

Infrastructure Planning
and Design

Microsoft® Forefront® Identity Manager 2010

Version 1.1

Published: June 2010

Updated: November 2011

For the latest information, please see [www.microsoft.com/ipd](http://www.microsoft.com/ipd)

Copyright © 2011 Microsoft Corporation. All rights reserved. Complying with the applicable copyright laws is your responsibility.  By using or providing feedback on this documentation, you agree to the license agreement below.

If you are using this documentation solely for non-commercial purposes internally within YOUR company or organization, then this documentation is licensed to you under the Creative Commons Attribution-NonCommercial License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc/2.5/> or send a letter to Creative Commons, 543 Howard Street, 5th Floor, San Francisco, California, 94105, USA.

This documentation is provided to you for informational purposes only, and is provided to you entirely "AS IS".  Your use of the documentation cannot be understood as substituting for customized service and information that might be developed by Microsoft Corporation for a particular user based upon that user’s particular environment. To the extent permitted by law, MICROSOFT MAKES NO WARRANTY OF ANY KIND, DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, AND ASSUMES NO LIABILITY TO YOU FOR ANY DAMAGES OF ANY TYPE IN CONNECTION WITH THESE MATERIALS OR ANY INTELLECTUAL PROPERTY IN THEM.

Microsoft may have patents, patent applications, trademarks, or other intellectual property rights covering subject matter within this documentation.  Except as provided in a separate agreement from Microsoft, your use of this document does not give you any license to these patents, trademarks or other intellectual property.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious.

Microsoft, Active Directory, Forefront, Hyper-V, Outlook, SharePoint, SQL Server, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries and regions.

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

You have no obligation to give Microsoft any suggestions, comments or other feedback ("Feedback") relating to the documentation. However, if you do provide any Feedback to Microsoft then you provide to Microsoft, without charge, the right to use, share and commercialize your Feedback in any way and for any purpose.  You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft software or service that includes the Feedback.  You will not give Feedback that is subject to a license that requires Microsoft to license its software or documentation to third parties because we include your Feedback in them.

Contents

[The Planning and Design Series Approach 1](#_Toc301518809)

[Introduction to the Microsoft Forefront Identity Manager 2010 Guide 2](#_Toc301518810)

[Step 1: Define the Project Scope 5](#_Toc301518811)

[Step 2: Determine the Required Roles 9](#_Toc301518812)

[Step 3: Design the FIM Synchronization Service Instances 12](#_Toc301518813)

[Step 4: Design the FIM Service Infrastructure 18](#_Toc301518814)

[Step 5: Design the FIM Certificate Management Infrastructure 24](#_Toc301518815)

[Dependencies 30](#_Toc301518816)

[Conclusion 31](#_Toc301518817)

[Appendix A: Job Aids 32](#_Toc301518818)

[Appendix B: IPD in Microsoft Operations Framework 4.0 36](#_Toc301518819)

[Appendix C: Forefront Identity Manager 2010 in Microsoft Infrastructure Optimization 37](#_Toc301518820)

[Version History 38](#_Toc301518821)

[Acknowledgments 39](#_Toc301518822)

#

# The Planning and Design Series Approach

This guide is one in a series of planning and design guides that clarify and streamline the planning and design process for Microsoft® infrastructure technologies.

Each guide in the series addresses a unique infrastructure technology or scenario. These guides include the following topics:

* Defining the technical decision flow (flow chart) through the planning process.
* Describing the decisions to be made and the commonly available options to consider in making the decisions.
* Relating the decisions and options to the business in terms of cost, complexity, and other characteristics.
* Framing the decision in terms of additional questions to the business to ensure a comprehensive understanding of the appropriate business landscape.

The guides in this series are intended to complement and augment the product documentation. It is assumed that the reader has a basic understanding of the technologies discussed in these guides. It is the intent of these guides to define business requirements, then align those business requirements to product capabilities, and design the appropriate infrastructure.

## Benefits of Using This Guide

Using this guide will help an organization to plan the best architecture for the business and to deliver the most cost-effective identity manager technology.

Benefits for Business Stakeholders/Decision Makers:

* Most cost-effective design solution for an implementation. Infrastructure Planning and Design (IPD) eliminates over-architecting and overspending by precisely matching the technology solution to the business needs.
* Alignment between the business and IT from the beginning of the design process to the end.

Benefits for Infrastructure Stakeholders/Decision Makers:

* Authoritative guidance. Microsoft is the best source for guidance about the design of Microsoft products.
* Business validation questions to ensure the solution meets the requirements of both business and infrastructure stakeholders.
* High integrity design criteria that includes product limitations.
* Fault-tolerant infrastructure, where necessary.
* Proportionate system and network availability to meet business requirements.
* Infrastructure that is sized appropriately to meet business requirements.

**Benefits for** Consultants or Partners:

* Rapid readiness for consulting engagements.
* Planning and design template to standardize design and peer reviews.
* A “leave-behind” for pre- and post-sales visits to customer sites.
* General classroom instruction/preparation.

Benefits for the Entire Organization:

Using this guide should result in a design that will be sized, configured, and appropriately placed to deliver a solution for achieving stated business requirements, while considering the performance, capacity, manageability, and fault tolerance of the system.

# Introduction to the Microsoft Forefront Identity Manager 2010 Guide

Microsoft Forefront® Identity Manager 2010 provides an integrated and comprehensive solution for managing the entire life cycle of user identities and their associated credentials. It provides identity synchronization, certificate and password management, and user provisioning in a single solution that works across Windows® operating systems and other organizational systems.

To develop and implement a successful Forefront Identity Manager (FIM) design, many decisions must be made and strategies determined. Considerations for performance, security, manageability, scalability, and other criteria must be addressed if the design is to be successful.

The purpose of this guide is to assist infrastructure architects in the decision-making process by providing a clear and concise path for designing the FIM infrastructure. This guide relies on best practices and real-world experience to offer considerations and alternatives at each point in the design.

This guide, when used in conjunction with product documentation, will help organizations confidently plan a FIM implementation. Appendix A includes sample job aids for recording the decisions made during the design process.

## Assumptions

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

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

## Forefront Identity Manager 2010 Design Process

This guide describes the process of planning a Forefront Identity Manager infrastructure. The guide addresses the following fundamental decisions and tasks:

* Defining the project scope by identifying which FIM features will be needed and the connected data sources and user population in scope.
* Mapping the features and scope into the FIM server roles that will be required.
* Designing the infrastructure for the FIM Synchronization Service, FIM Service, and Certificate Management.
* Designing the placement and fault tolerance of the supporting SQL Server databases.

Following the instructions in this guide should result in a design that is sized, configured, and appropriately placed to deliver the stated business benefits, while also considering the performance, capacity, and fault tolerance of the system.

This guide addresses the scenarios most likely to be encountered by someone designing a FIM infrastructure. Customers should consider having their architecture reviewed by Microsoft Customer Service and Support prior to implementation as that organization is best able to comment on the supportability of a particular design.

This guide addresses the following decisions and/or activities that need to occur in planning for FIM. The five steps below represent the most critical design elements in a well-planned FIM design:

* Step 1: Define the Project Scope
* Step 2: Determine the Required Roles
* Step 3: Design the FIM Synchronization Service Instances
* Step 4: Design the FIM Service Infrastructure
* Step 5: Design the FIM Certificate Management Infrastructure

Some of these items represent decisions that must be made. Where this is the case, a corresponding list of common response options will be presented.

Other items in this list represent tasks that must be carried out. These types of items are addressed because their presence is significant in order to complete the infrastructure design.

Figure 1 provides a graphical overview of the steps in designing a FIM infrastructure.



Figure 1. The FIM infrastructure decision flow

The primary components of a FIM architecture are shown in Figure 2.



Figure 2. Example FIM architecture

## Applicable Scenarios

This guide addresses considerations that are related to planning and designing the FIM infrastructure:

* Organizations with no identity life-cycle management solution that want to use FIM.
* Organizations that currently use another identity life-cycle management solution and are planning to move to FIM.
* Organizations that require the Lifecycle Certificate signing service, smart card management, and user management for Encrypting File System (EFS) for applications such as secure mail.
* Organizations upgrading from Microsoft Identity Lifecycle Manager (ILM) 2007 to FIM 2010.

## Out of Scope

The following activities are out of scope for this guide:

* Designing management agents.
* Designing and implementing specific customizations to the FIM Portal, including workflows.
* Designing an Active Directory Certificate Services infrastructure. See the *Infrastructure Planning and Design Guide for Active Directory Certificate Services* at <http://go.microsoft.com/fwlink/?LinkId=189608> for more information.

# Step 1: Define the Project Scope

Before designing a Forefront Identity Manager (FIM) infrastructure, an organization needs to determine the objectives for the project and which parts of its environment to include in the design. The connected data sources that are in scope for the FIM infrastructure project will be identified in this step. To understand the key performance characteristics that the FIM infrastructure will be subjected to and the expected response times for the service, the user load and fault-tolerance requirements for each service will also be determined.

The output of this step will in turn drive decisions related to which FIM server roles will be required and the size and placement of each.

## Task 1: Determine the Business Reasons to Implement FIM

FIM provides different levels of administrative and end-user access as well as functionality to help provide identity management. Which product features will be used to deliver the functionality that the business requires will be determined here since certain feature sets may change which infrastructure components will be required.

The first decision to be made is whether the organization is implementing FIM to deliver certificate management, identity management, or both. Review the descriptions below, and record the functionalities that will be implemented in Table A-1 in Appendix A: “Job Aids.”

### Certificate Management

Certificate management supplements Active Directory Certificate Services (AD CS) by automating the provisioning, renewal, and revocation of public key infrastructure (PKI) digital certificates for smart cards and other uses such as Encrypting File System (EFS) and web Secure Sockets Layer/Transport Layer Security (SSL/TLS).

This may be implemented with or without the identity management functionality listed below.

### Identity Management

Identity data in an enterprise environment is typically distributed among various connected data sources that may be managed by different departments. As a consequence of this, the managed data quickly becomes out of date, and identities may have to be manually managed in separate systems.

The classic identity management capability of FIM provides synchronization of data and provisioning of identity information for the organization in two fundamental areas:

* Synchronizes data between multiple sources. An example of this is synchronization of mobile telephone numbers from the enterprise’s Human Resource (HR) system with Active Directory Domain Services (AD DS) to make the telephone numbers available in an Exchange Server’s global address list (GAL).
* Identity life-cycle management is the automated provisioning and de-provisioning of identities in the connected systems. An example is creating an Active Directory account for users when they are added to the HR system. Accordingly, the account can be removed or disabled when users are no longer active in the HR system.

Classic identity management is the functionality provided by the FIM Synchronization Service and requires the use of manual coding unless implemented with the FIM Service. The FIM Service provides the additional functionality described below. Review the descriptions and select which features, if any, the organization requires.

* **Password synchronization.** Provides password change synchronization from AD DS to other connected systems.

Requires the Password Change Notification Service to be loaded on the organization’s Active Directory domain controllers, and requires the FIM Synchronization Service.

* Password self-service. Provides the ability for users to reset their own passwords either from a portal or from the Windows logon screen.

Requires the FIM Service, FIM Portal, FIM Synchronization Service, and the FIM client software.

* **User profile management.** Automates the maintenance of user information in various systems, directories, or applications. Allows users to update their own identity information, such as mobile telephone numbers, through a portal.

Requires the FIM Synchronization Service, FIM Service, and FIM Portal.

* **Group management from portal.** Provides the ability for end users to manage their own groups from a portal.

Requires the FIM Synchronization Service, FIM Service, and FIM Portal.

* **Group management from Outlook.** Provides the ability for end users to manage their own groups from within Microsoft Outlook® 2007 or later.

Requires the FIM Synchronization Service, FIM Service, FIM Portal, and a FIM Service mailbox on the Exchange server.

* **Declarative provisioning.** An organization can either use the FIM portal to declare attribute flows and to configure policies that control the provisioning and synchronization process, or write custom .NET code. If the organization is doing a new installation of FIM or does not have code already developed to support all flows and computations across the connected systems, implementing the declarative provisioning aspect of FIM by using the FIM Service and FIM Portal for provisioning will accelerate FIM deployment.

Requires the FIM Synchronization Service, FIM Service, and FIM Portal.

Identity management functionality may be implemented with or without the certificate management functionality described above.

Record the functionalities that will be implemented in Table A-1 in Appendix A.

## Task 2: Determine the Connected Data Sources in Scope

If it was decided to only implement certificate management, skip this task. To perform identity management, FIM must connect to at least one connected data source. A connected data source is defined as a directory, database, or other data repository that contains identity or user profile data to be integrated within FIM. The sources can be enterprise directories, network operating system directories, databases, data in flat files, or delimited text. A management agent (MA) will be required to link each specific connected data source to FIM. For each data source that will be connected to FIM, there will need to be one or more instantiations of a management agent for that kind of data source. For a list of management agents available for FIM 2010, see [http://technet.microsoft.com/en-us/library/ff608275(WS.10).aspx](http://technet.microsoft.com/en-us/library/ff608275%28WS.10%29.aspx).

For each connected data source identified:

* Determine how often the data in that source changes and how quickly those changes need to be synchronized (if synchronizing with multiple directories) to the other connected systems.
* Calculate the duration of the import (delta or full), the size of the delta synchronization, and the duration of the export for each connected system to determine the approximate run time of a synchronization cycle. These durations can be calculated by performing import, synchronization, and export operations on a representative subset of sample data.

**Note**Some data sources may require a full import each time, while others may be capable of performing a delta import, which will trigger synchronization only on objects that have changed. Full imports have a significant impact on the overall performance and efficiency of a FIM solution. Special care should be taken while analyzing and documenting connected data sources that require full imports. Exports are always performed as delta operations.

Operations to synchronize identity information with external systems are loads that must also be accounted for in capacity and performance planning. Determining the number and types of connected systems, combined with identifying the activities required for each system, will help determine the design of the FIM Synchronization Service. Use Table A-2 in Appendix A to collect and record the connected sources, frequency of changes, and approximate run times for each data source.

## Task 3: Determine User Load

In order to effectively implement FIM in an enterprise, it is critical to understand the key performance characteristics that it will be subjected to and the expected response times.

Record these details on the planned load for the FIM implementation in Table A-3 in Appendix A:

* Approximate number of users in each location. Assess the user population that will be served by each of the FIM functionality areas listed in Task 1, and record the physical locations, Active Directory forests, and approximate number of users. Knowing the number of users at each location will assist in determining server sizing and placement.
* Expected usage. Estimate the number of times the organization expects new groups or users to be created by administrators or users, passwords to be reset, and the portal to be visited in a given time period. Note that the load may vary during the course of an hour, day, week, or year, and the implementation should be designed to support peak load.

Additionally, categorize the usage as “administrator-type” or “user-type” or with a classification that makes sense for the organization’s structures and service priorities. One possible separation that will be considered later is having separate interfaces for administrators to help guarantee responsiveness of the system for regular end users.

The expected load will affect portal placement, scaling, and client deployment decisions in later steps.

## Task 4: Determine Fault-Tolerance Requirements

In this task, the organization’s fault-tolerance requirements will be determined.

For each FIM functionality area that was selected in Task 1, assess whether fault tolerance is required. Record the answers in Table A-1 in Appendix A so that those requirements can be used to design the fault-tolerance configuration in later steps.

Special care should be taken if password self-service, password synchronization, user profile management, or certificate management were selected in Task 1. These are end-user facing aspects of FIM. Determine what the business’s tolerance is for outages of these features. For example, the business may determine that unavailability of password self-service is not acceptable due to the volume of users, but that user profile management functionality can be out for a day, which might be the time it requires to manually recover a single-point-of-failure server. Additionally, review the types of users gathered in Task 3, as certain categories of users may have more stringent fault-tolerance needs than others, such as a requirement that systems used by executive-level end users not experience outages.

## Validating with the Business

In order to ensure that the project stays focused on delivering the required services, ask the following question about the business objectives for the project:

**Do any corporate policies prevent systems from being synchronized?** For example, country or regional regulations may prevent certain identity attributes from being shared across borders.

## Step Summary

The business reasons to implement FIM as well as the expected functionality were determined. The desired features were selected to implement identity management, if that was chosen. Additionally, the user load was determined, and the connected data sources were collected. Finally, the fault-tolerance requirements were determined. All of the data gathered in this step was recorded in Tables A-1, A-2, and A-3 in Appendix A.

## Additional Reading

* FIM 2010 Technical Overview: [http://technet.microsoft.com/en-us/library/ff621362(WS.10).aspx](http://technet.microsoft.com/en-us/library/ff621362%28WS.10%29.aspx)
* Microsoft Forefront Identity Manager home page: [www.microsoft.com/fim](http://www.microsoft.com/fim)

# Step 2: Determine the Required Roles

The functionalities and features that were selected in Step 1 will be the basis in this step to determine the required infrastructure components to support the desired feature sets. This information will be used in later steps to design the FIM infrastructure.

A FIM 2010 deployment has two major component groups: the server-side and the client-side. The server-side components that might be implemented include:

* FIM Synchronization Service and FIM Synchronization Service database.
* FIM Service, FIM Service database, and FIM Portal.
* FIM Certificate Management, FIM Certificate Management database, and FIM Certificate Management Portal.
* Password Change Notification Service (PCNS) on Active Directory domain controllers.

The client-side FIM Add-ins and Extensions components might include:

* FIM Add-in for Outlook.
* FIM Password and Authentication Client Service.
* FIM Password and Authentication Extensions.
* FIM Portal Authentication Extensions.

Consult the table below for descriptions of these FIM components.

Table 1. FIM Components with Descriptions

| **Components** | **Description** |
| --- | --- |
| FIM Synchronization Service | Synchronizes data with other identity stores. |
| FIM Synchronization Service database | SQL Server database for FIM Synchronization Service; contains the metaverse, the connector space for each management agent, and configuration data. |
| FIM Service | Web service that implements FIM identity management functionality. FIM Service is accessed through web services or the FIM clients and is used by most other components in a FIM solution. |
| FIM Service database | SQL Server database for FIM Service; the principal repository for objects and attributes that will be subject to FIM policies and workflows. Also contains the configuration for the portal including the schema, the workflows, and the policy rules. |
| FIM Portal | Interface for performing password resets, group management, and administrative operations. Runs on Windows SharePoint Services 3.0. |
| FIM Password Portal | A page within the FIM Portal that permits anonymous access, making it accessible from kiosks or coworkers’ computers, to enable resetting of end users’ passwords.  |
| FIM Client software | Software loaded on the client workstations that provides:* Self-service password reset from the Windows logon screen.
* Self-service group management from within Outlook.
 |
| FIM Service Mailbox on Exchange 2007 or Exchange 2010 | Used with the FIM Service and FIM Portal for group management when Outlook 2007 add-in is used. |
| Password Change Notification Service (PCNS) | A service installed onto each Active Directory Domain Services domain controller within the environment to intercept the password and to pass it to the FIM Synchronization Service for synchronization with other systems. |
| FIM Certificate Management  | Provides management of certificates and smart cards. A Web portal serves as the principal end user and administrative interface for certificate and smart card management. |
| FIM Certificate Management database | Uses SQL Server to store data for Certificate Management. |
| FIM Certificate Management Client software | Assists in client-side, smart card management activities such as changing the personal identification number (PIN) on a smart card. The FIM CM client is required to deploy smart cards, but not to deploy software-based certificates. |

To determine the FIM components that will be required, refer to the feature sets that were selected in Step 1. In Table 2, the X’s below each feature set indicate the infrastructure components that will be required to support that feature set. Record which components will be required in Table A-4 in Appendix A.

If multiple feature sets are selected, the components are additive, meaning that if identity management, user profile management, and certificate management functionalities are selected, the FIM Synchronization Service, FIM Synchronization Service database, FIM Service, FIM Service database, FIM Portal, FIM Certificate Management, and FIM Certificate Management database will all be required. However, multiple instances of the services will not necessarily be required because a single instance can be used to provide multiple capabilities.

Table 2. FIM Feature Set to Infrastructure Component Mapping

| Functionality | FIM Synchronization Service and FIM Synchronization Service database | FIM Service, FIM Service database, and FIM Portal | FIM Password Portal | FIM Client software | FIM Service mailbox on Exchange 2007 or Exchange 2010 | Password Change Notification Service (PCNS) on Domain Controllers | FIM CM, FIM CM database, and FIM CM Client |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Identity management (classic functionality) | X |  |  |  |  |  |  |
| Password synchronization | X | X |  |  |  | X |  |
| Password self-service | X | X | O | X |  |  |  |
| User profile management | X | X |  |  |  |  |  |
| Group management from portal | X | X |  |  |  |  |  |
| Group management from Outlook | X | X |  | X | X |  |  |
| Declarative provisioning | X | X |  |  |  |  |  |
| Certificate management | O | O |  |  |  |  | X |

X = Required

O = Optional

## Step Summary

In this step, the infrastructure components that will be required to support the desired feature sets were determined and recorded in Table A-4 in Appendix A.

# Step 3: Design the FIM Synchronization Service Instances

In the previous step, the Forefront Identity Manager 2010 infrastructure components that will be required to support the desired feature sets were determined. If it was determined that the FIM Synchronization Service was not required (that is, only the FIM certificate management feature set will be implemented), then skip to Step 5.

In this step, the number of FIM Synchronization Service instances will be determined. Next, the database storage requirements will be estimated. Then the placement, sizing, and fault-tolerance strategies will be decided. The FIM Service and FIM Service database will be designed in the next step, and the CM Server and database will be designed in Step 5.

Identity data in an enterprise environment is typically distributed among various connected data sources that may be managed by different departments. As a consequence of this, the managed data quickly becomes out of date.

The objective of the FIM Synchronization Service is to ensure that the managed resources converge to a desired state and to apply updates to them throughout an object’s life cycle, if necessary. To determine whether updates to an existing object are necessary, FIM needs to keep track of the current state of a resource in a connected data source. The objects and their attributes that FIM contains is a result of import operations from a connected data source.

The FIM Synchronization Service uses management agents to synchronize data between the FIM Synchronization Service database and the connected data sources in the enterprise, including the FIM Service.

**Note**   For readers familiar with Microsoft Identity Integration Server (MIIS) 2003 and ILM 2007, the Synchronization Service in FIM 2010 is fundamentally unchanged from an infrastructure standpoint.

## Task 1: Decide How Many FIM Synchronization Service Instances Will Be Required

In this task, the number of FIM Synchronization Service instances required will be determined. Most enterprises will have only one instance of the FIM Synchronization Service. This section will help determine if the organization needs more than one. If it is determined that more than one is needed, the customer is encouraged to consult with a knowledgeable Microsoft Partner or Microsoft Consulting Services as there are design considerations beyond the scope of what can be covered in this guide.

A FIM Synchronization Service instance is anchored by a single SQL Server database. Separate databases define separate instances since there is no way to manage them collectively. Additionally, a FIM Synchronization Service instance can only communicate with a single FIM Service instance, which is also defined by a database (in this case, the FIM Service database). Thus a FIM Synchronization Service instance consists of the FIM Synchronization Service and its supporting database, and optionally, the FIM Service and its corresponding database.

Start with one instance of the FIM Synchronization Service, and then add more instances as required by any of the following:

* Data consolidation prior to main implementation. Multiple FIM Synchronization Services instances might be used to flow data from multiple HR systems into a single data store for clean up before sending over to the main identity management system.
* Synchronization cycle length. Full imports have the largest impact on synchronization cycle run times. Delta imports and delta synchronizations may have a significant impact if there are a large number of imports or synchronizations.

Calculate the estimated length of a synchronization cycle by summing the time to import, synchronize, and export the data to each of the connected data sources. Determine if this total estimated time period is acceptable to the business. If it is not, a second FIM Synchronization Service instance may be needed.

Adding an additional FIM Synchronization Service reduces synchronization time because tasks can be run in parallel. For example, if one FIM Synchronization Service instance is responsible for group management and another for user management, then users can be created or changed in a short period of time without having to wait for the group management operation to complete. Multiple systems are integrated by having each system responsible for different areas, such as different object types or connected systems.

* Political**.** Different groups within the organization might each require their own installations.
* Regulatory requirements**.** Regulatory requirements can force an organization to manage certain data in an isolated environment. A dedicated FIM Synchronization Service will provide that isolated environment. Alternatively, the organization may also decide that those systems requiring isolation simply cannot be included in the FIM design.
* Limit fault domain. The FIM Synchronization Service cannot be clustered for fault tolerance (more about this in Task 3), so the organization may choose to implement additional instances to reduce the impact of a specific instance experiencing an outage.

If these considerations were reviewed, and it was determined that only one FIM Synchronization Service instance will be required, continue to Task 2 to determine the database storage requirements. If more than one instance will be required, it is recommended that the organization work with a Microsoft Partner or Microsoft Consulting Services to design the implementation’s complexity.

## Task 2: Determine FIM Synchronization Service Database Storage Requirements

Each FIM Synchronization Service instance has a single SQL Server database. The database can be hosted on a remote server running SQL Server or on the server where the FIM Synchronization Service is installed. It does not need to be a dedicated server as it can be co-located on the same SQL Server instances as other databases.

In this task, the storage needs for the database for each instance will be evaluated.

No updated guidance is available from the product group at the time of this writing to determine how the FIM Synchronization Service database will increase in size during normal operations, but it can be expected to be similar to its predecessors: MIIS and ILM. Factors that affected the database’s size in MIIS and ILM were:

* Number of management agents in the solution. Additional management agents require more storage for the connector space. The connector space stores a complete subset of the information staged from the connected directory.
* Number of objects in each management agent.
* Number of attributes being staged for each object.
* Size of each attribute.
* Number of multi-valued attributes and the size of their values.
* The schedule at which run profiles are executed in the solution. More frequent scheduling of run profiles will result in more run history data being collected.
* The frequency with which an organization clears the run history. Run history data is collected over time, and if the data is not periodically cleared, it can drastically increase database size. Additionally, the organization will need to maintain sufficient storage space to have the ability to clear the run history. After a SQL Server transaction occurs and before the transaction is committed, FIM deletes the run history information within the FIM database. This causes the SQL Server database log to expand in size in order to contain all of the deleted run history. The database requires sufficient additional storage to handle this expansion, the amount of which depends on the size of the FIM solution and the amount of run history the organization maintains.
* Number of objects in the metaverse.
* Number and size of attributes in the metaverse.

Refer to “MIIS 2003 Capacity Planning Test Summary – Database Size” at [http://technet.microsoft.com/en-us/library/cc720566(WS.10).aspx](http://technet.microsoft.com/en-us/library/cc720566%28WS.10%29.aspx) to determine the initial size and expected future growth of the FIM Synchronization Service database, and record it in Table A-5 in Appendix A.

## Task 3: Apply Fault-Tolerance Requirements

If the FIM Synchronization Service and the FIM Synchronization Service database are unavailable, identity synchronizations will not take place until the systems are returned to full functionality. Additionally, the following user-facing scenarios will be affected as well:

* Password synchronization
* Password self service
* Group management via the portal
* Group management via Outlook

Fault-tolerance requirements should be considered for all services that have an impact on user-facing scenarios. Fault tolerance for the FIM Synchronization Service and the FIM Synchronization Service database will be evaluated in this section. The FIM Service and FIM Portal will be considered in the next step.

### FIM Synchronization Service

The FIM Synchronization Service cannot be installed on a cluster as it is not cluster-aware, nor is load balancing supported. The service cannot be made available in a fault-tolerant configuration.

**Note**This single point of failure cannot be completely eliminated, but it can be minimized by implementing a warm-standby server for the FIM Synchronization Service. This warm standby server can often be brought online more quickly than recovering the primary server. Please refer to the following document for configuring and operating a warm standby server as the tasks are the same in FIM: “Plan High Availability for MIIS” at <http://technet.microsoft.com/en-us/library/cc526416.aspx>.

### FIM Synchronization Service Database

The FIM Synchronization Service database can be hosted on a clustered instance of SQL Server for fault tolerance. Other high availability and disaster recovery strategies like database mirroring and log shipping can also be used to provide fault tolerance for the SQL Server database, whether located locally or remotely. If SQL Server clustering is used, the FIM Synchronization Service database cannot be installed on the same server as the FIM Synchronization Service.

Refer to the fault-tolerance needs analyzed in Step 1, Task 4, and determine whether a standby server instance will need to be implemented for each FIM Synchronization Service instance and, if so, add it to the design and record it in Table A-6 in Appendix A. Determine the fault-tolerance option and the location where the FIM Synchronization Service database will reside, and record it in Table A-5. Then consult the Infrastructure Planning and Design Guide for Microsoft SQL Server 2008 and SQL Server 2008 R2 at <http://go.microsoft.com/fwlink/?LinkId=163302> to design the SQL Server infrastructure.

The following diagram illustrates a possible implementation of the FIM Synchronization Service in a warm standby configuration, with the FIM Synchronization Service database in a clustered configuration.



Figure 3. FIM Synchronization Service warm standby with fault-tolerant SQL Server service example diagram

## Task 4: Determine FIM Synchronization Service Server Placement

FIM supports a variety of deployment topologies. Each of the main components of FIM, including the FIM Synchronization Service, FIM Service, and Certificate Management Update Service, and respective portals and databases may be installed separately, or in combination, on individual servers.

In this task, the placement of each FIM Synchronization Service server will be decided.

The FIM Synchronization Service imports and exports data from the connected data sources and stores it in a SQL Server database. Therefore, it needs to have excellent connectivity to all connected data sources and to the FIM Synchronization Service database if the database is hosted on a separate server running SQL Server. Consider placing the FIM Synchronization Service on a network closest to the connected systems with the most changes to the data. Best practices for the FIM Synchronization Services’ predecessors, ILM 2007 and MIIS, advised placing the database on the same server as the service. However, with advancements in network performance, adequate synchronization performance can be achieved with the database on a separate server. The FIM product group has reported no performance penalty when gigabit network cards are used, and about a 25 percent performance penalty with 100-megabyte network cards.

Record the placement of each FIM Synchronization Service server in Table A-6 in Appendix A.

## Task 5: Determine FIM Synchronization Service Server Configuration

The FIM Synchronization Service can be run in a Microsoft Hyper-V® virtual machine or in a physical server environment. If a virtual machine will be used, ensure that it has access to CPU and memory resources equivalent to those specified for a physical machine. As stated in Task 4, the FIM Synchronization Service can be co-located with other FIM components. If this is done, the server should be sized to support the sum of the peak workloads.

FIM requires an x64-capable processor, 2 gigabytes (GB) or more of RAM, and 2 GB of hard-drive space to support installation of the components. These requirements from the product group assume that the database will run on a remote SQL Server-based server, thus the specifications would need to be increased if the database is hosted on the same server.

Per the FIM product group, testing performed for MIIS 2003 should also apply to the FIM Synchronization Service as the service has remained essentially unchanged in the new version. A summary of the results is as follows:

* **Processors.** The speed of the processors has more impact on the performance than the number of processors. No significant performance gains were seen when switching from a dual-processor platform to a quad-processor platform where the other configuration aspects remained constant. Significant performance improvements were seen when a 3.2-gigahertz (GHz) dual-processor platform was compared to a 2.8-GHz quad-processor platform.
* **Memory.** At a minimum, servers should be configured with a total of 2 GB of RAM. If the server will be managing 50,000 or more objects from more than two data sources, then it is recommended that at least 2 GB of RAM be used for each processor.

The hard drive usage should not be extremely large, as most storage will take place in the database. And as described in Task 4, communication with the database is critical, so using gigabit network adapters will reduce latency.

Determine the hardware configuration of each FIM Synchronization Service server, and record it in Table A-6 in Appendix A.

## Step Summary

In this step, the number of FIM Synchronization Service instances required was determined. Also, the database storage requirements were determined, and the fault-tolerance requirements were applied. The FIM Synchronization Service server placement was determined and its server was sized. The data gathered in this step was recorded in Tables A-5 and A-6 in Appendix A.

## Additional Reading

* Infrastructure Planning and Design Guide for Microsoft SQL Server 2008 and SQL Server 2008 R2: <http://go.microsoft.com/fwlink/?LinkId=163302>
* “MIIS 2003 Capacity Planning”: [http://technet.microsoft.com/en-us/library/cc720551(WS.10).aspx](http://technet.microsoft.com/en-us/library/cc720551%28WS.10%29.aspx)
* MIIS Design and Planning Collection: <http://go.microsoft.com/fwlink/?linkid=30436>
* “Estimating the Size of a Database”: <http://msdn.microsoft.com/en-us/library/ms187445.aspx>

# Step 4: Design the FIM Service Infrastructure

If the selected features indicated that the Forefront Identity Manager (FIM) Service will be required, follow this step to design the infrastructure. Otherwise, skip to the next step. In this step, it will be determined how many FIM Service servers and FIM Portal servers are necessary for performance and fault-tolerance requirements. Also, the FIM Service database storage requirements will be determined. Finally, the FIM Service components will be placed and configured.

The permissions, workflow, and other logic of the Portal occur in the FIM Service. It includes the following components:

* The FIM Service servers
* The FIM Service database
* The FIM Portal

The FIM Service only accepts ws-\* web service communications. The web service calls may be from the FIM Portal, the FIM client on user workstations, the FIM Synchronization Service, or custom applications.

The FIM Portal is a customizable, web-based user interface, based on Windows SharePoint Services 3.0, which allows end users to interact with FIM. The FIM Portal communicates with the FIM Service for each transaction and is completely dependent
on it.

**Note**   The FIM Portal is separate from the FIM CM Portal.

## Task 1: Determine the Number of FIM Service Servers Required

In this task, the number of FIM Service servers will be determined. There will only be one FIM Service database, but there can be multiple FIM Service servers that connect to that FIM Service database.

Multiple FIM Service servers may be implemented to provide different levels of responsiveness. The FIM Synchronization Service performs requests for data from the FIM Service, and these requests can trigger workflows and add a considerable load to the system, competing with end-user workflows for resources. Such issues can become pronounced with authentication workflows such as password resets, which are done in real time with an end user waiting for the process to complete. By providing one instance of the FIM Service for end-user operations and a separate instance for administrative data synchronization, better responsiveness for end-user operations can be provided.

Begin with one FIM Service server instance, and add more if needed to separate FIM Service usages. Record the number of FIM Service server instances required in Table
A-7 in Appendix A.

## Task 2: Determine the Number of FIM Portal Servers Required

In this task, the number of FIM Portal servers will be determined. The FIM Portal communicates with the FIM Service for each transaction and is completely dependent on the service. The FIM Portal can be scaled horizontally by adding additional servers in a load-balanced configuration. It may be installed separately or in combination with other FIM components on individual servers.

Typically, the database and service piece will use more resources than the portal, although this is partially determined by what custom workflows are in place and how many user transactions are expected. So if it is expected that the FIM Service will be heavily burdened, the first step is to move the database to a dedicated server and keep the FIM Service and FIM Portal together.

Start with one FIM Portal server, and add additional servers if the performance is found to be inadequate. Organizations that have a large number of users and are concerned about the performance of the FIM Portal can perform stress tests in a test environment to determine the exact server capacity for their environments.

Record the number of FIM Portal servers required in Table A-7 in Appendix A.

## Task 3: Determine FIM Service Database Storage Requirements

In this task, the storage needs for the database for each instance will be evaluated. Each FIM Service instance has a single SQL Server database. The database can be hosted on the same server as the FIM Service, or on a remote SQL Server-based server to support high availability or to conform to SQL Server standards for the organization. It can be co-located in the same instances of SQL Server as other databases.

The FIM 2010 Capacity Planning Guide at [http://technet.microsoft.com/en-us/library/ff400279(WS.10).aspx](http://technet.microsoft.com/en-us/library/ff400279%28WS.10%29.aspx) provides example capacity planning data that can be used as an initial reference point. However, there is no definitive methodology to determine how the FIM database will increase in size during normal operations, so organizations are expected to configure their own test environments to more accurately estimate capacity and performance. Note in the *Capacity Planning Guide* that the SQL Server data files were pre-allocated to ensure ample space for the expansion of the database. The reported increases in size are based on the usage of the pre-allocated space.

Determine the initial size plus the expected future growth of the FIM Service database, and record it in Table A-5 in Appendix A.

## Task 4: Apply Fault-Tolerance Requirements

The FIM Synchronization Service, FIM Synchronization Service database, FIM Service, and the FIM Service database are required for the following scenarios:

* Password self service
* Group management via Outlook
* Declarative provisioning

Additionally, the FIM Portal is required for the following:

* Group management via the portal
* Profile management

Fault-tolerance requirements should be considered for all services that have an impact on user-facing scenarios. Fault tolerance for the FIM Service, the FIM Service database, and the FIM Portal will be evaluated in this section. Fault tolerance for the FIM Synchronization Service was addressed in Step 3, Task 3, and is a single point of failure as it cannot be made available in a fault-tolerant configuration.

Refer to the requirements for availability and performance that were determined in Step 1. Use those requirements to determine the fault-tolerance configuration of the FIM Service components, and record it in Table A-7 in Appendix A.

### FIM Service

The FIM Service is not cluster-aware. Multiple servers may be deployed in a hardware or software load-balanced configuration to provide fault tolerance. Each server hosting the FIM Service must be configured to communicate with the same FIM Service database. The FIM Portal should communicate with the FIM Service via the load-balanced IP or host name and not the actual hosts in order to automatically adjust if one of the nodes in the load-balanced FIM Service fails.

### FIM Service Database

SQL Server can be clustered for fault tolerance. However, the FIM Service and the FIM Service database must be installed on separate servers if SQL Server clustering is used. Determine the fault-tolerance option and the location where the FIM Service database will reside, then consult the *Infrastructure Planning and Design Guide for Microsoft SQL Server 2008* and SQL Server 2008 R2 at <http://go.microsoft.com/fwlink/?LinkId=163302> to design the SQL Server infrastructure.

### FIM Portal

The FIM Portal is not cluster-aware. Multiple servers may be deployed in a hardware or software load-balancing configuration to provide fault tolerance. If it was decided in Task 2 to implement the FIM Portal in a load-balanced configuration for scale out, then fault tolerance is also provided by this configuration.

The following diagram illustrates a possible implementation of the FIM Service in a fault-tolerant configuration, with the FIM Service and Portal co-located.



Figure 4. FIM Service fault-tolerance example diagram

## Task 5: Determine the Placement of FIM Service Components

In this task, the placement of each FIM Service component will be decided. FIM supports a variety of deployment topologies. Similar to the FIM Synchronization Service, each of the main components of the FIM Service may be installed either separately or in combination on individual servers.

If a heavy load is anticipated, the first step is to move the FIM Service database to a dedicated server. It is unlikely that load alone will require the separation of the FIM Service and FIM Portal from each other. One possible driver for placing the FIM Portal on a separate server would be if the organization’s policies dictate that a separate team manages the SharePoint infrastructure. The FIM Portal may be installed in a SharePoint farm or on a stand-alone SharePoint server.

The FIM Portal, FIM Service, FIM Service database, and the FIM Synchronization Service servers should all be well-connected (via LAN or very high-speed WAN) and geographically located near any application that uses FIM services. The FIM Portal servers should not be separated across a WAN from the FIM Service. However, if the users are located across a WAN, and the WAN link fails, users will experience an outage.

Record the placement of the FIM Service components in Table A-7 in Appendix A.

## Task 6: Determine the Configuration of FIM Service Components

The FIM Service components can be run in a Hyper-V virtual machine or in a physical server environment. If a virtual machine will be used, ensure that it has access to CPU and memory resources equivalent to those specified for a physical machine. If it was determined that a server will host multiple FIM components, it should be sized to support the sum of the peak workloads.

The FIM 2010 Capacity Planning Guide at [http://technet.microsoft.com/en-us/library/ff400279(WS.10).aspx](http://technet.microsoft.com/en-us/library/ff400279%28WS.10%29.aspx) provides example capacity planning data that can be used as an initial reference point. However, organizations are expected to configure their own test environments to more accurately estimate capacity and performance.

FIM requires an x64-capable processor, 2 GB or more of RAM, and 2 GB of hard drive space to support installation of components. These requirements from the product group assume that the database will run on a remote server running SQL Server, thus the specifications would need to be increased if the database is hosted locally.

Relative to performance, the FIM Service database can be expected to have heavy I/O throughput requirements and be relatively processor-intensive in operation.

In the absence of specific architectural guidance on the configuration of the server hardware, design the server using the organization’s standard server deployment for each FIM Service and FIM Portal server and record it in Table A-7 in Appendix A.

## Step Summary

In this step, the FIM Service infrastructure was designed. The number of FIM Service servers and FIM Portal servers were determined. In addition, the FIM Service database storage requirements were determined, and the fault-tolerance requirements were applied. Finally, the FIM Service components were placed and configured. The data gathered in this step was recorded in Tables A-5 and A-7 in Appendix A.

## Additional Considerations

The items listed here are generally outside the scope of an infrastructure design; however, they are included here as additional considerations that the architect may need to take into account:

* Installing clients. If the design requires self-service password resets and Outlook integration for group management, then a client will need to be installed on all desktops.
* Exchange integration. If the workflows will be using Exchange integration, a FIM Service mailbox will need to be created on an Exchange 2007 or Exchange 2010 server. The Exchange forest can be either mixed or native mode.

## Additional Reading

* “Storage Top 10 Best Practices”: <http://technet.microsoft.com/en-us/library/cc966534.aspx>
* FIM 2010 Capacity Planning Guide: [http://technet.microsoft.com/en-us/library/ff400279(WS.10).aspx](http://technet.microsoft.com/en-us/library/ff400279%28WS.10%29.aspx)

# Step 5: Design the FIM Certificate Management Infrastructure

If it was determined in Step 2 that the Forefront Identity Manager (FIM) certificate management (CM) feature set will be required, the supporting infrastructure will be designed in this step. If not, the FIM infrastructure design is complete.

Several different components together provide certificate and smart card management services in and with FIM CM:

* FIM CM server
* FIM CM database
* FIM CM client (if smart cards will be issued)
* Active Directory Domain Services
* Active Directory Certificate Services

FIM CM does not require the FIM Synchronization Service, although there is an optional management agent available to connect the systems.

FIM CM can be considered as a management interface into the Active Directory Certificate Services (AD CS) functionality. It enables the certificate administrator to control and use the AD CS functionality on a higher level of abstraction. Many manual tasks are automated and integrated in the various systems. AD CS is used to store much of the CM configuration information and is also used for authentication and authorization within the CM web application.

FIM CM simplifies digital certificate and smart card deployment in the enterprise by acting as the registration authority for customer certification authorities, receiving and managing certificate-enrollment, renewal, validation, key-recovery, and revocation requests. FIM CM is exposed via a portal that is dedicated to the certificate management components of FIM 2010 and distinct from the FIM Service Portal. A FIM CM client can be set to run on client machines at logon, and this client checks with the FIM CM to see if there are certificates that need to be updated.

The certification authority services will be provided by the existing certification authorities (CAs) running either Active Directory Certificate Services or a third-party certification authority. This step will cover the infrastructure design to implement FIM CM with an existing AD CS infrastructure; designing an AD CS infrastructure is covered in the Infrastructure Planning and Design Guide for Active Directory Certificate Services. Third-party certification authorities require vendor-supplied software in order to interoperate with the CM component of FIM; more information is available in “Understanding Third-Party Certification Authority Extensions” at [http://technet.microsoft.com/en-us/library/ee534894(WS.10).aspx](http://technet.microsoft.com/en-us/library/ee534894%28WS.10%29.aspx).

One FIM CM server can be used to manage multiple CAs, or multiple FIM CM servers can manage one CA. Unlike the FIM Service, the FIM CM Portal is part of the FIM CM, but the FIM CM database can be separated. The FIM CM server and/or database can be installed separately or in combination with other FIM services.

## Task 1: Determine the Number of FIM CM Instances Required

The scope of a FIM CM installation is the Active Directory forest. If the organization has users deployed in multiple forests, then each forest will require its own CM server, CA, and SQL Server database.

Determine whether certificates or smart cards will be issued for multiple forests, and determine how many instances of FIM CM will be needed. The remainder of this step assumes a single instance and should be repeated for each instance if it is decided that multiples are needed.

Record the number of FIM CM instances required and the forests served in Table A-8 in Appendix A. The next tasks should be reiterated for each FIM CM instance identified.

## Task 2: Determine the Number of FIM CM Servers Required

In this task, the number of FIM CM servers will be determined. The FIM CM server can be scaled horizontally by adding additional servers in a load-balanced configuration. The FIM CM server may be installed separately or in combination with other FIM components on individual servers, including the FIM CM database.

Start with one FIM CM server, and add additional servers if the performance is found to be inadequate.

Record the number of FIM CM servers required in Table A-8 in Appendix A.

## Task 3: Determine FIM CM Database Storage Requirements

Each FIM CM instance has a single SQL Server database. The database can be hosted on a remote SQL Server-based server or locally with the FIM CM Update Service and Portal. It can be co-located in the same instances of SQL Server as other databases.

In this task, the storage needs for the database will be evaluated.

FIM CM uses a SQL Server database to store smart card information, audit logs, the current state of the card management workflows, and part of the configuration data.

The database size will increase in direct proportion to the number of smart cards and certificates managed by the solution and the frequency of operations performed upon them. The size of the database space should not be of great concern in FIM CM. In ILM 2007, which is the predecessor of FIM 2010, a CM installation managing 5,000 smart cards with two certificates per smart card required less than 0.4 GB of hard disk space, and even larger installations didn’t increase the database to sizes that required large amounts of storage. FIM 2010 CM can be expected to perform similarly.

Record the expected initial size plus space needed for future growth of the FIM CM database in Table A-5 in Appendix A.

**Note**   The Infrastructure Planning and Design Guide for SQL Server 2008 and SQL Server 2008 R2 at <http://go.microsoft.com/fwlink/?LinkId=163302> can be used to more specifically plan the SQL Server implementation. In addition to the storage space and clustering requirements, planning for adequate IOps (Input/Output per second) will be important to the databases’ performances.

## Task 4: Apply Fault-Tolerance Requirements

If the CM server or CM database is unavailable, the FIM CM system will be unavailable. AD CS will still work but without the benefit of FIM certificate management.

If the CA is unavailable but the CM system is still available, reporting operations such as querying user information and performing configuration tasks will still be available, but any operation that involves a certificate—enrollment, renewal, or revocation—will not be available.

### FIM CM Server

The FIM CM server is not cluster-aware. Multiple servers may be deployed in a hardware or software load-balancing configuration to provide fault tolerance when set up with a mutually accessible SQL Server database location.

### FIM CM Database

Fault tolerance for the SQL Server database is available via clustering or database mirroring. However, a separate server running SQL Server is necessary as the FIM CM server cannot be clustered.

Determine the fault-tolerance option for the FIM CM database, then consult the *Infrastructure Planning and Design Guide for Microsoft SQL Server 2008* and SQL Server 2008 R2 at <http://go.microsoft.com/fwlink/?LinkId=163302> to design the SQL Server infrastructure. Record the decision in Table A-5 in Appendix A.

### Certificate Services Connection

Windows Server® 2003 Certificate Services does not provide support for any clustering mechanisms other than clustering a virtual machine running the CA; the usual strategy for providing fault tolerance for Certificate Services is to deploy multiple CAs. However, FIM CM only supports designating a single CA for each certificate included in the profile template, and that profile template will be unavailable for performing certificate-based operations if the CA itself is not available.

Windows Server 2008 and Windows Server 2008 R2 Certificate Services does provide support for clustering, and thus the CA would not represent a single point of failure for FIM CM.

The following diagram illustrates a possible implementation of the FIM CM in a fault-tolerant configuration, with the FIM CM server load balanced and the SQL Server database clustered.



Figure 5. FIM CM fault-tolerance example diagram

## Task 5: Decide the Placement of the FIM CM Components

The FIM CM software can be installed on the same server as the CA or on its own server. Additionally, the FIM CM database can be installed on the same server as the FIM CM Update Service, FIM CM Portal, and/or CA, or on its own server.

If FIM CM is required to be available on the Internet for access by external users, it can be published via Microsoft Internet Security and Acceleration (ISA) Server 2006, Microsoft Forefront Threat Management Gateway, or Microsoft Forefront Unified Access Gateway.

The FIM CM server communicates with the FIM CM database, CAs, and domain controllers, so the product group recommends limiting the latency between these components. The FIM CM system is able to support remote users, so there is no architectural need to locate the server near the users.

Record the placement of the FIM CM components in Table A-8 in Appendix A.

## Task 6: Determine the Configurations of the FIM CM Components

The product group’s minimum requirements include Windows Server 2008 64-bit Enterprise edition with 1 GB of RAM, although 4 GB or more is recommended, especially if the SQL Server database is to be installed locally on the FIM CM server. Details on the minimum requirements are available at [http://technet.microsoft.com/en-us/library/ee534914(WS.10).aspx](http://technet.microsoft.com/en-us/library/ee534914%28WS.10%29.aspx).

The FIM CM Portal is an ASP.NET web application and, like most web applications, it is mostly CPU-bound. The server’s overall scalability and performance should improve with the use of higher-performance processors and with the increase in the number of processors.

No official capacity planning guidance is available from the product group. CM should not be very demanding in terms of requests/second. A managed smart card should require a very small number of requests be processed by FIM CM during its lifetime. A pair of high-performance servers should be sufficient to match the requirements of most if not all organizations. Additionally, the FIM CM server is largely stateless (data is mainly stored in Active Directory and SQL Server databases) and hence the total disk space requirement should be low.

Record the FIM CM components’ configurations in Table A-8 in Appendix A.

## Task 7: Designate SMTP Relay Server

To distribute one-time passwords and reminders that certificates need to be updated or renewed, FIM CM requires access to a Simple Mail Transfer Protocol (SMTP) relay service server. This can be on the same computer as the FIM CM server, or authenticated relaying can be configured to an SMTP server if the relaying operation can resolve a mail exchanger (MX) record.

Determine which server will be used for SMTP relaying, and record the name in
Table A-8 in Appendix A.

## Additional Considerations

The FIM CM client software is only needed to deploy smart cards, not software-based certificates. The FIM CM client assists in client-side, smart card management activities such as changing the personal identification number (PIN) on a smart card.

For details on the models of smart cards and middleware supported by FIM CM, see the FIM System Requirements page at [www.microsoft.com/forefront/identitymanager/en/us/system-requirements.aspx](http://www.microsoft.com/forefront/identitymanager/en/us/system-requirements.aspx).

## Step Summary

In this step, the FIM CM infrastructure was designed. The number of FIM CM instances and servers were determined. In addition, the FIM CM database storage requirements were determined and the fault-tolerance requirements were applied. Next, the FIM CM components were placed and configured. Finally, an SMTP relay server was designated. The data gathered in this step was recorded in Tables A-5 and A-8 in Appendix A.

## Additional Reading

* Certificate Management: [http://technet.microsoft.com/en-us/library/ee808052(WS.10).aspx](http://technet.microsoft.com/en-us/library/ee808052%28WS.10%29.aspx)
* FIM System Requirements: [www.microsoft.com/forefront/identitymanager/en/us/system-requirements.aspx](http://www.microsoft.com/forefront/identitymanager/en/us/system-requirements.aspx)
* “How to Set Up FIM CM Behind a Network Load Balancing (NLB) cluster”: [http://technet.microsoft.com/en-us/library/ff356872(WS.10).aspx](http://technet.microsoft.com/en-us/library/ff356872%28WS.10%29.aspx)
* FIM CM Backup and Restore Guide: [http://technet.microsoft.com/en-us/library/fim\_cm\_backup\_and\_restore(WS.10).aspx](http://technet.microsoft.com/en-us/library/fim_cm_backup_and_restore%28WS.10%29.aspx)

# Dependencies

A complete FIM installation requires the following infrastructure:

* Windows Server 2008. All FIM services require x64 versions of Windows Server 2008 or Windows Server 2008 R2 for the base operating system. Due to
the requirements for .NET Framework 3.5, Server Core is not supported for the deployment of FIM.
* Active Directory Domain Services. Active Directory Domain Services (AD DS) must be present in the organization in order for the server services to communicate with each other and their respective databases, as well as to allow users to perform self-service actions within the FIM Portal. AD DS is also required to provide user access to the FIM Portal and to store permissions for FIM Certificate Management. See the Infrastructure Planning and Design Guide for Windows Server 2008 and Windows Server 2008 R2 Active Directory Domain Services at <http://go.microsoft.com/fwlink/?LinkId=157704> for further information.
* Active Directory Certificate Services. Required when FIM Certificate Management is used to provide Certificate Authority services.
* Web server. Some of the clients discussed require interaction with a web services tier in order to present an interface via a web browser. Microsoft's Internet Information Services (IIS) 7.0 is required to host the website and services. In the FIM architecture, a web server is not required to interact with the web services directly, but it is required if users or administrators are expected to work with the FIM Portal application. Internet Explorer 7.0 and later are supported browsers. See the Infrastructure Planning and Design Guide for Internet Information Services 7.0 and Internet Information Services 7.5 at <http://go.microsoft.com/fwlink/?LinkId=157703> for further information.
* Windows SharePoint Services 3.0 SP1 or SP2. The FIM architecture uses Windows SharePoint Services 3.0 in conjunction with IIS 7 to host the FIM applications as native SharePoint solutions. In this manner, SharePoint provides the basic authentication and application hosting platform required.
* Microsoft SQL Server 2008 SP1. All FIM services use the Microsoft SQL Server 2008 SP1 x64 database engine. See the Infrastructure Planning and Design Guide for Microsoft SQL Server 2008 and SQL Server 2008 R2 at <http://go.microsoft.com/fwlink/?LinkId=160982> for further information.
* .NET Framework 3.5. FIM uses the latest features available in Windows .NET Framework 3.5, most notably:
* Windows Workflow Foundation. Workflow activities can be tailored to run in the FIM policy engine, allowing for customization of the request processing. FIM uses the normal workflow activities defining its own types: Authentication, Authorization, and Action. The encapsulation used here in the phases of the request management pipeline makes it easier for IT managers to express business policy without needing to understand or write custom code. Instead, they can take advantage of workflows and workflow activities that are out of the box as well as those created by others.
* Windows Communication Foundation. The ws-\* web services are the cornerstone of the FIM policy engine.

# Conclusion

This guide has outlined the step-by-step process for planning a FIM infrastructure. In each step, major decisions relative to the FIM infrastructure were determined and described. The guide has explained how to record choices of roles needed, server resources, scaling, and fault tolerance, which can then be made available to the infrastructure planners.

Using the information recorded from the steps completed in this guide, the organization can help ensure that the business and technical requirements are met for a successful FIM deployment.

This guide was produced to assist in customer planning, but it should not be used alone to determine the appropriate servers, hardware, or topologies required for a FIM deployment. Customers are encouraged and expected to configure their own test environments to more accurately estimate capacity and performance.

# Appendix A: Job Aids

The job aids below can be used to record data gathered throughout the FIM infrastructure planning process.

**Steps 1 and 2**

Table A-1. Requirements Gathering

| **Functionality** | **Select** | **Fault-tolerance requirements** |
| --- | --- | --- |
| Certificate Management |  |  |
| Classic Identity Management |  |  |
| **Identity Management options** |
| * Password synchronization
 |  |  |
| * Password self service
 |  |  |
| * User profile management
 |  |  |
| * Group management from portal
 |  |  |
| * Group management from Outlook
 |  |  |
| * Declarative provisioning
 |  |  |

**Step 1**

Table A-2. Connected Data Sources

|  |  |  |
| --- | --- | --- |
| **Data source** | **Frequency of changes** | **Approximate run time** |
|  |  |  |
|  |  |  |

**Step 1**

Table A-3. User Load

|  |  |  |
| --- | --- | --- |
| **Location** | **Location #1** | **Location #2** |
| Active Directory forest(s) |  |  |
| Number of users |  |  |
| Expected usage |  |  |
| Usage type |  |  |

**Step 2**

Table A-4. FIM Infrastructure Components Required

|  |  |
| --- | --- |
| **Component** | **Required** |
| FIM Synchronization Service |  |
| FIM Synchronization Service database |  |
| FIM Service |  |
| FIM Service database |  |
| FIM Portal |  |
| FIM Password Portal |  |
| FIM Client software |  |
| FIM Service Mailbox on Exchange 2007 or Exchange 2010 |  |
| Password Change Notification Service (PCNS) |  |
| Certificate Management |  |
| Certificate Management database |  |
| FIM CM Client software |  |

**Steps 3, 4, and 5**

Table A-5. SQL Server Database Selection

| **FIM system database** | **Expected size** | **SQL Server name** | **SQL Server instance name** | **SQL Server fault tolerance** |
| --- | --- | --- | --- | --- |
| FIM Synchronization Service database |  |  |  |  |
| FIM Service database |  |  |  |  |
| FIM CM database |  |  |  |  |

**Step 3**

Table A-6. FIM Synchronization Service Infrastructure

| **Server type** | **Primary** | **Warm standby (if applicable)** |
| --- | --- | --- |
| Name of server |  |  |
| Database location (same server or remote server) |  |  |
| Processor configuration |  |  |
| Memory |  |  |
| Disk configuration |  |  |
| Network |  |  |

**Step 4**

Table A-7. FIM Service Infrastructure

| **Instance** | **FIM Service instance #1** | **FIM Service instance #2 (if needed)** |
| --- | --- | --- |
| Service requirement |  |  |
| Number of FIM Portal servers in load-balanced configuration |  |  |
| Number of FIM Service servers in load-balanced configuration |  |  |
| Placement |  |  |
| Database location (same server or remote server) |  |  |
| Processor configuration |  |  |
| Memory |  |  |
| Disk configuration |  |  |
| Network |  |  |

**Step 5**

Table A-8. FIM Certificate Management Infrastructure

| **FIM CM instances** | **FIM CM instance #1** | **FIM CM instance #2** |
| --- | --- | --- |
| Forests served |  |  |
| Number of FIM CM servers for scaling |  |  |
| Number of FIM CM servers for fault tolerance |  |  |
| FIM CM database location |  |  |
| FIM CM placement |  |  |
| Processor configuration |  |  |
| Memory |  |  |
| Disk configuration |  |  |
| Network |  |  |
| SMTP relay service server name |  |  |

# Appendix B: IPD in Microsoft Operations Framework 4.0

Microsoft Operations Framework (MOF) offers integrated best practices, principles, and activities to assist an organization in achieving reliable solutions and services. MOF provides guidance to help individuals and organizations create, operate, and support technology services, while helping to ensure the investment in technology delivers expected business value at an acceptable level of risk. MOF’s question-based guidance helps to determine what is needed for an organization now, as well as providing activities that will keep the organization running efficiently and effectively in the future.

Use MOF with IPD guides to ensure that people and process considerations are addressed when changes to an organization’s technology services are being planned.

* Use the Plan Phase to maintain focus on meeting business needs, consider business requirements and constraints, and align business strategy with the technology strategy. IPD helps to define an architecture that delivers the right solution as determined in the Plan Phase.
* Use the Deliver Phase to build solutions and deploy updated technology. In this phase, IPD helps IT pros design their technology infrastructures.
* Use the Operate Phase to plan for operations, service monitoring and control, as well as troubleshooting. The appropriate infrastructure, built with the help of IPD guides, can increase the efficiency and effectiveness of operating activities.
* Use the Manage Layer to work effectively and efficiently to make decisions that are in compliance with management objectives. The full value of sound architectural practices embodied in IPD will help deliver value to the top levels of a business.



Figure B-1. The architecture of Microsoft Operations Framework (MOF) 4.0

# Appendix C: Forefront Identity Manager 2010 in Microsoft Infrastructure Optimization

The Infrastructure Optimization (IO) Model at Microsoft groups IT processes and technologies across a continuum of organizational maturity. (For more information, see [www.microsoft.com/infrastructure](http://www.microsoft.com/infrastructure).) The model was developed by industry analysts, the Massachusetts Institute of Technology (MIT) Center for Information Systems Research (CISR), and Microsoft's own experiences with its enterprise customers. A key goal for Microsoft in creating the Infrastructure Optimization Model was to develop a simple way to use a maturity framework that is flexible and can easily be applied as the benchmark for technical capability and business value.

IO is structured around three information technology models: Core Infrastructure Optimization, Application Platform Optimization, and Business Productivity Infrastructure Optimization. According to the Core Infrastructure Optimization Model, providing identity synchronization and automated provisioning/de-provisioning, including self-service tools for end users, will help move an organization to the Dynamic level.



Figure C-1. Mapping of Forefront Identity Manager 2010 technology into the Core Infrastructure Optimization Model

# Version History

|  |  |  |
| --- | --- | --- |
| **Version** | **Description** | **Date** |
| 1.1 | Minor updates for formatting consistencies. | November 2011 |
| 1.0 | First release. | June 2010 |

# Acknowledgments

The Solution Accelerators–Management and Infrastructure (SA-MI) team acknowledges and thanks the people who produced the *Infrastructure Planning and Design Guide for Forefront Identity Manager 2010*. The following people were either directly responsible for or made a substantial contribution to the writing, development, and testing of this guide.

**Contributors:**

* Jude Chosnyk – *GrandMasters*
* Joe Coulombe *– Microsoft*
* Mike Kaczmarek *– Microsoft*
* Jeremy Palenchar *– FIM Subject Matter Expert*
* Fergus Stewart – *Microsoft*
* Melissa Stowe *– Microsoft*
* Henry Webb *– Microsoft*

**Reviewers:**

* Brjann Brekkan – *Microsoft*
* Mark Wahl *– Microsoft*

**Editor:**

* Laurie Dunham – *Xtreme Consulting Group*
* Pat Rytkonen *– Volt*

## Feedback

Please direct questions and comments about this guide to ipdfdbk@microsoft.com.