

Forefront Identity Manager 2010 R2 Deployment Guide

Microsoft Corporation

Published: June 2012

Last Update:

Author: Bill Mathers

Version: 1.0

Acknowledgements

Special thanks to the following people for reviewing and providing invaluable feedback for this document:

Abstract

This document will assist architects, consultants, system engineers, and system administrators in deploying Microsoft® Forefront® Identity Manager 2010 R2.



This document supports a preliminary release of a software product that may be changed substantially prior to final commercial release. This document is provided for informational purposes only and Microsoft makes no warranties, either express or implied, in this document. Information in this document, including URL and other Internet Web site references, is subject to change without notice. The entire risk of the use or the results from the use of this document remains with the user. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. 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.

© 2012 Microsoft Corporation. All rights reserved.

Active Directory, ActiveX, Forefront, Internet Explorer, Microsoft, Outlook, SharePoint, SQL Server, Visual Studio, Windows, Windows PowerShell, Windows Server, and Windows Vista are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

Contents

[Forefront Identity Manager 2010 R2 Deployment Guide 7](#_Toc326301883)

[Forefront Identity Manager 2010 R2 Deployment Guide 7](#_Toc326301884)

[Planning for Forefront Identity Manager 2010 R2 7](#_Toc326301885)

[Planning for Forefront Identity Manager 2010 R2 7](#_Toc326301886)

[Considerations for New Installation of FIM 2010 R2 7](#_Toc326301887)

[What This Document Covers 8](#_Toc326301888)

[Prerequisite Knowledge 8](#_Toc326301889)

[Audience 8](#_Toc326301890)

[Topology 9](#_Toc326301891)

[Service Accounts 9](#_Toc326301892)

[Considerations for Upgrading to FIM 2010 R2 12](#_Toc326301893)

[General FIM 2010 R2 Upgrade Information 12](#_Toc326301894)

[Considerations when Upgrading to FIM 2010 R2 15](#_Toc326301895)

[Upgrading Outlook 2007 to Outlook 2010 and the FIM Add-ins and Extensions 15](#_Toc326301896)

[Specifying a Very Long File Path Can Cause Extraction to Fail 15](#_Toc326301897)

[Error when upgrading with existing certificate 15](#_Toc326301898)

[Considerations when Upgrading to FIM 2010 R2 Synchronization Service 16](#_Toc326301899)

[Synchronization engine database upgrade can fill up transaction log and fail when database recovery mode is set to Full 16](#_Toc326301900)

[Ignore message to delete MAdata folder during upgrade 16](#_Toc326301901)

[Considerations when Upgrading to FIM 2010 R2 Service and Portal 16](#_Toc326301902)

[All existing resources with the FIM owned schemas are deleted during installation 16](#_Toc326301903)

[Language packs must be uninstalled before the FIM Service 16](#_Toc326301904)

[“SharePoint Timer Service is not running” error during installation 17](#_Toc326301905)

[Verify the SharePoint 2010 Administration Service is running 17](#_Toc326301906)

[Considerations when Upgrading to FIM Certificate Management 2010 R2 17](#_Toc326301907)

[Upgrade Considerations 17](#_Toc326301908)

[Backup Information 18](#_Toc326301909)

[Backup the FIM Synchronization Service Server Configuration 18](#_Toc326301910)

[Backup the FIM Service and Portal Configuration 19](#_Toc326301911)

[Backup the FIM Synchronization Service and FIM Service databases 20](#_Toc326301912)

[Backup all Resource Control Display Configuration (RCDC) Objects 22](#_Toc326301913)

[Common FIM 2010 R2 Database Upgrade Issues 30](#_Toc326301914)

[Scenarios resulting in an incompatible state 31](#_Toc326301915)

[FIM 2010 R2 Kerberos Settings 34](#_Toc326301916)

[What is Kerberos? 34](#_Toc326301917)

[What are SPNs? 35](#_Toc326301918)

[How are tickets decrypted 35](#_Toc326301919)

[Kernel-Mode Authentication 36](#_Toc326301920)

[SPNs and the SharePoint Web Application Account 36](#_Toc326301921)

[SPNs and the FIM Service Account 38](#_Toc326301922)

[SPNs and the FIM Service Database 39](#_Toc326301923)

[SPNs and Self-Service Password Reset 39](#_Toc326301924)

[SPNs for FIM 2010 R2 42](#_Toc326301925)

[Duplicate SPNs 44](#_Toc326301926)

[Delegation 45](#_Toc326301927)

[Delegation and SharePoint Web Application Pool Account 45](#_Toc326301928)

[Delegation and FIM Service Account 47](#_Toc326301929)

[Delegation and Self-Service Password Reset 49](#_Toc326301930)

[Enforcing Kerberos on the FIM Portal 50](#_Toc326301931)

[Deploying Forefront Identity Manager 2010 R2 51](#_Toc326301932)

[Deploying Forefront Identity Manager 2010 R2 51](#_Toc326301933)

[Hardware and Software Requirements 51](#_Toc326301934)

[Required Hardware 51](#_Toc326301935)

[Required Software 52](#_Toc326301936)

[FIM Synchronization Service Software Requirements 52](#_Toc326301937)

[FIM Service Software Requirements 53](#_Toc326301938)

[FIM Portal, FIM Password Registration Portal, and FIM Password Reset Portal Software Requirements 55](#_Toc326301939)

[FIM Reporting Software Requirements 57](#_Toc326301940)

[FIM Add-ins and Extensions Components Software Requirements 57](#_Toc326301941)

[Before You Begin 58](#_Toc326301942)

[Creating an E-mail-Enabled Domain Service Account to Run the FIM Service 59](#_Toc326301943)

[Creating a Domain Service Account to Run the FIM Synchronization Service 59](#_Toc326301944)

[Creating a Domain FIM Service Management Agent Account 59](#_Toc326301945)

[Understanding the Purpose of the FIM Service Management Agent Account 59](#_Toc326301946)

[Create a domain service account to run the FIM Password Service 60](#_Toc326301947)

[Create a domain service account to run the SharePoint Service 60](#_Toc326301948)

[Configuring the Service Accounts Running the FIM 2010 R2 Server Components in a Secure Manner 60](#_Toc326301949)

[Ensuring That the Exchange Web Service and IIS Default Web Site are Not Both Configured to Use Port 80 61](#_Toc326301950)

[Ensuring That English Is Installed for SharePoint 61](#_Toc326301951)

[Ensuring That a SharePoint Default Web Site Is Installed 62](#_Toc326301952)

[Selecting the Correct Identity for the SharePoint Application Pool 62](#_Toc326301953)

[Implementing Secure Sockets Layer for FIM Portal 63](#_Toc326301954)

[Configuring SQL Server 64](#_Toc326301955)

[Configuring SQL Server Aliases 65](#_Toc326301956)

[Configuring SQL Server Collation Settings 65](#_Toc326301957)

[Configuring System Center Service Manager 2010 SP1 (SCSM 2010 SP1) 66](#_Toc326301958)

[Establishing SPNs for FIM 2010 R2 66](#_Toc326301959)

[Installing the FIM 2010 R2 Server Components 68](#_Toc326301960)

[Installing the FIM 2010 R2 Server Components 68](#_Toc326301961)

[FIM Synchronization Service 69](#_Toc326301962)

[FIM Service and Portal 75](#_Toc326301963)

[Post-Installation Tasks 87](#_Toc326301964)

[Add the FIM Service service account to the FIM Synchronization Service security groups 88](#_Toc326301965)

[Configuring the FIM Service Service Exchange mailbox 88](#_Toc326301966)

[Disabling SharePoint indexing 88](#_Toc326301967)

[Activating the Kerberos protocol only 89](#_Toc326301968)

[Uninstalling the FIM Service and Portal Component of FIM 2010 R2 90](#_Toc326301969)

[Installing the FIM 2010 R2 Add-ins and Extensions 90](#_Toc326301970)

[Installing the FIM 2010 R2 Add-ins and Extensions 90](#_Toc326301971)

[Installing the FIM 2010 R2 Language Packs 95](#_Toc326301972)

[Installing the FIM 2010 R2 Language Packs 95](#_Toc326301973)

[Unattended Installation of FIM 2010 R2 99](#_Toc326301974)

[Unattended installation of FIM 2010 R2 99](#_Toc326301975)

[Pass-in parameters on the command line 100](#_Toc326301976)

[Create an MST file 101](#_Toc326301977)

[Troubleshoot an installation 101](#_Toc326301978)

[Features and properties 101](#_Toc326301979)

[Common Post-installation Configuration for Forefront Identity Manager 2010 R2 114](#_Toc326301980)

[Create a Backup Administrator account for the FIMService after installation 115](#_Toc326301981)

[Isolate log files from data files 115](#_Toc326301982)

[Create additional tempdb files 116](#_Toc326301983)

[Ensure adequate space for log files 116](#_Toc326301984)

[Limit SQL Server memory use 116](#_Toc326301985)

[SQL Server Database Configuration - General 117](#_Toc326301986)

[Presize data and log files 117](#_Toc326301987)

[Configure synchronization rule provisioning 117](#_Toc326301988)

[Active Directory–to–FIM 2010 R2 Initial Data Load 118](#_Toc326301989)

[Step 1: Configure SQL Server for the initial data load 118](#_Toc326301990)

[Step 2: Apply minimum necessary FIM configuration during the load process 119](#_Toc326301991)

[Step 3: Configure and populate the FIM Service with external identity data 119](#_Toc326301992)

[Step 4: Apply your full FIM configuration 119](#_Toc326301993)

[Step 5: Reconfigure SQL Server to previous settings 119](#_Toc326301994)

[Configuring General MPRs 120](#_Toc326301995)

[Enable WCF Performance Counters 121](#_Toc326301996)

# Forefront Identity Manager 2010 R2 Deployment Guide

## Forefront Identity Manager 2010 R2 Deployment Guide

The Forefront Identity Manager 2010 R2 Deployment Guide contains information to help you plan for and deploy FIM 2010 R2, to help you upgrade from FIM 2010, and to help you maintain the FIM 2010 R2 infrastructure.

The following topics introduce the task areas covered in the Deployment Guide:

 [Planning for Forefront Identity Manager 2010 R2](#z15137483fed64fa4812f77e093c39f87)

 [Deploying Forefront Identity Manager 2010 R2](#zed4084eda1964c42b3e889189eca7aa9)

You can download a copy of this technical documentation from the Microsoft Download Center.

# Planning for Forefront Identity Manager 2010 R2

## Planning for Forefront Identity Manager 2010 R2

This section provides major concepts to consider in the design and planning phase. This section provides things that should be considered if you are upgrading or doing a clean installation.

The following topic areas are covered in this section:

 [Considerations for Upgrading to FIM 2010 R2](#z6af07a97afd64fcc83a63e1fd6cafc0f)

 [Considerations for New Installation of FIM 2010 R2](#z70157b620c054b2b90bdc89313c438ff)

 [FIM 2010 R2 Kerberos Settings](#z94c70f01fb454ff09907abc7acbaecbe)

# Considerations for New Installation of FIM 2010 R2

Information technology (IT) professionals can use this Microsoft® Forefront® Identity Manager (FIM) 2010 R2 Deployment Guide to install and maintain FIM 2010 R2. A FIM 2010 R2 deployment has two major groups of components—server side components and client side components.

The server-side components are as follows:

 FIM Synchronization Service

 FIM Service

 FIM Portal

 FIM Certificate Management

 FIM Reporting

 FIM Service and Portal Language Packs

 FIM Password Registration Portal

 FIM Password Reset Portal

The client-side components are as follows:

 FIM Add-in for Outlook®

 FIM Password Reset Extensions

 FIM Add-ins and Extensions Language Pack

## What This Document Covers

This document covers planning considerations, the installation or upgrade of FIM 2010 R2 and several topics to help maintain a FIM 210 R2 environment. It includes the steps that you need to successfully deploy FIM 2010 R2 in your environment. It also describes the installation of each of the components and subcomponents that make up a FIM 2010 R2 installation.

Notes

For a structured walkthrough of a complete FIM 2010 R2 test environment, see:.

 Test Lab Guide: Installing Microsoft® Forefront® Identity Manager (FIM) 2010 R2

 Test Lab Guide: Upgrading to Microsoft® Forefront® Identity Manager (FIM) 2010 R2

## Prerequisite Knowledge

This document assumes that you have a basic understanding of the following:

 Installing software on server and client computers.

 Active Directory® Domain Services (AD DS), Microsoft SQL Server® 2008 or Microsoft SQL Server® 2008 R2 database software, Windows® SharePoint® Services 3.0 or Windows SharePoint Foundation 2010, System Center Management Server, and Microsoft Exchange Server 2007 or 2010.

A description of how to set up and configure dependent technologies such as AD DS, SQL Server, SharePoint, and Exchange Server is outside the scope of this document.

### Audience

This document is intended for IT planners, systems architects, technology decision-makers, consultants, infrastructure planners, and IT personnel who plan to deploy FIM 2010 R2 .

## Topology

FIM 2010 R2 supports a variety of deployment topologies. Each of the main components may either be installed separately or in combination on individual servers. They include the following:

 FIM Service

 FIM Synchronization Service

 FIM Portal

 FIM Password Registration Portal

 FIM Password Reset Portal

 FIM Reporting

 SQL Server 2008 database for the FIM Service

 SQL Server 2008 database for the FIM Synchronization Service

In addition, the FIM Service and the FIM Portal can be scaled to support multiple servers. For more information, see [Overview of Network Load Balancing](http://go.microsoft.com/fwlink/?LinkID=164080) (http://go.microsoft.com/fwlink/?LinkID=164080) and [SharePoint Server Farm Architecture](http://go.microsoft.com/fwlink/?LinkID=129821) (http://go.microsoft.com/fwlink/?LinkID=129821).

## Service Accounts

The following is a list of service accounts and there use with FIM 2010 R2. Before installing FIM 2010 R2 either as a new installation or an upgrade, depending on the specific server components that are to be installed, these service accounts will need to be created.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Account | Server Component | Recommended additional Permissions | Additonal Group Requirements | SPN Required for Constrained Delegation |
| FIM Synchronization Service Account | FIM Synchronization Service | **** Deny logon as a batch job  **** Deny logon locally  **** Deny access to this computer from the network | NA | NA |
| FIM Service Account | FIM Service and Portal | **** Deny logon as a batch job  **** Deny logon locally  **** Deny access to this computer from the network  **** WMI and DCOM permissions for SSPR | **** FIMSyncAdmins  **** FIMSyncBrowse and FIMSyncPasswordSet - for SSPR | FIMService/<FIM Service Server> |
| FIM Management Agent Service Account | FIM Management Agent | NA | NA | NA |
| SharePoint Application Pool Account | SharePoint | NA | NA | HTTP/<FIM Portal Server> |
| FIM Password Registration Application Pool Account | FIM Password Registration | NA | NA | HTTP/<passwordregistration portal server>  See FIM 2010 R2 SSPR Deployment guide for more information |
| FIM Password Reset Application Pool Account | FIM Password Reset | NA | NA | HTTP/<passwordreset portal server>  See FIM 2010 R2 SSPR Deployment guide for more information |
| FIM CM Agent | FIM Certificate Management | No additional permissions required. Permissions will be set by the Configuration Wizard. | NA | NA |
| FIM CM Authorization Agent | FIM Certificate Management | No additional permissions required. Permissions will be set by the Configuration Wizard. | NA | NA |
| FIM CM CA Manager Agent | FIM Certificate Management | No additional permissions required. Permissions will be set by the Configuration Wizard. | NA | NA |
| FIM CM Enrollment Agent | FIM Certificate Management | No additional permissions required. Permissions will be set by the Configuration Wizard. | NA | NA |
| FIM CM Key Recovery Agent | FIM Certificate Management | No additional permissions required. Permissions will be set by the Configuration Wizard. | NA | NA |
| FIM CM Web Pool Agent | FIM Certificate Management | No additional permissions required. Permissions will be set by the Configuration Wizard. | NA | HTTP/<FIM CM Server> See FIM CM Deployment documentation |

# Considerations for Upgrading to FIM 2010 R2

The following sections will provide information on things that need to be considered prior to upgrading. For additional information see the [Forefront Identity Manager 2010 R2 Release Notes](http://technet.microsoft.com/en-us/library/hh322889(v=ws.10).aspx). For a detailed step-by-step guide for upgrading see [Test Lab Guide: Upgrading to Forefront Identity Manager 2010 R2](http://technet.microsoft.com/en-us/library/jj134458(v=ws.10).aspx). This portion of the deployment guide is made up of the following:

 [General FIM 2010 R2 Upgrade Information](#z2)

  [Considerations when Upgrading to FIM 2010 R2](#z3)

 [Considerations when Upgrading to FIM 2010 R2 Synchronization Service](#z4)

  [Considerations when Upgrading to FIM 2010 R2 Service and Portal](#z5)

 [Considerations when Upgrading to FIM Certificate Management 2010 R2](#z6)

 [Backup Information](#z7)

 [Common FIM 2010 R2 Database Upgrade Issues](#z8)

## General FIM 2010 R2 Upgrade Information

Upgrading from FIM 2010 to FIM 2010 R2 is supported for all server components, including those below:

 FIM Service

 FIM Portal

 FIM Synchronization Service

 Microsoft® Forefront Identity Manager Certificate Management (FIM CM) components

Upgrade to FIM 2010 R2 is supported from all builds prior to, and including, build 4.0.3617.2 . To find out what build you are using, click About Forefront Identity Manager on the administrator home page in the FIM portal.

Caution

It is strongly recommended that you upgrade all the FIM Server components in your environment to the same version. Mixing components from FIM 2010 and FIM 2010 R2 is not supported by the FIM product team.

Upgrading from FIM 2010 to FIM 2010 R2 is supported for the client components below:

 FIM Add-ins and Extensions

 FIM CM Bulk Client

 FIM CM Client

 FIM Password Change Notification Service (PCNS)

The following is the supported upgrade paths for Forefront Identity Manager 2010 R2.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Upgrade from-> | FIM 2010 RTM | FIM 2010 RTM Update 1 | FIM 2010 RTM Update 2 | FIM 2010 RTM Update 2 with June QFE | FIM 2010 R2 RC | FIM 2010 R2 RC Refresh |
|  | (4.0.2592.0) | (4.0.3531.2) | (4.0.3606.2) | (4.0.3617.2) | (4.1.1906.0) | (4.1.2089.0) |
| Is supported? | Yes | Yes | Yes | Yes | Yes\* | Yes\* |

Warning

If you have installed the FIM Portal on SharePoint whose URL is something other than http://localhost, you will be required to upgrade to QFE build 4.0.3617.2 prior to upgrading. For information about this see [KB 2688078](http://support.microsoft.com/kb/2688078).

\* Upgrading the FIM 2010 R2 RC Service and Portal is only supported for TAP customers.

\* Upgrading the FIM 2010 R2 RC SSPR Portals (Registration and Reset) is not supported even for TAP customers. These will need to be uninstalled and re-installed.

The following are the steps required in Upgrading. For a detailed step-by-step upgrade that includes upgrading SQL Server and SharePoint see Test Lab Guide: Upgrading to Forefront Identity Manager 2010 R2. The estimated time is based on internal Microsoft upgrades.

|  |  |  |
| --- | --- | --- |
| Step | Description | Estimated time |
| 1 | Backup FIM Synchronization Encryption key (see Backup the FIM Synchronization Service Encryption Key ) and FIM Synchronization Server configuration (see Backup the FIM Synchronization Service Server Configuration) |  |
| 2 | (Optional) If you are upgrading the Service and Portal Language Packs, you need to backup any customized RCDCs prior to upgrade (see [Backup all Resource Control Display Configuration (RCDC) Objects](#z9)). |  |
| 3 | Disable sync jobs and DB backup job (if applicable) on Sync Server |  |
| 4 | Backup FIM Service Server Configuration (see Backup the FIM Service Configuration) |  |
| 5 | Backup FIMService DB, FIMSync DB ([read more here](http://technet.microsoft.com/en-us/library/hh322919(v=ws.10).aspx) about backup) |  |
| 6 | Change SQL to Simple Recovery on all SQL servers |  |
| 7 | Upgrade sync engine to R2 | ~ 4 hours |
| 8 | Enable SQL Broker on the FIM Service DB by ALTER DATABASE <FIM Service DB name> SET ENABLE\_BROKER | < 5 min |
| 9 | Upgrade FIM Service and Portal | ~30 min |
| 10 | Upgrade FIM Language Pack(s) (if applicable) | 5-10 hours |
| 11 | [optional]Change SQL to Full Recovery on server with SharePoint | < 5 min |
| 12 | [optional] Backup SharePoint DB |  |
| 13 | [optional] Upgrade SharePoint to SP2010 | 30 min |
| 14 | [optional] Disable SharePoint 2010 search index job |  |
| 15 | Perform full Portal UI client side test to confirm major features are working | 30 min |
| 16 | Run all import / export jobs and verify sync operations are working | a few hours |
| 17 | Re-enable jobs disabled in Step 3 |  |

For a list of service accounts that may be required, depending on the server components that are to be installed during upgrade, see [Service Accounts](#z1) earlier in this document.

## Considerations when Upgrading to FIM 2010 R2

The following are considerations that must be taken into account when upgrading to FIM 2010 R2. These considerations are general things that need to be taken into account.

### Upgrading Outlook 2007 to Outlook 2010 and the FIM Add-ins and Extensions

Prior to upgrading to Outlook 2010 from Outlook 2007 you must uninstall the FIM add-in, then re-install it. It doesn’t matter if this is done before or after the upgrade to Outlook 2010

### Specifying a Very Long File Path Can Cause Extraction to Fail

If the directory you selected for extracting the product files is deep in the folder hierarchy, the total file path can exceed 255 characters. Extraction will fail with the message, "Can't create output file." To avoid this issue, select a short path name to the extraction directory.

### Error when upgrading with existing certificate

Users attempting to upgrade from FIM 2010 RTM QFE 4.0.3576.2 to FIM 2010 R2 while using the "Reuse Existing Certificate" option may experience the error "Service 'Forefront Identity Manager Service' (FIMService) failed to start. Verify that you have sufficient privileges to start system services." If you encounter this error, re-run setup with the "Generate New Certificate" option selected in the Service and Portal setup.

If you are using a custom certificate on FIM 2010, make sure that the certificate name is ForefrontIdentityManager, otherwise upgrade will fail. If your certificate is name differently, follow these steps:

1. Issue a new certificate with the name ForefrontIdentityManager as the subject.

2. On FIM 2010 (not FIM 2010 R2 ), run a re-install in Change mode.

3. Point to the new certificate.

4. Run the FIM 2010 R2 upgrade.

## Considerations when Upgrading to FIM 2010 R2 Synchronization Service

The following are considerations that must be taken into account when upgrading to FIM Certificate Management 2010 R2. These considerations deal strictly with upgrading.

### Synchronization engine database upgrade can fill up transaction log and fail when database recovery mode is set to Full

If you have a large database and configure the recovery mode for Full, it is possible that the database upgrade will fail due to the transaction log becoming full. In this case, the upgrade will be rolled back with an error message indicating the transaction log is full. Set the recovery mode to Simple and retry the upgrade.

### Ignore message to delete MAdata folder during upgrade

During upgrade of FIM Synchronization Service from FIM 2010 to FIM 2010 R2 you will see a popup asking you to manually remove the MAdata folder. This popup should be ignored and the MAdata folder should not be removed.

## Considerations when Upgrading to FIM 2010 R2 Service and Portal

The following are considerations that must be taken into account when upgrading to FIM Certificate Management 2010 R2. These considerations deal strictly with upgrading.

### All existing resources with the FIM owned schemas are deleted during installation

When installing FIM 2010 R2, the database upgrade scripts will delete all existing objects within the FIM owned schemas, (stored procedures, functions, etc...), with the exceptions of the tables themselves, and will replace them with the FIM 2010 R2 versions. If you've added your own stored procedures or functions to the FIM owned schemas, they will be deleted.

### Language packs must be uninstalled before the FIM Service

If you uninstall FIM 2010 R2, you must uninstall any FIM language packs before uninstalling the FIM Service. If you do not, you will see the error “SharePoint did not confirm the retraction of the FIM solution pack within the expected time”

### “SharePoint Timer Service is not running” error during installation

If you have already upgraded Window SharePoint Services 2007 to Microsoft SharePoint 2010, and then attempt to upgrade FIM 2010 to FIM 2010 R2, you may encounter the error “The SharePoint Timer Service is not running.” To resolve this issue, it is recommended that you upgrade to [FIM 2010 Update Rollup 2 (build 4.0.3606.2)](http://support.microsoft.com/kb/2635086)( or later before attempting to do a major upgrade to R2.

If you have not yet upgraded Window SharePoint Services 2007 to Microsoft SharePoint 2010, but plan to, first upgrade FIM 2010 to FIM 2010 R2, and then upgrade Windows SharePoint Services 2007.

### Verify the SharePoint 2010 Administration Service is running

If you upgraded SharePoint WSS 3.0 to SharePoint Foundation 2010 verify that the SharePoint Administration Service is running prior to beginning your upgrade. To do this use the following procedure:

To verify the SharePoint 2010 Administration Service is running

|  |
| --- |
| 1. Log on the FIM Portal server.  2. Click Start, select Administrative Tools, and then click Services. This will open the Services MMC.  3. On the right, scroll down to the SharePoint Administration Service and verify that it is Started.  4. If it is not Started, right-click on SharePoint Administration Service and select Start.  5. Once it starts, close Services. |

## Considerations when Upgrading to FIM Certificate Management 2010 R2

The following are considerations that must be taken into account when upgrading to FIM Certificate Management 2010 R2. These considerations deal strictly with upgrading.

### Upgrade Considerations

 When upgrading to FIM CM 2010 R2, the server should always be upgraded first and then the clients. The older clients will work with the newer version of the server but newer clients will not work with an older version of the server. Therefore, it is imperative that the upgrade be done in this order.

Warning

This is the only supported method of upgrading.

 If you are upgrading from CLM 2007 and want to upgrade to FIM CM 2010 R2, then the CLM 2007 server must first be upgraded to FIM CM 2010 RTM (build 4.0.2592.0) and then it can be upgraded to FIM CM 2010 R2 (build 4.1.2273). This is the only supported upgrade method. Upgrading from CLM 2007 directly to FIM 2010 R2 is not supported.

 When you upgrade from FIM CM 2010 RTM (build 4.0.2592.0) to FIM CM 2010 R2 RTM (build 4.1.2273) in a topology including a separated sub-CA, and the sub-CA upgrade is done before the FIM CM 2010 RTM server, the FIM CM database is not updated with the new version of FIM CM exit module for the sub-CA . As a result smartcard operations fail for profile templates that include certificate templates of the sub-CA, with error "The version of FIM CM Server [4.1.2273] does not match the version of the FIM CM CA Exit Module [4.0.2592.0] installed on the CA [the\_name\_of\_Sub-CA]".

This is because the way CA registration works is once Certificate Services starts, the FIM CM exit module will attempt to connect to the SQL database and register itself. It will attempt to write it’s version number to the database. The reason it fails, in this case, is because FIM CM 2010 RTM doesn’t have that particular stored procedure. Once you install FIM CM 2010 R2 on the server and restart certificate services on the sub-CA it will work correctly.

## Backup Information

The following sections provide information on the various components of a FIM 2010 deployment that should be backed up prior to upgrading. These include:

 [Backup the FIM Synchronization Service Server Configuration](#z10)

 [Backup the FIM Service and Portal Configuration](#z11)

 [Backup the FIM Synchronization Service and FIM Service databases](#z12)

### Backup the FIM Synchronization Service Server Configuration

The following procedure details how to backup the FIM Synchronization Service Server Configuration.

To back up the FIM Synchronization Service Server Configuration

|  |
| --- |
| 1. Log on to the FIM Synchronization Server  2. Click Start, select All Programs, click Microsoft Forefront Identity Manager, and click Synchronization Service. This will bring up the Forefront Identity Synchronization Service.  3. At the top, click File and select Export Server Configuration. You will be prompted with a window that says not to run any management agents or modify the server settings. Click OK.  4. This will bring up a Browse For Folder dialog. Navigate to a directory to save the configuration. Click OK.  5. Once this has completed, click OK. |

### Backup the FIM Service and Portal Configuration

The following procedure details how to backup the FIM Service Configuration using the new Configuration Backup Tool. Be aware that this occurs automatically when doing an upgrade to FIM 2010 R2.

To back backup the FIM Service Configuration

|  |
| --- |
| 1. Log on to the FIM Service server.  2. Open cmd.exe and navigate to the directory that has the FIM 2010 R2 binaries and proceed to the following location Service and Portal\Program Files\Microsoft Forefront Identity Manager\2010\Tools\ConfigurationBackup  3. Type Microsoft.IdentityManagement.ConfigurationBackup and hit enter. This will begin the backup.  4. Once this completes, navigate to C:\Program Files\Microsoft Forefront Identity Manger\2010\Previous Configuration\FIM1\(today's date and time) or (current timestamp)\ and notice the Portal, Service folders and the ConfigurationBackup text.    5. Copy the folder with the today’s date to a safe location. |

### Backup the FIM Synchronization Service and FIM Service databases

The following procedure details how to backup the FIM Synchronization Service and FIM Service databases. You may need to work with your SQL Administrators to make this happen. Ensure that nothing is running on the FIM Service Server or the FIM Synchronization Server prior to backing up the databases.

To backup the FIM Synchronization Service and FIM Service databases

|  |
| --- |
| 1. Log on to your SQL Server. This may be separate servers if the databases reside on different servers.  2. Click Start, click All Programs, click Microsoft SQL Server 2008, and then click SQL Server Management Studio. This will launch SQL Server Management Studio.  3. On the Connect to Server dialog box, under Server Type select Database Engine.  4. On the Connect to Server dialog box, under Server name select APP1.  5. On the Connect to Server dialog box, under Authentication select Windows Authentication.  6. Click Connect. This should be successful and the database information will be displayed on the left. The SQL Server Agent should have a green arrow.  7. On the left, expand Databases, right-click FIMService, and select Tasks, and the select Back Up…. This will bring up the Backup Database - FIMService screen.    8. Click OK.  9. Once this has completed you will see a window that says the backup was successful. Click OK.  10. On the left, under Databases, right-click FIMSynchronizationService, and select Tasks, and the select Back Up…. This will bring up the Backup Database - FIMService screen.  11. Click OK.  12. Once this has completed you will see a window that says the backup was successful. Click OK.  13. Now, navigate to C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Backup  14. Copy FIMService.bak and FIMSynchronizationService.bak to a safe location. |

### Backup all Resource Control Display Configuration (RCDC) Objects

An upgrade (or patch) of the Forefront Identity manager Language packs overwrites the Resource Control Display Configuration (RCDC) objects in the database. Due to this, customers can potentially lose all their customizations to localized strings used on the FIM Portal.

If you have customized localized resources on your FIM Portal, you must follow the guidelines in this document to make sure you don’t lose your customizations.

#------------------------------------------------------------------------------------------------------

# Copyright (c) Microsoft Corporation. All rights reserved.

# Script to back all the Resource Control Display Configuration Objects

# This script is intended to be run before upgrade to FIM 2010 R2

#------------------------------------------------------------------------------------------------------

#------------------------------------------------------------------------------------------------------

# Script Parameter Declarations

param

(

# Data Warehouse machine name

[parameter(Mandatory=$false)]

[String]$ConfigurationBackupPath = "C:\FIMBackup"

)

# End Script parameter declarations

#------------------------------------------------------------------------------------------------------

#------------------------------------------------------------------------------------------------------

# Script constant declarations

Set-Variable -Name constantFIMPowerShellSnapInName -Option Constant -Value "FIMAutomation" -ErrorAction SilentlyContinue

Set-Variable -Name constantRCDCFolderName -Option Constant -Value "ResourceControlDisplayConfiguration" -ErrorAction SilentlyContinue

Set-Variable -Name constantRCDCObjectFilter -Option Constant -Value "/ObjectVisualizationConfiguration" -ErrorAction SilentlyContinue

Set-Variable -Name constantLineSeperator -Option Constant -Value "----------------------------------------------------------------------------------------------------------" -ErrorAction SilentlyContinue

# End Script constant declarations

#------------------------------------------------------------------------------------------------------

#------------------------------------------------------------------------------------------------------

# Function definitions

#--------------------------------------------------------------

# Checks to see if the user running the script is an

# administrative user

#--------------------------------------------------------------

function In-Administrator-Mode

{

# check that current user is in administrators group.

try

{

# get the current user who is executing the script.

$currentUser = [System.Security.Principal.WindowsIdentity]::GetCurrent()

$windowsPrincipal = New-Object System.Security.Principal.WindowsPrincipal($CurrentUser)

# Is the user in the Admin grooup.

return $windowsPrincipal.IsInRole("Administrators")

}

catch

{

Write-Error $\_

return $false

}

}

#--------------------------------------------------------------

# Checks to see if the FIMAutomation is installed.

#--------------------------------------------------------------

function Is-FIM-Powershell-SnapIn-Registered

{

try

{

# get registry key value

Add-PSSnapin -Name $constantFIMPowerShellSnapInName -ErrorAction SilentlyContinue

return $true

}

catch

{

Write-Error $\_

return $false

}

}

#--------------------------------------------------------------

# Writes an informational message to the Console

# $message : message text to be written to the console

#--------------------------------------------------------------

function Write-Informational-Message([String]$message)

{

Write-Host $message -ForegroundColor "green"

}

#--------------------------------------------------------------

# Writes an error message to the Console

# $message : message text to be written to the console

#--------------------------------------------------------------

function Write-Error-Message([String]$message)

{

Write-Host $message -ForegroundColor "red"

}

#--------------------------------------------------------------

# Saves the RCDC objects to files

# $rcdcs : List of objects to be saved

# $filePath : Path to save the files at.

#--------------------------------------------------------------

function Save-RCDC-Objects([Object[]]$rcdcs, [String]$filePath)

{

foreach($rcdc in $rcdcs)

{

$fileName = $rcdc.ResourceManagementObject.ObjectIdentifier.Substring(9) + ".xml"

$fullPath = Join-Path -Path $filePath -ChildPath $fileName

ConvertFrom-FIMResource $rcdc -File $fullPath

}

}

# End Function declarations

#------------------------------------------------------------------------------------------------------

#------------------------------------------------------------------------------------------------------

# Main Script Logic

try

{

Write-Host $constantLineSeperator

Write-Informational-Message "Resource Control Display Configuration backup script."

Write-Informational-Message "This script will back up all resource control display configuration objects."

# Check to see if the script is being run by an administrative user

$inAdminMode = In-Administrator-Mode

if ($inAdminMode -ne $true)

{

Write-Error-Message "This script is not being run by an administrator. Please re-run script as an administrative user"

EXIT

}

# check to see if the FIM powershell snapin is installed

Write-Host $constantLineSeperator

Write-Informational-Message "Starting Pre-Requisite checks before script execution"

Write-Host $constantLineSeperator

Write-Informational-Message "Pre-Requisite check #1"

Write-Informational-Message "Checking to see if FIM commandlets are installed"

$isFIMPSSnapinInstalled = Is-FIM-Powershell-SnapIn-Registered

if($isFIMPSSnapinInstalled -eq $false)

{

Write-Error-Message "FIM commandlets are not installed on this machine. Please run the script on a machine where FIM service is installed."

Write-Host $constantLineSeperator

EXIT

}

Write-Informational-Message "FIM commandlets are installed on local machine"

# check to see if the configuration back-up path is valid

Write-Informational-Message "Pre-Requisite Check #2"

Write-Informational-Message "Checking to see if the configuration backup folder path is valid"

if((Test-Path $ConfigurationBackupPath -PathType container) -ne $true)

{

Write-Informational-Message "Configuration Backup directory does not exist. Creating the directory"

New-Item $ConfigurationBackupPath -type directory | out-null

Write-Informational-Message "Configuration Backup directory created"

}

Write-Informational-Message "All Pre-Requisite checks passed."

Write-Host $constantLineSeperator

Write-Host $constantLineSeperator

Write-Informational-Message "Setting up folders to backup the configuration settings"

Write-Host $constantLineSeperator

# check to see if the RCDC folder is already present. If not, create it.

$rcdcPath = Join-Path -Path $ConfigurationBackupPath -ChildPath $constantRCDCFolderName

$saveMessage = "The configuration settings will be saved at : " + $rcdcPath

Write-Host $saveMessage -foregroundcolor "yellow"

if((Test-Path $rcdcPath -PathType container) -eq $true)

{

Write-Informational-Message "The specified directory is already present"

if((Get-ChildItem $rcdcPath) -ne $null)

{

Write-Informational-Message "There is already a saved back-up in this directory"

Write-Informational-Message "Please save the contents in another directory before re-running this script"

Write-Host $constantLineSeperator

EXIT

}

}

else

{

Write-Informational-Message "Creating the resource control display configuration backup directory"

New-Item $rcdcPath -type directory | out-null

Write-Informational-Message "Created the resource control display configuration backup directory"

}

# get all the rcdc objects from the FIM Service store.

Write-Host $constantLineSeperator

Write-Informational-Message "Gathering all resource control display configuration objects"

$rcdcObjects = Export-FIMConfig -CustomConfig $constantRCDCObjectFilter

$resultMessage = "Found " + $rcdcObjects.Count + " objects"

Write-Informational-Message $resultMessage

Write-Host $constantLineSeperator

# Write them out to files as XML

Write-Host $constantLineSeperator

Write-Informational-Message "Saving all the resource control display configuration objects"

Save-RCDC-Objects $rcdcObjects $rcdcPath

Write-Informational-Message "Successfully saved all the resource control display configuration objects"

Write-Host $constantLineSeperator

}

catch [Exception]

{

Write-Error-Message "Script execution failed with the following exception message"

Write-Host $\_.Exception.ToString()

}

# End Script code

#------------------------------------------------------------------------------------------------------

Use the following procedure to backup and restore the RCDC once the upgrade is complete:

To backup and restore the RCDC configuration

|  |
| --- |
| 1. Run the PowerShell Script to back up your RCDCs  Warning  This should be the first step before upgrading / patching the langpacks  This script backs up all the ObjectVisualizationConfiguration objects as XML files which are exported by FIM Automation cmdlets. There is a file created for each object and the name of the file is the Object Identifier (GUID) for the object.  The script takes one parameter:  Parameter : ConfigurationBackupPath  Use this parameter to specify a custom backup folder. This parameter is optional.  The default is: C:\FIMBackup\ResourceControlDisplayConfiguration\  The script verifies whether the following three prerequisites are satisfied before processing the script code:  a. The script must be run by a user with administrative rights.  b. The script must be run on a computer running the FIM service.  c. The script must be run by a user that has write permissions to ConfigurationBackupPath.  If any of these conditions are not satisfied, the script stops and an error is displayed.  2. Upgrade / Patch the FIM Language Pack  Once you have backed up these resources, you may proceed to upgrade / patch the FIM language packs. When the upgrade completes, you will no longer see your localized customizations on the portal. The following steps describe how to bring your customizations back from the backed up resources.  3. Compare FIM Configurations  In order to make meaningful use of the backed up data, you will need to compare the backed up configuration with the new configuration that is in your database after the upgrade / patch. Each of these steps must be performed per configuration object that you believe was customized, using the GUID of the object.Export database configuration to begin the comparison process  $newConf = Export-FIMConfig –customConfig “/ObjectVisualizationConfiguration[ObjectID=”<ObjectGUID>”]”  Convert the saved XML files into FIM Objects for comparison  $oldConf = ConvertTo-FIMResource –file <full path to backed-up objectGUID.xml>  Join the two configurations lists  $matches = Join-FIMConfig –source $newConf –target $oldConf  Important  The command also requires a –join parameter that specifies attributes to join on. Ex : $joinCriteria = @{“ObjectVisualizationConfiguration” = “DisplayName”}  Compare the attributes of the objects (This needs to be done per match.)  $changes = Compare-FIMConfig $matches  4. Import FIM Config to finally bring back your customizations  To bring back your customizations, you must run the following cmdlet:  Import-FIMConfig $changes  When the cmdlet finishes, the object represented by <GUID> is imported into your database, and carries the changes that you had made previously.  Repeat steps 2 – 4 for each object that contains customized localization data in it for your portal. |

For additional information see [Compare-FIMConfig](http://technet.microsoft.com/en-us/library/ff394180.aspx) cmdlet.

For additional information see [Import-FIMConfig](http://technet.microsoft.com/en-us/library/ff394178) cmdlet.

## Common FIM 2010 R2 Database Upgrade Issues

This section outlines problems that can be faced during an upgrade of the Forefront Identity manager – the database upgrade step. It also outlines what needs to be done in these cases.

The Forefront Identity Manager 2010 (FIM) R2 supports an upgrade from prior versions of the product (e.g. FIM 2010 RTM).

Warning

An upgrade to FIM 2010 R2 is a ‘major’ upgrade. The older version of the product will be uninstalled before installing the new version.

During an upgrade of FIM, two high level operations take place:

1. Install the new FIM Service binaries

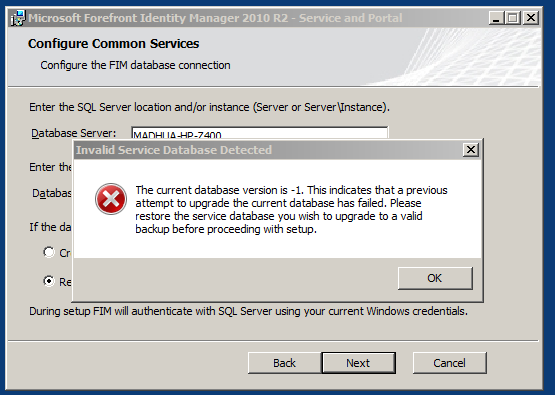
2. Upgrade of the FIM Service Database

Since the FIM Service and FIM Service Database are tied to each other, it is necessary that the version of the FIM Service Database be the same as the version that the FIM Service expects to work with. If the upgrade of the FIM Service Database fails during setup, it will cause a rollback of setup and may leave the FIM Service Database and FIM Service in an incompatible state.

### Scenarios resulting in an incompatible state

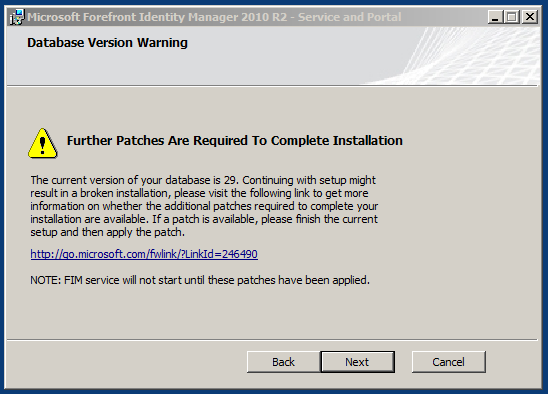
The issue appears during FIM Service and Portal setup with re-use database option selected and the database is in one of the following states:

1. Database is one where upgrade has previously failed– during an upgrade, database upgrade may have failed due the below two reasons or because requests to the SQL server may have failed. These failures leave the database in an inconsistent condition, and you will see the following error during setup:

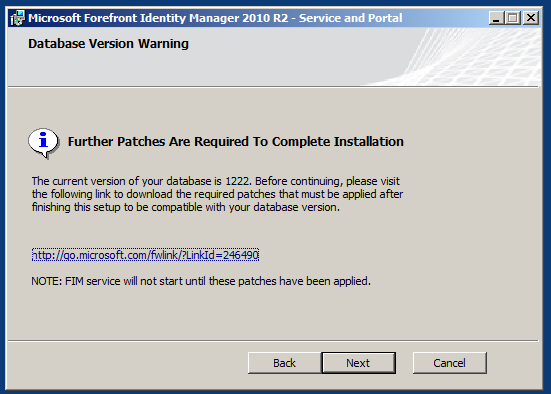


2. Database version is unknown to setup to upgrade from - this will happen when your current database is the result of applying a Hotfix / Update to your current product that was released before the latest version of the product was released.

For example, your current installation is FIM 2010 RTM + Update 3 and you want to upgrade to FIM 2010 R2 RTM. Since Update 3 (will be) released after FIM 2010 R2 RTM, database upgrade in FIM 2010 R2 RTM doesn’t know how to upgrade from Update 3. In this case you’ll need to install a patch that will make it possible for FIM 2010 R2 RTM to recognize your database version successfully. You will see a warning similar to the following during setup:



3. Database version is newer than what setup can upgrade to– this will happen when your current database is the result of applying a Hotfix / Update to the base release of the product. For example, you installed FIM 2010 RTM + Update 1 on one instance (machine). You now want to install another instance pointing to the same database using the ‘reuse database’ option. In this case your existing database (on the first instance) is newer (Update 1’s database version) than what FIM 2010 RTM’s setup can upgrade to. Database upgrade fails in this condition. You will see an information dialog similar to the below, during setup:



# FIM 2010 R2 Kerberos Settings

The following section is presented to explain Kerberos and how it pertains to FIM 2010 R2.

## What is Kerberos?

The Kerberos authentication protocol provides a mechanism for authentication — and mutual authentication — between a client and a server, or between one server and another server. The Kerberos authentication protocol originated at MIT more than a decade ago, where it was developed by engineers working on Project Athena. The Kerberos protocol is more secure, more flexible, and more efficient than NTLM. The benefits gained by using Kerberos authentication are:

 Delegated Authentication

 Interoperability

 More efficient authentication to servers.

 Mutual authentication

Kerberos authentication has the following authentication dependencies:

1. Operating System - client must be XP or later and server must be 2000

2. TCP/IP connectivity - network connectivity must exist between client, domain controller and target server

3. DNS - DNS must be functioning for the client to obtain the FQDN. The FQDN is used to access the domain controller.

4. Active Directory

5. Time Service

6. SPN - Service principal names (SPNs) are unique identifiers for services running on servers.

### What are SPNs?

Service principal names (SPNs) are unique identifiers for services running on servers. Every service that uses Kerberos authentication needs to have an SPN set for it so that clients can identify the service on the network. If an SPN is not set for a service, clients have no way of locating that service. Without correctly set SPNs, Kerberos authentication is not possible.

An SPN is registered in Active Directory under a user account as an attribute called Service-Principal-Name. The SPN is assigned to the account under which the service the SPN identifies is running. Any service can look up the SPN for another service. When a service wants to authenticate to another service, it uses that service's SPN to differentiate it from all of the other services running on that computer.

Because multiple services can run simultaneously under the same account, setting an SPN requires four unique pieces of information. These four pieces of information uniquely identify any service running on a network and can be used to mutually authenticate to any service.

For each SPN that is set, the following information is required:

1. The type of service, formally called a service class. This enables you to differentiate between multiple services running under the same account.

2. The account under which the service is running.

3. The computer on which the service is running, including any aliases that point to that computer.

4. The port on which the service is running (optional if the default port for the service of that type is used such as port 80 for HTTP).

The syntax of an SPN itself is service/hostname:port, where:

1. Service is the service class of the SPN.

2. Hostname is the computer to which the SPN belongs.

3. Port is the port on which the service that the SPN is registered to runs.

### How are tickets decrypted

A client makes a HTTP Request to an IIS server running SharePoint. The IIS server denies the request with a 401 Authorization Required and indicates to the client that it supports Kerberos authentication. The client then requests a Service Ticket from the KDC on a Domain Controller. This is done by sending the SPN for that service to the DC. The DC finds the domain account that matches the SPN and creates a ticket for the client. The ticket is encrypted with the password for the domain account of the receiving application, for example the SharePoint service account. The DC returns the Service ticket to the client. The client, then sends the ticket to IIS, in the authentication header to prove the identity of the client. To decrypt the ticket IIS must know the password of the domain account, in this case, the SharePoint service account. The password for this account is encrypted and stored in the applicationHost.config file. IIS will then decrypt the ticket.

### Kernel-Mode Authentication

With the release of IIS 7.0 on Windows Server 2008 and IIS 7.5 on Windows Server 2008 R2 a new mode kernel-mode authentication was introduced. This means that the ticket for the responding service is decrypted using the Machine account (Local System) of the IIS Server. It no longer depends on the application pool Identity for this purpose by default. You no longer need to worry about the correlation between HTTP SPNs and the Application pool Identity that was required in the earlier versions of IIS.

By default, UseKernelMode Authentication is set to true automatically on the applicationHost file after the password registration and password reset portals have been installed.

### SPNs and the SharePoint Web Application Account

FIM 2010 R2 requires either the use of IIS 7.0 or IIS 7.5. However, with regard to SharePoint we cannot take advantage of Kernel-Mode and use the machine account to decrypt tickets. This is because even in a single-mode install of SharePoint the server runs as a “farm”. In this instance, the KDC will not know in advance which individual server the request may go to and hence ticket decryption may fail. Also, kernel-mode authentication is currently not supported on SharePoint Foundation 2010 (http://technet.microsoft.com/en-us/library/gg502606.aspx).

The recommended way to set this up is to disable Kernel-mode authentication and then allow the Application pool's identity be used for Kerberos ticket decryption. In this instance you must ensure that useAppPoolCredentials is set to true. This will force IIS to use the appPoolCredentials to decrypt the ticket. Use the following procedure to use the Application pool’s identity for Kerberos ticket decryption.

To configure IIS to use CORP\SPService for Kerberos Ticket Decryption

|  |
| --- |
| 1. On the server running SharePoint navigate to the following directory: C:\Windows\System32\inetsrv\config.  2. Locate the ApplicationHost.config file, right-click and select Open. This will bring up a pop-up that states Windows cannot open this file and it will have two options. Choose Select a program from a list of installed program, and click OK.  Warning  Prior to making any changes to the ApplicationHost.config file you should make a backup of this file and store it in a safe place.  3. Select Notepad, and click OK. This will open the config file in Notepad.  4. At the top, select Edit, Find, type the following text in the box, and then click Find Next:  windowsAuthentication enabled=”true”  5. You should now see the first instance and it will look like the Before image below. Insert useKernelMode=”false” useAppPoolCredentials=”true” in the line so it looks like the After image.  ApplicationHost.config Before    ApplicationHost.config After    6. Click Find Next and repeat the above steps. There should be a total of three instances that need to have useKernelMode=”false” useAppPoolCredentials = “true” added. Two of the instances will have useKernelMode=”false” already present. These can be ignored.  Warning  There will be instances of windowsAuthentication enabled=”false”. These can be ignored. We only want to change the ones that are set to true.  7. When you finish the last one, a window will pop-up and state that it cannot find windowsAuthentication enable=”true”. Click OK.  8. On the Find box, click Cancel.  9. At the top of Notepad, select Save. Close Notepad.  10. Click Start, click All Programs, click Accessories, and then click Command Prompt. This will launch a Command Prompt window.  11. In the Command Prompt window, type the following text, and then hit Enter:  iisreset  This will stop and then restart IIS. Once this completes, close the Command Prompt window. |

Now set the SPN for the SharePoint Web Application Pool account using the following format:

 HTTP/<FIM Portal Alias>

The SPNs can be set on the Web Application Pool account from a command prompt using SetSPN.exe. The following is an example of setting an SPN on the CORP\SPService account. The FIM Portal alias is fim1. The FIM Portal FQDN is fim1.corp.contoso.com The examples:

Setspn -S HTTP/fim1 corp\SPService

Setspn -S HTTP/fim1.corp.contoso.com corp\SPService

### SPNs and the FIM Service Account

The FIM Service account requires only one SPN for the FIM Service. Use the following format:

 FIMService/<alias> <domain>\<serviceaccount>

 The <alias> above is the address that is entered during FIM Service setup and used by the clients and the FIM Portal to contact the Web Service. This can be a CNAME or host (A) resource record in DNS. If you are using Network Load Balancing (NLB), this is the name of the cluster.

 The <serviceaccount> above is the account that is used by the FIM Service.

 If you are using several different names—for instance, fully qualified domain names (FQDNs) and NetBIOS names—to contact the server, repeat the steps for every name.

The SPNs can be set on the FIM Service account from a command prompt using SetSPN.exe. The following is an example of setting an SPN on the CORP\FIMService account. The FIM Portal alias is fim1. The FIM Portal FQDN is fim1.corp.contoso.com The examples:

Setspn -S FIMService/fim1 corp\FIMService

Setspn -S FIMService/fim1.corp.contoso.com corp\FIMService

Note

If you want cross forest scenarios to work in a separated environment, that is, portal on different machine than FIM service, then you must also set the FQDN.  To accomplish this, use the following:  setspn.exe –S FIMService/FQDN <domain>\<serviceaccount>

### SPNs and the FIM Service Database

The FIM Service database account requires only one SPN. This allows clients the ability to locate the instance of SQL. Use the following format:

 MSSQLsvc/<SQLDatabase Server>

The SPNs can be set on the FIM Service database account from a command prompt using SetSPN.exe. The following is an example of setting an SPN on the CORP\sqldatabase account. The FIM Service database alias is app1. The FIM Service database FQDN is fim1.corp.contoso.com Port numbers are used to indicate the instance of SQL Server. If you have the FIM Service running on a port other than the default instance, specify that port. The examples:

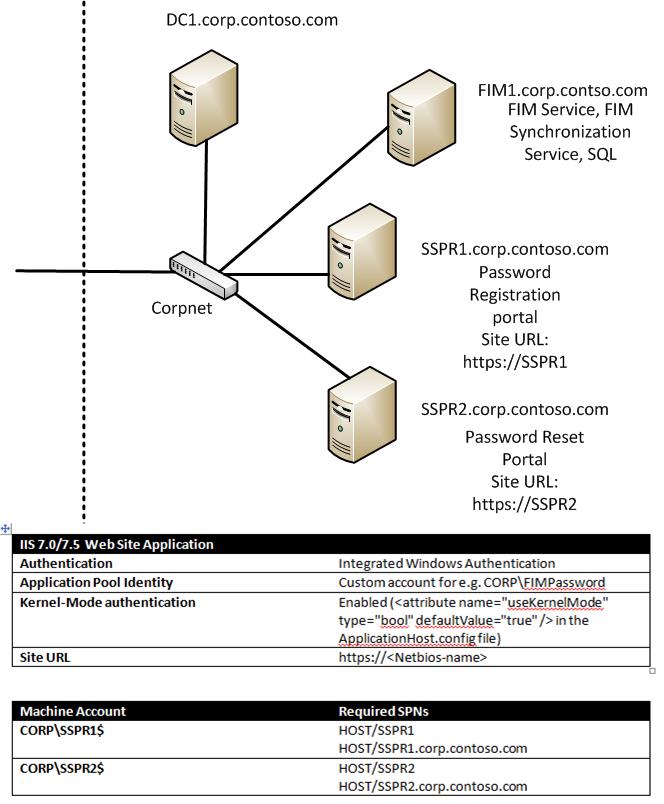
Setspn –S MSSQLsvc/app1:1433 corp\sqldatabase

Setspn –S MSSQLsvc/app1.corp.contoso.com:1433 corp\sqldatabase

### SPNs and Self-Service Password Reset

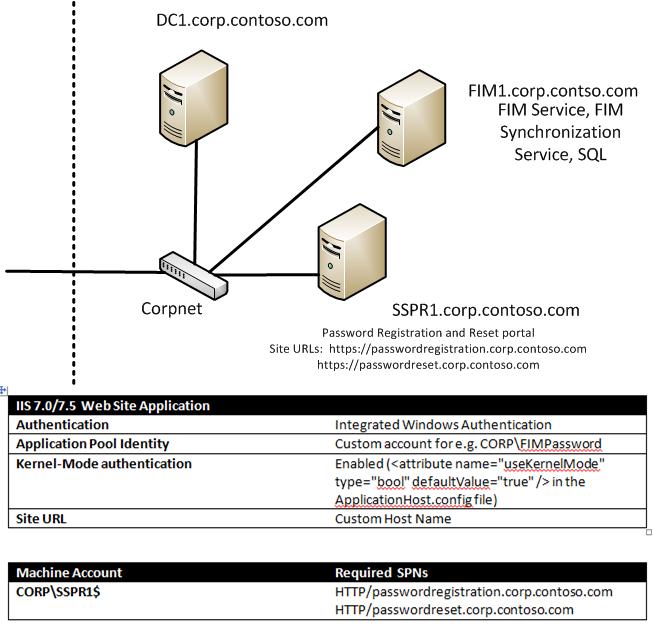
Self-Service Password Reset requires either the use of IIS 7.0 or IIS 7.5. This means that we can take advantage of Kernel-Mode and use the machine account to decrypt tickets. This does not mean however that we can forget entirely about SPNs. Depending on how you have SSPR setup is going to depend on whether or not additional SPNs are required.

Scenario 1



Under this scenario, it is assumed that the password registration and password portal sites are split and being hosted by two dedicated IIS servers. The site URLs used by both are https:<netbios-name>. In this case https://SSPR1 and https://SSPR2 are the site URLs. To access the Password Registration Portal we simply open Internet Explorer and enter https://SSPR1. Likewise, to access the Password Reset Portal we would enter https://SSPR2. In this scenario, the only SPNs that would be required would be on the SSPR1 machine account and the SSPR2 machine account. For instance, on SSPR1, the SPNs would be HOST/SSPR1 and HOST/SSPR1.corp.contoso.com. On SSPR2 they would be HOST/SSPR2 and HOST/SSPR2.corp.contoso.com. In this case, you would not have to set any SPNs because the HOST SPNs are set automatically when the machine is joined to the domain. This however, is not the most likely scenario.

Scenario 2



Under this scenario, the password registration and password portal sites are being hosted on the same IIS server. They have been configured with custom host headers. The site url for the Password Registration site is https://passwordregistration.corp.contoso.com. The site url for the Password Reset site is https://passwordreset.corp.contoso.com. Now because we are using custom host names, SPNs will be required but only for the IIS machine and in the following format:

 HTTP/<custom-site-name>

The SPNs can be set on the IIS machine account from a command prompt using SetSPN.exe. The following are examples:

Setspn -S HTTP/passwordregistration.corp.contoso.com corp\SSPR1$

Setspn -S HTTP/passwordreset.corp.contoso.com corp\SSPR1$

At this point no other SPNs are required. There are no SPNs required on the web application pool account that runs the password registration and the password reset portals. However, you will need to add related DNS A (IPV4) and/or AAAA (IPV6) records for each of the host headers. For a step-by-step example of adding a DNS A record see [Test Lab Guide: Demonstrating the FIM 2010 R2 Self-Service Password Reset with the Q/A Gate](http://technet.microsoft.com/en-us/library/hh826057(v=ws.10).aspx).

### SPNs for FIM 2010 R2

Use the following table for quick reference with regard to the required SPNs for FIM 2010 R2.

|  |  |  |  |
| --- | --- | --- | --- |
| SPN | Account | Setspn Syntax Example | Description |
| MSSQLsvc/<SQLDatabase Server> | SQL Database Account | **** Setspn –S MSSQLsvc/app1.corp.contoso.com:1433 corp\sqldatabase  **** Setspn –S MSSQLsvc/app1:1433 corp\sqldatabase | SPN required for the FIM Service database. Allows clients the ability to locate an instance of SQL. |
| FIMService/<FIM Service Server> | FIM Service Account | **** Setspn –S FIMService/FIM1.corp.contoso.com corp\FIMService  **** Setspn –S FIMService/FIM1 corp\FIMService | SPN required for the FIM Service. Allows clients the ability to locate an instance of the FIM Service. |
| HTTP/<FIM Portal Alias> | SharePoint Service Account | **** Setspn –S HTTP/FIM1.corp.contoso.com corp\SPService  **** Setspn –S HTTP/FIM1 corp\SPService | This is a requirement because SharePoint runs as a "farm" - even in single-server configurations - you have to run the site and authentication under the app pool account... AND still set up your SPN's. |
| HTTP/<passwordregistration portal server> | Password Registration Server Account | **** Setspn -S HTTP/passwordregistration.corp.contoso.com corp\FIM2$ | The SSPR portals use IIS 7.0/7.5. IIS 7.0/7.5 has an authentication feature - 'Enable Kernel Mode Authentication'. With this feature the Kerberos ticket for the requested service is decrypted using Machine account (Local system) of the IIS server. It no longer depends upon the application pool Identity for this purpose. The following assumes that the password registration and reset portals are being accessed through a custom host header. In this instance the SPN is required only for the IIS machine account and not for our FIM Password Service account. |
| HTTP/<passwordreset portal server> | Password Reset Server Account | **** Setspn -S HTTP/passwordreset.corp.contoso.com corp\FIM2$ | The SSPR portals use IIS 7.0/7.5. IIS 7.0/7.5 has an authentication feature - 'Enable Kernel Mode Authentication'. With this feature the Kerberos ticket for the requested service is decrypted using Machine account (Local system) of the IIS server. It no longer depends upon the application pool Identity for this purpose. The following assumes that the password registration and reset portals are being accessed through a custom host header. In this instance the SPN is required only for the IIS machine account and not for our FIM Password Service account. |
| HTTP/<FIM CM Server> | FIM CM Web Pool Agent Account | **** Setspn –S HTTP/FIMCM1.corp.contoso.com corp\FIMCMWeb  **** Setspn –S HTTP/FIMCM1 corp\FIMCMWeb | This is a special case even though we are running on IIS 7.0/7.5. In this instance you must ensure that useAppPoolCredentials is set to true. This will force IIS to use the appPoolCredentials to decrypt the ticket. KernelModeAuthentication is still enabled in this instance. |

## Duplicate SPNs

In general, only one SPN should be set for each service. Multiple SPNs can cause clients to connect to the wrong system or the ticket may be encrypted with the wrong key. Using the –s switch with the Setspn.exe helps ensure that no duplicates are created when you are configuring SPNs. This switch sets the spn only after verifying that no duplicates exist. For additional information on setspn.exe see [Setspn](http://technet.microsoft.com/en-us/library/cc731241(v=WS.10).aspx).

## Delegation

A client might need to let an application or a service connect to other servers or services on its behalf. A client might use a front-end server, for example, that then needs to authenticate with a back-end server. The front-end server needs to authenticate to the back-end server with the client's credentials, because if it authenticated under its own service account, it would have different authorization than the user.

Delegation of authentication allows the client to send its identity in the form of a Kerberos ticket to the front-end server. The front-end server can then impersonate the client and authenticate with the back-end server as if the front-end server were the client.

Delegation is not limited to a single pair of a front-end and a back-end server. A client can delegate its identity to a service that can then authenticate with any number of back-end services. It is also possible for the client to delegate its identity to Service A, and for Service A to in turn delegate the client's identity to Service B, for Service B to delegate the client's identity to Service C, and so on.Delegation is possible only with the Kerberos protocol. Thus, all parties involved in delegation scenarios must use the Kerberos protocol.

In a deployment with multiple FIMServices, ensure that each FIMService has constrained delegation configured so that each FIMService can successfully communicate to each other in order for Workflow Approvals to work properly. Approval Responses from users can come from any Portal or if Exchange is enabled from the FIMService that is polling. In all cases, the Approval Response will be directed to the FIMService machine that processed the original Request so cross-server communication: FIMPortal -> FIMService AND FIMService -> FIMService must work properly.

The following sections will provide some additional information regarding delegation for the FIM Service, the SharePoint Service account, and the Self-Service Password Registration and Rest Web application accounts. Also, be aware that the Delegation tab will not be present on a user’s properties until an SPN is set on that account. So if you do not see a Delegation tab, check to ensure that an SPN has been set on that account. This can be done by using a SetSpn.exe with a –l switch. The following will list all of the SPNs on the CORP\FIMService account.

Setspn –l corp\fimservice

### Delegation and SharePoint Web Application Pool Account

Delegation is required on the SharePoint service account. The following example shows how to turn on delegation for a SharePoint Web Application Pool Account named CORP\SPService in a domain named corp.contoso.com. Use the following procedure to enable delegation on the SharePoint Service account,

To turn on Delegation for CORP\SPService

|  |
| --- |
| 1. Click Start, select Administrative Tools, and click Active Directory Users and Computers. This will open the Active Directory Users and Computers MMC.  2. In the Active Directory Users and Computers MMC, from the tree-view on the left, expand corp.contoso.com, expand ServiceAccounts and in the center, right-click SharePoint Service, and then select Properties.  3. On the SharePoint Service Properties, select the Delegation tab.  4. In the middle, select Trust this user for delegation to specified services only.  5. Make sure Use Kerberos only is selected and click Add. This will bring up the Add Services dialog box.  6. On the Add Services dialog box, click Users or Computers. This will bring up the Select Users or Computers dialog box.  7. In the Select Users or Computers dialog box, enter FIM Service and click Check Names. This should resolve with an underline to the FIM Service account. Click OK. This will close the Select Users or Computers dialog box.  8. On the Add Services screen, select FIM Service under Available Services: and click OK. This will close the Add Services dialog box.  SharePoint Service Properties    9. On the SharePoint Service Properties screen, click Apply.  10. Click OK. |

### Delegation and FIM Service Account

Delegation is required on the SharePoint service account. The following example shows how to turn on delegation for a FIM Service Account named CORP\FIMService in a domain named corp.contoso.com. Use the following procedure to enable delegation on the SharePoint Service account,

To turn on Delegation for FIM Service Account

|  |
| --- |
| 1. Click Start, select Administrative Tools, and click Active Directory Users and Computers. This will open the Active Directory Users and Computers MMC.  2. In the Active Directory Users and Computers MMC, from the tree-view on the left, expand corp.contoso.com, expand ServiceAccounts and in the center, right-click SharePoint Service, and then select Properties.  3. On the SharePoint Service Properties, select the Delegation tab.  4. In the middle, select Trust this user for delegation to specified services only.  5. Make sure Use Kerberos only is selected and click Add. This will bring up the Add Services dialog box.  6. On the Add Services dialog box, click Users or Computers. This will bring up the Select Users or Computers dialog box.  7. In the Select Users or Computers dialog box, enter FIM Service and click Check Names. This should resolve with an underline to the FIM Service account. Click OK. This will close the Select Users or Computers dialog box.  8. On the Add Services screen, select FIM Service under Available Services: and click OK. This will close the Add Services dialog box.  SharePoint Service Properties    9. On the SharePoint Service Properties screen, click Apply.  10. Click OK. |

### Delegation and Self-Service Password Reset

The web application pool account(s), or the FIM Password Service account(s) does not need any SPNs set on it. Only the server that runs the FIM Password Reset and Registration portals may need additional SPNs. Likewise, the FIM Password Service account(s) do not need to be setup for delegation. This is because the FIM Service account is already aware of the FIM Password Service account. For more information on the FIM Service and portal communication see the FIM 2010 R2 Password Registration Portal and FIM 2010 R2 Password Reset Portal topics.

## Enforcing Kerberos on the FIM Portal

The FIM Portal can be configured to only accept Kerberos Authentication. Use the following procedure to enforce Kerberos on the FIM Portal.

To Enforce Kerberos for the FIM portal

|  |
| --- |
| 1. Log on to FIM Server as CORP\Administrator.  2. Navigate to the following directory: C:\inetpub\wwwroot\wss\VirtualDirectories\80.  3. Locate the Web.config file, right-click and select Open. This will bring up a pop-up that states Windows cannot open this file and it will have two options. Choose Select a program from a list of installed program, and then click OK.  4. Select Notepad, and click OK. This will open the config file in Notepad.  5. At the top, select Edit, Find, type the following text in in the box, and then click Find Next:  <resourceManagementClient  6. There should be only one instance and it will look like the following Before image. Insert requireKerberos=”true” in the line so it looks like the After image.  Web.config Before    Web.config After    7. At the top of the Notepad, select Save. Close Notepad.  8. Click Start, click All Programs, click Accessories, and then click Command Prompt. This will launch a Command Prompt window.  9. In the Command Prompt window, type the following text, and then hit Enter:  iisreset  This will stop and then restart IIS. Once this completes, close the Command Prompt window. |

# Deploying Forefront Identity Manager 2010 R2

## Deploying Forefront Identity Manager 2010 R2

This section provides information and step-by-step instructions on installing the various components that make up a Forefront Identity Manager 2010 R2 deployment. This section does not include installation instructions for installing FIM 2010 R2 Reporting or Self-Service Password Reset. For information on installing FIM 2010 R2 Reporting see the [Deployment Guide for Forefront Identity Manager 2010 R2 – Reporting](http://technet.microsoft.com/en-us/library/jj133858(v=ws.10).aspx). For information on installing Self-Service Password Reset see the [Deployment Guide for Forefront Identity Manager 2010 R2 - Self-Service Password Reset](http://technet.microsoft.com/en-us/library/jj134309(v=ws.10).aspx).

The following topic areas are covered in this section:

 [Hardware and Software Requirements](#zc812116267d747a4946f3ca88d76269b)

 [Before You Begin](#z914f2a1525a6446987f6c46e7b0b4574)

 [Installing the FIM 2010 R2 Server Components](#zd9833fc7dd9145ffb1682d3c24cfa777)

 [Installing the FIM 2010 R2 Add-ins and Extensions](#z77088ad7b54a4766a00161f7f8963807)

 [Installing the FIM 2010 R2 Language Packs](#zfe3a6f182e214df6a45a8e8bfacefb45)

 [Unattended Installation of FIM 2010 R2](#z0c2e372dc658426ea9576f54e5942b4f)

 [Common Post-installation Configuration for Forefront Identity Manager 2010 R2](#zbe7a99e8c44044cf895c12daf38d9447)

# Hardware and Software Requirements

## Required Hardware

The server or servers that host Microsoft® Forefront® Identity Manager (FIM) 2010 R2 server components must meet the following minimum hardware requirements:

 An x64-capable processor

 2 gigabytes (GB) of available hard disk space

 2 GB or more of RAM

 A monitor with a resolution of 1024 × 768

 A CD-ROM or DVD-ROM drive

The client computer that hosts the FIM 2010 R2 client-side components must meet the following minimum hardware requirements:

 512 megabytes (MB) of RAM (1 GB recommended)

 500 MB of free hard disk space

 A monitor that can display a resolution of 1024 × 768

The FIM Password Registration and Reset Portals are supported on mobile devices with screens with that have at least 320x480 resolution, or 480x320.

## Required Software

Each server that hosts the different FIM 2010 R2 server-side components has a different software requirement. This document contains the software requirements for each of the FIM 2010 R2 server-side components. If you decide to install all the server-side components on one server, you must install the software requirements for each of the FIM 2010 R2 server-side components on that server.

### FIM Synchronization Service Software Requirements

The server that hosts the FIM Synchronization Service must have the following prerequisite software installed:

 The 64-bit edition of the Windows Server 2008 Standard, Windows Server 2008 Enterprise, Windows Server 2008 R2 Standard, or Windows Server 2008 R2 Enterprise operating systems.

Important

When you install Windows Server 2008, do not install Windows Server 2008 Terminal Services (not to be confused with Remote Desktop Connection). If you install Terminal Services, the FIM 2010 R2 server components do not install.

 Windows Installer 4.5, if you are running Windows Server 2008. It is already included in Windows Server 2008 R2.

Windows Installer 4.5 can be downloaded from the Microsoft Download Center.

 Microsoft SQL Server 2008 64-bit Standard or Enterprise, Service Pack 1 (SP1) or later.

The following SQL Server features must be installed:

 Database Engine Services

Note

SQL Server can be installed on a remote server and does not have to be located on the same server as the FIM Synchronization Service server.

Note

You must install Management Tools – Basic on at least one server to be able to manage the computer running SQL Server.

 Microsoft Visual Studio® 2008.

Note

Visual Studio 2008 is required if you are planning to develop rules extensions for the FIM Synchronization Service on this server.

 Windows PowerShell 1.0 or 2.0 command-line interface.

Notes

Windows PowerShell 1.0 or 2.0 is required for provisioning resources for Microsoft Exchange Server 2007.

Windows PowerShell 2.0 is required for provisioning resources for Exchange 2010.

You cannot have both versions of Windows PowerShell installed at the same time.

Windows PowerShell 1.0 features can be installed from the Features options interface that is included with Windows Server 2008.

Windows Server 2008 R2 ships with Windows PowerShell 2.0. You can also download Windows PowerShell 2.0 from the Microsoft Download Center for Windows Server 2008.

 Microsoft .NET Framework 3.5 (Windows Server 2008) or .NET Framework 3.5.1 (Windows Server 2008 R2).

Note

You can also install .NET Framework Features from the Features options interface that is included with Windows Server 2008.

 It is necessary to install the .NET 3.5 SP1 Framework only on Windows Server 2008. The .NET 3.5 SP1 Framework is included in Windows Server 2008 R2.

To download .NET Framework 3.5 Service Pack 1, see [Microsoft .NET Framework 3.5 Service Pack 1](http://go.microsoft.com/fwlink/?LinkId=129538) (http://go.microsoft.com/fwlink/?LinkId=129538).

 Exchange 2007 SP1 Management Console.

Notes

Exchange 2007 SP1 Management Tools is required to fully provision Exchange 2007 mailboxes, contacts, and groups that the FIM Synchronization Service creates. You receive an extension-dll-exception error if you attempt to synchronize these objects to Active Directory Domain Services (AD DS) without installing the Exchange 2007 SP1 Management Console.

Exchange 2010 provisioning does not require any additional tools to be installed on the FIM Synchronization Service server.

### FIM Service Software Requirements

The server that hosts the FIM Service must have the following software installed:

 The 64-bit edition of Windows Server 2008 or Windows Server 2008 R2 Standard or Enterprise.

Important

When you install Windows Server 2008, do not install Windows Server 2008 Terminal Services (not to be confused with Remote Desktop). If you install Terminal Services, the FIM 2010 R2 server components do not install.

 Windows Installer 4.5, if you are running Windows Server 2008. It is already included in Windows Server 2008 R2.

Note

You can download Windows Installer 4.5 from Microsoft Download Center.

 64-bit SQL Server 2008 Standard or Enterprise Editions, SP1 or later.

The following SQL Server features must be installed:

 Database Engine Service

 Full-Text Search

Note

SQL Server can be installed on a remote server. It does not have to be located on the same server as the FIM Service server.

Note

You must install Management Tools – Basic on at least one server to be able to manage the SQL Server.

Note

You can use the same SQL Server 2008 instance that the FIM Synchronization Service uses.

Note

After you install SQL Server, ensure that the SQL Agent and the SQL Server Service Broker are running.

 Windows PowerShell 1.0 or Windows PowerShell 2.0.

Notes

FIM Service works with both Windows PowerShell 1.0 and Windows PowerShell 2.0.

You cannot have both versions of Windows PowerShell installed at the same time.

You can install Windows PowerShell 1.0 features from the Features options interface that is included with Windows Server 2008. Windows Server 2008 R2 ships with Windows PowerShell 2.0.

You can download Windows PowerShell 2.0 for Windows Server 2008 from the Microsoft Download Center.

 The .NET Framework 3.0 (Windows Server 2008) or .NET Framework 3.5.1 (Windows Server 2008 R2)

Notes

.NET Framework features can be installed from the Features options interface that is included with Windows Server 2008.

It is only necessary to install the .NET 3.5 SP1 Framework on Windows Server 2008. The .NET 3.5 SP1 Framework is included in Windows Server 2008 R2.

Visit the Microsoft Download center to download [.NET Framework 3.5 Service Pack 1](http://go.microsoft.com/fwlink/?LinkId=129538) (http://go.microsoft.com/fwlink/?LinkId=129538).

 System Center Service Manager 2010 Service Pack 1 (SCSM 2010 SP1)

Note

SCSM 2010 SP1 is only required if you are installing the new reporting features in FIM 2010 R2.

### FIM Portal, FIM Password Registration Portal, and FIM Password Reset Portal Software Requirements

The server or servers that host the FIM Portal, FIM Password Registration Portal, and FIM Password Reset Portal must have the following software installed:

Note

If you decide to install the FIM Portal and Password Portals on different servers, the software prerequisites for both servers are the same.

Note

The FIM Password Registration and Reset Portals may be installed on a server with other IIS sites.

 The 64-bit edition of Windows Server 2008 or Windows Server 2008 R2 Standard or Enterprise

Important

When you install Windows Server 2008, do not install Windows Server 2008 Terminal Services (not to be confused with Remote Desktop). If you install Terminal Services, the FIM 2010 R2 server components do not install.

 The .NET Framework 3.0 (Windows Server 2008) or .NET Framework 3.5.1 (Windows Server 2008 R2)

Notes

.NET Framework features can be installed from the Features options interface that is included with Windows Server 2008.

It is necessary to install the .NET 3.5 SP1 Framework only on Windows Server 2008. The .NET 3.5 SP1 Framework is included in Windows Server 2008 R2.

Visit the Microsoft Download Center to download [.NET Framework 3.5 Service Pack 1](http://go.microsoft.com/fwlink/?LinkId=129538) (http://go.microsoft.com/fwlink/?LinkId=129538).

 Windows SharePoint Services 3.0 Service Pack 2 (SP2) or Microsoft SharePoint Foundation 2010.

Note

Visit the Microsoft Download Center to download [Windows SharePoint Services 3.0 x64 with SP2](http://go.microsoft.com/fwlink/?LinkID=181113) (http://go.microsoft.com/fwlink/?LinkID=181113) or [Microsoft SharePoint Foundation 2010](http://www.microsoft.com/download/en/details.aspx?id=24983) (http://www.microsoft.com/download/en/details.aspx?id=24983).

Note

For more information, see these installation guides: [Deployment for Windows SharePoint Services 3.0 Technology](http://go.microsoft.com/fwlink/?LinkID=123878) (http://go.microsoft.com/fwlink/?LinkID=123878), [Deployment Guide for SharePoint Foundation 2010](http://www.microsoft.com/download/en/details.aspx?id=6841) (http://www.microsoft.com/download/en/details.aspx?id=6841) and, [Upgrading to SharePoint Foundation 2010](http://technet.microsoft.com/en-us/library/cc303309.aspx) (http://technet.microsoft.com/en-us/library/cc303309.aspx). For a step-by-step example of upgrading from WSS 3.0 to SharePoint Foundation 2010 see Test Lab Guide: Upgrading to FIM 2010 R2.

Note

If you upgrade to SharePoint 2010 prior to upgrading from FIM to FIM 2010 R2 the FIM help files will may no longer be accessible by end users. This is because of improved security in SharePoint 2010 which removes the authenticated users permissions from the FIM help files that was granted by SharePoint 2007. To fix this, re-apply the authenticated users permissions at the MSILM2 level with ‘Replace all child objects..’ checked

Warning

If the upgrade from FIM R2 Service and Portal setup fails half-way with an error that says SharePoint 2010 app not found. Then be aware that this can occur under certain topologies when upgrading from WSS 3.0 to SharePoint Foundation 2010.

The following topology experienced this issue:

 FIM Service and Portal on one IIS server (Server A). FIM Service DB on one SQL Server (Server B). FIM Sync Service on separate server with SQL Server (ServerC).

 The FIM Service and Portal that users connect to are separate from the Administrator instance of the FIM Service and Portal. Both connect to the same database. A virtual name for the FIM Portal (the users instance) maps to the IIS server name.

The workaround is to add computer name and localhost as internal name on SharePoint 2010.

 SharePoint Language Pack.

Note

If you have installed Windows SharePoint Services 3.0 or SharePoint Foundation 2010 in a language other than English, you must install the appropriate Language Pack. Visit the Microsoft Download Center to download the [Windows SharePoint Services 3.0 Language Pack Service Pack 2 (SP2), 64-Bit Edition](http://go.microsoft.com/fwlink/?LinkID=123878) (http://go.microsoft.com/fwlink/?LinkID=178266) or [Service Pack 1 for Microsoft Sharepoint Foundation 2010 Language Pack](http://www.microsoft.com/download/en/details.aspx?id=26629) (http://www.microsoft.com/download/en/details.aspx?id=26629).

 The FIM Password Registration and Reset Portals support the following browsers:

a. Microsoft Internet Explorer 9, 8, 7, and 6

b. Other browsers which support Javascript, have cookies enabled, and support CSS 3.0 media queries.

 The FIM Password Registration and Reset Portals are supported in production environments using https. The FIM Password and Registration and Reset Portals are supported in lab/pre-production environments using http or https.

 The FIM Password Registration Portal is supported on IIS with Kerberos, NTLM, and/or Basic Authentication enabled.

 The FIM Password Reset Portal is supported on IIS with Anonymous Authentication enabled.

 The FIM Password Registration and Reset Portals may be published via a proxy, such as Microsoft Threat Management Gateway.

### FIM Reporting Software Requirements

FIM Reporting requires the use of System Center Service Manager 2010 SP1 and has a unique set of requirements. This depends on the type of topology you are deploying. For a list of these requirements see the [Deployment Guide for Forefront Identity Manager 2010 R2 – Reporting](http://technet.microsoft.com/en-us/library/jj133858(v=ws.10).aspx).

### FIM Add-ins and Extensions Components Software Requirements

The client computers that host the FIM add-ins and extensions components must meet the following software requirements:

 Windows XP Professional SP3 or later, 32-bit, Windows Vista® Enterprise SP1 or later, 32-bit or 64-bit, or Windows 7 32-bit or 64-bit.

 Windows Installer 3.1 or later (only for Windows XP SP3).

Note

Visit the Microsoft Download Center to download [Windows Installer 3.1 Redistributable (v2)](http://go.microsoft.com/fwlink/?LinkID=62933) (http://go.microsoft.com/fwlink/?LinkID=62933).

 Microsoft .NET Framework 3.5 SP1.

Note

Visit the Microsoft Download Center to download [.NET Framework 3.5 SP1](http://go.microsoft.com/fwlink/?LinkId=129538) (http://go.microsoft.com/fwlink/?LinkId=129538).

 Microsoft Office Outlook 2010 or Microsoft Office Outlook 2007 SP2.

Note

This software is required only if you use the FIM 2010 R2 Add-in for Outlook.

 Microsoft Forms 2.0 .NET Programmability Support

Note

This software is an add-in feature of the 2007 Microsoft Office system. To install this software, select the Microsoft Forms 2.0 .NET Programmability Support option under Office Tools when you run the setup program for the Microsoft Office system.

 Smart Tag .NET Programmability Support

Note

This software is required only if you use Microsoft Office Outlook 2007.

Note

This software is an add-in feature of the Microsoft Office system. To install this software, select the Smart Tag .NET Programmability Support option under Office Tools when you run the setup program for the Microsoft Office system.

 .NET Programmability Support for Office Outlook

Note

This software is an add-in feature of the Microsoft Office system. To install this software, select the .NET Programmability Support option under Office Outlook when you run the setup program for the Microsoft Office system.

# Before You Begin

## 

Before you install the FIM 2010 R2 server and client components, you must complete the following configuration tasks:

1. Creating an email enabled domain service account to run the FIM Service component.

2. Creating a domain service account to run the FIM Synchronization Service.

3. Creating a domain service account to run the FIM Password Reset Portals.

4. Creating a domain service account to run the Share

point Service.

5. Creating a FIM Service Management Agent account.

6. Configuring the service accounts that are running the FIM server components in a secure manner.

7. If you are running the Exchange Web Service and Internet Information Services (IIS) default Web site (FIM Portal) on the same server, ensure that both are not configured to use port 80.

8. Ensuring that there is a default SharePoint Web site installed.

9. Ensuring that English is installed in SharePoint Services.

10. Selecting the correct identity for the SharePoint Application Pool.

11. Implementing Secure Sockets Layer (SSL) for FIM Portal.

12. Configuring the server running SQL Server.

13. Configuring the SQL Server aliases.

14. Configuring the SQL Server collation settings.

15. Configure the server running SCSM 2010 SP1.

16. Establishing Service Principal Names (SPNs) for FIM 2010 R2.

### Creating an E-mail-Enabled Domain Service Account to Run the FIM Service

To run the FIM Service component, you must have a dedicated domain service account. 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 2010 R2 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 you plan 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 R2 .

This account should not be granted local administrator permissions.

Important

You must reserve the domain service e-mail account for the exclusive use of the FIM Service. If e-mail messages are being processed by other applications, such as Office Outlook 2007, the functionality of FIM Service might be affected.

### Creating a Domain Service Account to Run the FIM Synchronization Service

You must create a service account to run the FIM Synchronization Service. This service account must be a domain service account. This account should not be a local administrator account.

### Creating a Domain FIM Service Management Agent Account

You must create a 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.

#### Understanding the Purpose of the FIM Service Management Agent Account

The purpose of this account is to make it possible for the FIM Service to be able to identify the FIM Synchronization Service when it is exporting to the FIM Service through the Web services. When the FIM Synchronization Service engine is exporting, all authentication (AuthN) and authorization (AuthZ) workflows are ignored and only action workflows run.

Important

The account that you use for the FIM MA should be considered a trusted account. You should not use it to access the FIM Portal. If you do, all requests that are made through the FIM Portal with this account will skip AuthN and AuthZ.

If you later change this account in the FIM Synchronization Service, you must also run a change install on the FIM Service to update the service with the new account information.

### Create a domain service account to run the FIM Password Service

If you are using FIM Password Reset, you must create a service account to run the FIM Password Service. This service account must be a domain service account. This account should not be a local administrator account.

### Create a domain service account to run the SharePoint Service

You must create a service account to run the Sharepoint Service. This service account must be a domain service account. This account should not be a local administrator account.

### Configuring the Service Accounts Running the FIM 2010 R2 Server Components in a Secure Manner

As mentioned previously, there are three service accounts that are used to run the FIM server components. They are called the FIM Service service account, the FIM Synchronization Service service account, and the FIM Password service account in this guide. The FIM MA account is not considered a service account, and it should be a regular user account. For the FIM Synchronization Service service account to be able to impersonate the FIM MA account, the FIM MA must be able to log on locally.

To enable the FIM MA to log on locally

|  |
| --- |
| 1. Click Start, and then click Administrative Tools.  2. Click Local Security Policy, and then click Local Policies\User Rights Assignment.  3. In the policy Allow log on locally, ensure that the FIM MA account is explicitly specified, or add it to one of the groups that is already granted access. |

To configure the server or servers running the FIM 2010 R2 server components in a secure manner, the service accounts should be restricted. The easiest way to do this is by running Local Security Policy from Administrative Tools, navigate to Local Policies\User Rights Assignment, and then add the service account to the policy.

Important

On the server running the FIM Synchronization Service, you must restrict only the FIM Synchronization Service service account and not the FIM Service service account. On the server running the FIM Service, you must only restrict the FIM Service service account, and not the FIM Synchronization Service service account.

Use the following restrictions on the service accounts:

 Deny logon as a batch job

 Deny logon locally

 Deny access to this computer from the network

Note

Domain-based Group Policy objects (GPOs) might override settings in the Local Security Policy.

The service accounts should not be members of the local administrators group.

The FIM Synchronization Service service account should not be a member of the security groups that are used to control access to FIM Synchronization Service (groups starting with FIMSync, for example, FIMSyncAdmins).

Important

If you are deploying password reset, do not use the Deny access to this computer from the network restriction option.

If you choose to use the same account for both service accounts and you separate the FIM Service and the FIM Synchronization Service, you cannot set Deny access to this computer from the network on the FIM Synchronization Service server. If access is denied, that action prohibits the FIM Service from contacting the FIM Synchronization Service to change configuration and manage passwords.

### Ensuring That the Exchange Web Service and IIS Default Web Site are Not Both Configured to Use Port 80

In a lab environment, you may want to run Exchange on the same server as the FIM Service. If you do, ensure that you are reconfiguring Exchange Web Service to not use the default port 80, or Exchange Web Service will not be reachable.

You must either specify a different port, a different IP, or a different host name in IIS.

### Ensuring That English Is Installed for SharePoint

If the installed version of SharePoint is not English, the FIM 2010 R2 setup fails. Before you can install FIM 2010 R2 , you must first install the latest SharePoint Service English Language Pack Service Pack for your version of SharePoint. Visit the Microsoft download Center to download the [Windows SharePoint Services 3.0 Language Pack Service Pack 2 (SP2), 64-Bit Edition](http://go.microsoft.com/fwlink/?LinkID=178266) (http://go.microsoft.com/fwlink/?LinkID=178266) or the [Service Pack 1 for Microsoft SharePoint Foundation 2010 Language Pack](http://www.microsoft.com/download/en/details.aspx?id=26629) (http://www.microsoft.com/download/en/details.aspx?id=26629).

### Ensuring That a SharePoint Default Web Site Is Installed

Before you install the FIM Password Registration Portal and FIM Password Reset Portal, run the SharePoint Configuration Wizard. This creates a default SharePoint site for you.

If you installed SharePoint in a SharePoint farm, the default site cannot be created by the wizard and must be created manually. How to set up a SharePoint farm is outside the scope of this installation guide.

Verify the installation by navigating to http://localhost:80 on the server where you will install the FIM Portal. You should see a SharePoint site and not the standard Welcome to IIS7 message. If you see the Welcome to IIS7 message, reconfigure SharePoint to display a default SharePoint site at this server address or the address where you installed SharePoint.

If you do not perform this task, you may have to reinstall the FIM Portal and Password Portal components of FIM 2010 R2 .

### Selecting the Correct Identity for the SharePoint Application Pool

By default, IIS uses the Network Service account for the Application Pool. In the steps above, you created a service account for SharePoint, which you will use for the following procedures. Later in this guide you will enable Kerberos delegation, and only one identity can use one SPN.

By default, an application pool running under a specific service account will not use the service account for Kerberos. In the second configuration step, you will configure IIS to use the service account for Kerberos.

To run the SharePoint Application Pool using an account that is located in the domain using WSS 3.0

|  |
| --- |
| 1. Start SharePoint 3.0 Central Administration from Administrative Tools.  2. Select Operations and Service Accounts.  3. Select Web Application Pool, and select Windows SharePoint Services Web Application. Select the SharePoint Application Pool where the FIM Portal will be installed, which by default is SharePoint – 80.  4. Enter the user name and password for the service account that you created earlier.  5. Click OK to save your changes. |

To run the SharePoint Application Pool using an account that is located in the domain using Sharepoint Foundation 2010

|  |
| --- |
| 1. Click Start, click All Programs, click Microsoft SharePoint 2010 Products and then click SharePoint 2010 Central Administration.  2. Under Security, click Configure service accounts.  3. From the first drop-down list select Web Application Pool – SharePoint 80.  4. Under Select an account for this component click the link Register new managed account.  5. Enter the name and password of the service account you created earlier.  6. Under Select an account for this component, select the service account.  7. Click OK three times to save your changes. |

Enable the Application Pool to use the service account for Kerberos.

 To configure IIS to use the service account for Kerberos delegation, set useAppPoolCredentials as described in [Service Principal Name (SPN) checklist for Kerberos authentication with IIS 7.0](http://go.microsoft.com/fwlink/?LinkId=188290) (http://go.microsoft.com/fwlink/?LinkId=188290).

### Implementing Secure Sockets Layer for FIM Portal

We highly recommend that you implement Secure Sockets Layer (SSL) on the FIM Portal server to secure the traffic between the client and server computers.

To implement SSL with a certificate from an existing internal CA

|  |
| --- |
| 1. Open IIS Manager on the FIM Portal server.  2. Click the local computer name.  3. Click Server Certificates.  4. Click Create Certificate Request.  5. For Common Name, enter the name of the server.  6. Click Next, and then Next.  7. Save the file to any location. You will need to access this location in subsequent steps.  8. In Windows Internet Explorer, browse to https://servername/certsrv. Replace servername with the name of the server that is issuing certificates.  9. Click Request a new Certificate.  10. Click Submit an Advanced Request.  11. Click Submit a Certificate Request by using a base-64-encoded.  12. Paste the contents of the file that you saved in the previous step.  13. From Certificate Template, select Web Server.  14. Click Submit.  15. Save the certificate to your Desktop.  16. In IIS Manager, click Complete Certification Request.  17. Point IIS Manager to the certificate you just saved to the Desktop.  18. For Friendly name, type the name of the server.  19. Click Sites, and then select Sharepoint – 80.  20. Click Bindings, and then click Add.  21. Select https.  22. For certificate, select the certificate that has the same name as the server. (This is the certificate that you just imported.)  23. Click OK.  24. Remove the HTTP binding.  25. Click SSL Settings, and then check Require SSL.  26. Save the settings.  27. If you are using SharePoint Foundation 2010  a. Click Start, click All Programs, click Microsoft SharePoint 2010 Products, and then click SharePoint 2010 Central Administration.  b. Under System Settings, click Configure alternate access mappings.  c. Click http://servername.  d. Change http://servername to https://servername, and then click OK.  e. Click Start, Run, enter iisreset, and then click OK.  28. If you are using WSS 3.0  a. Click Start, click Administrative Tools, and then click Sharepoint 3.0 Central Administration.  b. Click Operations, and then click Alternate Access Mappings.  c. Click http://servername.  d. Change http://servername to https://servername, and then click OK.  e. Click Start, Run, enter iisreset, and then click OK. |

### Configuring SQL Server

Before you install the FIM Service, certain tasks should be completed and verified on the server that is running SQL Server.

If you are using FIM Reporting, you will need to create two additional service accounts:

 SQL Reporting Service Account

 SQL Analysis Service Account

Ensure that the service accounts used by SQL Server Database and SQL Server Agent are either domain accounts or built-in service accounts (for example, Network Service). You cannot use local computer accounts.

When you configure the service accounts for SQL Server, consult the following articles:

 [Service Account Types Supported for SQL Server Agent](http://go.microsoft.com/fwlink/?LinkId=183624) (http://go.microsoft.com/fwlink/?LinkId=183624)

 [Selecting an Account for the SQL Server Agent Service](http://go.microsoft.com/fwlink/?LinkId=122956) (http://go.microsoft.com/fwlink/?LinkId=122956)

Important

The SQL Server service account should not be a local computer account. A local account cannot impersonate domain accounts and the FIM Service will not behave as expected.

Important

Make sure that the SQL Server Agent service and the SQL Server Service Broker is set to start automatically.

Important

If you install the SQL Server 2008 database on a different server than the FIM Service or FIM Synchronization Service, open additional ports so that FIM 2010 R2 setup can communicate with SQL Server 2008. For more information, see [Configuring the Windows Firewall to Allow SQL Server Access](http://go.microsoft.com/fwlink/?LinkID=94001) (http://go.microsoft.com/fwlink/?LinkID=94001).

When the FIM Service and FIM Synchronization Service are installed, the data and log files are created in the default locations that are specified by SQL Server. For optimal performance, these log files should be located on different drives and on different spindles.

To locate databases on different drives

|  |
| --- |
| 1. Start Microsoft SQL Server Enterprise Manager.  2. Right-click the server, and then click Properties.  3. Go to Database settings. Make the necessary adjustments on the Data and Log settings to ensure that the database files are located on a different drive than the operating system. |

### Configuring SQL Server Aliases

If you plan to install FIM Service or FIM Synchronization Service on a server running SQL Server that is using a nondefault port, you must create a SQL Server alias for Setup to be able to contact the server running SQL Server.

To create a SQL Server alias for Setup to be able to contact the server running SQL Server

|  |
| --- |
| 1. Start the SQL Server Configuration Manager.  2. Navigate to SQL Native Client 10.0 Configuration/Aliases.  3. Create a new alias with your server information. |

### Configuring SQL Server Collation Settings

Work with your SQL Server database administrator (DBA) to determine the correct collation setting to use for your FIM Service database. The collation setting determines the sorting order and how indexing works.

The default collation set during installation is SQL\_LATIN1\_General\_CP1\_CI\_AS.

If the server running Windows is using a character set that is different from the Latin alphabet, then you might consider a different collation based on the table found in [Windows Collation Name (Transact-SQL)](http://go.microsoft.com/fwlink/?LinkId=185630) (http://go.microsoft.com/fwlink/?LinkId=185630).

Ensure that the selected collation is case insensitive (indicated by \_CI\_).

If you change the collation setting, ensure that the collation setting is the same on the FIM Service database and on the system databases master and tempdb.

If you install the FIM Service and later decide to change the collation setting, you must manually change the collation setting on every table in the FIM Service database, as described in [Setting and Changing the Database Collation](http://go.microsoft.com/fwlink/?LinkId=185247) (http://go.microsoft.com/fwlink/?LinkId=185247).

### Configuring System Center Service Manager 2010 SP1 (SCSM 2010 SP1)

If you are using FIM Reporting in FIM 2010 R2 , you must install and configure the SCSM 2010 SP1 Server before installing FIM 2010 R2 .

Note

For guidance on installing SCSM 2010 SP1, see the [Test Lab Guide: System Center Service Manager 2010 SP1](http://www.microsoft.com/downloads/en/details.aspx?FamilyID=b276879e-380f-4b40-809e-1574f4059277)(http://www.microsoft.com/downloads/en/details.aspx?FamilyID=b276879e-380f-4b40-809e-1574f4059277)

 Use the steps outlined in the following article to ensure reporting is setup and functioning correctly [Registering with the Service Manager 2010 SP1 Data Warehouse to Enable Reporting](http://technet.microsoft.com/en-us/library/ff461143.aspx) (http://technet.microsoft.com/en-us/library/ff461143.aspx).

 Install the Microsoft Report Viewer Redistributable Security Update on the FIM 2010 R2 server. The Report Viewer installation files are located on the SCSM 2010 installation media, in the amd64/Prerequisites folder.

 Install the Service Manager Console on the FIM 2010 R2 server. The Service Manager Console installation files are located on the SCSM 2010 installation media, in the amd64 folder. Run setup.exe and follow the steps to install a Service Manager console.

 Install [Cumulative Update 2 for SCSM 2010 SP1](http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=12342) (http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=12342) on the SCSM 2010 SP1 server and the FIM 2010 R2 server.

### Establishing SPNs for FIM 2010 R2

SPNs are necessary for the Kerberos v5 protocol to be used for authentication. Enabling Kerberos helps to make the traffic secure, and it is required for the clients to be able to communicate with the FIM Service. SPNs must be registered in the domain for Kerberos to work.

We recommend that you use aliases for your FIM Service, FIM Password Portals and FIM Portal. They can be represented as host (A) or alias CNAME resource records in Domain Name System (DNS). For the FIM Service server and FIM Password service server, complete the following procedure:

To establish the SPNs for the FIM Service service and FIM Password Portals

|  |
| --- |
| 1. Establish the SPNs for the FIM Service by running the following command:   setspn –S FIMService/<alias> <domain>\<serviceaccount>   The <alias> above is the address that is entered during FIM Service setup and used by the clients and the FIM Portal to contact the Web Service. This can be an alias (CNAME) or host (A) resource record in DNS. If you are using Network Load Balancing (NLB), this is the name of the cluster.   The <serviceaccount> above is the account that is used by the FIM Service.   If you are using several different names—for instance, fully qualified domain names (FQDNs) and NetBIOS names—to contact the server, repeat the steps for every name.  Note  If you want cross forest scenarios to work in a separated environment, that is, portal on different machine than FIM service, then you must also set the FQDN.  To accomplish this, use the following:  setspn.exe –S FIMService/FQDN <domain>\<serviceaccount>  2. Repeat the above step for each of the FIM Password portals, using setspn.exe –S HTTP/<ssprPortalHostHeaderName> <domain>\<ssprPortalMachineAccount$>, where <ssprPortalHostHeaderName> is the binding information for the FIM Password portal Host Name that was entered during setup. This is the name that will be used by clients to contact the portals.  3. Turn on Kerberos delegation for the FIM Service and FIM Password service accounts in AD DS. You can turn on delegation for all services either by selecting Trust this user for delegation to any service (not recommended) or by using constrained delegation (recommended) by selecting Trust this user for delegation to the specified services only. If you use constrained delegation, search for the FIM Service service account, and then select the entry that you added in the previous step. |

Warning

In a deployment with multiple FIMServices, ensure that each FIMService has constrained delegation configured so that each FIMService can successfully communicate to each other in order for Workflow Approvals to work properly. Approval Responses from users can come from any Portal or if Exchange is enabled from the FIMService that is polling. In all cases, the Approval Response will be directed to the FIMService machine that processed the original Request so cross-server communication: FIMPortal -> FIMService AND FIMService -> FIMService must work properly.

For the FIM Portal server, complete the steps in the next procedure.

 If the address that the clients use to contact the FIM Portal is not the same as the server address, you have to establish an SPN for Hypertext Transfer Protocol (HTTP). That is, if you use an alias (CNAME) resource record in DNS, have a SharePoint farm, or use Networking Load Balancing (NLB), this address must be registered or Internet Explorer cannot use the Kerberos protocol when it contacts the portal. Run the following command:

setspn –S HTTP/<FIMPortalAlias> <domain>\<sharepointserviceaccount>

 The <FIMPortalAlias> is the address that clients use to contact the FIM Portal server.

 The <domain>\sharepointserviceaccount> is the account that the SharePoint Application Pool uses, as defined in IIS.

 If you are using several different names, that is, FQDN and NetBIOS names, to contact the server, repeat the steps for every name.

 The SharePoint service account must be allowed to delegate to the FIM Service. You can choose to enable delegation for all services either by selecting Trust this user for delegation to any service (not recommended) or by using constrained delegation (recommended) by selecting Trust this user for delegation to the selected services only. If you use constrained delegation, search for the FIM Service service account, and then select the entry that you added in the FIM Service step.

Note

You do not have to create delegation for HTTP/FIMPortalAlias.

# Installing the FIM 2010 R2 Server Components

## Installing the FIM 2010 R2 Server Components

You must use an account with local administrator privileges to install the Microsoft® Forefront® Identity Manager (FIM) 2010 R2 server components. To be able to install the FIM Portal, the account must be a SharePoint administrator. To be able to install FIM Synchronization Service or FIM Service, the account must be a SQL sysadmin. The account that you use does not have to be a SQL sysadmin after the installation is complete.

This section covers the following components:

 FIM Synchronization Service

 FIM Service

 FIM Portal

Notes

During installation, Setup tries to contact the other components to validate that the service is running. For the contact to function correctly, remote administration must be activated in Windows Firewall.

To turn on remote administration, start Windows Firewall in Control Panel, click Allow a program through the Windows Firewall, and then click Remote Administration.

You can install FIM 2010 R2 without remote administration turned on. You must also be an administrator of the other server. If either one of those two requirements is not fulfilled, several warning messages appear, telling you that the service could not be contacted. There is no functional impact to ignoring those warnings during Setup if you know that all the settings are correct and if you chose not to allow remote administration.

### FIM Synchronization Service

The FIM Synchronization Service consists of the metadirectory, provisioning engine, and management agents (MAs) for various connected data sources. It supports synchronization of data between the FIM Synchronization Service database and other identity stores in the enterprise.

During the installation of the Synchronization Service, the firewall on the server that hosts this service is configured to allow Dynamic Remote Procedure Call (RPC) and RPC endpoint mapper access to the FIM Synchronization Service.

The FIM Synchronization Service creates five security groups. The first three groups correspond to the FIM Synchronization Service user roles: Administrator, Operator, and Joiner. The other two groups are used for granting access to the Windows Management Instrumentation (WMI) interfaces: Connector Browse and Password Set.

By default, the FIM Synchronization Service creates the five security groups as local computer groups instead of domain global groups. If you plan to use domain global groups, you must create the groups before you install the FIM Synchronization Service.

Caution

Only one FIM Synchronization Service instance can exist in a deployment.

To install the FIM Synchronization Service

|  |
| --- |
| 1. Navigate to the directory that contains the binaries for Forefront Identity Manager 2010 R2 and double-click FIMSplash.htm. This will bring up the Forefront Identity Manager 2010 R2 splash screen.  2. On the splash screen, click Install Synchronization Service. You will see a pop-up that says Do you want to run or save this file? Click Run. This will take a minute. Then you will see another pop-up asking Do you want to run this software? Click Run. This will start the Forefront Identity Manager 2010 R2 Setup Wizard.  3. On the Welcome page, click Next.  Important  Setup.exe runs with elevated privileges. If User Account Control (UAC) is turned on, installing the FIM Synchronization Service without elevated privileges causes the installation to fail.  Important  If you are reusing an existing FIM Synchronization Service database during installation, User Account Control (UAC) must be turned on.  Important  The user account that is used to install the FIM Synchronization Service must be granted the sysadmin role in SQL Server 2008. By default, members of the Local Administrators group do not have the necessary permissions. Unless the user account is either the built-in administrator account or the user account used to install SQL Server 2008, the user account must be given the sysadmin role in SQL Server 2008.  Welcome to the Forefront Identity Manager Synchronization Service Setup Wizard    4. On the End User License Agreement page, read the License Agreement, if you agree with the terms, select I accept the terms in the License Agreement, and then click Next.  5. On the Custom Setup page, click Next.  6. On the Configure Forefront Identity Manager Synchronization Service page, under SQL Server is located on, click the radio button next to A remote machine, enter the SQL server name and click Next.  Configure Forefront Identity Manager Synchronization Service    7. Next to Service account enter the service account, next to Password enter the service account password, and next to Service Account Domain or local computer name enter the service account domain. Click Next.  Configure Forefront Identity Manager Synchronization Service    8. Leave the default groups, and click Next.  Configure Forefront Identity Manager Synchronization Service    9. Select Enable firewall rules for inbound RPC communications, and click Next.  Configure Forefront Identity Manager Synchronization Service    10. Click Install.  11. This will bring up a pop-up box that says the setup will now create a backup key. Click OK. In the File name box, enter a name and location for the backup key and click Save. This will continue the installation.  Backup Key Dialog Box    12. Once the installation completes, click Finish. This will bring up a pop-up box that says you must log off and log on to your system again for the security group membership changes to take effect. Click Yes. This will log you off.  13. Log back on to the Synchronization Service server. |

### FIM Service and Portal

Installing the FIM Service installs the Web services parts of FIM 2010 R2 and also configures the FIM Service database on the server that hosts SQL Server 2008. This section describes the steps to install each component individually, however, any or all the components may be installed at the same time.

During the installation of FIM Service, port 5725 and port 5726 are opened and exceptions for these ports are added to the Windows Server 2008 firewall settings. Opening these ports permits communication to the FIM Service from the FIM Portal, FIM Password Reset Portal, FIM Synchronization Service, and FIM Password Reset Extensions components that may be installed on other computers in your organization.

The FIM Portal allows users who have authorized access to manage the activities that are requested and sent to the FIM Service.

Note

To be able to install the FIM Portal, it is assumed that SharePoint is installed with the default settings, that the default SharePoint site can be reached using the address specified in the user interface, and that the user who is installing the FIM Portal is authorized as an administrator of that SharePoint site.

Notes

If you install the FIM Portal on a SharePoint server farm, the address http://localhost is not available by default. To add localhost to the list of known addresses:

 Start SharePoint 2010 Central Administration, and navigate to System Settings, Configure alternate access mappings, Edit Public Zone URLs, or

 Start SharePoint 3.0 Central Administration, and navigate to Operations, Alternate Access Mappings, Edit Public Zone URLs

Add http://localhost to the Intranet zone, leaving the Default zone with the SharePoint server farm address.

Important

For security purposes, we highly recommend that you implement Secure Sockets Layer (SSL) on the server that is running Internet Information Services (IIS). For a procedure to do this, see [Before You Begin](#z914f2a1525a6446987f6c46e7b0b4574).

Note

You can activate SSL before or after the installation of the FIM Portal. If you add SSL after installation of the FIM Portal, ensure that you run a change installation on the FIM Service and FIM Portal and change the address of the FIM Portal. If you do not provide the correct address to the installer, future updates to the product will not install successfully.

To install the FIM Service and Portal use the following procedure:

To install the FIM Service and Portal

|  |
| --- |
| 1. Navigate to the directory that contains the binaries for Forefront Identity Manager 2010 R2 and double-click FIMSplash.htm. This will bring up the Forefront Identity Manager 2010 R2 splash screen.  2. On the splash screen, click Install Service and Portal. You will see a pop-up that says Do you want to run or save this file? Click Run. This will take a minute. Then you will see another pop-up asking Do you want to run this software? Click Run. This will start the Forefront Identity Manager 2010 Service and Portal Setup Wizard.  Important  The SQL Agent must be running on the server running SQL before you run the installation of the FIM Service.  Important  The user account used to install the FIM Service must be granted the sysadmin role in SQL Server 2008. By default, members of the Local Administrators group do not have the necessary permissions. Unless the user account is either the built-in administrator account, or the user account used to install SQL Server 2008, then the user account must be granted the sysadmin role in SQL Server 2008.  3. On the Welcome page, click Next.  4. On the End User License Agreement page, read the License Agreement, if you agree with the terms, select I accept the terms in the License Agreement, and then click Next.  5. On the FIM Customer Experience Improvement Program page, select one of the options and then click Next.  6. On the Custom Setup page, click the drop-down list next to FIM Password Registration, select Entire feature will be unavailable.  7. On the Custom Setup page, click the drop-down list next to FIM Password Reset Portal, select Entire feature will be unavailable.  8. Click Next.  9. On the Configure Common Services page, next to Database Server, enter the name of the database server. Leave the remaining defaults, and click Next.  Configure Common Services    10. Next to Mail Server, type the following name of the email server if it is relevant. Either clear or leave the SSL box and either check or uncheck the Mail Server is Exchange 2007 or Exchange Server 2010 and Enable polling for Exchange Server 2007 or Exchange Server 2010 boxes, then click Next.  Important  If you have several FIM Service servers using the same database, ensure that you select only the Enable polling of Exchange Server 2007 check box on one of the servers. This setting is also applicable for Exchange 2010. This server is responsible for obtaining e-mail messages from the Exchange Web Service interface and turning them into requests.  Configure Common Services    11. On the Configure service certificate page, select Generate a self-signed certificate.  Note  The certificate is validated only by the server; therefore, you do not have to trust it on the clients. For this reason you can safely use a self-issued certificate, and do not need one that is issued by your enterprise CA.  Note  If your organization has already created an in-house certification authority (CA), a public key pair can be generated for the service to use.  Configure Common Services    12. On the Configure FIM Service account page, next to Service Account Name, enter the FIM Service account.  13. On the Configure FIM Service account page, next to Service Account Password enter the FIM Service account password.On the Configure FIM Service account page, next to Service Account Password, type the following text:  Pass1word$  14. On the Configure FIM Service account page, next to Service Account Domain enter the FIM Service account domain.  15. On the Configure FIM Service account page, next to Service Email Account enter the FIM Service account email.  Configure Common Services    16. Click Next.  17. On the Configure the Forefront Identity Manager Service and Portal synchronization page, next to Synchronization Server , enter the Synchronization Server name.  18. On the Configure the Forefront Identity Manager Service and Portal synchronization page, next to FIM Management Agent Account\*, enter the FIM MA account.  Configure Common Services    19. Click Next.  20. On the Configure connection to the FIM Service page, next to FIM Service Server address, enter the server name or the alias that the clients should use to contact the FIM Service. If you plan to use an alternative name (that is, a CNAME resource record in Domain Name System (DNS)), type the alternative name. If you plan to have several FIM Service servers in a Network Load Balancing (NLB) cluster, type the name of the cluster address.  Important  Do not specify localhost. This is not supported and will result in an error.  Note  The names should match the Service Principal Names (SPNs) that you created in the pre-installation tasks.  Important  This name must be stable, and clients must be able to resolve it to the IP address of the server where the FIM Service is installed. This server name is also used by password reset clients to reach the server.  Important  The FQDN should be used here if the FIM Service and the FIM Portal are on separate machines and you plan to use cross forest scenarios.  Configure FIM Service and Portal    21. Click Next.  22. On the Configure connection to the FIM Service page, leave the default of http://localhost and click next.  Configure FIM Service and Portal    23. On the Configure optional portal homepage configuration page, in the box next to Registration Portal URL: either enter a url or leave it blank and then click Next.  Registration Portal URL    24. On the Configure security changes configured by setup page, select Open ports 5725 and 5726 in firewall, select Grant authenticated users access to the FIM Portal site, and then click Next.  Configure FIM Service and Portal    25. On the Enter optional password portal configuration page, either place a check in FIM Password Registration Portal will be installed on another host and under Enter the existing account under which the password registration application pool will run in IIS, next to Account Name, enter the FIM Password Registration Application Pool account or leave unchecked.  26. On the Enter optional password portal configuration page, either place a check in FIM Password Reset Portal will be installed on another host and under Enter the existing account under which the application pool will run in IIS, next to Account Name, enter the FIM Password Reset Application Pool account or leave unchecked.  Important  One important thing that must be done in order for Self-Service Password Reset to work properly is that the FIM Service account must be aware of the application pool account or accounts that are running the Registration and Reset Portals. This is because these become well-known identities to the FIM Service. The FIM Service recognizes requests which originate from these identities and respond accordingly. If you plan to run the Registration and Reset portals on a server other than the one that is running the FIM Service, then these accounts need to be specified during the FIM Service setup. In other words, to associate the FIM Service with these accounts, you must specify these accounts at the end of installation wizard when setting up the FIM Service. To do this, place a check in FIM Password Registration Portal will be installed on another host and then specify the Registration account and place a check in FIM Password Reset Portal will be installed on another host and specify the Reset account.  If you plan to run the Registration and Reset portals on the same server as the FIM Service, then these boxes can be left blank when you are installing the FIM Service. This is only if you plan to run the SSPR portals on the same server as the FIM Service.For additional information see the [Forefront Identity Manager 2010 R2 Self-Service Password Reset Deployment Guide](http://technet.microsoft.com/en-us/library/jj134309(v=ws.10).aspx).Also, be aware that if this account changes or you need to do a change mode install that you will need to ensure the FIM Service is associated with the app pool accounts by running a change mode install on the FIM Service server first, then on the servers that are hosting the Registration and Reset portals. For more information on this see [Forefront Identity Manager 2010 R2 Self-Service Password Reset Deployment Guide](http://technet.microsoft.com/en-us/library/jj134309(v=ws.10).aspx).  Enter information for FIM Password Portals    27. Click Next.  28. Click Install. This will begin the installation.  29. Once the installation completes, click Finish.  30. Close the Splash screen.  31. Restart the server. |

Test the FIM Portal by opening Internet Explorer and navigating to http://servername/identitymanagement.

If you want to redirect the FIM Portal URL, for example to let the user type http://servername and be redirected to http://servername/identitymanagement, follow the steps in the following procedure.

To redirect the FIM Portal

|  |
| --- |
| 1. Navigate to the website installation directory. By default this path is c:\inetpub\wwwroot\wss\VirtualDirectories\80.  2. Make sure the file system is showing file extensions.  3. Create a new text file named default.aspx.  4. Edit default.aspx as follows:  <%@ Page Language="C#" %> <script runat="server"> protected override void OnLoad(EventArgs e)  { base.OnLoad(e);  Response.Redirect("~/IdentityManagement/default.aspx"); } </script>  5. Save the file, and run iisreset. |

Note

When using the FIM Portal in Windows Server 2008 or Windows Server 2008 R2, the controls or buttons do not work unless the browser security settings for Internet Explorer are adjusted to turn on JavaScript.

## Post-Installation Tasks

After you install the FIM 2010 R2 server components, you must complete several configuration tasks.

Tasks in the domain:

 Add the FIM Service service account to the FIM Synchronization Service security groups.

 Configure the FIM Service service Exchange Server mailbox.

Tasks on the FIM Portal:

 Turn off the SharePoint indexing.

 Turn on the Kerberos v5 protocol only.

Tasks on FIM Service:

 Install Exchange 2007 and Exchange 2010 Web Service Certificate.

### Add the FIM Service service account to the FIM Synchronization Service security groups

 Add the service account used by the FIM Service to the FIMSyncAdmins group. This allows the FIM Service to configure the FIM Synchronization Service.

 If you plan to use the Password Reset feature of FIM 2010 R2, add the service account that the FIM Service uses to the security group FIMSyncPasswordSet.

 So that the group membership is effective, restart the FIMService service.

### Configuring the FIM Service Service Exchange mailbox

The following are best practices for configuring Exchange Server for the FIM Service service account:

1. Configure the service account so that it can accept mail only from internal e-mail addresses. Specifically, the service account mailbox should never be able to receive mail from external SMTP servers.

In the Exchange Management Console, select the FIM Service service account, click Properties, click Mail Flow Settings, and then click Mail Delivery Restrictions. Select the Require that all senders are authenticated check box. For more information, see:

[Configure Message Delivery Restrictions](http://go.microsoft.com/fwlink/?LinkId=183625) (http://go.microsoft.com/fwlink/?LinkId=183625)

2. Configure the service account so that it rejects mail messages with sizes greater than 1 MB.

Follow the best practice of configuring the Exchange 2007 message size limits:

[Configure Message Size Limits for a Mailbox or a Mail-enabled Public Folder](http://go.microsoft.com/fwlink/?LinkId=183626) (http://go.microsoft.com/fwlink/?LinkId=183626)

3. Configure the service account so that it has a mailbox storage quota of 5 gigabytes (GB).

Follow the best practice of configuring the Exchange 2007 mailbox size limits:

[Configure Storage Quotas for a Mailbox](http://go.microsoft.com/fwlink/?LinkId=156929) (http://go.microsoft.com/fwlink/?LinkId=156929)

### Disabling SharePoint indexing

It is recommended that you disable SharePoint indexing. There are no documents that need to be indexed, and indexing causes many error log entries and potential performance problems with FIM 2010 R2.

To disable SharePoint indexing in SharePoint Foundation 2010

|  |
| --- |
| 1. On the server that hosts the FIM Portal, click Start, click All Programs, click Microsoft SharePoint 2010 Products and then click SharePoint 2010 Central Administration.  2. Under Monitoring, click Check job status.  3. Click SharePoint Services Search Refresh.  4. On the Edit Timer Job page, click Disable. |

To disable SharePoint indexing in WSS 3.0

|  |
| --- |
| 1. On the server that hosts the FIM Portal, click Start.  2. Click All Programs.  3. In the All Programs list, click Administrative Tools.  4. Under Administrative Tools, click SharePoint 3.0 Central Administration.  5. On the Central Administration page, click Operations.  6. On the Operations page, under Global Configuration, click Timer job definitions.  7. On the Timer Job Definitions page, click SharePoint Services Search Refresh.  8. On the Edit Timer Job page, click Disable. |

### Activating the Kerberos protocol only

We highly recommend that you turn off portal authentication that uses NTLM. The Kerberos protocol is a more secure protocol to use.

To activate Kerberos protocol only

|  |
| --- |
| 1. Open the Web.config file, which is usually located at C:\inetpub\wwwroot\wss\VirtualDirectories\80.  Note  You need an elevated command prompt or Windows Explorer to access this folder.  2. Locate the element <resourceManagementClient . . . />  3. Add requireKerberos=”true” so that it reads <resourceManagementClient requireKerberos="true" . . . />  4. Save the Web.config file.  5. Run iisreset from a command prompt. |

## Uninstalling the FIM Service and Portal Component of FIM 2010 R2

If you encounter an unrecoverable error and need to uninstall and then reinstall the FIM Service and Portal component of FIM 2010 R2, complete the following procedure to uninstall this component of FIM 2010 R2.

To uninstall the FIM Service component of FIM 2010 R2

|  |
| --- |
| 1. On the FIM 2010 R2 startup screen, click Install Service and Portal.  2. Run Setup.exe /l\*v logfile.txt from a command-line, and then follow the instructions in the installation wizard to remove the installation.  3. Delete the FIM Service database.  a. Open SQL Server Management Studio.  b. Select the FIMService database.  c. Right-click the database name, and then click Delete. |

Note

To be able to uninstall the FIM Portal component, you must be a SharePoint administrator. By default, a local server administrator is not granted administrator permissions in SharePoint. You must explicitly grant either SharePoint site administrator or secondary administrator permissions.

# Installing the FIM 2010 R2 Add-ins and Extensions

## Installing the FIM 2010 R2 Add-ins and Extensions

The FIM 2010 R2 Add-ins and Extensions components consist of the FIM 2010 R2 Add-in for Outlook and FIM 2010 R2 Password Reset Extensions.

With the FIM 2010 R2 Add-in for Outlook, users can join or leave an email enabled group. In addition, owners and approvers can approve or reject a request of any type made from the FIM Portal or FIM 2010 R2 Add-in for Outlook component.

With Password Reset, users can reset their passwords by using the Password Reset Portal, or 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.

To install the FIM 2010 R2 Add-ins and Extensions

|  |
| --- |
| 1. Exit Office Outlook, if it is running.  2. Depending on the client computer’s architecture, on the FIM 2010 R2 startup screen, click either the Install Add-ins and Extensions, 64 bit or the Install Add-ins and Extensions, 32 bit link.  3. Run setup.exe /l\*v logfile.txt from a command-line, and then follow the instructions in the installation wizard.  4. On the Welcome screen click Next.  Add-in Welcome    5. On the End User License Agreement page, read the License Agreement, select I accept the terms in the License Agreement, and then click Next.  6. On the FIM Customer Experience Improvement Program page, select I don’t want to join the program at this time, and then click Next.  7. On the Custom Setup page, select the features to install and click Next.  Custom Setup    8. On the Configure FIM Add-ins and Extensions page, in FIM Portal Server address, type the name or alias of the server that hosts the FIM Portal.  Note  This is the hostname, not the URL, of the FIM Service.  9. In FIM Service service account e-mail address, type the e-mail address in SMTP format—that is, in a format similar to someone@example.com—of the FIM Service service account. Do not type the alias or display name of the account.  Configure FIM Add-ins and Extensions    10. On the Configure FIM Add-ins and Extensions page, in FIM Service Server address, type the name or alias of the server that hosts the FIM Service. If the Service and Portal components are installed on the same server, this will be the same value as on the previous page.  Configure FIM Add-ins and Extensions    11. On the Configure FIM Add-ins and Extensions page, in the Intranet Registration Portal URL: box, enter the URL of the FIM 2010 R2 password registration portal that the rich client will navigate to by default. As part of the rich client password registration, the rich client will invoke the user's default browser to navigate to that URL if password registration be required.  Registration Portal URL    12. Click Install. |

# Installing the FIM 2010 R2 Language Packs

## Installing the FIM 2010 R2 Language Packs

With the release of FIM 2010 R2, the SSPR Registration and Reset portals and the Add-ins and Extensions are available in 33 languages. The FIM Service and Portal is available in 19 languages.

The FIM 2010 R2 Language Packs consist of the Add-ins and Extensions Language Pack and the Service and Portal Language Pack.

These language packs are a separate download and are not shipped on the installation media. These language packs can be downloaded from http://go.microsoft.com/fwlink/?LinkID=215308.

The FIM Add-ins and Extensions client must be installed on a client machine before attempting to install the language packs.

The following procedures can be used when deploying either the Add-ins and Extensions Language Pack or the Service and Portal Language Pack.

Tip

Be aware that the installer UI has also been translated to 33 different languages so if you choose an MSI other than the English one, setup will appear in that particular language.

To install the FIM 2010 R2 Add-ins and Extensions Language Pack

|  |
| --- |
| 1. Navigate to the directory that has the Add-ins and Extensions Language Pack that is relevant for your client, either x86 (32-bit) or x64 (64-bit) and double-click Add-ins and Extensions Language Pack.msi. This will begin the installation.  2. On the Welcome screen click Next.  Add-in Welcome    3. On the End User License Agreement page, read the License Agreement, select I accept the terms in the License Agreement, and then click Next.  4. On the Custom Setup page, select the languages you wish to install and click Next.  Custom Setup    5. Click Install.  Warning  This may take some time if you are installing all of the language packs for the FIM Service.  6. Once the installation is done, click Finish. |

To install the FIM 2010 R2 Service and Portal Language Pack

|  |
| --- |
| 1. Navigate to the directory that has the Service and Portal Language Pack and double-click Service and Portal Language Pack.msi. This will begin the installation.  2. On the Welcome screen click Next.  Add-in Welcome    3. On the End User License Agreement page, read the License Agreement, select I accept the terms in the License Agreement, and then click Next.  4. On the Custom Setup page, select the features and the languages for those features and click Next.  Custom Setup    5. Click Install.  Warning  This may take some time if you are installing all of the language packs for the FIM Service.  6. Once the installation is done, click Finish. |

# Unattended Installation of FIM 2010 R2

## Unattended installation of FIM 2010 R2

All components of the FIM 2010 R2 accept properties that allow unattended and silent installation. Those properties can either be set in a Windows Installer Transform (MST) file or specified at the command line during installation.

The FIM 2010 R2 installation packages do not support advertisement (msiexec /j) or administrative (msiexec /a) installations.

There are several different ways to install FIM 2010 R2 silently (unattended). Two methods are described in this section: pass-in parameters in a command line and MST files. It is outside the scope of this document to describe unattended installations in general.

### Pass-in parameters on the command line

This can be used with Microsoft System Center Configuration Manager 2007. To install silently, use the command msiexec with an option, followed by properties, for example:

Msiexec /q /i NameofMSI.msi /Option ADDLOCAL=MSIFeatureName Property=Value

The possible values of MSIFeatureName and Property can be found in Features and properties later in this document. Note that all parameters are case sensitive.

The following is an example command for an installation of FIM Add-ins and Extensions from a file server where only the FIM Outlook add-in is installed:

msiexec /i “\\MyServer\Distribution\FIM\32\Add-ins and extensions.msi” /quiet ADDLOCAL=OfficeClient PORTAL\_LOCATION=MyPortalServer PORTAL\_PREFIX=https MONITORED\_EMAIL=fimservice@contoso.com

Msiexec has several command line switches for silent installations. Of those, only a limited number are supported. The following table is a list of supported switches.

|  |  |  |
| --- | --- | --- |
| Switch | Supported or Not Supported | Description |
| /quiet/q:n | Supported | Installation with no UI at all |
| /q:f | Supported | (Full UI) The usual User Interface Wizard behavior. |
| /q:b | Not supported | (Basic) No pop-ups, except error messages. |
| /q:r | Not supported | (Reduced) Similar to basic. |
| /a | Not supported | (Admin) Will unpack an MSI to have all files external. Since this is how we deliver the MSI, no need to support this. Will run the Admin sequences, but no compelling scenario for this. |
| /x | Supported | Uninstall of the product |
| /j | Not supported | No scenarios. (We don’t have install on demand.) |

Note

Windows Installer has a limit of 256 characters in the path when for installation of applications. Ensure that you do not place the root of the tree in a very deep structure, or the installation might fail.

### Create an MST file

Another solution is to use an MST file. MST files can be created with tools such as Orca (shipped with the Windows Software Development Kit (SDK)), and they contain the same settings as are passed in on the command line.

### Troubleshoot an installation

If an unattended installation fails, add the option /l\*v NameOfLogFile.txt to the command line. This option creates a log file that you can use for troubleshooting. You can identify an error in a Windows Installer log file by looking for the text Return Value 3.

Also, you can you the msiexec file without the /q switch. This will cause the UI to appear and the values you have specified in the msiexec command-line will be populated in their respective locations. This is good for determining if the correct value is being set or not.

### Features and properties

The first table is listing the feature name in the UI and its feature name in the Synchronization Service.msi, Service and Portal.msi and the Add-ins and Extensions.msi. The second table is listing the feature name in the UI and its feature name in the Add-ins and Extensions.msi. The third table is the feature name in the UI and its feature name in the Service and Portal Language Pack.msi. These can all be used by the ADDLOCAL, REINSTALL, and REMOVE properties above.The tables in this section list the settings in the order that they appear during the user interface (UI) installation. Default values are in brackets.

Table 1  FIM 2010 R2 Windows Installer Features

|  |  |
| --- | --- |
| Name of the feature in the UI | Windows Installer feature name |
| FIM Add-in for Outlook | OfficeClient |
| FIM Password and Authentication Extensions | PasswordClient |
| FIM Service | CommonServices |
| FIM Portal | WebPortals |
| FIM Password Reset Portal | PwdPortals |
| FIM Synchronization Service | N/A (only one feature in the installer) |
| Forefront Identity Manager Certificate Management (FIM CM) Update Service | CLM\_Service |
| FIM CM Portal | Web\_Files |
| FIM CM CA Modules | CA\_Modules |
| FIM CM Smart Card PIN Reset Tool | ChangePin |
| FIM CM Smart Card Personalization Control | AppletManagement |
| FIM CM Smart Card Client | SelfServiceControl |
| FIM CM Update Client | ProfileUpdateControl |
| FIM CM Bulk Issuance Client | ClientFiles |
| Microsoft Password Change Notification Service | PCNSSVC |
| FIM Password and Authentication Extensions  FIM Password and Authentication Extensions for Windows XP  FIM Password and Authentication Extensions for Windows Vista | PasswordClient |
| FIM Password Registration Portal | RegistrationPortal |
| FIM Password Reset Portal | ResetPortal |

Table 2 Service and Portal Language Pack Features

|  |  |
| --- | --- |
| Feature | Description |
| FIMPortalLP | Installs Languages for the FIM Portal |
| FIMServiceLP | Installs Languages for the FIM Service |
| FIMResetPortalLP | Installs Languages for the FIM Password Reset Portal |
| FIMRegistrationPortalLP | Installs Languages for the FIM Password Registration Portal |
| PortalzhCN | Chinese (Simplified) language pack for FIM Portal. |
| PortalzhTW | Chinese (Taiwan) language pack for FIM Portal. |
| PortalcsCZ | Czech language pack for FIM Portal. |
| PortaldaDK | Danish language pack for FIM Portal. |
| PortalnlNL | Dutch language pack for FIM Portal. |
| PortalfiFI | Finnish language pack for FIM Portal. |
| PortalfrFR | French language pack for FIM Portal. |
| PortaldeDE | German language pack for FIM Portal. |
| PortalitIT | Italian language pack for FIM Portal. |
| PortaljaJP | Japanese language pack for FIM Portal. |
| PortalkoKR | Korean language pack for FIM Portal. |
| PortalnbNO | Norwegian language pack for FIM Portal. |
| PortalplPL | Polish language pack for FIM Portal. |
| PortalptBR | Portuguese (Brazil) language pack for FIM Portal. |
| PortalptPT | Portuguese (Portugal) language pack for FIM Portal. |
| PortalruRU | Russian language pack for FIM Portal. |
| PortalesES | Spanish language pack for FIM Portal. |
| PortalsvSE | Swedish language pack for FIM Portal. |
| PortaltrTR | Turkish language pack for FIM Portal. |
| MTzhCN | Chinese (Simplified) language pack for FIM Service. |
| MTzhTW | Chinese (Taiwan) language pack for FIM Service. |
| MTcsCZ | Czech language pack for FIM Service. |
| MTdaDK | Danish language pack for FIM Service. |
| MTnlNL | Dutch language pack for FIM Service. |
| MTfiFI | Finnish language pack for FIM Service. |
| MTfrFR | French language pack for FIM Service. |
| MTdeDE | German language pack for FIM Service. |
| MTitIT | Italian language pack for FIM Service. |
| MTjaJP | Japanese language pack for FIM Service. |
| MTkoKR | Korean language pack for FIM Service. |
| MTnbNO | Norwegian language pack for FIM Service. |
| MTplPL | Polish language pack for FIM Service. |
| MTptBR | Portuguese (Brazil) language pack for FIM Service. |
| MTptPT | Portuguese (Portugal) language pack for FIM Service. |
| MTruRU | Russian language pack for FIM Service. |
| MTesES | Spanish language pack for FIM Service. |
| MTsvSE | Swedish language pack for FIM Service. |
| MTtrTR | Turkish language pack for FIM Service. |
| ResetbgBG | Bulgarian language pack for FIM Password Reset Portal. |
| ResetzhCN | Chinese (Simplified) language pack for FIM Password Reset Portal. |
| ResetzhTW | Chinese (Taiwan) language pack for FIM Password Reset Portal. |
| ResethrHR | Croatian language pack for FIM Password Reset Portal. |
| ResetcsCZ | Czech language pack for FIM Password Reset Portal. |
| ResetdaDK | Danish language pack for FIM Password Reset Portal. |
| ResetnlNL | Dutch language pack for FIM Password Reset Portal. |
| ResetetEE | Estonian language pack for FIM Password Reset Portal. |
| ResetfiFI | Finnish language pack for FIM Password Reset Portal. |
| ResetfrFR | French language pack for FIM Password Reset Portal. |
| ResetdeDE | German language pack for FIM Password Reset Portal. |
| ResetelGR | Greek language pack for FIM Password Reset Portal. |
| ResethiIN | Hindi language pack for FIM Password Reset Portal. |
| ResethuHU | Hungarian language pack for FIM Password Reset Portal. |
| ResetitIT | Italian language pack for FIM Password Reset Portal. |
| ResetjaJP | Japanese language pack for FIM Password Reset Portal. |
| ResetkoKR | Korean language pack for FIM Password Reset Portal. |
| ResetlvLV | Latvian language pack for FIM Password Reset Portal. |
| ResetltLT | Lithuanian language pack for FIM Password Reset Portal. |
| ResetnbNO | Norwegian language pack for FIM Password Reset Portal. |
| ResetplPL | Polish language pack for FIM Password Reset Portal. |
| ResetptBR | Portuguese (Brazil) language pack for FIM Password Reset Portal. |
| ResetptPT | Portuguese (Portugal) language pack for FIM Password Reset Portal. |
| ResetroRO | Romanian language pack for FIM Password Reset Portal. |
| ResetruRU | Russian language pack for FIM Password Reset Portal. |
| ResetsrCS | Serbian language pack for FIM Password Reset Portal. |
| ResetskSK | Slovak language pack for FIM Password Reset Portal. |
| ResetslSI | Slovenian language pack for FIM Password Reset Portal. |
| ResetesES | Spanish language pack for FIM Password Reset Portal. |
| ResetsvSE | Swedish language pack for FIM Password Reset Portal. |
| ResetthTH | Thai language pack for FIM Password Reset Portal. |
| ResettrTR | Turkish language pack for FIM Password Reset Portal. |
| ResetukUA | Ukranian language pack for FIM Password Reset Portal. |
| RegistrationbgBG | Bulgarian language pack for FIM Password Registration Portal. |
| RegistrationzhCN | Chinese (Simplified) language pack for FIM Password Registration Portal. |
| RegistrationzhTW | Chinese (Taiwan) language pack for FIM Password Registration Portal. |
| RegistrationhrHR | Croatian language pack for FIM Password Registration Portal. |
| RegistrationcsCZ | Czech language pack for FIM Password Registration Portal. |
| RegistrationdaDK | Danish language pack for FIM Password Registration Portal. |
| RegistrationnlNL | Dutch language pack for FIM Password Registration Portal. |
| RegistrationetEE | Estonian language pack for FIM Password Registration Portal. |
| RegistrationfiFI | Finnish language pack for FIM Password Registration Portal. |
| RegistrationfrFR | French language pack for FIM Password Registration Portal. |
| RegistrationdeDE | German language pack for FIM Password Registration Portal. |
| RegistrationelGR | Greek language pack for FIM Password Registration Portal. |
| RegistrationhiIN | Hindi language pack for FIM Password Registration Portal. |
| RegistrationhuHU | Hungarian language pack for FIM Password Registration Portal. |
| RegistrationitIT | Italian language pack for FIM Password Registration Portal. |
| RegistrationjaJP | Japanese language pack for FIM Password Registration Portal. |
| RegistrationkoKR | Korean language pack for FIM Password Registration Portal. |
| RegistrationlvLV | Latvian language pack for FIM Password Registration Portal. |
| RegistrationltLT | Lithuanian language pack for FIM Password Registration Portal. |
| RegistrationnbNO | Norwegian language pack for FIM Password Registration Portal. |
| RegistrationplPL | Polish language pack for FIM Password Registration Portal. |
| RegistrationptBR | Portuguese (Brazil) language pack for FIM Password Registration Portal. |
| RegistrationptPT | Portuguese (Portugal) language pack for FIM Password Registration Portal. |
| RegistrationroRO | Romanian language pack for FIM Password Registration Portal. |
| RegistrationruRU | Russian language pack for FIM Password Registration Portal. |
| RegistrationsrCS | Serbian language pack for FIM Password Registration Portal. |
| RegistrationskSK | Slovak language pack for FIM Password Registration Portal. |
| RegistrationslSI | Slovenian language pack for FIM Password Registration Portal. |
| RegistrationesES | Spanish language pack for FIM Password Registration Portal. |
| RegistrationsvSE | Swedish language pack for FIM Password Registration Portal. |
| RegistrationthTH | Thai language pack for FIM Password Registration Portal. |
| RegistrationtrTR | Turkish language pack for FIM Password Registration Portal. |
| RegistrationukUA | Ukranian language pack for FIM Password Registration Portal. |

Table 3 Add-ins and Extensions Language Pack Features

|  |  |
| --- | --- |
| Feature | Description |
| FIMALP | FIM Add-ins and Extensions Language Pack |
| bgBG | Bulgarian language |
| zhCN | Chinese (Simplified) language |
| zhTW | Chinese (Taiwan) language |
| hrHR | Croatian language |
| csCZ | Czech language |
| daDK | Danish language |
| nlNL | Dutch language |
| etEE | Estonian language |
| fiFI | Finnish language |
| frFR | French language |
| deDE | German language |
| elGR | Greek language |
| hiIN | Hindi language |
| huHU | Hungarian language |
| itIT | Italian language |
| jaJP | Japanese language |
| koKR | Korean language |
| lvLV | Latvian language |
| ltLT | Lithuanian language |
| nbNO | Norwegian language |
| plPL | Polish language |
| ptBR | Portuguese (Brazil) language |
| ptPT | Portuguese (Portugal) language |
| roRO | Romanian language |
| ruRU | Russian language |
| srCS | Serbian language |
| skSK | Slovak language |
| slSI | Slovenian language |
| esES | Spanish language |
| svSE | Swedish language |
| thTH | Thai language |
| trTR | Turkish language |
| ukUA | Ukranian language |

The following tables list the properties that are associated with the features from above.

Table 4  Synchronization Service properties

|  |  |
| --- | --- |
| Property Name | Description |
| STORESERVER | Name of SQL Server |
| SQLDB | Name of database (FIMSynchronization) |
| SQLINSTANCE | Name of database instance |
| SERVICEACCOUNT | (Required) Service account name |
| SERVICEPASSWORD | Required) Service account password |
| SERVICEDOMAIN | (Required) Service account domain |
| GROUPADMINS | Name of admin group (FIMSyncAdmins) |
| GROUPOPERATORS | Name of operators group (FIMSyncOperators) |
| GROUPACCOUNTJOINERS | Name of joiners group (FIMSyncJoiners) |
| GROUPBROWSE | Name of browse group (FIMSyncBrowse) |
| GROUPPASSWORDSET | Name of password set group (FIMSyncPasswordSet) |
| FIREWALL\_CONF | 0 – Do not configure firewall (default)1 – Configure firewall |

Table 5  FIM Service and FIM Portal properties

|  |  |
| --- | --- |
| Property name | Description |
| SQMOPTINSETTING | 1 – opt in, 0 – opt out (default) |
| SQLSERVER\_SERVER | (Required) Name of SQL Server instance |
| SQLSERVER\_DATABASE | Name of database (FIMService) |
| EXISTINGDATABASE | 0 – New database (default), 1 – Existing database |
| MAIL\_SERVER | (Required) Name of mailserver |
| MAIL\_SERVER\_USE\_SSL | 0 – Disable SSL, 1 – Enable SSL (default) |
| MAIL\_SERVER\_IS\_EXCHANGE | 0 – SMTP, 1 – Exchange (default) |
| SERVICE\_MANAGER\_SERVER | Name of the FIM Reporting Service Manager management server. |
| POLL\_EXCHANGE\_ENABLED | 0 – Server will not poll for e-mail messages1 – Server will poll for e-mail messages (default) |
| CERTIFICATE\_NAME | Name of certificate to generate (ForefrontIdentityManager) |
| SERVICE\_ACCOUNT\_NAME | (Required) Service account name |
| SERVICE\_ACCOUNT\_PASSWORD | (Required) Service account password |
| SERVICE\_ACCOUNT\_DOMAIN | (Required) Service account domain |
| SERVICE\_ACCOUNT\_EMAIL | (Required) Service account e-mail address |
| SYNCHRONIZATION\_SERVER | (Required) Address of FIM Synchronization Service server |
| SYNCHRONIZATION\_SERVER\_ACCOUNT | FIM Service Management Agent account in format domain\accountname |
| SERVICEADDRESS | Address used by clients to contact the server |
| SHAREPOINT\_URL | URL used to contact the SharePoint server |
| REGISTRATION\_PORTAL\_URL | An optional URL of the FIM 2010 R2 password registration portal that the FIM portal will redirect to when the user clicks on the "Register for password reset" FIM portal homepage link. |
| FIREWALL\_CONF | 0 – Do not configure firewall (default)1 – Configure firewall |
| SHAREPOINTUSERS\_CONF | 0 – Do not add authenticated users (default1 – Add authenticated users |
| PASSWORDUSERS\_CONF | 0 – Do not add authenticated users (default1 – Add authenticated users |
| REQUIRE\_REGISTRATIONPORTAL\_INFO | 0 – Do not require password registration information (default)1 – Require password registration information |
| REGISTRATION\_ACCOUNT\_NAME | Account name of the application pool account that will run the password registration portal. |
| REGISTRATION\_ACCOUNT\_DOMAIN | Domain of the application pool account that will run the password registration portal. |
| REQUIRE\_RESET\_INFO | 0 – Do not require password reset information (default)1 – Require password reset information |
| RESET\_ACCOUNT\_NAME | Account name of the application pool account that will run the password reset portal. |
| RESET\_ACCOUNT\_DOMAIN | Domain of the application pool account that will run the password reset portal. |
| SHAREPOINTTIMEOUT | Timeout in seconds the installer should wait for Office SharePoint to deploy the solution packs. |

Table 6 FIM 2010 R2 Certificate Management properties

|  |  |
| --- | --- |
| Property Name | Description |
| WEBAPPNAME | Name of the virtual folder for certificate Management. |
| SITELOCK\_DOMAIN | List of sites used by FIM CM installations. This list is used for ActiveX controls to initiate. |

Table 7  Add-ins and Extensions properties

|  |  |
| --- | --- |
| Property name | Description |
| SQMOPTINSETTING | 1 – opt in, 0 – opt out (default) |
| PORTAL\_LOCATION | Address to the FIM Portal. Used by Outlook add-in. |
| PORTAL\_PREFIX | Prefix used to contact the FIM Portal. http or https (default) |
| MONITORED\_EMAIL | FIM Service e-mail address. Used by the Outlook add-in when sending e-mail messages. |
| RMS\_LOCATION | Address to the FIM Service. Used by Password Reset extensions |
| REGISTRATION\_PORTAL\_URL | The URL of the FIM 2010 R2 password registration portal that the rich client will navigate to by default. As part of the rich client password registration, the rich client will invoke the user's default browser to navigate to that URL if password registration be required. As part of the rich client password registration, the rich client will invoke the user's default browser to navigate to this URL if password registration be required. |
| BEST\_EFFORT\_INSTALL | If both components are selected, but one cannot be installed due to failed prerequisites, silently continue installation with the other component.  0 – Fail installation (default)  1 – Silently continue |

The following is an example of installing the FIM 2010 R2 Synchronization Service:

msiexec /q /i “D:\Synchronization Service\Synchronization Service.msi" STORESERVER=LocalMachine SQLDB=FIMSynchronization SERVICEACCOUNT=FimSynchService SERVICEPASSWORD=Pass1word! SERVICEDOMAIN=CORP GROUPADMINS=FIMSyncAdmins GROUPOPERATORS=FIMSyncOperators GROUPACCOUNTJOINERS=FIMSyncJoiners GROUPBROWSE=FIMSyncBrowse GROUPPASSWORDSET=FIMSyncPasswordSet FIREWALL\_CONF=1 /L\*v C:\mylogfile.txt

The following is an example of installing the FIM 2010 R2 Service and Portal:

msiexec /q /i "D:\Service and Portal\Service and Portal.msi" ADDLOCAL=CommonServices,WebPortals SQMOPTINSETTING=0 SQLSERVER\_SERVER=APP1 SQLSERVER\_DATABASE=FIMService EXISTINGDATABASE=0 MAIL\_SERVER=EX1.corp.contoso.com MAIL\_SERVER\_USE\_SSL=0 MAIL\_SERVER\_IS\_EXCHANGE=1 POLL\_EXCHANGE\_ENABLED=1 CERTIFICATE\_NAME=ForefrontIdentityManager SERVICE\_ACCOUNT\_NAME=FIMService SERVICE\_ACCOUNT\_PASSWORD=abc123\*2k SERVICE\_ACCOUNT\_DOMAIN=CORP SERVICE\_ACCOUNT\_EMAIL=FIMService@corp.contoso.com SERVICE\_MANAGER\_SERVER=APP2 SYNCHRONIZATION\_SERVER=FIM1 SYNCHRONIZATION\_SERVER\_ACCOUNT=CORP\FIMMA SERVICEADDRESS=FIM1 SHAREPOINT\_URL=http://localhost REGISTRATION\_PORTAL\_URL=https://passwordregistration.corp.contoso.com FIREWALL\_CONF=1 SHAREPOINTUSERS\_CONF=1 REQUIRE\_REGISTRATION\_INFO=1 REGISTRATION\_ACCOUNT\_NAME=FIMPassword REGISTRATION\_ACCOUNT\_DOMAIN=CORP REQUIRE\_RESET\_INFO=1 RESET\_ACCOUNT\_NAME=FIMPassword RESET\_ACCOUNT\_DOMAIN=CORP /L\*v C:\fimservicelog.txt

The following is an example of a command-line installation for the Password Reset and Registration Portal.

msiexec /q /i “D:\Service and Portal\Service and Portal.msi" ADDLOCAL=RegistrationPortal,ResetPortal REGISTRATION\_ACCOUNT=CORP\FIMPassword REGISTRATION\_ACCOUNT\_PASSWORD=Pass1word$ REGISTRATION\_HOSTNAME=passwordregistration.corp.contoso.com REGISTRATION\_PORT=80 REGISTRATION\_FIREWALL\_CONFIG=1 REGISTRATION\_SERVERNAME=FIM1 IS\_REGISTRATION\_EXTRANET=Extranet RESET\_ACCOUNT=CORP\FIMPassword RESET\_ACCOUNT\_PASSWORD=Pass1word$ RESET\_HOSTNAME=passwordreset.corp.contoso.com RESET\_PORT=81 RESET\_FIREWALL\_CONF=1 RESET\_SERVERNAME=FIM1 IS\_RESET\_EXTRANET=Extranet /L\*v C:\mylogfile.txt

The following is an example of a command-line installation for the FIM CM Web Portal and FIM CM Update Service of FIM 2010 Certificate Management

msiexec /q /i “D:\Certificate Management\x64\Certificate Management.msi" ADDLOCAL=CLM\_Service,Web\_Files WEBAPPNAME=CertificateManagement /L\*v C:\mylogfile.txt

The following is an example of a command-line installation for the FIM CM CA Modules of FIM 2010 Certificate Management

msiexec /q /i “D:\Certificate Management\x64\Certificate Management.msi" ADDLOCAL=CA\_Modules /L\*v C:\mylogfile.txt

The following is an example of a command-line installation for the FIM CM Client of FIM 2010 Certificate Management

msiexec /q /i “D:\CM Client\x64\CM Client.msi" ADDLOCAL=CMClient,ChangePin,AppletManagement,SelfServiceControl,ProfileUpdateControl /L\*v C:\mylogfile.txt

The following is an example of installing the Add-ins and Extensions:

msiexec /q /i “D:\Add-ins and extesnisons\x64\Add-ins and extensions.msi" ADDLOCAL=OfficeClient,PasswordClient PORTAL\_LOCATION=FIM1 PORTAL\_PREFIX=http RMS\_LOCATION=FIM1 MONITORED\_EMAIL=FIMService@corp.contoso.com REGISTRATION\_PORTAL\_URL=https://passwordregistratio.corp.contoso.com /L\*v C:\mylogfile.txt

The following is an example of installing the Service and Portal Language Pack. It shows how to install the Japanese language pack for all of the components

msiexec /q /i “D:\Service and Portal Language Pack\Service and Portal Language Pack.msi" ADDLOCAL=FIMPortalLP,PortaljaJP,FIMServiceLP,MTjaJP, FIMResetPortalLP,ResetjaJP,FIMRegistrationPortalLP,RegistrationjaJP /L\*v C:\mylogfile.txt

The following is an example of installing the Add-ins and Extensions Language Pack. It shows how to install the Japanese language.

msiexec /q /i “D:\Add-ins and Extensions Language Pack\Add-ins and Extensions Language Pack.msi" ADDLOCAL=FIMALP,jaJP /L\*v C:\mylogfile.txt

# Common Post-installation Configuration for Forefront Identity Manager 2010 R2

The Microsoft® Forefront® Identity Manager (FIM) 2010 R2 Post-Installation Configuration provides information and procedures to information technology (IT) professionals regarding common post-installation FIM 2010 R2 configuration steps. Depending on your deployment scenarios, some of the steps in this guide may be optional.

This section provides information on the following:

 [Create a Backup Administrator account for the FIMService after installation](#z21)

 [Isolate log files from data files](#z22)

 [Create additional tempdb files](#z23)

 [Ensure adequate space for log files](#z24)

 [Limit SQL Server memory use](#z25)

 [SQL Server Database Configuration - General](#z26)

 [Presize data and log files](#z27)

 [Configure synchronization rule provisioning](#z28)

 [Active Directory–to–FIM 2010 R2 Initial Data Load](#z29)

 [Configuring General MPRs](#z30)

 [Enable WCF Performance Counters](#z31)

## Create a Backup Administrator account for the FIMService after installation

Members of the FIMService Administrators set have unique permissions critical to the operation of your FIM 2010 R2 deployment. If you are unable to logon as part of the Administrators set, the only resolution is to roll back to a previous backup of the system. To mitigate this situation, we recommend that you add other users to the FIM Administrative set as part of your post-installation configuration.

Warning

Deleting or modifying certain resources

Deleting or modifying certain default resources within the FIM Portal can disrupt operations or even render the portal inoperable. The following is a list of resources that should never be deleted from the FIM portal:

 Default Administrator in the Administrators Set

 Administrators Set

 DefaultRCDC objects

 Default MPRs

To resolve this issue, you will need to restore the FIM database from backup or contact Microsoft Product Support.

Additionally, changes to certain default RCDC resource attributes will result in the RCDC object being replaced. The FIM Portal references default RCDC resources by their GUID. When these are deleted the GUID is no longer available and the FIM Portal is unable to reference them. The following is a list of these attributes:

 DisplayName

 AppliesToCreate

 AppliesToEdit

 AppliesToView

When these attributes are modified, a new GUID is created for the RCDC object. At this point, the FIM Portal is unaware of the RCDC object because it is unaware of the new GUID.

## Isolate log files from data files

Follow SQL Server best practices for isolating the transaction files and the data log files for the databases onto separate physical disks. For more information see [Storage Top 10 Practices](http://technet.microsoft.com/en-us/library/cc966534.aspx)

## Create additional tempdb files

For optimal performance, we recommend that you create one data file per CPU core in the tempdb. As for log and data files, you should also adequately presize your tempdb files and rely on AUTOGROW ON only for safety reasons.

To create additional tempdb files

|  |
| --- |
| 1. Start SQL Server Enterprise Manager.  2. Navigate to the database tempdb in System Databases, right-click tempdb, and then click Properties.  3. On the Files page, create one data file per CPU core. Make sure that you separate the tempdb Data and Log files on different drives and spindles. |

## Ensure adequate space for log files

Make sure that you know your recovery model’s disk requirements. Simple recovery mode may be appropriate during initial system load, to limit the use of disk space, but you might have exposure to data loss since the most recent backup. When you use full recovery mode, you have to manage the disk use through backups, which includes frequent backups of the transaction log to prevent high disk space usage. For more information about managing recovery, see [Recovery Model Overview](http://go.microsoft.com/fwlink/?LinkID=185370) (http://go.microsoft.com/fwlink/?LinkID=185370)

## Limit SQL Server memory use

Depending on how much memory you have on your computer running SQL Server and if you share the SQL Server on that computer with other services, such as FIMService and FIMSynchronizationService, you might want to restrict the memory consumption of SQL Server. You can use the following procedure to limit SQL Server memory use.

To limit SQL Server memory use

|  |
| --- |
| 1. Start SQL Enterprise Manager.  2. Click New Query.  3. Run the following query:  USE master  EXEC sp\_configure 'show advanced options', 1  RECONFIGURE WITH OVERRIDE  The following example reconfigures SQL Server so that it will not use more than 12 gigabytes (GB) of memory.  USE master  EXEC sp\_configure 'max server memory (MB)', 12000--- max=12G  RECONFIGURE WITH OVERRIDE  4. Verify the setting using the following query:  USE master  EXEC sp\_configure 'max server memory (MB)'--- verify the setting  USE master  EXEC sp\_configure 'show advanced options', 0  Reconfigure with override |

## SQL Server Database Configuration - General

Configuration of SQL Server is critical for optimal system performance. Achieving optimal FIM performance in large-scale deployment scenarios depends on applying best practices for SQL Server. The guidance in this section applies to both the FIM Service Database and the FIM Synchronization Database. We recommend that you apply the following SQL Server best practices:

 [Storage Top 10 Best Practices](http://go.microsoft.com/fwlink/?LinkID=183663) (http://go.microsoft.com/fwlink/?LinkID=183663)

 [Optimizing tempdb Performance](http://go.microsoft.com/fwlink/?LinkId=188267) (http://go.microsoft.com/fwlink/?LinkId=188267)

 [Predeployment I/O Best Practices](http://go.microsoft.com/fwlink/?LinkId=188268) (http://go.microsoft.com/fwlink/?LinkId=188268)

 [Reorganizing and Rebuilding Indexes](http://go.microsoft.com/fwlink/?LinkId=188269) (http://go.microsoft.com/fwlink/?LinkId=188269)

## Presize data and log files

Do not rely on AUTOGROW. Instead, manage the growth of these files manually. You may leave AUTOGROW ON for safety reasons, but you should manage the growth of the data files proactively. You can find sample sizes for the FIM database in the [FIM Capacity Planning Guide](http://go.microsoft.com/fwlink/?LinkID=185246).

To presize data and log files

|  |
| --- |
| 1. Start SQL Server Enterprise Manager.  2. Right-click the database FIMService, and then click Properties.  3. On the Files page, expand the database files to the required size. |

## Configure synchronization rule provisioning

This section explains how to configure the FIM Synchronization Service to support declarative provisioning and the use of synchronization rules in FIM 2010 R2. First, you have to turn on synchronization rule processing in the Synchronization Service Manager.

Note

To perform this procedure, you must be a member of the FIMSyncAdmins role for the FIM Synchronization Service.

To turn on synchronization rule provisioning

|  |
| --- |
| 1. Open the Synchronization Service Manager.  2. On the Tools menu, click Options.  3. Select Enable Synchronization Rule Provisioning.  4. To close the Options dialog box, click OK. |

## Active Directory–to–FIM 2010 R2 Initial Data Load

One basic requirement of an identity management system is the ability to import and process identity data from an external system. One of the first steps in your deployments is to import and process existing users and possibly groups from Active Directory or AD DS to FIM 2010 R2. Before you do this, you should have completed the System Data Flow design to establish the connection systems relationships and required data flows. This is a one-time operation; it is not a continuous synchronization.

For details about setting up the synchronization of user data from Active Directory to FIM, see [How Do I Synchronize Users from Active Directory Domain Services to FIM](http://go.microsoft.com/fwlink/?LinkID=188277). Before you perform the procedures in this guide, complete the following steps to optimize your system for the initial, one-time configuration. The settings described here are temporary. You should set them only for the initial load of the data into the system.

### Step 1: Configure SQL Server for the initial data load

When you load a large amount of data, you can shorten the time it takes to populate the database by temporarily turning off the full text search. You can enable it again after the export on the FIM Management Agent is complete. Complete the following steps to temporarily turn off full text search:

To configure SQL Server for the initial data load

|  |
| --- |
| 1. Start SQL Enterprise Manager.  2. Select New Query.  3. Run the following SQL statements:  ALTER FULLTEXT INDEX ON [fim].[ObjectValueString] SET CHANGE\_TRACKING = MANUAL  ALTER FULLTEXT INDEX ON [fim].[ObjectValueXml] SET CHANGE\_TRACKING = MANUAL |

It is important to understand the disk requirements in the SQL Server recovery model. Depending on your backup schedule, you may consider using simple recovery mode during initial system load to limit disk space usage. However, you should be aware of the implications regarding potential data loss. When you use full recovery mode, you must manage disk use through backups, including frequent backups of the transaction log to prevent high disk space use.

Important

Not implementing these procedures can result in high disk space use, possibly resulting in running out of disk space. For more information, see [Recovery Model Overview](http://go.microsoft.com/fwlink/?LinkID=185370) (http://go.microsoft.com/fwlink/?LinkID=185370). The [FIM 2010 Backup and Restore Guide](http://technet.microsoft.com/en-us/library/fim-2010-backup-and-restore-guide(WS.10).aspx) (http://technet.microsoft.com/en-us/library/fim-2010-backup-and-restore-guide(WS.10).aspx) contains additional information.

### Step 2: Apply minimum necessary FIM configuration during the load process

During the initial load process, apply only the minimum configuration required to your FIM configuration in terms of MPRs and set definitions. After the data is loaded, create the additional sets required for your deployment. Use the run-on policy update setting on action workflows to apply those policies retroactively on the loaded data.

### Step 3: Configure and populate the FIM Service with external identity data

At this point, you should follow the procedures in [How Do I Synchronize Users from Active Directory Domain Services to FIM](http://go.microsoft.com/fwlink/?LinkID=188277) to configure and synchronize your system with users from Active Directory or AD DS. To synchronize Group information, see [How Do I Synchronize Groups from Active Directory Domain Services to FIM](http://go.microsoft.com/fwlink/?LinkID=188278).

### Step 4: Apply your full FIM configuration

When your initial data load is complete, you are ready to apply the full FIM configuration for your deployment. Depending on your scenarios, this may include the creation of additional sets, MPRs, and workflows. For any policies that you need to apply retroactively to all existing objects in the system, use the run-on policy update setting on action workflows to apply those policies retroactively on the loaded data.

### Step 5: Reconfigure SQL Server to previous settings

Remember to change the SQL Server settings to the normal settings, including the following:

 Turning on full text search

 Updating your backup policy in accordance with your organization policies

When you complete the initial data load, turn on full text search again. Run the following Structured Query Language (SQL) statements to turn on full text search again:

 ALTER FULLTEXT INDEX ON [fim].[ObjectValueString] SET CHANGE\_TRACKING = AUTO

 ALTER FULLTEXT INDEX ON [fim].[ObjectValueXml] SET CHANGE\_TRACKING = AUTO

If you have switch to simple recovery mode, ensure that you reconfigure your backup schedule in accordance with your organization’s backup policy. Additional details of FIM backup schedules are available in the [FIM 2010 Backup and Restore Guide](http://technet.microsoft.com/en-us/library/fim-2010-backup-and-restore-guide(WS.10).aspx) (http://technet.microsoft.com/en-us/library/fim-2010-backup-and-restore-guide(WS.10).aspx).

## Configuring General MPRs

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 mms Service. You do this by configuring existing MPRs in the system.

Configure the MPRs in the following table.

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

To enable required MPRs

|  |
| --- |
| 1. To open the FIM Portal, start Internet Explorer, and then navigate to http://localhost/identitymanagement/default.aspx.  Note  You may need to substitute this with the URL you have configured for your FIM portal.  2. On the FIM Portal home page, click Management Policy Rules in the navigation bar to open the Management Policy Rules page.  3. In the Search for text box, type the display name of each of the MPRs from the previous table, and then click the Search for button.  4. For each MPR that is listed as disabled, do the following:  a. To open the configuration dialog box, click the Display Name of the disabled MPR.  b. Clear the Policy is disabled check box, and then click OK.  c. On the Summary page, click Submit. |

You may plan 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 table using the previous procedure.

|  |
| --- |
| Display name |
| User management: Users can read selected attributes of other users |

Note

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

## Enable WCF Performance Counters

FIM 2010 R2 uses WCF performance counters to monitor service use. Monitoring service use with WCF performance counters is an optional step to enable when you are diagnosing performance problems. It is not necessary to leave performance counters enabled for normal operations. To enable and configure WCF performance counters, see [WCF Performance Counters](http://go.microsoft.com/fwlink/?LinkId=164848) (http://go.microsoft.com/fwlink/?LinkId=164848).

We recommend that you configure ServiceOnly WCF performance counters. However, to see Endpoint and Operation instances, it is necessary to configure all WCF performance counters.