toc307383673)

[Installing the FIM Add-ins and Extensions 33](#_Toc307383674)

[Appendix A – Find valid distinguishedName for Exchange mailbox 35](#_Toc307383675)

[Appendix B – Scheduling the Run Profiles 35](#_Toc307383676)

# Document Overview

This document is intended for technical consultants, including IT Architects, and IT Security Analysts and other technical implementers. Consultants are required to have prior knowledge of Microsoft Identity Integration Server 2003, Microsoft Identity Lifecycle Manager 2007, ILM “2” (old code name for Forefront Identity Manager), or Microsoft Forefront Identity Manager 2010. This document will provide the technical consultants with a guide for implementing a standard setup for management of users and groups and self-service password reset for users and as well as the policy-based management capabilities provided by Forefront Identity Manager 2010.

Besides this document a kit consisting of scripts and other configuration documents is also part of the solution. These scripts and documents are also subject to change and updates.

## Revision History

### December 23, 2010 | Version 0.8

Initial version ready for internal review and testing

### February 1, 2011 | Version 0.9

Version released for pilot training and subject for minor changes and bug fixes; findings from pilot will be included in document.

### March 22, 2011 | Version 1.0

Fixed bugs and minor discrepancies discovered in pilot.

### October 26, 2011 | Version 1.0

Fixed minor bugs and misspellings.

# Introduction to the FIM-in-a-Box guide

FIM-in-a-Box is guide to a low entry level solution into Identity Management and is meant as a way for customers to get started with a packaged solution. The packaged solution will include basic features and will not be a complete solution, however, will provide a solid platform to build on.

## Audience

This document is solely intended for IT planners, Systems Architects, Technology decision-makers, consultants, infrastructure planners at Microsoft Partners who plan to deploy FIM 2010 as a packaged solution under the FIM-in-a-Box solution offering.

## Benefits of Using This Guide

By using this guide the FIM 2010 setup that is delivered to customers will have a reference architecture that will support future extension of the solution at the customer. Also, it enable the customer to get an entry level Identity Management architecture introduced in their business in a fixed-price, cost-effective manner.

### Benefits for Customers Business Stakeholders/Decision Makers

* Most cost-effective design solution for an implementation. The fixed setup eliminates over-architecting and overspending by precisely matching the technology solution to the basic business needs.
* Alignment between the business and IT from the beginning of the design process to the end.

### Benefits for Infrastructure Stakeholders/Decision Makers

* Authoritative guidance. Microsoft and other partners can more easily support a standard setup.
* High integrity design criteria that includes product limitations.
* A foundation on which to add functionality
* Proportionate system and network availability to meet business requirements. Infrastructure that is sized appropriately to meet business requirements.

### Benefits for Consultants or Partners

* Attach business value to Windows 7 and Active Directory upgrade projects.
* ISVs can add modules and expect a standard platform to integrate into
* Rapid readiness for consulting engagements.
* Planning and design template to standardize design and peer reviews.

## Assumptions

To limit the scope of material in this guide, the following assumptions have been made:

* The decision to implement FIM 2010 has already been made. This guide does not address the business or technical decisions involved in choosing an identity management platform. Please refer to relevant sales material for this.
* This design is for use in a production environment. It is expected that a test environment will also be created to mirror the production environment‘s configuration. Large implementations will benefit from having separate development and test environments in addition to the production environment.
* The reader and implementer are comfortable with common technologies and networking components including Active Directory® Domain Services (AD DS), Microsoft SQL Server®, Windows PowerShell and Windows SharePoint® Services. This guide does not attempt to educate the reader on the features and capabilities of these or other Microsoft products. The product documentation covers that information.

## Feedback

Please direct questions and comments about this guide to Søren Granfeldt (sg@inceptio.dk).

# FIM-in-a-Box Prescriptive Guide

This guide describes the process of implementing a standard feature set of the Forefront Identity Manager (FIM) infrastructure with a set of features that are supported out of the box by the product. The guide addresses the following fundamental tasks:

* Configuring FIM 2010 for automated simple user management, including creating new users in Active Directory
* Configuring FIM 2010 for automated simple management of Active Directory security and distribution groups
* Enabling users for Self Service Password Reset
* Configuring the infrastructure for the FIM Synchronization Service and FIM Service.

Following the instructions in this guide will result in a setup that is configured, and appropriately prepared to deliver the stated business benefits, while also considering the existing infrastructure that the setup will interact with.

## Prerequisites

The following prerequisites are expected to be in-place before proceeding with the configuration of Forefront Identity Manager 2010 for the FIM-in-a-box setup:

1. An Active Directory is in place with a minimum functionality of Windows 2003 Forest Functionality.
2. FIM supports a variety of deployment topologies. Each of the main components may be installed separately or in combination on individual servers. This guide assumes that Forefront Identity Manager 2010 is installed on Windows Server 2008 R2 Standard or Enterprise and that the Microsoft SQL Server 2008 server that is used as repository for Synchronization Service and FIM Service resides on the same server Forefront Identity Manager 2010 installation.
3. Optionally, Exchange 2003, Exchange 2007 or Exchange 2010 is supported for creating mailboxes.
4. All PowerShell scripts should be run using an administrative PowerShell prompt (Run As Administrator)

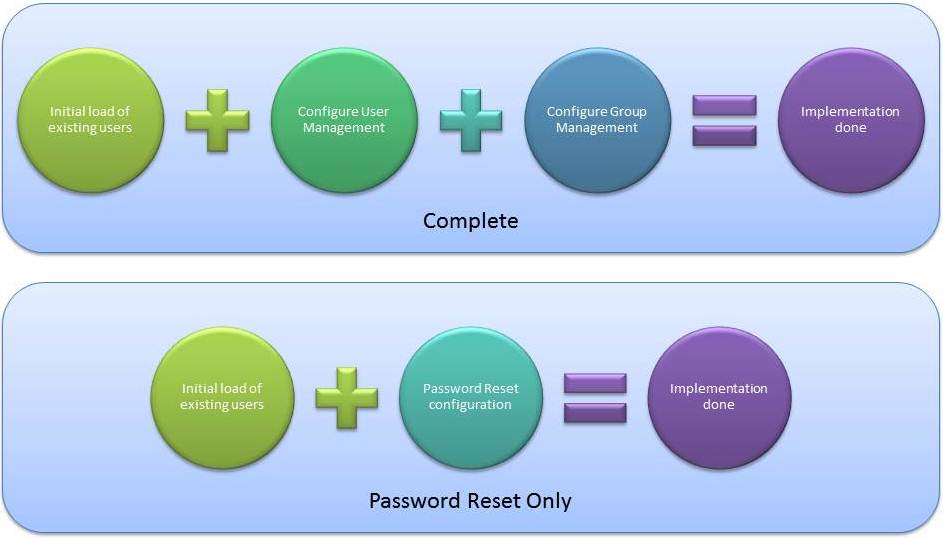
# Step-through guide

The following steps need to be completed in the order written since some of the steps have dependencies on the other task being completed successfully.

## How to use the steps

There are two possible tracks to take when doing the implementation; these are –

1. Full Implementation (user and group management and password reset functionality)
2. Password Reset Only



1. To complete either track a number of steps from different sections of this guide should be completed. No matter which track was selected, these first common sections to complete are:Optional, but recommended: Appendix B – Scheduling the Run Profiles
2. Prepare the Active Directory
3. Installing Forefront Identity Manager 2010
4. Setting up the Synchronization Service
5. Configuring Run Profiles
6. Configuring Deprovisioning
7. Configuring provisioning
8. Loading existing users to the FIM Portal

To do the full implementation track, you should then continue to complete the steps in the following sections in this order:

1. Configuring User Management through FIM portal
2. Optional: Configuring Exchange mailbox creation for new users
3. Configuring simple Group Management through FIM portal
4. Complete the steps in the Password Reset track
5. Optional, but recommended: Appendix B – Scheduling the Run Profiles
6. Optional, but recommended: Appendix B – Scheduling the Run Profiles

To do the Password Reset track, you should then complete the steps in the following sections in this order:

1. Configuring Password Reset through FIM portal
2. Optional, but recommended: Appendix B – Scheduling the Run Profiles

## Prepare the Active Directory

The following steps should be completed prior to continuing:

1. Create an Organizational Unit (OU) in the root of the domain called “FIM Service Accounts”
2. If FIM 2010 has already been installed, move all FIM 2010-related service accounts to this organizational unit created in step 1

The following usernames and group names will be used throughout the guide. If you have already installed FIM 2010, use the table below to map your own service account names to the account names used in this guide.

Note: You can use the script ‘Create-OUs.ps1’ to create the default organizational units and the script ‘Create-InstallationUsersAndGroups.ps1’ included in the kit to create the users from the table below. Please change the default passwords to more secure values after creating the users and set ‘Password Never Expires’ for the relevant accounts. If the initial password in the script ‘Create-InstallationUsersAndGroups.ps1’ does not meet customer’s password requirements, please adjust script accordingly.

Table 1 Service Accounts

|  |  |
| --- | --- |
| Account Name | Function |
| SVC-FIM-Service | A dedicated domain service account to run the FIM Service component. To be able to use the Office Outlook integration feature, an Exchange Server mailbox must also be created for this account. To use the FIM Add-in for Outlook feature, you must set up the domain service e-mail account on a server that hosts Exchange Server 2007 or Exchange Server 2010. If the customer plans to use SMTP for notifications rather than Exchange Server, ensure that this service account has the required permissions on the SMTP gateway. This account also is used to send e-mail notifications from FIM 2010. This account should not be granted local administrator permissions. |
| SVC-FIM-MA | Domain account that is reserved for the exclusive use of the FIM Service management agent (FIM MA) used by the FIM Synchronization Service to communicate with the FIM Service. The FIM Service has to know the name of the account that the FIM MA is using so that during setup it can give the account the required permissions. This account should not be a local administrator account. |
| SVC-FIM-Sync | A service account to run the FIM Synchronization Service. This service account must be a domain account. This account should not be a local administrator account. |
| SVC-FIM-SPAppPool | It is recommended that you create a service account for SharePoint to use and use Kerberos delegation. Please refer to installation guide for more on this. |
| SVC-FIM-ADMA | Domain account that is reserved for the exclusive use of the Active Directory Management Agent that is used for creating, modifying and deleting users and groups in the Active Directory that FIM manages.  This account should be given exactly the required permissions in the relevant part of the customers Active Directory. Delegation of these user rights is out of scope for this guide. Though not recommended, it’s possible to make this user a member of Domain Admins for it to have the necessary permissions to act on objects. |

Table 2 FIM Permission Groups

|  |  |
| --- | --- |
| Group Name | Function |
| FIMSyncAdmins | Members of this group have full access to everything in Synchronization Service Manager. |
| FIMSyncBrowse | Members of this group have permission to gather information about a user's lineage when resetting passwords by using Windows Management Instrumentation (WMI) queries. |
| FIMSyncJoiners | Members of this group have access to Joiner and Metaverse Search in Synchronization Service Manager. FIMSyncJoiners can join or project disconnectors by using Joiner, and they can use Metaverse Search to view object properties and disconnect objects from the metaverse. |
| FIMSyncOperators | Members of this group have access to Operations in the Synchronization Service Manager only. FIMSyncOperators can run management agents, view synchronization statistics for each run, and save the run histories to a file. Members of the FIMSyncOperators group must also be members of the FIMSyncBrowse group to open links in synchronization statistics. |
| FIMSyncPasswordSet | Members of this group have permission to perform all operations by using the password management interfaces with WMI. Members in this group inherit all FIMSyncBrowse permissions. |

By default the permission groups for FIM are created as computer local groups. If you want to have domain groups the groups should be created before the installation. It is recommended to use domain groups, mainly if you later want to extend the solution or use a SQL cluster. Please consult the Forefront Identity Manager 2010 installation guide on TechNet for more information on this. The installation guide can be found at <http://technet.microsoft.com/en-us/library/ee534909(WS.10).aspx>.

If the customer has Exchange 2007 or later implemented, please make sure to mailbox-enable the account SVC-FIM-Service account using the standard Exchange administrative tools. See installation guide for more information on this.

Note: During installation and setup, FIM adds the user account that is running the installation to the FIMSyncAdmins group, but only if the FIMSyncAdmins group is also created during setup. If you specify a preexisting group during setup, the user account that is running the installation will not be added to the preexisting group.

## Installing Forefront Identity Manager 2010

This section describes how to install Forefront Identity Manager 2010 software in a manner that is compliant with the FIM-in-a-Box setup.

The following conditions should be met for the installation in order to be able to able to follow the steps in this guide:

1. All FIM 2010 components should be installed on one server, including the Microsoft SQL Server 2008 software needed for both Synchronization Service and the FIM Service.
2. The operating system should be Windows Server 2008 R2 64-bit version

This guide does not hold a complete description on how to install Forefront Identity Manager 2010. For a step-through guide on how to do the product installation, please refer to the online TechNet installation guide that can be found at <http://technet.microsoft.com/en-us/library/ee621261(WS.10).aspx>.

To install FIM 2010 on the server, please follow the steps in the TechNet guide files included in this kit in the Guide folder –

1. 01 - FIM 2010 - Installation Guide
2. 02 - FIM 2010 - Hardware and Software Requirements
3. 03 - FIM 2010 - Before You Begin
4. 04 - FIM 2010 - Installing the FIM 2010 Server Components
5. Optional 05 - FIM 2010 - Password Reset Deployment Guide
6. Optional 06 - FIM 2010 - Installing the FIM Add-ins and Extensions
7. Optional 07 - FIM 2010 - Post-Installation and Configuration Guide

You should start the installation from ‘03 - FIM 2010 - Before You Begin’ and continue through ‘04 - FIM 2010 - Installing the FIM 2010 Server Components’. Please make sure that SharePoint is properly configured before installation the FIM Portal, otherwise you will have trouble installing the FIM Service and FIM Portal correctly.

You should also install Active Directory Domain Services tools on the FIM box to better be able to complete the setup –

1. From a command prompt run the following command
   1. ServerManagerCMD –install RSAT-ADDS
2. If the server wants to reboot after running the above command, please do so.

The following settings deviate from the installation guide, please adjust accordingly –

*(Nothing in current version)*

During installation, please use the service account names and the group names specified above in order to be fully compliant with this guide. The group names should be used and prefixed with the NetBIOS domain name when installing the Synchronization Service. However, if other account names or group names have been used, either by customer request or for some other reason, please map the account names and group names above to the ones used in the customer’s installation.

Be aware that the account that you use for installing Forefront Identity Manager 2010 is the only account that by default will have permission to use the portal. You’ll have to import additional users into the portal and add these to the ‘Administrators’ set, if you want other account to be able to manage the FIM portal.

After installing FIM 2010, please verify the installation by checking the event logs on the server and attend to any errors that may indicate a problem with the SQL server or FIM 2010 installation.

Also, it is good practice to make sure that post-installation configuration is done, in order to make sure that the server runs smoothly. Please consult the ‘Post-Installation and Configuration Guide’ (<http://technet.microsoft.com/en-us/library/ff608272(WS.10).aspx)> on Microsoft TechNet for the latest configuration recommendations.

## Setting up the Synchronization Service

The Forefront Identity Manager 2010 Synchronization Service will be configured with two Management Agents for synchronization information about users and groups between the FIM Portal and one Active Directory domain.

## Importing and configuring the Management Agents

Two standard configured Management Agents (MA’s) are delivered with the kit. These hold the default settings for the Management Agents and are modified to fit the customer’s environment using scripts. After modifications they are imported to the Synchronization Service Manager.

Before continuing this step, make sure that the account that you are using for the following steps is either the domain administrator or an account with similar permissions. Also, make sure that the account used is a member of the FIMSyncAdmins global security group.

Follow these steps to import the Management Agents:

1. Start a PowerShell Shell
2. Create the directory C:\MSFIAB and copy all files from the kit to this directory
3. Run the PowerShell script to modify the Management Agent XML import files to match the customer’s environment by running the Prepare-CustomerManagementAgents.ps1 script.
   1. Running this script creates customized version of the Management Agent XML import files in the directory CustomerFiles
4. Start the Synchronization Service Manager
5. Click on the Management Agents tab to enable Import Management Agent menu in the Actions menu
6. From the Actions menu, select Import Management Agent and select the AD.XML file from C:\MSFIAB\CustomerFiles directory
7. The Create Management Agent wizard opens.
8. Click next to go to the Connect to Active Directory forest.
9. Verify that the forest name hold the customers Active Directory forest name
10. Verify that the username is SVC-FIM-ADMA
11. Verify that the domain is the customers Active Directory NetBIOS name
12. Type in the password for the SVC-FIM-ADMA user and click Next
13. Continue to click ‘Next’ without changing anything and finish the wizard.
    1. If you are presented with a dialog box pertaining to configuring partitions, please configure appropriately. You will most likely be able to just deselect all partitions and accept the default mapping.
14. From the Actions menu, select Import Management Agent again and select the ‘FIMMA (Password Reset and Initial Load).XML’ file from C:\MSFIAB\CustomerFiles directory
15. The Create Management wizard opens.
16. Click Next to go to the Connect to Database page
17. Under Primary connection information, verify the settings for server (should be the NetBIOS name of the local machine); if it is not, please replace with hostname of the FIM server. Verify that the Database parameter is FIMService and the FIM Service base address is http://localhost:5725
18. In the Authentication mode section, make sure that the Windows integrated authentication is selected
19. Verify that the username is SVC-FIM-MA and that the Domain is the NetBIOS name of the customers Active Directory domain.
20. Continue to click ‘Next’ without changing anything and finish the wizard.

## Configuring Run Profiles

The needed Run Profiles should already be included in the Management Agents supplied with the kit. However, for reference the following table shows the pre-created Run Profiles:

| Run Profile Name | Included Run Profile Step(s) | Partition | Log File |
| --- | --- | --- | --- |
| FI | Full Import (Stage Only) | N/A | N/A |
| DI | Delta Import (Stage Only) | N/A | N/A |
| FS | Full Synchronization | N/A | N/A |
| DS | Delta Synchronization | N/A | N/A |
| FIFS | Full Import and Full Synchronization | N/A | N/A |
| FIDS | Full Import and Delta Synchronization | N/A | N/A |
| DIDS | Delta Import and Delta Synchronization | N/A | N/A |
| E.FI | (1) Export | N/A | N/A |
| (2) Full Import (Stage Only) | N/A | N/A |
| E.DI | (1) Export | N/A | N/A |
| (2) Delta Import (Stage Only) | N/A | N/A |

These Run Profiles are common for both the FIM MA Management Agent and the Active Directory Management Agent.

## Configuring Deprovisioning

Deprovisioning is an important part of the solution in order to control the lifecycle of object correctly according to the customer’s needs. There is no golden rule on how to implement this and no specific scenario will suffice for all customers. Therefore, a setup has been provided that ensures that the Active Directory objects are kept safe and the actual deletion of objects from Active Directory will trigger the deletion of objects in the metaverse and in FIM Service DB.

Unless your customer notes otherwise, you are probably safe configuring your deprovisioning rule on the FIM MA management agent to “Stage a delete on the object for the next export run”. This setting is default with the Management Agent delivered in the kit. You can alter that based upon the needs of your customer.

Unless your customer notes otherwise, you are probably safe configuring your deprovisioning rule on the Active Directory Management Agent “Make them disconnectors”. This setting is default in the Management Agent delivered in the kit and should make sure that you don’t physically delete any objects in the Active Directory. You can alter that based upon the needs of your customer.

Follow these steps to configure or check the settings for the deprovisioning:

1. Start the Synchronization Service Manager
2. Click on the Management Agent tab
3. Right-click the AD Management Agent and select Properties
4. Go to the Configure Deprovisioning
5. Make sure that ‘Make them disconnectors” are selected
6. Repeat the step 3-5 for the FIM MA, only make sure that ‘Stage a delete on the object for next export run’ is selected of FIM MA.

## Configuring the Metaverse Schema

There are no customized attributes or alterations to precedence made to the metaverse person or group object type for the delivery of the base offering scenario. Therefore, the deletion rule for the objects should be set as follows:

|  |  |  |
| --- | --- | --- |
| Object Type | Deletion Rule Type | Details |
| Person | Delete metaverse object when connector from any of the following management agents is disconnected | AD |
| Group | Delete metaverse object when connector from any of the following management agents is disconnected | AD |

If your customer desires otherwise, you should discuss the implications of this and decide together with the customer whether to deviate from this. If you change these settings, please make sure that the customer understands the implications.

To configure and check these settings, follow these steps:

1. Start the Synchronization Service Manager
2. Click on the Metaverse Designer tab
3. Highlight the person object type and select Configure Object Deletion Rule from the Actions menu
4. Select ‘Delete metaverse object when connector from any of the following managements agents is disconnected’
5. Make sure that only the AD Management Agent is selected
6. Repeat the steps for 3-5 the group object type

With settings in place, the only way to delete a user or group physically is by deleting the object in Active Directory. The deletion will then be propagated to the portal and removed from the portal.

## Configuring provisioning

This offering scenario has been developed to take full advantage of FIM declarative provisioning. Therefore, you should not have anything to document here as you will not leverage a management agent rules extension for the programmatic definition of advanced synchronization rules.

To enable declarative provisioning follow these steps:

1. Start the Synchronization Service Manager
2. In the menu, select Tools 🡺 Options
3. Tick of the ‘Enable Synchronization Rule Provisioning’
4. Click OK to exit the dialog box

## Loading existing users to the FIM Portal

It is most likely that the customer will already have a solution or method in place to create users and groups in the their Active Directory and therefore there will be a number of users already created in Active Directory that needs to be loaded to the FIM Portal. We need to load the existing users into the portal, in order to be able to manage them through the portal and for them to be able to enroll in the Password Management solution.

The basic information that we need to get into the FIM portal for each user is the following:

1. The username (sAMAccountName)
2. The users security identifier (objectSID)
3. The NetBIOS domain name
4. The users given name (givenName) and last name (sn) and display name (displayName)

The username, objectSID and domain name are required information on a user object in order for that user to be able to log in to the portal and to enroll in the password reset solution.

You will need to be a FIM Synchronization Service administrator and a FIM Service administrator to complete the following steps. Follow these steps to import the necessary users and their information to the FIM portal from the customers Active Directory:

1. Start the FIM Synchronization Service Manager and select the properties for the Active Directory Management Agent (MA).
2. Under ‘Configure Directory Partitions’, click the Containers button to select container for this partition
3. Enter the password again for the SVC-FIM-ADMA and click OK to continue
4. Select all containers (organizational units) that contain users that need to go into the portal.
   1. You may need to consult your customer to be able to select all relevant containers
5. Make sure that the default container ‘FIM Managed Users and Groups’ is selected, since we need these for the creation of new users and groups from the portal
6. Make sure all other containers are not selected, since we don’t want to manage objects in these OU’s.

Next step is to create an Inbound Synchronization Rule that imports only the necessary attribute values from all users in Active Directory. Follow these steps to create the Synchronization Rule:

1. Log in to the FIM Portal as a FIM Service administrator (for now, most likely the account that was used to install Forefront Identity Manager 2010)
2. Create a new Inbound Synchronization Rule called ‘FIAB: All Users synchronize basic information with portal’
3. Configure the Synchronization Rule as shown below

|  |
| --- |
| **Synchronization Rule Configuration** |
| |  |  | | --- | --- | | Name | FIAB: All Users synchronize basic information with portal | | Flow Type | Inbound | |
| **Scope** |
| |  |  | | --- | --- | | Metaverse Object Type | person | | Data Source | AD | | Data Source Object Type | user | |
| **Relationship** |
| |  |  | | --- | --- | | Create object in FIM | true | | Create object in Connected System | false | | Relationship termination | false | |
| **Relationship Criteria** |
| |  |  | | --- | --- | | ILM Attribute | Data Source Attribute | | accountName | sAMAccountName | |
| **Inbound Attribute Flows** |
| |  |  | | --- | --- | | Destination | Source | | displayName | displayName | | firstName | givenName | | domain | IIF(Eq(Left(ConvertSidToString(objectSid),38),"S-1-5-21-1761788947-87510805-225257529"),"FABRIKAM","Unknown") | | objectSid | objectSid | | accountName | sAMAccountName | | lastName | Sn | |

You need to adjust the custom expression with the flow of the NetBIOS domain name to fit the customer’s environment.

Note: To have the Custom Expression for the attribute domain automatically generated for you, run the Powershell scripts called ‘Get-DomainSynchronizationRuleCustomExpression.ps1’ supplied with the kit. This script will generate the statement and put it in to you clipboard, ready for pasting directly into your Synchronization Rule.

At this point, you may want to discuss with your customer any additional information on the existing users in Active Directory that they want to go into the FIM portal initially. If so, please adjust the Synchronization Rule above to include these attributes. Examples of such attributes could be the mobile or telephone number or company and department.

Note: If the customer is only interested in the password reset functionality, you should only import the necessary information, as sAMAccountName, objectSid, displayName and Domain, as no other information is necessary.

Once you have configured the Synchronization Rule, you need to bring this into play, by doing a Full Import and Full Sync from the FIM Portal and after that bring all users into the Synchronization Service and finally into the FIM portal.

1. Start the Synchronization Service Manager
2. Open the FIM MA properties and make sure that you have export attribute flow configured as in the following table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data Source Attribute |  | Metaverse Attribute | Mapping Type | Flow Nulls |
| Object Type: Person |  | **Object Type: Person** |  |  |
| dn | 🡸 |  | sync-rule-mapping |  |
| MVObjectID | 🡸 | <object-id> | Direct |  |
| Domain | 🡸 | domain | Direct |  |
| ObjectSID | 🡸 | objectSid | Direct |  |
| AccountName | 🡸 | accountName | Direct |  |
| LastName | 🡸 | lastName | Direct |  |
| FirstName | 🡸 | firstName | Direct |  |
| DisplayName | 🡸 | displayName | Direct |  |
| ExpectedRulesList | 🡺 | expectedRulesList | Direct |  |
| <dn> | 🡺 | csObjectID | Direct |  |

1. On the FIM MA, run the FIFS profile to get all changes (namely the new Synchronization Rule) from the FIM portal to the Synchronization Service
2. On the AD MA, run the FI profile to get all users imported (staged) to the Connector Space.
3. Once you are happy with the number of users being staged, you can go ahead and run the FS profile on the ADMA to have new metaverse objects for the users created and be ready for exporting to the FIM portal
4. Before you run the Export profile for the FIM MA, please use the Metaverse Search option in the Synchronization Service to locate the newly created users in the metaverse and verify that they appear as expected. Also, you may want to use the Search Connector Space option on the FIM MA and verify the Pending Exports
5. When you are comfortable with the information awaiting export to the portal, you can go ahead and run the E.DI profile on the FIM MA
6. Verify the results on the confirming import in the Synchronization Service and in the FIM Portal.

If you plan to allow non-administrator users to have access to the portal and the ability to view other users’ basic information, enable this configuration in the FIM Service. You do this by configuring existing MPRs in the system; please enable the following Management Policy Rules (MPR’s), if so desired –

* General: Users can read schema related resources
* General: Users can read non-administrative configuration resources
* User management: Users can read attributes of their own

You may plan with the customer to allow users to view the basic attributes of other users, for example, to be able to search and view information of users before adding them to distribution groups. If so, you should also configure the MPR in the following list –

* User management: Users can read selected attributes of other users

You may need to customize the list of attributes in this MPR based on your customers organizational policy and needs.

Having completed the steps (including the MPR’s) above the existing users are now able to log into the portal, if the customer wants this. Also, the users that have been imported are ready to use the Password Reset solution. If the customer wants to deploy the Password Reset solution, please complete the steps in this guide with regards to configuring the Password Reset solution.

## Configuring User Management through FIM portal

The following section guides you through the default configuration for letting the customer manage their users and selected attributes of users through the FIM portal.

When these steps are completed, the customer will be able to:

1. Create new users through the portal
2. Manage selected attributes on users through the portal
3. Delegate the management of users and associated attributes to other users (not a part of this guide)

Note: This guide does not implement logic to delete users physically from Active Directory; the actual delete of a user account must be done through Active Directory Users and Computers (ADUC). If the user is deleted from Active Directory, the user will also be deleted from FIM.

Before you continue with these steps, please make sure, that you have completed the steps in ‘Loading existing users to the FIM Portal’, since this is a prerequisite for the steps in this section. You could omit the previous steps, if you decide so with your customer, however, this is not recommended, since the customer may later want to build on the solution to take advantage of the automated group management feature of FIM and therefore will need all users to be in the portal for proper group management.

To enable synchronization of user information from the portal to Active Directory, please follow these steps to configure:

1. Log in to the FIM Portal as an FIM service administrator
2. Under Administration, create a new Synchronization Rule called ‘FIAB: All Users synchronize with Active Directory’ with the following settings:

|  |
| --- |
| **Synchronization Rule Configuration** |
| |  |  | | --- | --- | | Name | FIAB: All Users synchronize with Active Directory | | Connector | AD | | Flow Type | Inbound and Outbound | |
| **Scope** |
| |  |  | | --- | --- | | Metaverse Object Type | person | | Data Source | AD | | Data Source Object Type | user | |
| **Relationship** |
| |  |  | | --- | --- | | Create object in FIM | false | | Create object in Connected System | true | | Relationship termination | false | |
| **Relationship Criteria** |
| |  |  | | --- | --- | | ILM Attribute | Data Source Attribute | | accountName | sAMAccountName | |
| **Inbound Attribute Flows** |
| |  |  | | --- | --- | | Destination | Source | | email | mail | |
| **Initial Outbound Attribute Flows** |
| |  |  |  | | --- | --- | --- | | Allow Nulls | Destination | Source | | false | userAccountControl | **Constant:** 512 | | false | Dn | **CustomExpression🡺EscapeDNComponent("CN="+accountName)+",OU=FIM Managed Users and Groups"+",DC=test,DC=intern"** | | false | sAMAccountName | accountName | | false | unicodePwd | **Constant:** Password2010 | |
| **Persistent Outbound Attribute Flows** |
| |  |  |  | | --- | --- | --- | | Allow Nulls | Destination | Source | | false | sAMAccountName | accountName | | false | displayName | displayName | | false | givenName | firstName | | false | Sn | lastName | |

With the Synchronization Rule created, we need to make sure that it is applied to all users in the portal. This is done by creating an Action Workflow that adds the Synchronization Rule to the user when they meet a certain criteria. The criterion is configured using a Management Policy Rule (MPR) that we will also create.

Please follow these steps to create the Action Workflow and the Management Policy Rule to go with it:

1. Log in to the portal as a FIM service administrator
2. Under Administration 🡺 Workflows, create a new workflow called ‘FIAB: All Users synchronize with Active Directory’
3. Select ‘Action’ as Workflow Type
4. Since we want this workflow to be applied to existing users in the Set ‘All People’, we select ‘Run on Policy Update’
   1. This will make sure that the workflow gets applied to users that have already been created or the users that were initially loaded from the customer Active Directory in the previous steps. We will later remove the tick mark in ‘Run on Policy Update’.
5. On the Activities tab, select ‘Synchronization Rule Activity’ and click Select
6. When editing, select the newly created Synchronization Rule in the dropdown and make sure that the option ‘Add’ is selected.
7. Click ‘Save’ and ‘Finish’ to create to the workflow

We now need a Management Policy Rule (MPR) that will run the workflow on all users. Follow these steps to create a MPR that will complete this:

1. Log in to the portal as a FIM Service administrator
2. Under Administration 🡺 Management Policy Rules, click ‘New’ to create a new MPR
3. Follow the wizard and fill in the following values (default values are omitted below) as you go along
   1. On the General tab
      1. Display Name: “FIAB: Add AD Synchronization Rule to All Users”
      2. Type: Set Transition
   2. On the Requestors and Operations tab
      1. Transition Set: All People
      2. Transition Type: Transition In
   3. On the Policy Workflows tab
      1. Select the Action Workflow ‘FIAB: All Users synchronize with Active Directory’ that was just created in the previous steps
4. Once you click ‘Finish’ to create the MPR, all existing users will have the Synchronization Rule applied since the workflow is triggered by the “Run on Policy Update’

Important: To stop the workflow from triggering multiple times on the same users, please go back and edit the workflow ‘FIAB: All Users synchronize with Active Directory’ and remove the tick mark in ‘Run on Policy Update’.

Once the Synchronization Rule has been created, you need to modify the attribute flows for the FIM MA accordingly. Follow the steps below to configure this:

1. Start the Synchronization Service Manager
2. It is recommended that you run a Full Import and Full Sync for the FIM MA and the AD MA before making changes. This is to ensure that you don’t have any pending exports that have not been committed to the data sources before you make changes.
   1. If you choose to follow this recommendation, please run the profile FIFS for the FIM MA and afterwards for the AD MA. Check for any pending exports to either MA agent and have these committed / exported before proceeding, so that the metaverse is “consistent” before making changes.
3. Adjust the properties on the FIM MA attribute flow to follow the schema below
   1. Please make sure that you keep the export flow of the mandatory attributes, domain and objectSid; otherwise users will not be able to log in to the portal or use the password reset functionality. Do not specify ‘Allow Nulls’ for objectSid and domain as you potentially could erase existing values on, i.e. Portal administrators and basically locking these users out of the portal.

Table 3 FIM MA attribute flow for person

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data Source Attribute |  | Metaverse Attribute | Mapping Type | Flow Nulls |
| Object Type: Person |  | **Object Type: Person** |  |  |
| dn | 🡸 |  | sync-rule-mapping |  |
| MVObjectID | 🡸 | <object-id> | Direct |  |
| Domain | 🡸 | domain | Direct |  |
| ObjectSID | 🡸 | objectSid | Direct |  |
| AccountName | 🡺 | accountName | Direct |  |
| LastName | 🡺 | lastName | Direct |  |
| FirstName | 🡺 | firstName | Direct |  |
| DisplayName | 🡺 | displayName | Direct |  |
| ExpectedRulesList | 🡺 | expectedRulesList | Direct |  |
| <dn> | 🡺 | csObjectID | Direct |  |

Since you previously should have completed the ‘Loading existing users to the FIM Portal’ step to get all existing users loaded to into the portal you need modify the Synchronization Rule to NOT synchronize the attributes that conflict with this Synchronization Rule, that you just created. Please remove any attributes, i.e. FirstName from the earlier configured Synchronization Rule, since these are now being managed using this new Synchronization Rule.

Important: At this point you need to verify with your customer that the attributes that are flowing from the portal to Active Directory are indeed the attributes that the customer wants to be managed through the FIM Portal. If you need to adjust these make sure that adjustments are made both on the FIM MA Management Agent in the Synchronization Service Manager and in the Synchronization Rule.

The following attributes should be modified in the Synchronization Rule after a discussion with the customer:

|  |  |  |
| --- | --- | --- |
| Attribute Name | Reason | Note |
| unicodePwd | The initial password for newly created users should be compliant with the customer’s password policy. Discuss the password policy with the customer and adjust the formula for generating the initial password. You can use the built-in function to generate a password that is secure and compliant with the customer’s policies. | When discussing with the customer also, agree on how the new password will be communicated to the user for their first logon. |
| dn | The default CN in Active Directory will be the sAMAccountName. If the customer wants a different CN, please adjust accordingly. Another way to define this could be CN=FirstName+” “+LastName+” (“+accountName+”)” | Whichever way, you choose to compile the value for this attribute, you need to make sure that the CN is unique within the OU that the user object is stored in. |
| userAccountControl | Initially, the value that flows to newly created users is 512. This means that the user is enabled. The customer may have other preferences for this, so please adjust this accordingly. | Please refer to KB305144 / ‘How to use the userAccountControl flags to manipulate user account properties’ for more information on how to build the initial value. |

Once you are satisfied that you have created the correct flows, please follow these steps to enable the new and the modified Synchronization Rule:

1. Start the Synchronization Service Manager
2. On the FIM MA, run the FIFS profile to get all the configuration changes made in the portal into the Synchronization Service
3. Verify the Declarative Provisioning is enabled (you may refer to the section ‘Configuring provisioning’ to enable this)
4. Verify that the new Synchronization Rule was brought into the metaverse
   1. Correct any problems before continuing
5. Verify that the modified Synchronization Rule was brought into the metaverse
   1. Correct any problems before continuing
6. On the AD MA run the profile FIFS to able all users to use the new Synchronization Rule.
7. Verify that any pending exports, that may be generated, are valid.
   1. Correct any unwanted mistakes by modified the attribute flows on the FIM MA and on the Synchronization Rule
   2. Repeat step 2-6 until you are satisfied with the results
8. On the AD MA, run the E.DI profile to export any changes from the portal to Active Directory
9. On the AD MA, run the DS profile to synchronize any changes from the connector space to the metaverse
10. On the FIM MA, run the E.DI to export any changes from the metaverse to the portal

You may see some provisioning errors against the Active Directory, namely the “Built-in Synchronization Account” and perhaps the Administrator account or the account that was used to install FIM. If you encounter any of these errors, it is most likely that the accounts in question are not located in the organizational units (partitions) that you selected in the configuration on the Active Directory MA earlier in this guide and therefore not a part of the synchronization. To remove the errors, you could include the additional partitions or add the accounts to the connector filter of the FIM MA – or a combination of the two.

1. Please implement the necessary Connector Filter on the FIM MA as appropriate for your customers environment
   1. Mostly you would have a Declared filter for AccountName Equals ‘Built-in Synchronization Account’ and perhaps for Account Equals ‘Administrator’

If the customer has Exchange 2003, Exchange 2007 or Exchange 2010 there are additional steps to complete to be able to create mailboxes for new users. Please complete steps in ‘Enabling the creation of Exchange 2003 mailbox for new users’, ‘Enabling the creation of Exchange 2007 mailbox for new users’ or ‘Enabling the creation of Exchange 2010 mailbox for new users’ to enable for provisioning of mailboxes for new users.

At this point, you should perform a number of verification tests of attribute flow and account creation. Also, now would be a good time to get the customers personnel even more involved in the process by making them do the tests together with you. Letting the customer do the actual testing with you, will allow the customer to build confidence in the solution.

It is important that you test the flows and account creation thoroughly and examples of tests could be:

1. Create a new account in the portal and verify that this account gets created successfully in Active Directory
2. Move existing accounts to other OU’s and verify that they are still be managed properly by FIM
3. Change attribute values in Active Directory that are under control on FIM and verify that FIM corrects the values again

Note: There are a number of third-party ISV’s that have solutions that built on the setup, i.e. compliance reports and such. These solutions may require additional attributes to be populated in the FIM portal or in Active Directory, such as the attribute pwdLastSet. If you are engaging with any of these partners, please refer to their documentation to meet additional requirements for attribute flow or modifications.

## Configuring Exchange mailbox creation for new users

The following steps should be done in addendum to steps concluded in the ‘Configuring User Management through FIM portal’ section and depend on these being completed.

When an Exchange mailbox is created, it needs an identifier and needs a location where it should be stored. The identifier can be split into two parts, being the "Alias" to identify the mailbox itself as a minimum to generate the mail address if no custom e-mail address policy has been specified, or when one has been specified to use the Alias AND to generate the legacyExchangeDN. For the GAL, the identifier of the mailbox is the "Display Name" and it is required by Exchange. It is not required by Active Directory.

When creating a mailbox in Exchange where there is no Display Name, the Display Name will still be populated and is derived from the CN. With regards to the location we need to at least specify an Exchange Server and preferably a mailbox database on that Exchange Server. If you do not specify a mailbox database, Exchange will select a mailbox database randomly. It is recommended to specify both the Exchange Server and the mailbox database. Other attributes such homeMTA and msExchHomeServerName are derived from the specified value for homeMDB.

Note: These steps only handle the creation of mailboxes in one specific mailbox database for new users. Doing load balancing or other selection methods for placing user’s mailboxes in different mailbox stores are out of scope for this guide. You may discuss various options for doing this with the customer and maybe develop a plan together with the customer for extending the solution in this area.

No matter which Exchange version is installed, you need to configure the AD MA to have the following attributes selected on the Select Attributes tab, since they are needed by the Active Directory Management Agent to be able to successfully create mailbox for new users:

|  |  |
| --- | --- |
| Attribute Name | Description |
| mailNickName | This attribute is the alias to the mailbox. |
| homeMDB | This attribute is a distinguished name to the private Messaging Database (MDB) where the mailbox resides. |
| mDBUseDefaults | Indicates whether the store should use the default quota, rather than the per-mailbox quota. This is optional. |
| msExchMailboxSecurityDescriptor | The mailbox rights are stored on a security descriptor property on the mailbox in the information store. The attribute on the Active Directory user object that is named msExchMailboxSecurityDescriptor is designed to reflect the mailbox rights on the user's mailbox. |
| msExchHomeServerName |  |

After selecting these attributes on the AD MA, run the profile FIFS to make sure that the attributes are available in the metaverse and subsequently in the portal.

Note: The steps to enable the creation of mailboxes for new users assume that the displayName attribute is being populated as the previous steps instruct.

Microsoft Exchange Server adds many new attributes and classes to the Active Directory service schema and makes other modifications to existing classes and attributes. It is possible to leverage some of these attributes to make a more granular creation of mailbox, i.e. setting quota and such. You may discuss this with the customer; however, it is out of scope for this guide to elaborate on this.

Make sure that the Service Account for Active Directory has the necessary permissions for accessing Exchange-related attributes on users and groups. These permissions differ between Exchange versions.

### Importing the mail attribute

Optionally, when you have enabled FIM for mailbox creation, you may want to adjust the FIM MA and the Synchronization Rule to import the mail attribute to the portal. A good reason for doing this is that the customer may later want to extend the solution with capabilities to send mail when certain events happen, such as alerting when group membership is changed or requested.

To adjust for importing the mail attribute to the FIM portal, please follow these steps:

1. Using the Synchronization Service Manager, open the Properties of the FIM MA
2. Under Attribute Flow, add an export attribute flow rule for the person object
   1. Metaverse attribute: email
   2. Data source attribute: Email
   3. Flow Direction: Export (tick ‘Allow Nulls’)
3. In the FIM portal, modify the Inbound attribute flow for the Synchronization Rule ‘FIAB: All Users synchronize with Active Directory’ to include the mail attribute inbound flow
   1. Source: mail
   2. Destination: email
4. Be sure to run full synchronizations on both Management Agents when you change Synchronization Rule and/or attribute flows to ensure that the new settings are applied to all object affected by the rules

### Enabling the creation of Exchange 2003 mailbox for new users

For Exchange 2003, FIM 2010 relies on the Recipient Update Service (RUS) feature of Exchange 2003 to complete the provisioning process. During export, AD MA connects to an available domain controller and adds the mail-enabled object (as determined by the provisioning configuration) to the directory.

As mentioned earlier, RUS watches for changes to mail-enabled objects in the directory and completes the provisioning process for each object created by ILM 2007 and FIM 2010. And once again, Exchange writes each of these objects to the directory with the minimal set of attributes needed to create the objects. Because of this, RUS applies an Exchange Policy to them and adds the remaining required attributes so that they support the full set of Exchange features.

To enable the creation of an Exchange 2003 mailbox on new users, complete these steps:

1. Modify the Synchronization Rule ‘FIAB: All Users synchronize with Active Directory’ to include the following outbound attribute flows:

Table 4 Exchange attributes for Synchronization Rule

|  |  |  |
| --- | --- | --- |
| Initial Flow | Source | Destination |
| X | mailNickname | mailNickname |
| X | CN=MailDB01,CN=First Storage Group,CN=InformationStore,CN=MBX01,CN=Servers,  CN=First Administrative Group,CN=Administrative Groups,CN=MyOrg,CN=Microsoft Exchange, CN=Services,CN=Configuration,DC=Fabrikam,DC=com | homeMDB |

1. On the FIM MA, run the FIFS profile to get the modified Synchronization Rule into the metaverse

Note: You should always adjust the actual value of the homeMDB to point to a valid distinguishedName in the customer’s environment. To find a valid distinguishedName for a mailbox store, use adsiedit.msc and follow the steps in ‘Appendix A – Find valid distinguishedName for Exchange mailbox’.

Please make sure that the Service Account has the necessary permissions for manipulation Exchange-related attributes on the users and groups in scope. For more information on the security model of Exchange 2003, please refer to <http://technet.microsoft.com/en-us/library/bb124053(EXCHG.65).aspx>.

### Enabling the creation of Exchange 2007 mailbox for new users

From a FIM perspective, provisioning mailboxes in Exchange 2007 is not much different from provisioning mailboxes in Exchange 2003, so please refer to ‘Enabling the creation of Exchange 2003 mailbox for new users’ for setting up the flow in the Synchronization Rule. You also need to at least specify the following attributes:

* mailNickname
* homeMDB

Note the fact that homeMDB in Exchange 2007 contains both the Mailbox Database Name and the Exchange Server Name. In addition to specifying the minimum required attributes, you need to configure the AD MA as follows to enable for Exchange 2007 provisioning. Follow these steps to configure this:

1. Using the Synchronization Service Manager, open the properties of the AD MA
2. Navigate to the ‘Configure Extension’ tab
3. In the dropdown ‘Provision for:’, select ‘Exchange 2007’
4. Leave the textbox ‘Exchange 2007 RUS Server (optional)’ blank; you could specify an Exchange 2007 server here if there are good reason, such replication issues etc.

Actually Recipient Update Service (RUS) still exists in Exchange 2007. Instead of being a separate service, it is now just a synchronous step inside the System Attendant which the PowerShell cmdlet make an RPC call to. Service Pack 2 for Exchange 2007 added a parameter (the same as the optional option in the AD MA) to the various cmdlets to specify which Exchange server the cmdlet should call out to for RUS.

1. Click OK to save changes

 Exchange Server 2007 Mailbox Provisioning requires at least the following to be installed on the FIM Server:

* PowerShell v1.0 (or PowerShell v2.0) for the execution of local PowerShell cmdlets.
* Exchange Management Console providing the required cmdlets

Also the Service Account for the Active Directory needs to have permissions to create mailbox for users and manipulate Exchange-related attribute for groups. One suggested model is to add the account to the ‘Exchange Recipient Administrator role’; however, you should discuss the security model with your customer.

### Enabling the creation of Exchange 2010 mailbox for new users

From a FIM perspective, provisioning mailboxes in Exchange 2010 is not much different than provisioning mailboxes in Exchange 2003 or Exchange 2007, so please refer to ‘Enabling the creation of Exchange 2003 mailbox for new users’ for setting up the flow in the Synchronization Rule. You also need to at least specify the following attributes in your Synchronization Rule:

* mailNickname
* homeMDB
* msExchHomeServerName

Note the fact that homeMDB in Exchange 2010 only contains the Mailbox Database Name and NOT the Exchange Server Name. The Exchange Server Name is stored in the value for the attribute called msExchHomeServerName.

The modifications to the Synchronization Rule should therefore contain something very similar to this:

|  |  |  |
| --- | --- | --- |
| Initial Flow | Source | Destination |
| X | mailNickname | mailNickname |
| X | CN=Mailbox Database 1891753935,CN=Databases,CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=MyOrg,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=Fabrikam,DC=com | homeMDB |
| X | CN=MBX01,CN=Servers,CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=MyOrg,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=Fabrikam,DC=com | msExchHomeServerName |

Note: You should always adjust the actual value of the homeMDB and msExchHomeServerName to point to a valid distinguishedName in the customer’s environment. To find a valid distinguishedName for a mailbox store and server, use adsiedit.msc and follow the steps in ‘Appendix A – Find valid distinguishedName for Exchange mailbox’.

In addition to specifying the minimum required attributes, you need to configure the AD MA as follows to enable for Exchange 2010 provisioning. Follow these steps to configure this:

1. Using the Synchronization Service Manager, open the properties of the AD MA
2. Navigate to the ‘Configure Extension’ tab
3. In the dropdown ‘Provision for:’, select ‘Exchange 2010’
4. In the textbox ‘Exchange 2010 RPS URI’, specify a valid Exchange 2010 Client Access Server

For the option "Exchange 2010 RPS URI" you need to specify a URL in the form ‘http(s)://<server name>/PowerShell’ that is hosting the "Client Access Server Role" so that the FIM server can use remote PowerShell cmdlets against it.

1. Click OK to save changes

 Exchange Server 2010 Mailbox Provisioning requires at least the following to be installed on the FIM Server:

* PowerShell v2.0 for the execution of remote PowerShell cmdlets.

Provisioning of Exchange 2010 mailboxes does not require the Exchange Management Console to be installed on the FIM server as remote PowerShell cmdlets are used.

Also the Service Account for the Active Directory needs to have permissions to create mailbox for users and manipulate Exchange-related attribute for groups. One suggested model is to add the account to the ‘Recipient Management’ role group; however, you should discuss the security model with your customer.

## Configuring simple Group Management through FIM portal

These steps walks you through the main building blocks that are involved in the process of provisioning groups from Microsoft® Forefront Identity Manager (FIM) 2010 to Active Directory and outlines how you can verify whether your scenario works as expected.

The steps are only a guide on how to create new groups in the portal and have these created in Active Directory. The solution in the current version does not include information on how to get existing groups into the portal. This is out of scope.

The steps involved in enabling group management from the portal involved are overall:

1. Create a Synchronization Rule for groups
2. Modify the attribute flow for group objects on the FIM MA.
3. Create workflows to add groups to Synchronization Rules
4. Create Management Policy Rule (MPR) to enable the workflows for the groups
5. Instruct the customer on how to install the Outlook plug-in for managing Distribution Groups through Outlook

When these steps are complete, the customer will be able to create new groups using the portal. It is not in scope to describe a delegation model for managing groups through the portal. You may discuss the various possibilities for this with the customer.

To configure FIM for simple group management, follow these steps:

1. Using the portal, create a new Synchronization Rule called ‘FIAB: All Groups synchronize with Active Directory’
2. Configure the Synchronization Rule as shown below.

Note: You could include additional attribute flow in the Synchronization Rule if agreed so with the customer. Just remember adjust the attribute flow on the FIM MA in the Synchronization Service as well.

|  |
| --- |
| **Synchronization Rule Configuration** |
| |  |  | | --- | --- | | Name | FIAB: All Groups synchronize with Active Directory | | Created Time | 21/12/2010 | | Flow Type | Inbound and Outbound | |
| **Scope** |
| |  |  | | --- | --- | | Metaverse Object Type | group | | Data Source | AD | | Data Source Object Type | group | |
| **Relationship** |
| |  |  | | --- | --- | | Create object in FIM | false | | Create object in Connected System | true | | Relationship termination | false | |
| **Relationship Criteria** |
| |  |  | | --- | --- | | ILM Attribute | Data Source Attribute | | accountName | sAMAccountName | |
| **Initial Outbound Attribute Flows** |
| |  |  |  | | --- | --- | --- | | Allow Nulls | Destination | Source | | False | dn | **CustomExpression🡺EscapeDNComponent("CN="+displayName)+",OU=FIM Managed Users and Groups,DC=test,DC=intern”** | |
| **Persistent Outbound Attribute Flows** |
| |  |  |  | | --- | --- | --- | | Allow Nulls | Destination | Source | | true | sAMAccountName | CustomerExpression🡺IIF(IsPresent(accountName),accountName,mailNickname) | | false | displayName | displayName | | false | managedBy | displayedOwner | | true | member | member | | false | groupType | **CustomExpression🡺IIF(Eq(type,"Distribution"),IIF(Eq(scope,"Universal"),8,IIF(Eq(scope,"Global"),2,4)),IIF(Eq(scope,"Universal"),-2147483640,IIF(Eq(scope,"Global"),-2147483646,-2147483644)))** | | true | mailNickName | mailNickname | |

Note(\*): If the customer’s environment does NOT include Exchange, you don’t need to have the Outbound Attribute flow from ‘mailNickname’ to ‘mailNickName’. The mailNickName attribute will also only be available in the Active Directory schema if Exchange has been installed. Also note, that the sAMAccountName is populated by either accountName or mailNickName; this is to handle the population of the sAMAccountName for Distribution Groups where the AccountName attribute is not directly available in the FIM Portal GUI by default.

Note: Verify that you have selected Initial Flow Only for the attribute flow that has the DN as the destination.

1. Next, using the Synchronization Service Manager, reconfigure the existing FIM MA to include attribute flows for groups as shown in the table below

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data Source Attribute |  | Metaverse Attribute | Mapping Type | Flow Nulls |
| Object Type: Group |  | **Object Type: Group** |  |  |
| Dn | 🡸 |  | sync-rule-mapping |  |
| MVObjectID | 🡸 | <object-id> | Direct |  |
| DisplayedOwner | 🡺 | displayedOwner | Direct |  |
| Type | 🡺 | type | Direct |  |
| Scope | 🡺 | scope | Direct |  |
| Member | 🡺 | member | Direct |  |
| MailNickName | 🡺 | mailNickname | Direct |  |
| AccountName | 🡺 | accountName | Direct |  |
| DisplayName | 🡺 | displayName | Direct |  |
| ExpectedRulesList | 🡺 | expectedRulesList | Direct |  |
| Description | 🡺 | description | Direct |  |
| <dn> | 🡺 | csObjectID | Direct |  |

1. Now, we will create an Action workflow called ‘FIAB: All Groups synchronize with Active Directory’.
   1. The objective of this Action Workflow is to bring the groups into the scope of the Synchronization Rule.
2. Select ‘Action’ as Workflow Type
3. Leave the ‘Run on Policy Update’ unchecked, since there are no existing group objects that we need this workflow applied to
4. On the Activities tab, select ‘Synchronization Rule Activity’ and click Select
5. When editing, select the newly created Synchronization Rule in the dropdown and make sure that the option ‘Add’ is selected.
6. Click ‘Save’ and ‘Finish’ to create to the workflow

Now all that is left is to create a Management Policy Rule (MPR) of type Set Transition that triggers when a resource becomes a member of the All Groups set. Follow the steps to create the necessary MPR:

1. Under Administration 🡺 Management Policy Rules, click ‘New’ to create a new MPR
2. Follow the wizard and fill in the following values (default values are omitted below) as you go along
   1. On the General tab
      1. Display Name: “FIAB: Add AD Synchronization Rule to All Groups”
      2. Type: Set Transition
   2. On the Requestors and Operations tab
      1. Transition Set: All Groups
      2. Transition Type: Transition In
   3. On the Policy Workflows tab
      1. Select the Action Workflow ‘FIAB: All Groups synchronize with Active Directory’ that was just created in the previous steps
3. Once you click ‘Finish’ to create the MPR, all new groups will have the Synchronization Rule applied

## Configuring Password Reset through FIM portal

With Password Reset, users can reset their passwords by using an authentication gate from the native Windows logon screen. If users cannot remember their passwords, Password Reset takes the user through the process of gaining a new password.

This section may be implemented separately provided the prerequisites are fulfilled.

Please refer to <http://technet.microsoft.com/en-us/library/ee534892(WS.10).aspx#step_12> for further information.

The following prerequisites must be met before continuing:

1. The section ‘Loading existing users to the FIM Portal’ in this document must be completed before starting the Password Reset section
2. No firewall is blocking network traffic between the FIM portal and the Active Directory domain controllers
3. Only one language variant of authentication questions is required
4. The actual use of the Password Reset functionality requires client software to be deployed. As customers typically use different methods for this, the deployment is not included in this guide. But to test and use the functionality, the client software is required. See ‘Installing the FIM Add-ins and Extensions’.
5. Setting up a kiosk PC to perform the password reset is not in scope. See the above link for instructions.

To implement password Reset, follow these steps:

1. [Make the FIM 2010 Service account SVC-FIM-Service a member of the FIMSyncBrowse and FIMSyncPasswordSet groups](http://technet.microsoft.com/en-us/library/ee534892(WS.10).aspx#step_1)
2. [Enable password management on the AD management agent on the FIM Synchronization Server](http://technet.microsoft.com/en-us/library/ee534892(WS.10).aspx#step_2)
3. Assign rights in Active Directory to allow the AD MA
   1. The account SVC-FIM-ADMA must be delegated the read and write of the properties userAccountControl and lockoutTime on the user objects of the OU’s used
   2. The account SVC-FIM-ADMA must be delegated the reset and change password on the user objects of the OU’s
   3. The account SVC-FIM-ADMA must be delegated the “Replicating Directory Changes” right on the AD domain itself.
4. [Enable FIM 2010 service account SVC-FIM-Service privileges in Windows Management Instrumentation on the FIM Synchronization Server](http://technet.microsoft.com/en-us/library/ee534892(WS.10).aspx#step_3)
   1. In Server Manager click “Configuration”
   2. Click “WMI Control”, then right-click and select “Properties”
   3. Click the “Security” tab
   4. Expand “Root” and click “CIMV2” and then click the “Security” button
   5. Add the SVC-FIM-Service account and ensure it has “Allow” for “Remote Enable” and “Enable Account”
   6. With the service account still selected, click “Advanced”
   7. Select the service account and click “Edit”
   8. Ensure that the “Apply to” is “This namespace and subnamespaces”
5. If the Windows Firewall is enabled on the FIM Synchronization Server [allow Windows Management Instrumentation traffic](http://technet.microsoft.com/en-us/library/ee534892(WS.10).aspx#step_4)
   1. Enable an exception for “Windows Management Instrumentation (WMI)” in the Windows Firewall control panel
6. Configure DCOM for the SVC-FIM-Service account. A standard installation will perform some of this configuration correctly
   1. Verify that SVC-FIM-Service is a member of the FIMSyncAdmins group
   2. Using the Administrative Tool, Component Services configure FIMSyncAdmins to have “Local Access” and “Remote Access” both when checking “Edit Limits” and “Edit Default” on the “COM Security” tab of “My Computer” of “Access Permissions”
   3. Configure “Launch and Activation Permissions” so that FIMSyncAdmins has Local Launch, Remote Launch, Local Activation, and Remote Activation in the same way
7. [Update the Password Reset Users Set in the FIM Portal to ensure it contains all the users you would like to participate in password reset](http://technet.microsoft.com/en-us/library/ee534892(WS.10).aspx#step_6)
   1. In the FIM portal, under Administration, check the “Password Reset users Set” and modify “Criteria-based Members” if required
8. [Update the password reset workflow in the FIM Portal](http://technet.microsoft.com/en-us/library/ee534892(WS.10).aspx#step_7). This guide only covers a very simple workflow. Much more complex workflows may be implemented if your customer requires it. The simple scenario of a malicious user locking out other users by answering their questions with bogus answers is not mitigated in this simple workflow.
   1. In the FIM Portal under Workflows check the “Password Reset AuthN Workflow”
   2. Under Activities, click QA Gate and edit the number of questions and other parameters. The suggested starting point is 6 questions with 4 being presented and 3 answered correctly
   3. Add the questions. You may find more examples at <http://www.goodsecurityquestions.com/examples.htm>. The questions may be translated into your local language if required.
      1. “Where were you when you first heard of 9/11?”
      2. “How old was your mother when you were born?”
      3. “What is your oldest sibling’s birthday month and year? (e.g., January 1900)?”
      4. “What was the last name of your third grade teacher?”
      5. “In what city or town was your first job?”
      6. “What is the first name of your oldest cousin?”
   4. Expand the Lockout Gate and enter a Lockout duration of 5 minutes, a Lockout threshold of 2 and a permanent lockout of 5. These numbers are examples and may be configured for your customer’s needs.
9. [Enable the Management Policy Rule named Anonymous users can reset their password](http://technet.microsoft.com/en-us/library/ee534892(WS.10).aspx#step_8)
10. [Enable the Management Policy Rule named Password reset users can read password reset resources](http://technet.microsoft.com/en-us/library/ee534892(WS.10).aspx#step_9)
11. [Enable the Management Policy Rule named Users can create registration resources for themselves](http://technet.microsoft.com/en-us/library/ee534892(WS.10).aspx#step_10)
12. [Enable the Management Policy Rule named Password reset users can update the lockout attribute of themselves](http://technet.microsoft.com/en-us/library/ee534892(WS.10).aspx#step_11)
13. [Enable the Management Policy rule named User management: Users can read attributes of their own](http://technet.microsoft.com/en-us/library/ee534892(WS.10).aspx#step_12)
14. [Enable the Management Policy Rule named General: Users can read non-administrative configuration resources](http://technet.microsoft.com/en-us/library/ee534892(WS.10).aspx#step_13)

Before a user can utilize the password reset functionality he or she has to enroll. Enrollment can be performed through a web browser to the FIM portal or by using the client software. In the latter case client software must be deployed.

Discuss different enrollment scenarios with the customer and help them agree on a feasible way to get their users enrolled. The actual enroll process and facilitating this is not part of the offering in the current version. The different enrollment methods and test options can be found in the section ‘Test the configuration’ (scroll down a few pages) at <http://technet.microsoft.com/en-us/library/ee534892(WS.10).aspx#step_13>.

The Microsoft TechNet Step-Through guide also shows the necessary steps to enable helpdesk users or other support team to manage user. These steps are necessary only if the customer plan to have a support team manage users when they are locked out of password reset. Configuring this is not part of the current offering; however, you should discuss the possibility to implement this later with your customer.

## Installing the FIM Add-ins and Extensions

The FIM Add-ins and Extensions components consist of the FIM Add-in for Outlook and FIM Password Reset Extensions. The deployment of Outlook Add-ins is not in scope for the guide; however there may be good reason to discuss with the customer the value of deploying the Outlook Add-in.

With Password Reset, users can reset their passwords by using an authentication gate from the native Windows logon screen. If users cannot remember their passwords, Password Reset takes the user through the process of gaining a new password.

For group management, the FIM Add-in for Outlook is interesting, since it allows users to join or leave an e-mail-enabled group from Outlook. In addition, owners and approvers can approve or reject a request of any type made from the FIM Portal or FIM 2010 Office Integration add-in component.

Typically customers have a software deployment solution implemented that is able to deploy MSI files to client computers. The Add-ins for FIM is delivered as MSI-files and can be deployed with almost any recognized software deployment solution.

For a complete guide for installing the Outlook Add-in, please refer the TechNet article ‘Installing the FIM Add-ins and Extensions’ located at <http://technet.microsoft.com/en-us/library/ff512688(WS.10).aspx>.

# Appendix A – Find valid distinguishedName for Exchange mailbox

To determine the distinguished name of the Exchange database

1. Start the ADSI Edit tool. To do this, click Start, click Run, type adsiedit.msc, and then click OK.

Note: In Windows Server 2008, ADSI Edit is installed by default. In Windows Server 2003, ADSI Edit is included with the Windows Support Tools. To install the Windows Support Tools, double-click Suptools.msi in the Support\Tools folder on the Windows Server 2003 CD.

1. Connect to the Configuration container if ADSI Edit is not already connected. To do this, follow these steps:
2. On the Action menu, click Connect to. In the Select a well-known Naming Context list, click Configuration, and then click OK.
3. Expand the following path:
   1. Configuration [<domainController>.contoso.com]
   2. CN=Configuration,DC=contoso,DC=com
   3. CN=Services
   4. CN=Microsoft Exchange
   5. CN=<OrganizationName>
   6. CN=Administrative Groups
   7. CN=Exchange Administrative Group (<ID>)
   8. CN=Servers
   9. CN=<MailboxServerName>
   10. CN=Information Store
   11. CN=<StorageGroupName>
4. In the details pane, right-click the CN=<DataBaseName> entry that has a Class value of msExchPrivateMDB, and then click Properties.
5. On the Attribute Editor tab, click distinguishedName, and then click View.
6. Copy the path that appears in the Value box, and then click Cancel.
7. Click Cancel, and then exit the ADSI Edit tool.

# Appendix B – Scheduling the Run Profiles

The final operations in any Forefront Identity Manager solution, besides documentation, are to automate the execution of Run Profiles. This can be done in several different ways. The Synchronization Service Manager offers the possibility to generate a VBScript for each Run Profile, which can then be scheduled using the built-in Scheduled Tasks.

Included in this kit is a VBScripts that only needs minor changes to be able to run different profiles for the two Management Agents that are part of the solution.

To use this script with the customer solution, please follow these steps:

1. Edit the script ‘FIM-Schedule.vbs’ located in C:\MSFIB\Schedule on the customers FIM server.
2. Make sure that the runs that are specified fits your customers environment
3. There is a command ‘ClearRuns(7)’ in the script that cleans up the Run History in the Synchronization Service. You can delete this statement if you don’t want automatic cleanup of the Run History or you could decide on a different number (number of days to keep) together with your customer and change it accordingly.
4. Create an account with a secure password in the Active Directory and make this a member of the FIMSyncOperators group.
5. Create a scheduled task to run the VBScript on a schedule that fits your customer’s environment.
   1. Remember to use CSCRIPT.EXE for the scheduled command or the script will no run properly
6. Run the Schedule Task and verify that it runs the selected profiles.

If you run into problems with the Run Profiles not being executed, it is mostl likely a permission problem, so verify the permission with regards to FIM for the account that is running the Scheduled Task

For reference, the schedule script is included below

Set Service = GetObject("winmgmts:{authenticationLevel=PktPrivacy}!root/MicrosoftIdentityIntegrationServer")

Set FIM = Service.ExecQuery("select \* from MIIS\_ManagementAgent where Name = 'FIM MA'")

Set AD = Service.ExecQuery("select \* from MIIS\_ManagementAgent where Name = 'AD'")

' main processing

ClearRuns(7)

Run FIM, "DIDS"

Run AD, "DIDS"

Run FIM, "E.DI"

'allow for FIM to do some processing

Wait 5

Run FIM, "DS"

Run AD, "E.DI"

RUN AD, "DS"

Sub Wait(Seconds)

WScript.Echo "Waiting " & Seconds & " seconds..."

WScript.Sleep(Seconds\*1000)

End Sub

Sub Run(MASet, Profile)

For Each MA In MASet

WScript.Echo "Running " + MA.name + ".Execute('" & Profile & "')..."

WScript.Echo "Run completed with result: " + MA.Execute(Profile)

Next

End Sub

Sub ClearRuns(DaysAgo)

Set Server = Service.Get("MIIS\_Server.Name='localhost'")

DeleteDate = FormatDateTime(Now()-DaysAgo, 2)

WScript.Echo "Deleting Run Histories from " & DeleteDate

WScript.Echo "Result: " & Server.ClearRuns(DeleteDate)

End Sub