

Test Lab Guide: Forefront Identity Manager 2010

Microsoft Corporation

Published: December 2010

Last Update: June 2011

Author: Bill Mathers

Version: 4.0

Acknowledgements

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

Glenn Zuckerman, Microsoft Corp.

Bahram Rushenas, Microsoft Corp.

Abstract

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

Copyright

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

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

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

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

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred.

© 2010 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Forefront, MSDN, Outlook, SharePoint, SQL Server, Windows, Windows PowerShell, and Windows Server are trademarks of the Microsoft group of companies.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

[Test Lab Guide: Forefront Identity Manager 2010 5](#_Toc296075503)

[In This Guide 5](#_Toc296075504)

[Test Lab Overview 6](#_Toc296075505)

[Hardware and Software Requirements 7](#_Toc296075506)

[Steps for Configuring the Forefront Identity Manager 2010 Test Lab 9](#_Toc296075507)

[Test Lab Guide Specific Information and Instructions 9](#_Toc296075508)

[Step 1: Set Up the Base Configuration Test Lab 10](#_Toc296075509)

[Step 2: Set Up the Exchange Server 2010 with Service Pack 1 Test Lab 10](#_Toc296075510)

[Step 3: Set Up the SQL Server 2008 Enterprise with Service Pack 2 Test Lab 10](#_Toc296075511)

[Step 4: Configure FIM1 10](#_Toc296075512)

[Install Windows Server 2008 R2 on FIM1 11](#_Toc296075513)

[Configure TCP/IP Properties on FIM1 11](#_Toc296075514)

[Rename and Join the Domain on FIM1 12](#_Toc296075515)

[Step 5: Install FIM 2010 Prerequisite Software 12](#_Toc296075516)

[Install the .NET Framework 3.5.1, IIS 7.5, and Windows PowerShell on FIM1 13](#_Toc296075517)

[Install Exchange Server 2010 with Service Pack 1 Management Console on FIM1 15](#_Toc296075518)

[Disable Internet Explorer Enhanced Security for Administrators on FIM1 17](#_Toc296075519)

[Install and Configure Windows SharePoint Services 3.0 with SP2 on FIM1 18](#_Toc296075520)

[Install Full Text Search on APP1 20](#_Toc296075521)

[Re-apply SQL Server 2008 Service Pack 2 on APP1 22](#_Toc296075522)

[Install the SQL Server 2008 Native Client on FIM1 22](#_Toc296075523)

[Step 6: Perform FIM 2010 Prerequisite Tasks 23](#_Toc296075524)

[Create the FIM Service Accounts 24](#_Toc296075525)

[Mailbox-Enable the CORP\FIMService Account 25](#_Toc296075526)

[Secure the CORP\FIMService and CORP\FIMSynchService Accounts 27](#_Toc296075527)

[Set the SQL Server Agent Service to Start Automatically 30](#_Toc296075528)

[Enable SQL Firewall Ports 31](#_Toc296075529)

[Enable SQL Server Network Protocols 32](#_Toc296075530)

[Verify That the FIM Installation Account Has SharePoint Permissions 34](#_Toc296075531)

[Change the SharePoint Application Pool Account to Use CORP\SPService 36](#_Toc296075532)

[Configure IIS to Use CORP\SPService for Kerberos Delegation 37](#_Toc296075533)

[Set the SPNs for CORP\SPService 39](#_Toc296075534)

[Set the SPNs for CORP\FIMService 40](#_Toc296075535)

[Turn on Delegation for CORP\SPService 41](#_Toc296075536)

[Turn on Delegation for CORP\FIMService 43](#_Toc296075537)

[Step 7: Install FIM Synchronization Service and FIM Portal 43](#_Toc296075538)

[Install the FIM Synchronization Service on FIM1 43](#_Toc296075539)

[Install the FIM Portal on FIM1 49](#_Toc296075540)

[Install the FIM Synchronization Service Update 1 on FIM1 58](#_Toc296075541)

[Install the FIM Portal and Service Update 1 on FIM1 59](#_Toc296075542)

[Step 8: Perform FIM 2010 Post-Installation Tasks 60](#_Toc296075543)

[Add CORP\FIMService to the FIMSyncAdmins Group 60](#_Toc296075544)

[Configure the CORP\FIMService Mailbox to Only Accept Mail from Internal E-mail Addresses 62](#_Toc296075545)

[Configure the CORP\FIMService Mailbox to Reject E-mail Greater Than 1 MB 63](#_Toc296075546)

[Turn Off NTLM Authentication for the FIM Portal 64](#_Toc296075547)

[Disable SharePoint Indexing 65](#_Toc296075548)

[Implement Secure Sockets Layer (SSL) for the FIM Portal 66](#_Toc296075549)

[Add the FIM Portal URL to Local Intranet Sites for CORP\Administrator 68](#_Toc296075550)

[Restrict Membership in the User Administrators Set 69](#_Toc296075551)

[Pre-allocate Space in the FIM Service Database 70](#_Toc296075552)

[Pre-allocate Space in the FIM Synchronization Service Database 71](#_Toc296075553)

[Step 9: Verify the Installation 71](#_Toc296075554)

[Verify the E-mail Server, Database Server, and MA Account 72](#_Toc296075555)

[Verify the Build Numbers of the FIM Service and the FIM Synchronization Service 72](#_Toc296075556)

[Snapshot the Configuration 73](#_Toc296075557)

# Test Lab Guide: Forefront Identity Manager 2010

Microsoft® Forefront® Identity Manager (FIM) 2010 changes the current state of identity management by providing powerful end user self-service capabilities. IT pros are also given more tools to solve day-to-day tasks, such as delegating administration and creating workflows for common identity management tasks. In addition, FIM 2010 is built on a .NET and WS-\* based foundation for developers to build more customized and extensible solutions.

Microsoft Forefront Identity Manager 2010 helps IT pros achieve new levels of reliability with greater flexibility, enhanced user experiences, and increased protection for business communications by doing the following:

 Empowering people:

 With FIM 2010 end-users can easily perform self-service tasks, such as group and distribution list management with self-help tools integrated into a Microsoft SharePoint® based console as well as directly in Microsoft Office Outlook®.

 FIM 2010 provides IT professionals with the tools they need to manage identities through a SharePoint-based policy and workflow management console.

 Developers have access to extensibility features through extensive public APIs.

 Delivering agility and efficiency:

 FIM 2010 integrates an enterprises' heterogeneous infrastructure, including directories, databases, and line-of-business applications.

 FIM 2010 enables management of heterogeneous strong-authentication systems, such as third-party certificate authorities.

 Increasing security and compliance:

 FIM 2010 provides management features that enable system auditing and compliance. By integrating the tools IT pros use to manage identities, credentials, and resources, FIM 2010 helps organizations integrate policies across the organization and secure the enterprise.

 Integrated management tools allow organizations to better enjoy the security benefits of strong authentication.

## In This Guide

This guide contains instructions for setting up a test lab based on the Forefront Identity Manager 2010 Test Lab Guide and deploying Forefront Identity Manager 2010 using one new server computer, two preexisting server computers, and one preexisting client computer. The resulting Forefront Identity Manager 2010 test lab demonstrates and verifies installation. Future test lab guides will demonstrate the powerful functionalities of FIM 2010.

Important

The following instructions are for configuring a Forefront Identity Manager 2010 test lab using a scaled-out deployment. That is, the FIM Portal and the FIM database will not be residing on the same server. Individual computers are needed to separate the services provided on the network and to clearly show the desired functionality. This configuration is neither designed to reflect best practices nor does it reflect a desired or recommended configuration for a production network. The configuration, including IP addresses and all other configuration parameters, is designed only to work on a separate test lab network.

Attempting to adapt this Forefront Identity Manager 2010 test lab configuration to a pilot or production deployment can result in configuration or functionality issues. To ensure proper configuration and operation for your pilot or production Forefront Identity Manager 2010 deployment, use the information in [Planning and Architecture](http://go.microsoft.com/fwlink/?LinkId=204576) (http://go.microsoft.com/fwlink/?LinkId=204576) for planning and design decisions and [Deployment](http://go.microsoft.com/fwlink/?LinkId=204575) (http://go.microsoft.com/fwlink/?LinkId=204575) for the steps to properly configure the Forefront Identity Manager 2010 and supporting infrastructure servers.

## Test Lab Overview

In this test lab, Forefront Identity Manager 2010 is deployed with:

 One computer running the FIM Synchronization Service and FIM Portal named FIM1. FIM1 uses the Windows Server® 2008 R2 Enterprise Edition operating system.

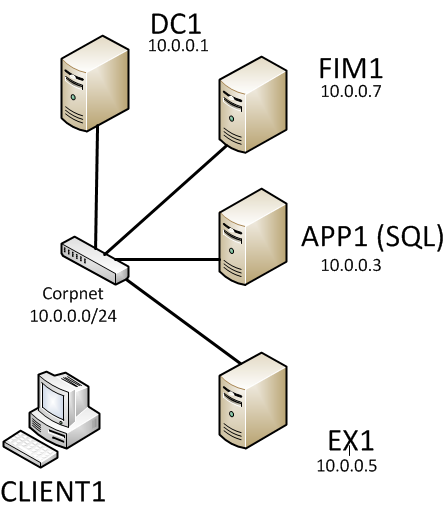
 One preexisting server running SQL Server® 2008 Enterprise with Service Pack 2, named APP1.

 One preexisting server running Microsoft Exchange Server 2010 with Service Pack 1, named EX1.

The Forefront Identity Manager test lab uses the following subnet:

 The intranet established by the Base Configuration Test Lab Guide, referred to as the Corpnet subnet (10.0.0.0/24).

Computers on each subnet connect using a hub or switch. See the following figure.



This test lab will guide you through the Forefront Identity Manager 2010 installation process. The purpose of this test lab is to allow for the creation of a basic test lab environment that consists of Forefront Identity Manager 2010. This test lab guide can be used as a building block for additional test lab guides that demonstrate increased functionality or additional features of Forefront Identity Manager 2010.

## Hardware and Software Requirements

The following are required components of the test lab:

 The product disc or files for Windows Server 2008 R2 Enterprise Edition.

 The product disc or files for Exchange Server 2010 with Service Pack 1.

 The product disc or files for SQL Server 2008 Enterprise .

 The product disc or files for Microsoft SQL Server 2008 Enterprise Service Pack 2 64-bit.

 The product disc or files for Windows SharePoint Services 3.0 with Service Pack 2.

 The product disc or files for Forefront Identity Manager 2010.

 The files for Forefront Identity Manager 2010 Synchronization Service Update (KB978864).

 The files for Forefront Identity Manager 2010 Service and Portal Update (KB978864).

 The files for Microsoft SQL Server 2008 Feature Pack, April 2009 - Microsoft SQL Server 2008 Native Client.

The following table provides a summary of the Microsoft software that is used in this guide.

|  |  |
| --- | --- |
| Software | Additional information |
| Microsoft Exchange Server 2010 with Service Pack 1 – 64-bit | [Microsoft Exchange Server 2010 with Service Pack 1](http://go.microsoft.com/fwlink/?LinkId=202857) (http://go.microsoft.com/fwlink/?LinkId=202857). |
| Microsoft SQL Server 2008 Enterprise – 64-bit | [Microsoft SQL Server 2008 Enterprise](http://go.microsoft.com/fwlink/?LinkId=207697) (http://go.microsoft.com/fwlink/?LinkId=207697). |
| Microsoft SQL Server 2008 Enterprise Service Pack 2 – SQLServer2008SP2-KB2285068-x64-ENU.exe | [SQLServer2008SP2-KB2285068-x64-ENU.exe](http://go.microsoft.com/fwlink/?LinkId=207700)(http://go.microsoft.com/fwlink/?LinkId=207700) |
| Windows SharePoint Services 3.0 with Service Pack 2 | [Windows SharePoint Service 3.0 with Service Pack 2](http://www.microsoft.com/download/en/details.aspx?id=5719) (http://www.microsoft.com/download/en/details.aspx?id=5719). |
| Forefront Identity Manager 2010 | [Forefront Identity Manager 2010](http://go.microsoft.com/fwlink/?LinkId=204577) (http://go.microsoft.com/fwlink/?LinkId=204577). |
| Forefront Identity Manager 2010 Synchronization Service Update (KB978864) | This is a [recommended update](http://go.microsoft.com/fwlink/?LinkId=204578) for the RTM of Forefront Identity Manager 2010. This release provides additional product fixes since the last update release. (http://go.microsoft.com/fwlink/?LinkId=204578) |
| Forefront Identity Manager 2010 Service and Portal Update (KB978864) | This is a [recommended update](http://go.microsoft.com/fwlink/?LinkId=204578) for RTM of Forefront Identity Manager 2010. This release provides additional product fixes since the last update release. (http://go.microsoft.com/fwlink/?LinkId=204578) |
| Microsoft SQL Server 2008 Feature Pack, April 2009 - Microsoft SQL Server 2008 Native Client | [Microsoft SQL Server 2008 Native Client (SQL Server Native Client)](http://go.microsoft.com/fwlink/?LinkId=204702) (http://go.microsoft.com/fwlink/?LinkId=204702) is a single dynamic-link library (DLL) containing both the SQL OLE DB provider and SQL ODBC driver. It contains run-time support for applications using native-code APIs (ODBC, OLE DB, and ADO) to connect to Microsoft SQL Server 2000, 2005, or 2008. SQL Server Native Client should be used to create new applications or enhance existing applications that need to take advantage of new SQL Server 2008 features. This redistributable installer for SQL Server Native Client installs the client components needed during run time to take advantage of new SQL Server 2008 features, and optionally installs the header files needed to develop an application that uses the SQL Server Native Client API. |

## Steps for Configuring the Forefront Identity Manager 2010 Test Lab

There are nine steps to follow when setting up the Forefront Identity Manager 2010 test lab based on the Forefront Identity Manager 2010 Test Lab Guide.

 Step 1: Set up the Base Configuration—The Base Configuration is the core of all Test Lab Guide scenarios. The first step is to complete the Base Configuration.

 Step 2: Set up the Exchange Server 2010 with Service Pack 1 Test Lab Guide (TLG)—The second step is to complete the Exchange Server 2010 with Service Pack 1 test lab guide. This provides Active Directory® attributes and e-mail functionality for the FIM Service account.

 Step 3: Set up the SQL Server 2008 Enterprise with Service Pack 2 TLG—The third step is to complete the SQL Server 2008 Enterprise with Service Pack 2 test lab guide. This provides the database server for your FIM installation.

 Step 4: Configure FIM1—The fourth step includes installing the operating system, and then configuring and joining FIM1 to the domain.

 Step 5: Install FIM 2010 Prerequisite Software—The fifth step walks you through installing prerequisite software.

 Step 6: Perform FIM 2010 Prerequisites Tasks—The sixth step includes performing prerequisite tasks.

 Step 7: Install FIM 2010 Synchronization Service and FIM Portal—The seventh step includes performing installation tasks.

 Step 8: Perform FIM 2010 Post-Installation Tasks— The eighth step includes performing post installation tasks

 Step 9: Verify the Installation— The ninth step includes verifying the installation was successful

This guide provides steps for configuring the computers of the Forefront Identity Manager 2010 test lab. The following sections provide details about how to perform these tasks.

## Test Lab Guide Specific Information and Instructions

The following section is a list of additional information on configuring the test lab. It also includes items that may be omitted from the test lab guides that this test lab builds upon. This is to allow for quicker deployment.

 The Base Configuration TLG—EDGE1 and INET1 are not required. The steps requiring setup and configuration may be excluded from the setup of the base configuration.

 The Exchange Server 2010 with Service Pack 1 TLG— EX1 is not required but a valid mail attribute is required for the FIMService account. A work around is to populate the mail attribute using ADSIEDIT. Please note that future test lab guides that demonstrate workflow and notification will probably use an Exchange server.

 The SQL Server 2008 with SP 2 TLG—The SQL Server 2008 R2 TLG may be substituted for this TLG. SQL Server 2008 R2 is now fully supported with FIM 2010.

This guide provides steps for configuring the computers of the Forefront Identity Manager 2010 test lab. The following sections provide details about how to perform these tasks.

# Step 1: Set Up the Base Configuration Test Lab

Set up the Base Configuration test lab for both the Corpnet and Internet subnets using the procedures in the “Steps for Configuring the Corpnet Subnet” and “Steps for Configuring the Internet Subnet” sections of the [Test Lab Guide: Base Configuration](http://go.microsoft.com/fwlink/?LinkId=198140) (http://go.microsoft.com/fwlink/?LinkId=198140).

# Step 2: Set Up the Exchange Server 2010 with Service Pack 1 Test Lab

Set up the Exchange Server 2010 with Service Pack 1 test lab using the procedures outlined in [Test Lab Guide: Exchange Server 2010 with Service Pack 1](http://go.microsoft.com/fwlink/?LinkId=206341) (http://go.microsoft.com/fwlink/?LinkId=206341).

# Step 3: Set Up the SQL Server 2008 Enterprise with Service Pack 2 Test Lab

Set up the SQL Server 2008 Enterprise with Service Pack 2 test lab using the procedures outlined in [Test Lab Guide: SQL Server 2008 Enterprise with Service Pack 2](http://go.microsoft.com/fwlink/?LinkID=207698) (http://go.microsoft.com/fwlink/?LinkID=207698).

# Step 4: Configure FIM1

FIM1 configuration for the Forefront Identity Manager 2010 test lab consists of the following:

 Install Windows Server 2008 R2 on FIM1

 Configure TCP/IP Properties on FIM1

 Rename and Joining the Domain on FIM1

## Install Windows Server 2008 R2 on FIM1

Install the Windows Server 2008 R2 operating system on FIM1.

To install Windows Server 2008 R2 on FIM1

|  |
| --- |
| 1. Start the installation of Windows Server 2008 R2.  2. Follow the instructions to complete the installation, specifying Windows Server 2008 R2 Enterprise Edition (full installation) and a strong password for the local Administrator account.  3. Once the installation completes, log on using the local Administrator account.  4. Connect FIM1 to a network that has Internet access and run Windows Update to install the latest updates for Windows Server 2008 R2.  5. Once the updates are complete, restart FIM1 and log on as the local Administrator. |

## Configure TCP/IP Properties on FIM1

Configure the TCP/IP properties on FIM1 so that it can join the corp.contoso.com domain.

To configure the TCP/IP properties on FIM1

|  |
| --- |
| 1. In Initial Configuration Tasks, click Configure networking.  2. In the Network Connections window, right-click Local Area Connection, and then click Properties.  3. Click Internet Protocol Version 4 (TCP/IPv4), and then click Properties.  4. Select Use the following IP address. In IP address, type 10.0.0.7. In Subnet mask, type 255.255.255.0. In Default Gateway, type 10.0.0.1. In Preferred DNS server, type 10.0.0.1.  5. Click Advanced, and then click the DNS tab. In DNS suffix for this connection, type the following text, click OK twice, and then click Close:  corp.contoso.com  6. Close the Network Connections window and leave the Initial Configuration Tasks window open.  7. To check name resolution and network communication between FIM1 and DC1, click Start, click All Programs, click Accessories, and then click Command Prompt.  8. In the Command Prompt window, type the following text:  ping dc1.corp.contoso.com  9. Verify that there are four replies from 10.0.0.1.  10. Close the Command Prompt window. |

## Rename and Join the Domain on FIM1

Now, rename FIM1 and join it to the corp.contoso.com domain.

To rename FIM1 and join the corp.contoso.com domain

|  |
| --- |
| 1. In Initial Configuration Tasks, click Provide Computer Name and Domain.  2. In the System Properties dialog box, on the Computer Name tab, click Change.  3. In Computer Name, type the following text:  FIM1 In Member of, click Domain, and then type the following text:  corp.contoso.com  4. Click OK.  5. When you are prompted for a user name and password, type the following text and its password, and then click OK:  User1  Note  You can also use the CORP\Administrator account to join FIM1 to the domain.  6. When you see a dialog box welcoming you to the corp.contoso.com domain, click OK.  7. When you are prompted that you must restart the computer, click OK.  8. On the System Properties dialog box, click Close.  9. When you are prompted to restart the computer, click Restart Now.  10. After the computer restarts, click Switch User, and then click Other User and log on to the CORP domain with the Administrator account.  11. In Initial Configuration Tasks, click Do not show this window at logon, and then click Close. |

# Step 5: Install FIM 2010 Prerequisite Software

FIM1 prerequisite software for the Forefront Identity Manager 2010 test lab consists of the following:

 Install the .NET Framework 3.5.1, Internet Information Services (IIS) 7.5, and Windows PowerShell® on FIM1

 Install the Exchange 2010 Management Console on FIM1

 Disable Internet Explorer Enhanced Security for Administrators on FIM1

 Install and Configure Windows SharePoint Services 3.0 with SP2 on FIM1

 Install Full Text Search on APP1

 Re-apply SQL Server 2008 Service Pack 2 on APP1

 Install the SQL Server 2008 Native Client on FIM1

## Install the .NET Framework 3.5.1, IIS 7.5, and Windows PowerShell on FIM1

Install the .NET Framework 3.5.1, IIS 7.5, and Windows PowerShell Integrated Scripting Environment (ISE) on FIM1.

To install the .NET Framework 3.5.1, IIS 7.5, and the Windows PowerShell Integrated Scripting Environment (ISE)

|  |
| --- |
| 1. In Server Manager, on the left, click Features and on the right, click Add Features. This will launch the Add Features Wizard and you will see the Select Features page.  2. Scroll down the list of features and select .NET Framework 3.5.1. This will bring up a box that asks to install Web Server (IIS). Click Add Required Role Services. The box will disappear.  3. Scroll down the list of features and select Windows PowerShell Integrated Scripting Environment (ISE), and then click Next. You will see the Confirm Installation Selections page.  4. On the Web Server (IIS) page, click Next.  5. On the Role Services page, place a check in all of the items that are listed in tables 1 and 2 below.  Note  When you select ASP.NET this will bring up a pop-up box with the title Add features required for Web Server (IIS). Click the Add Required Features button. This will automatically select ISAPI Extensions, ISAPI Filters, and .NET Extensibility. This will also add the .NET Environment to the Windows Process Activation Service.  6. On the Confirm Installation Selections page, click Install. This will begin the installation. When this completes you will see the Installation Results page. Click Close.  .NET Framework 3.5.1, IIS 7.5, and Windows PowerShell Installation |

Table 1 Required IIS 7.5 Web Server Role Services

|  |  |
| --- | --- |
| Role service | Required features |
| Common HTTP Features | **** Static Content  **** Default Document  **** Directory Browsing  **** HTTP Errors  **** HTTP Redirection |
| Application Development | **** ASP .NET  **** .NET Extensibility  **** ISAPI Extensions  **** ISAPI Filters |
| Health and Diagnostics | **** HTTP Logging  **** Request Monitor |
| Security | **** Basic Authentication  **** Windows Authentication  **** Request Filtering |
| Performance | **** Static Content Compression  **** Dynamic Content Compression |

Table 2 Required IIS 7.5 Management Tools Role Services

|  |  |
| --- | --- |
| Role service | Required features |
| IIS Management Console |  |
| IIS 6 Management Compatibility | **** IIS 6 Metabase Compatibility  **** IIS 6 WMI Compatibility  **** IIS 6 Scripting Tools  **** IIS 6 Management Console |

## Install Exchange Server 2010 with Service Pack 1 Management Console on FIM1

Now install the Exchange Server 2010 with Service Pack 1 Management Console on FIM1. The Exchange Management console is required for provisioning users that are mail-enabled or mailbox-enabled. Although this will not be demonstrated in this test lab guide, future test lab guides will demonstrate this functionality.

To install Exchange Server 2010 with Service Pack 1 Management Console

|  |
| --- |
| 1. Navigate to the directory that contains the Exchange Server 2010 binaries and double-click Setup.EXE. This will launch the Exchange Server 2010 Splash Screen.  2. On the Splash Screen, click Step 3: Choose Exchange language option. Select Install only languages from the DVD.  3. On the Splash Screen, click Step 4: Install Microsoft Exchange. This will close the Splash Screen and bring up a box stating it is copying items. Once this completes a box will appear that says Microsoft Exchange Server 2010 Setup initializing. When this completes t the Exchange Server 2010 Setup Wizard will launch.  4. On the Introduction page, click Next.  5. On the License Agreement page, read the License Agreement, select I accept the items in the license agreement, and then click Next.  6. On the Error Reporting page, leave the default of No selected, and then click Next.  7. On the Installation Type page, select Custom Exchange Server Installation and the default path of C:\Program Files\Microsoft\Exchange Server\V14. Place a check in the box next to Automatically install Windows Server roles and features required for Exchange Server, and then click Next.  8. On the Server Role Selection page, place a check in the box next to Management Tools, and then click Next. This will launch the Readiness Checks. This may take several moments.  Exchange Management Console Server Role Selection    9. Once the Readiness Checks completes, click Install. This will begin the installation. This will take several minutes.  10. Once the installation completes, click Finish.  11. On the Splash Screen, click Close. This will bring up the Confirm Exit window. Click Yes.  12. At this point, the Exchange Management Console will automatically launch. You can close the Exchange Management Console. |

## Disable Internet Explorer Enhanced Security for Administrators on FIM1

This section lists the steps for disabling Internet Explorer Enhanced Security.

To disable Internet Explorer Enhanced Security for Administrators

|  |
| --- |
| 1. In Server Manager, on the right-hand side, scroll down to Security Information, and then select Configure IE ESC.  2. From the Internet Explorer Enhanced Security Configuration screen, under Administrators, select Off.  Internet Explorer Enhanced Security Configuration    3. Click OK. |

## Install and Configure Windows SharePoint Services 3.0 with SP2 on FIM1

Now install Windows SharePoint Services 3.0 with SP2 on FIM1. The FIM Portal requires SharePoint Services.

To install and configure Windows SharePoint Services 3.0 with SP2

|  |
| --- |
| 1. Navigate to the directory that contains Windows SharePoint Services 3.0 binaries and double-click SharePoint.EXE. This will launch a Microsoft SharePoint Services screen that will indicate that files are being extracted. Once this completes you will see the License Agreement.  2. On the License Agreement screen, read the License Agreement, select I accept the terms of this agreement, and then click Continue.  3. On the Choose the installation you want screen, click Basic. This will begin the installation.  4. Once this completes, click Close. This will launch the SharePoint Products and Technologies Configuration Wizard.  5. On the Welcome to SharePoint Products and Technologies page, click Next. This will bring up a dialog box that says The following service may have to be started or reset during configuration. Click Yes.  6. This will start Configuring SharePoint Products and Technologies. This will perform 10 configuration tasks. Once this completes you will see Configuration Successful. Click Finish. This will launch Internet Explorer.  Configuring SharePoint Products and Technologies    7. In Internet Explorer, the URL will be http://fim1. When prompted, enter your credentials. The Windows SharePoint Services page will come up.  SharePoint Services Home Page    Warning  You may be prompted for credentials while this page loads. If so, type the following text for the username and the password:  Administrator  8. Close Internet Explorer. |

## Install Full Text Search on APP1

Now you need to add Full Text Search to your installed instance of SQL Server 2008 Enterprise with Service Pack 2 on APP1.

To install Full Text Search on APP1

|  |
| --- |
| 1. Log on to APP1 as CORP\Administrator.  2. On APP1, navigate to the directory that contains the SQL Server 2008 Enterprise binaries and double-click Setup.EXE. This will bring up a box that says This program has known compatibility issues. Click Run Program. This will launch the SQL Server Installation Center..  3. On the SQL Server Installation Center, on the left, click Installation.  4. On the right, click New SQL Server stand-alone installation or add features to an existing installation. This will bring up a box that says This program has known compatibility issues. Click Run Program. This will launch the SQL Server 2008 Setup.  5. On the Setup Support Rules screen, click OK. This will close the Setup Support Rules screen and will bring up the Setup Support Files screen.  6. On the Setup Support Files screen, click Install. This will take a few moments to complete. Once this completes the Setup Support Rules screen will appear again.  7. On the Setup Support Rules screen, click Next.  8. On the Installation Type screen, select Add features to an existing instance of SQL Server 2008, and then click Next.  9. On the Feature Selection screen, under Instance Features place a check in Full-Text Search, and then click Next.    10. On the Disk Space Requirements screen, click Next.  11. On the Server Configuration screen, click Next.  12. On the Error and Usage Reporting screen, click Next.  13. On the Installation Rules screen, click Next.  14. On the Ready to Install screen, click Install.  15. On the Installation Progress screen, wait until the installation completes. Click Next.  16. On the Complete screen, click Close.  17. Close the SQL Server Installation Center. |

## Re-apply SQL Server 2008 Service Pack 2 on APP1

Because we added a new feature, and want to ensure it is up-to-date, we must re-install the SQL Server 2008 Enterprise Service Pack 2 binaries on APP1.

To re-apply SQL Server 2008 Service Pack 2 on APP1

|  |
| --- |
| 1. On APP1, navigate to the directory that contains the SQL Server 2008 Enterprise Service Pack 2 binaries and double-click SQLServer2008SP2-KB2285068-x64-ENU.exe. This will begin the extraction process. Once this completes, the SQL Server 2008 Service Pack 2 installation wizard will begin.  2. On the Welcome screen, click Next.  3. On the License Terms screen, read the Licensing terms, select the I accept the license terms check box, and then click Next.  4. On the Select Features screen, click Next.  5. On the Check Files In Use screen, click Next.  6. On the Ready to Update screen, click Update. This will begin the update.  7. Once the update is complete, on the Update Progress screen, click Next.  8. On the Complete screen, click Close. |

## Install the SQL Server 2008 Native Client on FIM1

Install the SQL Server 2008 Native Client on FIM1. This is a requirement prior to installing the updates.

To install the SQL Server 2008 Native Client on FIM1

|  |
| --- |
| 1. Log on to FIM1 as CORP\Administrator.  2. Navigate to the directory that contains the binaries for the SQL Server 2008 Native Client and double-click sqlncli.msi. This will begin the SQL Server 2008 Native Client Setup Wizard.  3. On the Welcome page, click Next.  Welcome to the Installation Wizard for SQL Server 2008 Native Client    4. On the License Agreement page, read the License Agreement, select I accept the terms in the License Agreement, and then click Next.  5. Click Next.  6. Click Next.  7. Click Install.  8. Once the installation completes, click Finish. |

# Step 6: Perform FIM 2010 Prerequisite Tasks

FIM1 prerequisites for the Forefront Identity Manager 2010 test lab consists of the following:

 Create the FIM Service Accounts

 Mailbox-Enable the CORP\FIMService Account

 Secure the CORP\FIMService and CORP\FIMSynchService Accounts

 Set the SQL Server Agent Service to Start Automatically

 Enable SQL Firewall Ports

 Enable SQL Server Network Protocols

 Verify That the FIM Installation Account Has SharePoint Permissions

 Change the SharePoint Application Pool Account to Use CORP\SPService

 Configure IIS to Use CORP\SPService for Kerberos Delegation

 Set the SPNs for CORP\SPService

 Set the SPNs for CORP\FIMService

 Turn on Delegation for CORP\SPService

 Turn on Delegation for CORP\FIMService

## Create the FIM Service Accounts

Four service accounts need to be created in corp.contoso.com that will be used with the Forefront Identity Manager 2010 installation.

Table 1 – Service Accounts

|  |  |  |  |
| --- | --- | --- | --- |
| Full name | User logon name | Forest | Password |
| FIM Service | FIMService | corp.contoso.com | Pass1word$ |
| FIM Synch Service | FIMSynchService | corp.contoso.com | Pass1word$ |
| FIM MA | FIMMA | corp.contoso.com | Pass1word$ |
| SharePoint Service | SPService | corp.contoso.com | Pass1word$ |

To create the Service Accounts

|  |
| --- |
| 1. Log on to DC1.corp.contoso.com as Administrator.  2. Click Start, select Administrative Tools, and then click Active Directory Users and Computers. This will open the Active Directory Users and Computers MMC.  3. In the Active Directory Users and Computers MMC, from the tree-view on the left, expand corp.contoso.com.  4. Now, right-click ServiceAccounts, select New, and then select User. This will bring up the New Object – User window.  5. On the New Object – User screen, in the Full Name box, type the following text:  FIM Service  6. On the New Object – User screen, in the User logon name box, type the following text, and then click Next:  FIMService  7. On the New Object – User screen, in the Password box, type the following text:  Pass1word!  8. On the New Object – User screen, in the Confirm Password box, type the following text:  Pass1word!  9. On the New Object – User screen, clear the User must change password at next logon check box.  10. On the New Object – User screen, select Password never expires, and then click Next.  11. Click Finish.  12. Repeat these steps for all of the accounts listed in the Account Summary table.  FIM Service Accounts    13. Log off DC1.corp.contoso.com. |

## Mailbox-Enable the CORP\FIMService Account

Now, create a mailbox for the CORP\FIMService account. This account is used to send e-mail notifications from FIM 2010. Also, in order to use the Office Outlook integration feature, this account must be mailbox-enabled and the e-mail account must be hosted by Exchange 2007 or Exchange 2010.

To mailbox-enable the CORP\FIMService account

|  |
| --- |
| 1. Log on to the EX1.corp.contoso.com server as Administrator.  2. Click Start, click All Programs, click Microsoft Exchange Server 2010, and then click Exchange Management Console.  3. In the Exchange Management Console, click Microsoft Exchange On-Premises. This will start an Initialization.  Warning  This may bring up a Microsoft Exchange box that says The following servers in your organization running Exchange Server 2010 are unlicensed. It will list EX1. If you plan to use this test lab for more than 120 days you will need to enter a product key. For now, just hit OK.  4. In the Exchange Management Console, expand Microsoft Exchange On-Premises (ex1.corp.contoso.com), expand Recipient Configuration, and then click Mailbox.  5. On the right, in the Actions pane, click New Mailbox to start the New Mailbox Wizard.  6. On the Introduction page, select User Mailbox, and then click Next.  7. On the User Type page, select Existing users, and then click Add. This will bring up the Select User – Entire Forest page.  8. From the list, select FIM Service, click OK, and then click Next.  Mailbox-enable FIM Service Account    9. On the Mailbox Settings page, click Next.  10. On the New Mailbox page, click New.  11. On the Completion page, verify that it was successful, and then click Finish.  12. Close the Exchange Management Console.  13. Log off EX1.corp.contoso.com. |

## Secure the CORP\FIMService and CORP\FIMSynchService Accounts

Now, you will secure the CORP\FIMService and CORP\FIMSynchService account by restricting its permissions.

Table 2 – FIMService Account and FIMSynchService Permissions

|  |  |
| --- | --- |
| Account | Permissions |
| CORP\FIMService | **** Deny logon as batch job  **** Deny logon locally  **** Deny access to this computer from the network |
| CORP\FIMSynchService | **** Deny logon as batch job  **** Deny logon locally  **** Deny access to this computer from the network |

To secure the CORP\FIMService accounts

|  |
| --- |
| 1. Log on to FIM1.corp.contoso.com as Administrator.  2. Click Start, select Administrative Tools, and then click Local Security Policy. This will open the Local Security Policy MMC.  3. In the Local Security Policy MMC, on the left, expand Local Policies, and then click User Rights Assignment.  4. Now, on the right, scroll down and double-click Deny access to the computer from the network.This will open the Deny access to the computer from the network Properties window.  5. Now, click Add User of Group. This will bring up the Select Users, Computers, Service Accounts, or Groups window.  6. In the box, below Enter the object names to select (examples), type the following text, and then click Check Names:  FIMService;FIMSynchService.  This should resolve to the FIM Service account and the FIM Synch Service account. Click OK.  7. On the Deny access to the computer from the network Properties screen, click Apply, and then click OK.  8. In the Local Security Policy, scroll down and double-click Deny logon as batch job. This will open the Deny logon as batch job Properties window.  9. Now, click Add User of Group. This will bring up the Select Users, Computers, Service Accounts, or Groups window.  10. In the box, below Enter the object names to select (examples), type the following text, and then click Check Names:  FIMService;FIMSynchService  This should resolve to the FIM Service account and the FIM Synch Service account. Click OK.  11. On the Deny logon as batch Properties screen, click Apply, and then click OK.  12. In the Local Security Policy, scroll down and double-click Deny logon locally. This will open the Deny logon locally Properties window.  13. Now, click Add User of Group. This will bring up the Select Users, Computers, Service Accounts, or Groups window.  14. In the box, below Enter the object names to select (examples), type then following text, and then click Check Names:  FIMService;FIMSynchService  This should resolve to the FIM Service account and the FIM Synch Service account. Click OK.  15. On the Deny logon locally Properties screen, click Apply, and then click OK.  Local Security Policy    16. Close the Local Security Policy. |

## Set the SQL Server Agent Service to Start Automatically

To set SQL Server Agent service to start automatically

|  |
| --- |
| 1. Log on to APP1 as CORP\Administrator.  2. Click Start, select Administrative Tools, and then click Services.  3. Scroll down to SQL Server Agent (MSSQLSERVER) and double-click it. This will bring up the SQL Server Agent (MSSQLSERVER) Properties.  4. In the middle, next to Startup Type, select Automatic from the drop-down list. Click Apply, and then click OK.  SQL Server Agent Properties    5. In Services, right-click SQL Server Agent (MSSQLSERVER), and then click Start. This will start the SQL Server Agent.  6. When this completes, verify that the SQL Server Agent (MSSQLSERVER) has a status of Started.  7. Close Services. |

## Enable SQL Firewall Ports

To enable the firewall ports on APP1

|  |
| --- |
| 1. Click Start, select Administrative Tools, and then click Windows Firewall with Advanced Security. This will bring up Windows Firewall with Advanced Security.  2. On the left, select Inbound Rules, and on the right click New Rule. This will bring up the New Inbound Rule Wizard.  3. On the Rule Type page, select Port, and then click Next.  4. On the Protocol and ports page, select TCP, and type the following text in the box next to Specific local ports, and then click Next:  445  5. On the Action page, select Allow the connection, and then click Next.  6. On the Profile page, select Domain, Private, and Public, and then click Next.  7. On the Name page, type the following text in the box, and then click Finish:  SQL Server Named Pipes  8. Repeat these steps for all of the entries in the table below.  Windows Firewall with Advanced Security    9. Close Windows Firewall with Advanced Security. |

Table 3 – SQL Server Firewall Port Exceptions

|  |  |  |
| --- | --- | --- |
| Protocol | Port number | Name |
| TCP | 445 | SQL Server Named Pipes |
| TCP | 1433 | SQL Server Listening Port |
| UDP | 1434 | SQL Server Browser Service |

## Enable SQL Server Network Protocols

To enable SQL Server Network Protocols

|  |
| --- |
| 1. Click Start, select All Programs, click Microsoft SQL Server 2008, click Configuration Tools, and then select SQL Server Configuration Manager. This will bring up the SQL Server Configuration Manager.  2. In SQL Server Configuration Manager, on the left, expand SQL Server Network Configuration, and then click Protocols for MSSQLSERVER. This will populate the right pane with four protocols and their statuses.  3. On the right, right-click Disabled next to Named Pipes, and then select Enable. This will bring up a pop-up box that says Any changes made will be saved; however, they will not take effect until the service is stopped and restarted. Click OK.  SQL Server Configuration Manager    4. In SQL Server Configuration Manager, on the left, click SQL Server Services. This will populate the right pane with three services and their states.  5. On the right, right-click SQL Server (MSSQLSERVER), and select Stop. This will bring up a pop-up box that says stopping this service will also stop the SQLServerAgent. Do you wish to continue? Click Yes. This will stop the SQL Server service.  6. In the SQL Services pane, right-click on a blank area of the screen. This will bring up a small pop-up box. Click Refresh. You should now see both services stopped.  7. On the right, right-click SQL Server (MSSQLSERVER), and select Start. This will start the SQL Server service.  8. On the right, right-click SQL Server Agent, and select Start. This will start the SQL Server Agent service.  9. Close SQL Server Configuration Manager. |

## Verify That the FIM Installation Account Has SharePoint Permissions

In this step, you will verify that the FIM Installation account, for example, CORP\Administrator, has SharePoint permissions. If the account that is used to install FIM does not have the correct permissions, the installation will fail.

To verify that the FIM Installation account has SharePoint permissions

|  |
| --- |
| 1. Log on to FIM1.corp.contoso.com as Administrator.  2. Click Start, click Administrative Tools, and then click SharePoint 3.0 Central Administration. This will bring up the SharePoint Central Administration in Internet Explorer.  3. On the left, click Application Management. This may bring up a Credentials box. If so, enter the following text for user name and the password, and then click OK:  Administrator Now the Application Management page will appear.  4. Under SharePoint Site Management, click Site Collection Administrators. This will bring up the Site Collection Administrators page.  5. Under Primary site collection administration, verify that it says Administrator.  Application Management – Site Collection Administrators    6. At the top of Internet Explorer, enter the new URL http://fim1 in the address box, and then hit Enter. This will bring up the Windows SharePoint Service home page.  7. In the upper right corner, click Site Actions and the select Site Settings from the drop-down list. This will bring up the Site Settings page.  8. Under Users and Permissions, click Site Collection Administrators. This will bring up the Site Collection Administrators page.  9. Verify that Administrator appears in the box next to Site Collection Administrators.  Team Site – Site Collection Administrators    10. Close Internet Explorer. |

## Change the SharePoint Application Pool Account to Use CORP\SPService

By default, IIS uses the Network Service account for the Application Pool. The recommended guidance is to use a service account.

To change the SharePoint Application Pool account to use CORP\SPService

|  |
| --- |
| 1. Click Start, click Administrative Tools, and then click SharePoint 3.0 Central Administration. This will bring up the SharePoint Central Administration in Internet Explorer.  2. On the left, click Operations. This may bring up a Credentials box. If so, enter the following text for the user name and the password, and then click OK:  Administrator Now the Operations page will appear.  3. Under Security Configuration, click Service Accounts. This will bring up the Service Accounts page.  4. Click the Web Application Pool radio button and from the drop-down list select Windows SharePoint Services Web Application. This will activate Application Pool.  5. Under Application Pool, from the drop-down list, select SharePoint-80.  6. Click the Configurable radio button and enter CORP\SPService for user name and Pass1word$ for the password.  Central Administration – Service Accounts    7. Click OK. This will bring up a pop-up that says the SPN must be updated by a domain administrator. This will be done later in this step. Click OK. This will bring up another pop-up that says that iisrest/NOFORCE must be run. Click OK. It may take a minute or two, but then the Operations page will come up.  8. Close Internet Explorer. |

## Configure IIS to Use CORP\SPService for Kerberos Delegation

By default, an application pool running under a specific service account will not use the service account for Kerberos. This section will configure IIS to use the CORP\SPService account for Kerberos Delegation.

To configure IIS to use CORP\SPService for Kerberos Delegation

|  |
| --- |
| 1. 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.  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=”true” 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 six instances that need to have useKernelMode=”true” useAppPoolCredentials = “true” added.  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. |

## Set the SPNs for CORP\SPService

In this step, you will be setting the service principal names (SPNs) for the CORP\SPService account.

To set the SPNs for CORP\SPService

|  |
| --- |
| 1. Log on to DC1 as CORP\Administrator.  2. Click Start, select Administrative Tools, and then click ADSI Edit. This will bring up ADSI Edit.  3. At the top, right-click ADSI Edit and select Connect to. This will bring up a Connections Settings box. Leave the defaults and click OK.  4. On the right, expand Default Naming Context [DC1.corp.contoso.com], double-click DC=corp,DC=contoso,DC=com, expand DC=corp,DC=contoso,DC=com, and then select OU=ServiceAccounts.  5. In the center, right-click CN=SharePoint Service and select Properties. This will bring up CN=SharePoint Service Properties.  6. Scroll through the list of attributes and double-click servicePrincipalName. This will bring up the Multi-valued String Editor.  7. In the box, under Value to add, type the following text, and then click Add:   HTTP/fim1  8. In the box, under Value to add, type the following text, and then click Add:   HTTP/fim1.corp.contoso.com  9. Click OK.  servicePrincipalName    10. Click Apply.  11. Click OK. |

## Set the SPNs for CORP\FIMService

In this step, you will be setting the SPNs for the CORP\FIMService account.

To set the SPNs for CORP\FIMService

|  |
| --- |
| 1. In the center, right-click CN=FIM Service and select Properties. This will bring up CN=SharePoint Service Properties.  2. Scroll through the list of attributes and double-click servicePrincipalName. This will bring up the Multi-valued String Editor.  3. In the box, under Value to add, type the following text, and then click Add:   FIMService/fim1  4. In the box, under Value to add, type the following text, and then click Add:   FIMService/fim1.corp.contoso.com  5. Click OK.  servicePrincipalName    6. Click Apply.  7. Click OK.  8. Close ADSI Edit. |

## Turn on Delegation for CORP\SPService

Now you will enable Kerberos Delegation for 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 any service (Kerberos only).  SharePoint Service Properties    5. Click Apply.  6. Click OK. |

## Turn on Delegation for CORP\FIMService

Now you will enable Kerberos delegation for the FIM Service account.

To turn on Delegation for CORP\FIMService

|  |
| --- |
| 1. Right-click FIM Service, and select Properties.  2. On the FIM Service Properties, select the Delegation tab.  3. In the middle, select Trust this user for delegation to any service (Kerberos only).  4. Click Apply.  5. Click OK.  6. Close Active Directory Users and Computers. |

# Step 7: Install FIM Synchronization Service and FIM Portal

Installation of the FIM Synchronization Service and the FIM Portal for the Forefront Identity Manager 2010 test lab consists of the following:

 Install the FIM Synchronization Service on FIM1

 Install the FIM Portal

 Install Update 1 for the FIM Synchronization Service

 Install the FIM Portal and Service Update 1 on FIM1

## Install the FIM Synchronization Service on FIM1

Install the FIM Synchronization Service on FIM1.

To install the FIM Synchronization Service on FIM1

|  |
| --- |
| 1. Log on to FIM1 as CORP\Administrator.  2. Navigate to the directory that contains the binaries for Forefront Identity Manager 2010 and double-click FIMSplash.htm. This will bring up the Forefront Identity Manager 2010 splash screen.  3. 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 Setup Wizard.  4. On the Welcome page, click Next.  Welcome to the Forefront Identity Manager Synchronization Service Setup Wizard    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 Custom Setup page, click Next.  7. On the Configure Forefront Identity Manager Synchronization Service page, under SQL Server is located on, click the radio button next to A remote machine, type the following text for the Computer name, and then click Next:  APP1  Configure Forefront Identity Manager Synchronization Service    8. Next to Service account enter FIMSynchService, next to Password enter Pass1word$, and next to Service Account Domain or local computer name enter CORP. Click Next.  Configure Forefront Identity Manager Synchronization Service    9. Leave the default groups, and click Next.  Configure Forefront Identity Manager Synchronization Service    10. Select Enable firewall rules for inbound RPC communications, and click Next.  Configure Forefront Identity Manager Synchronization Service    11. Click Install.  12. 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, type the following text, and then click Save:  BackupKey  This will continue the installation.  Backup Key Dialog Box    13. 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 FIM1.  14. Log on to FIM1 as CORP\Administrator. |

## Install the FIM Portal on FIM1

Next, you need to install the FIM Portal on FIM1.

To install the FIM Portal on FIM1

|  |
| --- |
| 1. Navigate to the directory that contains the binaries for Forefront Identity Manager 2010 and double-click FIMSplash.htm. This will bring up the Forefront Identity Manager 2010 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.  3. On the Welcome page, click Next.  4. On the End User License Agreement page, read the License Agreement, select I accept the terms in the License Agreement, and then click Next.  5. On the FIM Customer Experience Improvement Program page, select I don’t want to join the program at this time, and then click Next.  6. On the Custom Setup page, click the drop-down list next to FIM Password Reset Portal, select Entire feature will be unavailable, and then click Next.  Custom Setup    7. On the Configure Common Services page, next to Database Server, remove the FIM1 value, and then type the following text:  APP1 Leave the remaining defaults, and click Next.  Configure Common Services    8. Next to Mail Server, type the following text, clear all three check boxes, and then click Next:   EX1.corp.contoso.com  Configure Common Services    9. On the Configure service certificate page, select Generate a self-signed certificate and then click Next.  Security  Be aware that FIM does not use this certificate for client authentication. This certificate is only used internally by the FIM Synchronization Service.  Configure Common Services    10. On the Configure FIM Service account page, next to Service Account Name, type the following text:  FIMService.  11. On the Configure FIM Service account page, next to Service Account Password, type the following text:  Pass1word$  12. On the Configure FIM Service account page, next to Service Account Domain, type the following text: CORP  13. On the Configure FIM Service account page, next to Service Email Account, type the following text:  FIMService@corp.contoso.com  Configure Common Services    14. Click Next.  15. On the Configure the Forefront Identity Manager Service and Portal synchronization page, next to FIM Management Agent Account\*, type the following text:  CORP\FIMMA  Configure Common Services    16. Click Next.  17. On the Configure connection to the FIM Service page, next to FIM Service Server address, type the following text:  FIM1  Configure FIM Service and Portal    18. Click Next.  19. On the Configure connection to the FIM Service page, leave the default of http://localhost and click Next.  Configure FIM Service and Portal    20. 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    21. Click Install. This will begin the installation.  22. Once the installation completes, click Finish.  23. Close the Splash screen.  24. Restart FIM1. |

## Install the FIM Synchronization Service Update 1 on FIM1

Next, you need to install the FIM Synchronization Service Update 1 on FIM1.

To install the FIM Synchronization Service Update 1 on FIM1

|  |
| --- |
| 1. Click Start, select Administrative Tools, and then click Services.  2. Scroll down and right-click Forefront Identity Manager Synchronization Service, and then select Stop. This will stop the Forefront Identity Manager Synchronization Service.  3. Close Services.  4. Navigate to the directory that contains the binaries for Forefront Identity Manager 2010 Synchronization Service Update (KB978864) and double-click AMD64-aa-fimsyncservice\_kb978864\_528513e44779ba22e2e04a3c0013339c5060cb5d.exe. This will begin the update installation and start the Update Wizard.  5. On the Welcome page, click Update. This will begin the update.  Welcome to the Update for Forefront Identity Manager Synchronization Service    6. This will bring up a box that says Warning 25008. The Setup wizard is about to upgrade the database. Before continuing installation it is recommended that you backup the database and key set. To continue setup, click Yes. Click Yes.  7. Once the installation completes, click Finish. |

## Install the FIM Portal and Service Update 1 on FIM1

Next, you need to install the FIM Synchronization Service Update 1 on FIM1.

To install the FIM Portal and Service Update 1 on FIM1

|  |
| --- |
| 1. Click Start, select Administrative Tools, and then then click Services.  2. Scroll down and right-click Forefront Identity Manager Service, and then select Stop. This will stop the Forefront Identity Manager Service.  3. Close Services.  4. Navigate to the directory that contains the binaries for Forefront Identity Manager 2010 Synchronization Service Update (KB978864) and double-click AMD64-all-fimservice\_kb978864\_278035fa26956c67250afaa87b94ff34e490f82.exe. This will begin the update installation and start the Update Wizard.  5. On the Welcome screen, click Update. This will begin the update.  6. Once the installation completes, click Finish.  7. Click Start, select Administrative Tools, and then click Services.  8. Scroll down and right-click Forefront Identity Manager Service and select Start. This will start the Forefront Identity Manager Service. |

# Step 8: Perform FIM 2010 Post-Installation Tasks

The FIM1 post installation tasks for the Forefront Identity Manager 2010 test lab consists of the following:

 Add CORP\FIMService to the FIMSyncAdmins Group

 Configure the CORP\FIMService Mailbox to Only Accept Mail from Internal E-mail Addresses

 Configure the CORP\FIMService Mailbox to Reject E-mail Greater Than 1 MB

 Turn Off NTLM Authentication for the FIM Portal

 Disable SharePoint Indexing

 Implement Secure Sockets Layer (SSL) for the FIM Portal

 Add the FIM Portal URL to Local Intranet Sites for CORP\Administrator

 Restrict Membership in the User Administrators Set

 Pre-allocate Space in the FIM Service Database

 Pre-allocate Space in the FIM Synchronization Service Database

## Add CORP\FIMService to the FIMSyncAdmins Group

By adding the CORP\FIMService account to the FIMSyncAdmins group, it allows the FIM Service to configure the FIM Synchronization service.

To add CORP\FIMService to the local FIMSyncAdmins group

|  |
| --- |
| 1. Log on to FIM1.corp.contoso.com as Administrator.  2. Click Start, select Administrative Tools, and then click Computer Management. This will open the Computer Management MMC.  3. In the Computer Management MMC, from the tree-view on the left, expand Local Users and Groups, and then select Groups.  Computer Management    4. In the center pane, right-click FIMSynchAdmins and select Properties. This will bring up the FIMSynchAdmins Properties.  5. Click Add.  6. This will bring up the Select Users, Computers, Service Accounts, Groups dialog box.  7. In the box, below Enter the object names to select (examples), type the following text, and then click Check Names:  CORP\FIMService  This should resolve to the FIM Service account and the FIM Synch Service account. Click OK.  8. Click Apply.  9. Click OK.  10. Close Computer Management. |

## Configure the CORP\FIMService Mailbox to Only Accept Mail from Internal E-mail Addresses

Now you will need to configure the CORP\FIMService mailbox so that it will only accept e-mail from internal addresses.

To configure the CORP\FIMService mailbox to only accept mail from internal e-mail addresses

|  |
| --- |
| 1. Log on to the EX1.corp.contoso.com server as Administrator.  2. Click Start, click All Programs, click Microsoft Exchange Server 2010, and then click Exchange Management Console.  3. In the Exchange Management Console, click Microsoft Exchange On-Premises.  Warning  This may bring up a Microsoft Exchange box that says The following servers in your organization running Exchange Server 2010 are unlicensed. It will list EX1. If you plan to use this test lab for more than 120 days you will need to enter a product key. For now, just hit OK.  4. In the Exchange Management Console, expand Microsoft Exchange On-Premises (ex1.corp.contoso.com), click Recipient Configuration, in the center pane, right-click FIM Service, and then select Properties. This will bring up the FIM Service Properties.  5. In FIM Service Properties, click the Mail Flow Settings tab, and then double-click Message Delivery Restrictions. This will bring up the Mail Delivery Restrictions.  Mail Flow Settings    6. In Message Delivery Restrictions, select the Require that all senders are authenticated check box, and then click OK. |

## Configure the CORP\FIMService Mailbox to Reject E-mail Greater Than 1 MB

Now you will need to configure the CORP\FIMService mailbox so that it will only accept e-mail that is less than or equal to 1 MB in size.

To configure the CORP\FIMService mailbox to reject e-mail greater than 1 MB

|  |
| --- |
| 1. Double-click Message Size Restrictions. This will bring up the Message Size Restrictions.  2. In Message Size Restrictions, select the Maximum Message Size (in KB) check box, and enter 1024 in the box.  3. Click OK. Click Apply and then click OK.  Message Size Restrictions    4. Close the Exchange Management Console. |

## Turn Off NTLM Authentication for the FIM Portal

In order to make the FIM portal more secure, it is recommended that NTLM Authentication be disabled.

To turn off NTLM Authentication for the FIM portal

|  |
| --- |
| 1. Log on to FIM1.corp.contoso.com 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. |

## Disable SharePoint Indexing

Because SharePoint Indexing is not required and it can decrease performance, you will need to disable it now.

To disable SharePoint indexing

|  |
| --- |
| 1. Log on to FIM1.corp.contoso.com as CORP\Administrator.  2. Click Start, click Administrative Tools, and then click SharePoint 3.0 Central Administration. This will bring up the SharePoint Central Administration in Internet Explorer.  3. On the left, click Operations.  Warning  This may bring up a Credentials box. If so, enter the following text for the user name and password, and then click OK:   Administrator  4. Under Global Configuration, click Timer job definitions. This will bring up the Timer Job Definitions page.  Timer Job Definitions    5. Click SharePoint Services Search Refresh. This will bring up the Edit Timer Job page.  6. Click Disable.  7. Close Internet Explorer. |

## Implement Secure Sockets Layer (SSL) for the FIM Portal

In this step, you will implement SSL for the FIM Portal. You will be requesting a new domain certificate and binding it to SharePoint site. If you recall, the Base Configuration Test Lab guide automatically issues a server certificate to FIM1 when it joins the domain. However, because this certificate uses the FQDN (FIM1.corp.contoso.com) as its common name and not the NetBIOS name (FIM1), you will receive a certificate error when attempting to access the site with the URL https://fim1. If you used https://FIM1.corp.contoso.com as the URL you will not receive the error. However, because this site will be used inside the domain and primarily accessed using https://fim1, you should request a new certificate to use.

To implement Secure Sockets Layer (SSL) for the FIM portal

|  |
| --- |
| 1. Click Start, click Administrative Tools, and then click Internet Information Services (IIS) Manager. This will bring up the Internet Information Services (IIS) Manager.  2. On the left, expand FIM1 (CORP\Administrator). This will populate the center pane with icons. Make sure that FIM1(CORP\Administrator) is still selected.  3. In the center, double-click Server Certificates.  4. On the right, click Create Domain Certificate. This will launch the Create Certificate Wizard.  5. For Common Name, type the following text: FIM1  6. For Organization, type the following text: Contoso  7. For Organizational Unit, type the following text: IT  8. For City, type the following text: Anywhere  9. For State, type the following text: NC  Create Certificate    10. Click Next.  11. On the On-line Certificate Authority page, under Specify Online-Certificate Authority, click Select. This will bring up a Select Certificate Authority page.  12. Select corp-DC1-ca, and click OK.  13. On the On-line Certificate Authority page, under Friendly Name, type the following text, and then click Finish: FIM1\_SSL.  This will close the Create Certificate Wizard and you should see the newly created certificate in the center pane.  14. On the left, expand Sites, right-click SharePoint-80, and then select Edit Bindings. This will bring up the Site Bindings window.  15. Click Add.  16. Under type, select https from the drop-down list.  17. Under SSL Certificate, select FIM1\_SSL from the drop-down list. Click OK, and then click Close.  18. On the left, select SharePoint-80 and from the center pane double-click SSL Settings.  19. Place a check in Require SSL. On the right, click Apply.  20. Close Internet Information Services (IIS) Manager.  21. Click Start, click All Programs, click Accessories, and click Command Prompt. This will launch a command prompt window.  22. In the command prompt window, type iisreset and hit enter. This will stop and then re-start IIS. Once this completes, close the command prompt window. |

## Add the FIM Portal URL to Local Intranet Sites for CORP\Administrator

In this step you will add the FIM Portal URL to the local intranet sites.

To add the FIM Portal URL to Local Intranet Sites

|  |
| --- |
| 1. Click Start, click All Programs, and then click Internet Explorer (64-bit).  2. At the top of Internet Explorer, under Tools, click Internet Options.  3. Click the Security tab and select Local intranet from the Select a zone to view or change security settings box.  4. Click Sites to show a Local intranet window. Click Advanced.  5. In the Add this website to the zone: box, type https://fim1. Click Add.  Local Intranet    6. Place a check in Require server verification (https:) for all sites in this zone and click Close. Click Ok.  7. Click OK to close the Internet Options dialog box. |

## Restrict Membership in the User Administrators Set

By default, everyone is a member of the User Administrators set. In order to increase security, you will want to prevent users from having too much authority.

To restrict membership in the user administrators set

|  |
| --- |
| 1. In Internet Explorer, in the address bar at the top, enter https://fim1/identitymanagement and hit enter. This should bring up the Forefront Identity Manager 2010 page.  2. On the left, under Management Policy Rules, click Sets. This will bring up the Sets Page.  3. Scroll through the list of sets and select User Administrators. This will be on the last page of the sets.  4. On the User Administrators pop-up, at the top, click Criteria-based Members.  5. Click to select Add Statement.  6. Click to select <Click to select attribute>.  7. From the drop-down list that appears, select Resource ID.  8. Next to Resource ID, click the word is. This will change to a drop-down box. Select in.  9. Next to in, click to select <click to select value>. This will bring up a Select Set pop-up.  10. At the top, next to the Search for box, click the magnifying glass.  Tip  Leave the box empty before clicking to select the magnifying glass. This will return a list of all the sets.  11. Select Administrators in the check box, and then click OK. It should now look like the following image.  Restrict User Administrators Set    12. Click OK.  13. Click Submit. |

## Pre-allocate Space in the FIM Service Database

Because SQL Server performance can suffer when SQL Server must allocate space during processing, you will want to prevent this by pre-allocating space for the FIM Service database.

To pre-allocate space in the FIM Service database

|  |
| --- |
| 1. Log on to APP1.corp.contoso.com as Administrator.  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 then select Properties. This will bring up the Database Properties – FIMService screen.  8. On the left, click Files.  9. For the row with FIMService, under Initial Size, change the value to 5000.  10. For the row with FIMService\_log, under Initial Size, change the value to 1000. It should now look like the following image.  FIM Service database change    11. Click OK. This may take a few minutes to complete. |

## Pre-allocate Space in the FIM Synchronization Service Database

Because SQL Server performance can suffer when SQL Server must allocate space during processing, you will want to prevent this by preallocating space for the FIM Synchronization Service database.

To pre-allocate space in the FIM Synchronization Service database

|  |
| --- |
| 1. In SQL Server Management Studio, right-click FIMSynchronizationService, and then select Properties. This will bring up the Database Properties – FIMSyncrhonizationService screen.  2. On the left, click Files.  3. For the row with FIMSynchronizationService, under Initial Size, change the value to 5000.  4. For the row with FIMSynchronizationService\_log, under Initial Size, change the value to 1000. It should now look like the following image.  5. Click OK. This may take a few minutes to complete. |

# Step 9: Verify the Installation

Verifying the FIM1 installation for the Forefront Identity Manager 2010 test lab consists of the following:

 Verify the E-mail Server, Database Server, and MA Account

 Verify the Build Numbers of the FIM Service and the FIM Synchronization Service

## Verify the E-mail Server, Database Server, and MA Account

To verify the e-mail server, database server, and MA account

|  |
| --- |
| 1. Log on to FIM1 as CORP\Administrator.  2. Navigate to the following directory: c:\Program Files\Microsoft Forefront Identity Manager\2010\Service .  3. Locate the Microsoft ResourceManagement.Service.exe.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.  4. Select Notepad, and click OK. This will open the config file in Notepad.  5. Look for mailServer and note the value. It should be EX1.corp.contoso.com.  6. Look for SynchronizationServerName and note the value. It should be FIM1.  7. Close the config file.  8. Click Start. Click Run. Type the following text, and then click OK:   Regedit  9. Navigate to the HKLM\SYSTEM\CurrentControlSet\services\FIMService key.  10. Look for DatabaseName and note the value. It should be FIMService.  11. Look for DatabaseServer and note the value. It should be APP1.  12. Look for SynchronizationAccount and note the value. It should be CORP\FIMMA.  13. Look for SynchronizationAccountSid and note the value. It should have a SID.  14. Close the Registry Editor. |

## Verify the Build Numbers of the FIM Service and the FIM Synchronization Service

To verify the build numbers of the FIM Service and the FIM Synchronization Service

|  |
| --- |
| 1. Log on to FIM1 as CORP\Administrator.  2. Navigate to the following directory: c:\Program Files\Microsoft Forefront Identity Manager\2010\Service.  3. Locate the Microsoft ResourceManagement.Service.exe file, right-click and select Properties. This will bring up the Properties dialog box.  4. At the top, click the Details tab.  5. Look for Product Version and note the value. It should be 4.0.3531.2. Click Cancel.  6. Navigate to the following directory: c:\Program Files\Microsoft Forefront Identity Manager\2010\Synchronization Service\Bin .  7. Locate the miiserver.exe file, right-click and select Properties. This will bring up the Properties dialog box.  8. At the top, click the Details tab.  9. Look for Product Version and note the value. It should be 4.0.3531.2. Click Cancel. |

## Snapshot the Configuration

This completes the Forefront Identity Manager 2010 test lab. To save this configuration for additional test labs, do the following:

1. On all physical computers or virtual machines in the test lab, close all windows and then perform a graceful shutdown.

2. If your lab is based on virtual machines, save a snapshot of each virtual machine and name the snapshots FIM Test Lab. If your lab uses physical computers, create disk images to save the FIM Test Lab.