

Infrastructure Planning
and Design

Microsoft® System Center Configuration Manager 2007 R3 and Forefront® Endpoint Protection

Version 2.0

Published: October 2008

Updated: July 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, 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](#_Toc298856508)

[Introduction to the Microsoft System Center Configuration Manager 2007 R3 and Forefront Endpoint Protection Guide 3](#_Toc298856509)

[Step 1: Define the Project Scope 8](#_Toc298856510)

[Step 2: Determine Which Roles Will Be Deployed 14](#_Toc298856511)

[Step 3: Determine the Number of Sites Required 18](#_Toc298856512)

[Step 4: Design the Sites 20](#_Toc298856513)

[Step 5: Determine the Number of Hierarchies Required 31](#_Toc298856514)

[Step 6: Design Each Hierarchy 32](#_Toc298856515)

[Step 7: Design the Forefront Endpoint Protection Integration 33](#_Toc298856516)

[Conclusion 37](#_Toc298856517)

[Appendix A: Client Population Job Aid 38](#_Toc298856518)

[Appendix B: Number of Configuration Manager Sites and Hierarchies Requirements Job Aid 40](#_Toc298856519)

[Appendix C: Forefront Endpoint Protection Integration Job Aid 41](#_Toc298856520)

[Appendix D: Forefront Endpoint Protection Fringe Scenarios 42](#_Toc298856521)

[Appendix E: IPD in Microsoft Operations Framework 4.0 43](#_Toc298856522)

[Appendix F: System Center Configuration Manager and Forefront Endpoint Protection in Microsoft Infrastructure Optimization 44](#_Toc298856523)

[Version History 45](#_Toc298856524)

[Acknowledgments 46](#_Toc298856525)

# 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 Microsoft System Center Configuration Manager 2007 R3 and Forefront® Endpoint Protection (FEP) infrastructure.

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 System Center Configuration Manager 2007 R3 and Forefront Endpoint Protection Guide

This guide leads the reader through the process of planning a System Center Configuration Manager infrastructure and optionally a Forefront Endpoint Protection (FEP) infrastructure. This guide presents both of these products together, as FEP requires an operational Configuration Manager infrastructure as its operational foundation. The guide addresses the following fundamental decisions and tasks:

* Identifying which Configuration Manager and FEP capabilities will be needed.
* Designing the components, layout, security, and connectivity of the Configuration Manager infrastructure.
* Designing the components and the dependencies that FEP requires.

Business objectives should be prioritized at the start of the project so that they are clearly understood and agreed on by IT and business managers.

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

The guide addresses the scenarios most likely to be encountered by someone designing a Configuration Manager infrastructure, with or without FEP functionality. An existing Configuration Manager infrastructure may be used in lieu of designing one specifically for FEP, as long as it supports the FEP design outlined in this guide.

Customers should consider having their architecture reviewed by Microsoft Customer Service and Support prior to implementation because that organization is best able to comment on the supportability of a particular design.

## What’s New in System Center Configuration Manager 2007 R3 and Forefront Endpoint Protection

This guide has been revised to include these new enhancements in Configuration Manager 2007 R3 that may affect the infrastructure choices and design:

* **Enhanced scalability and performance.** Increased number of supported clients to 100,000 per primary site and 300,000 per entire hierarchy.
* **Power management.** Provides a set of tools that enable the site administrator to configure standard Windows® power settings across computers.
* Operating system deployment improvements. Provides prestaging of boot images and Windows Imaging Format (.wim) files on new computers, enabling the administrator to apply a task sequence to the device that can use the prestaged media.
* Dynamic collection evaluation. Enables rapid evaluation of a collection membership by adding only newly discovered resources.
* Active Directory Delta Discovery. Performs an intermediate discovery cycle that adds only new resources to the Configuration Manager 2007 database.
* Simplified resource management. Enables searching for and adding resources to a specified collection.
* Desired configuration management. Enables creation of a collection of compliant or noncompliant computers in desired configuration management.

In addition, this guide contains new material about designing a Forefront Endpoint Protection infrastructure. FEP uses Configuration Manager’s capabilities to perform tasks such as deploying antimalware clients, enforcing security policies on endpoints, managing devices, and alerting administrators to events related to FEP.

## Assumptions

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

* The design being created is for Configuration Manager 2007 R3 and/or Forefront Endpoint Protection.
* Active Directory® Domain System (AD DS) is already designed. For assistance in designing AD DS, 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>.

## System Center Configuration Manager 2007 R3 and Forefront Endpoint Protection Design Process

This guide addresses the following decisions and activities that must occur in planning the design for a functional infrastructure. The seven steps that follow represent the most critical design elements in a well-planned Configuration Manager and Forefront Endpoint Protection design:

* Step 1: Define the Project Scope
* Step 2: Determine Which Roles Will Be Deployed
* Step 3: Determine the Number of Sites Required
* Step 4: Design the Sites
* Step 5: Determine the Number of Hierarchies Required
* Step 6: Design Each Hierarchy
* Step 7: Design the Forefront Endpoint Protection Integration

Figure 1 provides a graphic overview of the steps involved in designing a Configuration Manager infrastructure.



Figure 1. The Configuration Manager and Forefront Endpoint Protection infrastructure decision flow

Figure 2 is a graphical representation of one Configuration Manager and FEP implementation. Note that the figure does not provide a comprehensive view of all possible options; rather, it is a single representation that shows the architectural items that must be considered for each Configuration Manager and FEP design.



Figure 2. Example Configuration Manager and FEP architecture

The components can be designed in many ways. Figure 2 shows the components in one implementation for illustrative purposes only.

A Configuration Manager instance can include three types of sites:

* Central site. There is one central site, which is the top of the site hierarchy. If there is only one site in the hierarchy, that site is both a central site and a primary site. This site requires a site server and a site database.
* Primary sites. These sites report up to either the central site or another primary site; there can be an unlimited number of tiers of primary sites. Each primary site requires a site server and a site database.
* Secondary sites. Each secondary site reports up to one primary site. A secondary site requires a site server but not a database.

A FEP instance can be integrated into Configuration Manager in the following ways:

* Centralization of services. All FEP services exist in a single location: the central primary site. This allows for management of all FEP resources in a single place.
* Decentralization of services. FEP services exist in each individual child primary site. This provides distributed management that is delegated at the child primary site level. FEP reporting is also done at the child primary site level, with only that subset of devices available to reports.
* A combination of both. FEP services are distributed across central primary and child sites. This provides a finer level of manageability while also providing a roll-up reporting view of all FEP resources.

## Applicable Scenarios

This guide addresses the planning and design decisions involved in creating a successful infrastructure. It is written to address the needs of the following groups:

* Organizations with no configuration management solution that want to use Configuration Manager.
* Organizations that presently use another configuration management solution and are planning to move to Configuration Manager.
* Organizations with multiforest environments in which Configuration Manager will be employed to manage systems that span AD DS forest boundaries.
* Organizations that have distributed environments with systems separated by wide area network (WAN) links.
* Organizations with mobile devices, such as smart phones, that operate beyond firewalls but must be managed centrally.
* Organizations upgrading from Microsoft Systems Management Server 2003 to System Center Configuration Manager.
* Organizations that want to use Forefront Endpoint Protection.

The design of non–Microsoft System Center–integrated Forefront Endpoint Protection scenarios are described in Appendix C: “Forefront Endpoint Protection Integration Job Aid.” These scenarios include:

* The use of Microsoft System Center Operations Manager for event alerting.
* Implementing FEP without client update distribution servers.
* Client-only implementations of FEP (no monitoring or management servers).

## Out of Scope

This guide does not address the following topics:

* Multi-tenancy. Configuration Manager can be delivered as a hosted service for shared use by more than one organization.
* System Center Essentials. Microsoft System Center Essentials 2007 is a separate product that includes both software update and operations management functions. It is specifically designed for midsized businesses (up to 500 client computers and 30 servers).
* Configuration Pack development. The standard Configuration Packs provided for use with desired configuration management (DCM) on Microsoft server applications, such as Microsoft Exchange Server, can be extended. New Configuration Packs can be created for other applications, as well.
* In-place upgrade. If an organization is planning an in-place upgrade, the architectural choices will likely be significantly constrained by limitations of the existing system and its specific implementation. This guide does not attempt to address these permutations.
* Migration. If an organization is planning to install Configuration Manager as a new installation alongside an existing system, and then switch over, this guide considers that to be a new installation. This guide, however, does not address the migration from the legacy system to Configuration Manager.

# Step 1: Define the Project Scope

In Step 1, the project scope is defined to align the goals of the project with the business motivation. At this point, the decision of whether to include Forefront Endpoint Protection in the project is determined. The appropriate parts of the organization are identified for inclusion in the project. Then, one or more features are selected to meet the business goals. Configuration Manager is a powerful product with a rich feature set, and so it is important to determine which of its features to use.

The specific target machines that will become Configuration Manager clients are identified based on the project scope and the selected features. Computers that will also become FEP clients are then identified based on the same criteria. Finally, the organization’s service level expectations and future growth plans are documented to assist in the planning process. This information is used in Step 2 to determine which roles are needed.

**Note**   Items relating to FEP in this step and throughout this guide can be skipped if FEP will not be in scope for the project.

## Task 1: Determine Whether the Project Will Encompass the Entire Enterprise

Before beginning to plan and design a Configuration Manager and FEP infrastructure, an organization needs to determine which parts of its environment to include in the design, the locations containing resources that Configuration Manager will manage, the locations that FEP will protect, and the type of Configuration Manager and FEP deployments.

Configuration Manager can be deployed across the entire enterprise, to specific hub locations (a regionalized approach), or to individual satellite offices (a decentralized approach):

* **Enterprise-wide.** Deployment across the enterprise, including all corporate data centers, delivers standardization and the associated economies of scale over time. Deployment across the enterprise can maximize the return on investment (ROI) but it takes time for that return to be realized, and the risk will be increased because of the number of systems involved.
* **Regionalized (hub).** Configuration Manager can also be deployed to one or more hub locations where there are concentrations of users, computers, and/or network connectivity. This deployment provides a pilot environment to prove the process and benefits before deploying on a wider scale. Deploying to hub locations delivers standardization across a region and some economies of scale, but upfront costs are relatively high.
* **Decentralized (satellite).** A deployment to satellite locations reduces the upfront costs and risk of the project, because fewer systems will be involved. Such a deployment provides a pilot environment. Deployment to satellite locations is achieved at the risk of creating nonstandard configurations in the remote locations; this deployment may be difficult to support because of a lack of specialized staff. The ROI will also be lower.

Forefront Endpoint Protection is implemented in the Configuration Manager design based on operational requirements concerning the level at which administration and reporting are managed. The possible deployment options are:

* **Centralized.** With centralized deployments, FEP is implemented only at the highest (parent) level, which allows for the reporting of all machines in the design and requires that client management be performed at the same level. This deployment type maximizes the reach of the system but requires that all clients be managed in exactly the same way across all computers.
* **Decentralized.** In decentralized deployments, FEP is implemented at the hub (child) level. This option provides a distributed method of managing client machines but provides reporting of only a limited subset of the entire client population (only the clients in a child site).
* **Blended model.** The combination of a decentralized management deployment with a centralized reporting deployment enables granular administration with global reporting; management is distributed throughout the organization at the child level, while reporting of all FEP clients rolls up into a single database that is accessible to any person with permissions.

Determine which locations throughout the enterprise have client computers that require Configuration Manager functionality and which locations have workstations that require FEP functionality. Each location that requires FEP must also have Configuration Manager client components, as FEP client functionality is delivered through the Configuration Manager client. Locations that require only Configuration Manager functionality do not need FEP.

Then, identify the type of deployment as “enterprise,” “hub,” or “satellite.” Record this information in Table A-1 in Appendix A: “Client Population Job Aid.”

## Validating with the Business

To ensure that there is a complete understanding of how the planned infrastructure will affect the business, ask business stakeholders the following questions when deciding on which part of the infrastructure to implement Configuration Manager and/or FEP:

* **What is the primary reason for implementing** **Configuration Manager and/or FEP?** For example, the business goal may be to reduce deployment time for new applications.
* **What is the expected timeline for moving to Configuration Manager and/or FEP?** In many cases, organizations start with a limited deployment to gain expertise with the technology and test various configurations.
* **What are the expectations for growth or contraction?** Are there significant planned changes in the size or usage patterns of applications or locations?

## Task 2: Determine Which Product Capabilities This Project Will Address

This task will be used first to determine the business motivation for implementing Configuration Manager and/or FEP, and then to identify which product features will be used to deliver the functionality that the business requires.

Use the product capabilities descriptions in Table 1, and put a check mark in the Select column for each capability needed. For example, if the business goal is to automate software installation, check the boxes for Operating System Deployment, Software Distribution, and Software Updates. Then, add the client locations for each required capability based on the output of Task 1.

Table 1. Product Feature Selection

| Business goal | Capability | Description | Select | Location |
| --- | --- | --- | --- | --- |
| Automate software installation | Operating system deployment | Installs a configured operating system, even on systems that have no operating systems (bare metal) |  |  |
| Software distribution | Installs and configures software programs |  |  |
| Application Virtualization | Streams applications that have been sequenced by Microsoft Application Virtualization (App-V). |  |  |
| Software updates | Scans servers and client computers for software updates, then deploys those updates. |  |  |
| Asset inventory | Hardware inventory | Collects hardware information from business servers and client systems, such as available disk space, processor type, and operating system. |  |  |
| Software inventory | Collects software information, such as versions. |  |  |
| Asset intelligence | Recognizes Microsoft and non-Microsoft software “signatures” by checking and verifying information in a database—for example, checking executable file names. |  |  |
| Standardize configurations and compliance | Network Access Protection | Provides enforcement of software updates on client computers before they can access network resources. |  |  |
| DCM | Defines configuration standards and policies and audits standards compliance throughout the enterprise against those defined configurations. |  |  |
| Software metering | Collects and reports on software in use so that this data can be compared against licenses to ensure software license compliance. |  |  |
| Manage outside the enterprise | Internet-based client management | Enables management of clients that are beyond the organization’s firewall boundary—for example, on the Internet. |  |  |
| Mobile device management  | Mobile devices, such as phones, can run a capabilities subset, such as inventory and software distribution (cannot be managed by remote control or receive operating system deployments like desktop clients). |  |  |
| Manage machines off hours | Wake on LAN | Can power on a system, even when it is switched off, which is useful for performing software distribution or software updates during off hours. |  |  |
| Out-of-band management | Can manage systems when they are turned off, in sleep mode, in hibernation mode, or otherwise unresponsive; the managed computer must have the Intel V-Pro chip installed. |  |  |
| Take the help desk to the user | Remote control | Remotely administer client computers; useful for help desk personnel needing to troubleshoot individual user issues. |  |  |
| Antimalware protection, policy-based security management, and reporting | Forefront Endpoint Protection | Provides antimalware security for client computers and servers that can be integrated directly into System Center applications; also provides historical reporting of malware events and client status. |  |  |

The infrastructure can be designed for more roles than will be initially implemented, so plan with the future in mind. First, conduct the design process for the complete desired feature set, and then repeat the design process for each capability. Once that is done, decide how to implement an infrastructure subset to provide the first-priority capabilities. Do this with a design that can grow to deliver the final and complete set of required capabilities.

Plan to implement each desired capability one at a time to keep the project as easily manageable as possible. Doing so will require performing the following steps in the guide for each capability, as appropriate, and potentially redesigning the hierarchies and sites in each iteration.

## Task 3: Define the Client Population to Be Managed

Now that the part of the organization to be included has been selected, the next task is to define the machines (both business clients and business servers) for which Configuration Manager functions, FEP functions, or both will be deployed. This, in turn, will be used to determine the number of computers to which the Configuration Manager and FEP clients will be deployed, as well as the Configuration Manager sites’ size and the server infrastructures in them.

Assess the client population. Refer to the Microsoft TechNet articles “Configuration Manager 2007 R3 Supported Configurations,” <http://technet.microsoft.com/en-us/library/ff977062.aspx>, and “Forefront Endpoint Protection Client,” <http://technet.microsoft.com/en-us/library/gg398033.aspx>, to determine which clients Configuration Manager and Forefront Endpoint Protection, respectively, support. Then, use Table A-2 in Appendix A to record the following client population information:

* **Configuration Manager-specific.** These questions are focused on identifying the clients that Configuration Manager will manage. This must also be done for all computers that FEP will protect, as FEP requires the Configuration Manager client for management and updates:
* **Where are the client locations**? How many clients are in each location? This is used to determine site server locations and server sizing and to design the site boundaries in Step 5.
* **What are the client device types?** Different Configuration Manager capabilities are relevant to the different client types. For example, remote control cannot be used with mobile phones.
* **Are there security boundaries in the client population**? If different clients are subject to different security restrictions, they may need to be placed in sites or hierarchies that are administered separately.
* **How are the clients connected**? Are they connected via local area network (LAN), WAN, dial-up, or virtual private network (VPN)? How busy are those network links? Will clients be always connected, sometimes connected, or never connected? Obtain a network infrastructure diagram that shows client locations. This diagram will help determine the number of sites required in Step 3 and determine which site system roles to deploy in Step 4.
* **Will clients move between locations**? This answer helps determine whether site capacity needs to be planned in more than one location for roaming clients. This information will be used in Step 4 to determine the site design.
* **Forefront Endpoint Protection-specific.** These questions are focused on identifying where FEP must be deployed and are in addition to the Configuration Manager items above:
* **Which computers will require antimalware protection?** Identify which machines will receive the FEP client. This information will be used in Step 4 to design the FEP requirements of the Configuration Manager infrastructure.

**Note**Computers that need FEP also require the Configuration Manager client. Make sure that all clients identified for FEP protection have also been included in the list for Configuration Manager.

## Task 4: Determine the Organization’s Service Expectations

Determine the service expectations of business stakeholders for the solution. For example, what is the acceptable time window if critical updates need to be deployed? What are the service windows within which deployments and updates can take place? How long are computers allowed to operate with out-of-date antimalware signatures? How quickly must malware incidents be reported, and then acted upon? Must historical malware security reporting be highly available?

Validate whether the expectations are achievable; if they are not, engage with the stakeholders to ensure that they understand what can be achieved. Record the agreed-upon service expectations, if any, in Table A-3 in Appendix A so that they can be used to design the server infrastructure in Step 4 and the hierarchies in Step 6.

## Validating with the Business

Ask business stakeholders the following questions to understand any other factors that may affect the design:

* Are any acquisitions or divestitures planned in the environment in which Configuration Manager and FEP will be implemented? These could affect the size of the Configuration Manager and FEP client population and, therefore, the infrastructure sizing.
* Will any license agreements expire in the future for existing configuration management products? A requirement to replace them could increase the project’s scope and cost.

## Step Summary

In Step 1, the business motivation and the project scope were determined and a decision was reached on which Configuration Manager and Forefront Endpoint Protection capabilities to implement to deliver the required functionality.

To assist in the planning process, information was collected on the current infrastructure and future plans for growth. Finally, future environment changes that could affect infrastructure sizing were determined.

The output of Step 1 is:

* A table of selected features in Task 1. This information will be used in Step 2 to identify which server roles are required for the project.
* A table in Appendix A of deployment scope, client locations, and service expectations.

## Additional Reading

* System Center Configuration Manager 2007: <http://technet.microsoft.com/en-us/library/bb735860.aspx>
* Fundamentals of Configuration Manager 2007: <http://technet.microsoft.com/en-us/library/bb693852.aspx>
* Microsoft Security Compliance Manager: <http://technet.microsoft.com/en-us/library/cc677002.aspx>
* Microsoft Forefront Endpoint Protection 2010: <http://technet.microsoft.com/en-us/library/ff823816.aspx> .
* Forefront Endpoint Protection 2010: <http://technet.microsoft.com/en-us/library/gg412484.aspx>

# Step 2: Determine Which Roles Will Be Deployed

The capabilities selections that were made in Step 1 are the basis in Step 2 for selecting the Configuration Manager site roles and FEP components for each location. A Configuration Manager deployment includes one or more sites, and each site includes a number of roles to deliver specific functions. Forefront Endpoint Protection relies on the Configuration Manager infrastructure to deliver its antimalware capabilities. Establishing which site roles are required and where they are located determines site design and sizing, network sizing, and whether the Configuration Manager client and Forefront Endpoint Protection client will be deployed.

At the end of this step, the required roles will have been selected and documented. The site roles will be used to design the site systems and Forefront Endpoint Protection infrastructure in Step 4. This step will be repeated for each business requirement included in the design.

## Task 1: Select the Required Roles

Limit the design of the optional and function-specific roles to those necessary to deliver the business requirements determined in Step 1. Refer to the functions and locations that were selected in Step 1. In Table 2, record the locations at which each function is required, then read across to select the required roles. The selection of optional roles is covered in Step 4.

Note   The role descriptions are listed in Table 3.

This information will be used in Step 4 to determine site design and sizing.

Table 2. Capabilities vs. Configuration Manager Site System and FEP Roles

|  | Configuration Manager site system roles | FEP roles |
| --- | --- | --- |
|  | Required | Optional | Feature-specific | Required |
| Capability | Locations selectedin Step 1 | SMS provider | MP/PMP | SLP | FSP | RP | RSP | SUP/WSUS | Dist. Pt./PDP/BDP | AISP | SHV | OoBSP | PXE | SMP | Database | Reporting database |
| Operating system distribution |  | X | X |  |  |  |  |  | X |  |  |  | O\* | O\* |  |  |
| Software distribution |  | X | X |  |  |  |  |  | X |  |  |  |  |  |  |  |
| Application Virtualiza-tion |  | X |  |  |  |  |  |  | X |  |  |  |  |  |  |  |
| Software updates |  | X | X |  |  |  |  | X | X |  |  |  |  |  |  |  |
| Hardware inventory |  | X | X |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Software inventory |  | X | X |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Asset intelligence |  | X | X |  |  |  |  |  |  | X |  |  |  |  |  |  |
| Network Access Protection |  | X |  |  |  |  |  | X |  |  | X |  |  |  |  |  |
| DCM |  | X | X |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Software metering |  | X | X |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Internet-based client manage-ment |  | X | X |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Mobile device manage-ment |  | X | X |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Wake on LAN |  | X |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Out-of-band manage-ment |  | X |  |  |  |  |  |  |  |  |  | X |  |  |  |  |
| Remote control |  | X |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Forefront Endpoint Protection |  | X | X |  |  |  |  | X | X |  |  |  |  |  | X | X |

O\* = Optional; X = Required

Consult Table 3 for the role descriptions.

Table 3. Configuration Manager Site and FEP Roles with Descriptions

| **Site / FEP role** | **Description** |
| --- | --- |
| SMS Provider | The interface between the Configuration Manager console and the site database. |
| Management point (MP) | The site system role that serves as the primary point of contact between Configuration Manager clients and the Configuration Manager site server. |
| Proxy MP (PMP) | A management point residing in a secondary site that proxies most MP data between clients within that site and the primary site where they are assigned. |
| Server locator point (SLP) | A site system role that locates MPs for Configuration Manager clients. |
| Fallback status point (FSP) | A site system role that gathers state messages from clients that cannot properly complete installation, cannot assign to a Configuration Manager site, or cannot communicate securely with their assigned MP. |
| Reporting point (RP) | A site system role that hosts the Report Viewer component for web-based reporting functionality. |
| Reporting services point (RSP) | A site system role assigned to a computer running Microsoft SQL Server® Reporting Services; provides tools and resources that enable advanced report generation from the Configuration Manager console. |
| Software update point (SUP) | A site system role that is used to integrate with Windows Server® Update Services (WSUS). |
| Distribution point  | A site system role that stores package source files for deployment to clients. |
| Protected distribution point (PDP) | A Configuration Manager distribution point that has boundaries configured to prevent clients outside the boundaries from retrieving packages. |
| Branch distribution point (BDP) | A Configuration Manager site system that stores package source files and is designed to be located in a distributed location with limited network bandwidth or a limited number of clients. |
| Asset Intelligence synchronization point (AISP) | A site role used to connect to System Center Online to manage Asset Intelligence catalog information updates. |
| System Health Validator (SHV) point | Used with Network Access Protection to provide remediation. |
| Out of band service point (OoBSP) | A site system role that discovers, provisions, and manages client computers that have management controllers (Intel Active Management Technology [AMT]–based computers). |
| PXE service point (PXE) | A site system role that has been configured to respond to and initiate operating system deployments from computers whose network adapter is configured to allow PXE boot requests. |
| State migration point (SMP) | A site system role that stores user state data when a new system is built for that user. |
| Forefront Endpoint Protection database | A SQL Server database that stores Forefront Endpoint Protection–specific configuration data. |
| Forefront Endpoint Protection data warehouse | A SQL Server database that stores Forefront Endpoint Protection historical client protection status and malware activity. |

## Step Summary

In this step, the required roles were selected. Selection was based on the product capabilities that were chosen in Step 1.

The output of Step 2 is the identification of the site roles for the chosen capabilities for each location. This information will be used in Step 4 to determine site design and sizing.

## Additional Reading

* Understanding Configuration Manager Sites: <http://technet.microsoft.com/en-us/library/bb632547.aspx>.
* Understanding Configuration Manager Features: <http://technet.microsoft.com/en-us/library/bb693873.aspx>
* About Configuration Manager Site Topologies and FEP 2010: <http://technet.microsoft.com/en-us/library/gg412503.aspx>

# Step 3: Determine the Number of Sites Required

Now that the required roles have been identified, the number of sites required to host these roles is determined in Step 3. Forefront Endpoint Protection depends on the Configuration Manager site design and does not impose additional product constraints of its own that would affect the number of required Configuration Manager sites determined in this step.

## Task 1: Determine the Number of Sites

Start with one site, and then add more sites as required by any of the following:

* **Scale**. A site can include a maximum of 200,000 clients per hierarchy (increased to 300,000 with System Center Configuration Manager 2007 R3). Additionally, there is a limit per primary site of 100,000 directly assigned clients. Refer to the number of clients that were determined to be within the scope of the project; if that number exceeds these values, plan for additional sites.
* **Privacy concerns**. Details of files on the client computer that are exposed to the administrator are the same for all client computers site-wide. If some client computers require a higher level of privacy than others, a separate site may need to be created for them.
* **Internet-connected client computers**. In this case, a separate site can be placed in the perimeter network (also known as DMA, demilitarized zone, and screened subnet) so that ports do not have to be opened into the secure zone for client-to-site connections. For a list of the ports that must be open for each site connection and for site-to-site connections, see the Microsoft TechNet article “Ports Used by Configuration Manager” at <http://technet.microsoft.com/en-us/library/bb632618.aspx>.
* **AD DS forests.** All the server roles within a site must be within the same AD DS forest, with the following exceptions:
* SHV point
* SLP
* PXE service point
* Internet-based client management, which supports the following site systems installed in a separate forest to the site server: MP, distribution point, SUP, and FSP

If a server role must be implemented on a server that is in a different forest from the site server, it will be necessary to design it in a different site.

**Note**   Clients can be outside the forest boundary or in another forest.

* **Network location.** Clients that are in locations separated from the site by a slow link could require a separate site that is local to them to protect the network from overload. A link between sites can be bandwidth-throttled, but links within a site (between site systems) cannot. When a large distribution occurs on an intrasite link from a site server to a client, all of the bandwidth could be consumed, effectively excluding other traffic from that link. Avoid this problem by designing a separate local site for those clients. If clients are separated from the site by slow links, design additional local sites for those clients.
* International languages. Many organizations that operate internationally or across linguistic barriers must support multiple languages on their site systems and clients. Each localized site server supports only certain localized clients. Confirm whether the planned sites will support the localized clients by referring to the information at <http://technet.microsoft.com/en-us/library/bb680663.aspx>. If the sites will not support localized clients, design additional sites.
* **Organization.** There may be reasons for separating a group of clients into a different site, such as when a newly acquired company is being integrated or when a part of the organization is being divested.

Record the number of sites required in Appendix B: “Number of Configuration Manager Sites and Hierarchies Requirements Job Aid.” For each site, record the clients that will be included in the site. Proceed to Step 4 to design the sites.

## Step Summary

In Step 3, the number of sites required for the project was determined. It was recommended that one site be selected to begin with and more sites added only if necessary. This information will be used in Step 4 to design the sites.

## Additional Reading

* Configuration Manager Site Capacity Planning: <http://technet.microsoft.com/en-us/library/bb680869.aspx>
* Planning and Deploying Your Multilingual Site Hierarchy: <http://technet.microsoft.com/en-us/library/bb680663.aspx>
* About Configuration Manager Site Topologies and FEP 2010: <http://technet.microsoft.com/en-us/library/gg412503.aspx>

# Step 4: Design the Sites

Now that the number of sites has been determined, this step designs the site systems, including determining the number of servers to be located in each site and the form factor of those servers.

Start by referring to “Configuration Manager Site Capacity Planning” at <http://technet.microsoft.com/en-us/library/bb680869.aspx> to understand the support limits for the scale of the site servers and some of the roles. Each site will be designed within these limits. This step must be repeated for each site listed in Step 3. The sites will then be grouped into hierarchies in Step 6.

**Note**The following recommendations can be used as a baseline for Configuration Manager 2007 site system capacity planning. Actual site capacity requirements may vary from the listed recommendations depending on the specific networking environment and how Configuration Manager 2007 features are implemented. The hardware used to host Configuration Manager 2007 site systems also contributes to the performance of Configuration Manager 2007. The number of Configuration Manager 2007 component servers, number of clients installed, and the features enabled also affect server performance.

## Task 1: Plan the Required Roles

Refer to Step 2 for the site roles required. For each role, compare the number of clients that will use it against the scale limits for the role. Record the selections for each site in Appendix B.

Table 4. Required Site System Roles

|  |  |  |  |
| --- | --- | --- | --- |
| Role | Description | Scale limits | Minimum number required |
| SMS Provider | The interface between the Configuration Manager console and the site database. It cannot be installed on a clustered SQL Server database server or on the same computer as the SMS Provider for another site. | Scales to primary site capacity, which is 100,000 clients, or 300,000 clients with System Center Configuration Manager 2007 R3. | One per site. |
| MP | The primary point of contact between Configuration Manager clients and the Configuration Manager site server. It distributes policy to the clients and receives state messages, status messages, and inventory and discovery data as well as software usage data from them. | Up to 25,000 clients. | Up to 25,000 clients supported on one MP; if more clients or redundancy of MPs is required, then up to four MPs in a Network Load Balancing (NLB) cluster to support up to 100,000 clients per site. |

If the SLP role is required, design it in only one site—the site that will likely become the central site—so that it can service all the sites below it in a site hierarchy.

## Task 2: Plan the Optional Roles

Add the optional roles (see Table 5) that will be used in the site design. Record the selections for each site in Appendix B.

Table 5. Optional Site System Roles

| Role | Description | When to use the role | Scale limits | Minimum number required (if role is used) |
| --- | --- | --- | --- | --- |
| SLP | Locates management points for Configuration Manager clients. | Clients are in a workgroup or in a different forest from the site and cannot query their site assignments in AD DS. | Scales to primary site capacity, which is 100,000 clients, or 300,000 clients with System Center Configuration Manager 2007 R3. | One per hierarchy. |
| FSP | Gathers state messages from clients that cannot be installed properly, cannot be assigned to a Configuration Manager site, or cannot communicate securely with their assigned MPs. | Useful for troubleshooting, particularly at client installation. Receives communications from clients using unsecured HTTP and so represents a security exposure—may be inappropriate in Internet-based sites. | Up to 100,000 clients (or one per site). | One per site. |
| RP | Hosts the site’s reporting website. It delivers reports using data from the database to the SMS Provider interface for display in the web console. | If reports are required from Configuration Manager, which will usually be the case. | Scales to primary site capacity, which is 100,000 clients, or 300,000 clients with System Center Configuration Manager 2007 R3. | One per site. |
| RSP | A site system role assigned to a computer running SQL Server Reporting Services. It provides tools and resources that enable advanced report generation from the Configuration Manager console. | If custom reports are required, particularly for use by business users. | Scales to site capacity, which is 200,000 clients or 300,000 clients with System Center Configuration Manager 2007 R3. | One per site. |

## Task 3: Plan the Feature-Specific Roles

The remaining site system roles are feature-specific (see Table 6). Refer to Step 2 where it was determined which roles were relevant to the location. Use the information below to select the relevant roles for the site, and record the selections for each site in Appendix B.

Table 6. Feature-Specific Site System Roles

| Role | Description | Scale limits | Minimum number required |
| --- | --- | --- | --- |
| SUP | A site system role used to integrate with WSUS.  | Up to 25,000 clients when using WSUS 3.0 SP2 with another site system role.Up to 100,000 clients when using WSUS 3.0 with SP2 without other site system roles on the same server. | Up to 25,000 clients supported on one SUP. If more clients or redundancy of SUPs is required, then up to four SUPs in an NLB cluster to support up to 100,000 clients per site. |
| Distribution point | Stores package source files for deployment to clients; can also work as a streamer for App-V–sequenced applications. | Up to 100 distribution points per site; each distribution point supports up to 4,000 clients. | One for every 4,000 clients. |
| BDP | Stores package source files and is designed to be located in a distributed location with limited network bandwidth or a limited number of clients. It is able to use bandwidth throttling. It can also work as a streamer for App-V–sequenced applications. | Up to 2,000 connected to each central or primary site. Each BDP can support up to 100 clients. | One for each 100 clients in the BDP location.Note   If the BDP runs on a client operating system, only 10 Configuration Manager clients can connect to it at one time. |
| AISP | Used to synchronize with the external System Center Online Asset Intelligence catalog. | Not applicable | One per hierarchy. |
| SHV | Used with Network Access Protection to provide remediation. Note   SHV can only run on Windows Server 2008. | Up to 100,000 clients (or one per hierarchy if fewer than 100,000 clients). | One per hierarchy. |
| OoBSP | A site system role that discovers, provisions, and manages client computers that have management controllers (such as AMT-based computers). | Up to 100,000 clients. | One per site. |
| PXE service point | Initiates operating system deployments from computers whose network adapter is configured to allow Pre-Boot Execution Environment (PXE) boot requests. | Up to 100,000 clients per PXE service point. Up to 10 PXE service points per site, with a maximum of 75 PXE service points per primary site database. | One per site. |
| SMP | Stores user state data when a new system is built for that user. | Up to 100,000 clients. | One per site. |
| Forefront Endpoint Protection database | Auxiliary database used by Forefront Endpoint Protection; contains the last reporting date and time for each Forefront Endpoint Protection client and is used to populate the Forefront Endpoint Protection data warehouse. Must be in the same SQL Server instance as the Configuration Manager site database. | Scales to site capacity, which is 200,000 clients or 300,000 clients with System Center Configuration Manager 2007 R3. | One per site. |
| Forefront Endpoint Protection reporting database | Holds historical reports on client malware activity and client protection status. | Up to 200,000 clients, 300,000 with System Center Configuration Manager 2007 R3. Historical data aging bounded by SQL Server capacity limits. | One per hierarchy. |

## Task 4: Determine Where to Place Hierarchy Roles

If any of the following roles are required, design each of them in only one site in the hierarchy:

* The Asset Intelligence service point should be designed in a site that enables it to connect with the external System Center Online database.
* The SHV point should be designed in a site that allows it to run on Windows Server 2008.
* The SUP role should be designed so that it can access the Internet to synchronize with WSUS.

## Task 5: Determine Where to Place Primary and Secondary Sites and Branch Distribution Points

Sites can be primary or secondary or, if the business requirement is to automate software installation, a BDP could be used to represent a package distribution site. The intrasite link to a BDP can be bandwidth-throttled and, for that reason, is treated here as a separate site. No other intrasite links can be bandwidth-throttled.

A primary site can include all of the available roles. It requires a site server and a site database.

**Important**   Forefront Endpoint Protection can only be implemented in primary and central sites; secondary sites are not supported.

A secondary site can include only a subset of the roles: DPs, SUPs, PMPs, and clients. Each secondary site requires a site server, but it does not have a database. A secondary site reports up to a primary site and is always a child site; it cannot have children. There can be up to 500 secondary sites per primary site. Each secondary site can have a distribution point that supports 4,000 clients; however, performance may vary depending on the size of the packages.

A BDP is a Configuration Manager site system that can be installed on a client computer to store package source files. It is part of a central primary or secondary site. There can be up to 2,000 BDPs per site, each supporting 100 clients. But if the BDP runs on a client operating system, only 10 clients can connect to it at any one time. Note that the BDP, like all site systems, must be within the AD DS trust boundary.

Refer to the business requirements that were determined in Step 1 and to the required roles that were determined in Step 2. If the requirement is for automated software installation using package source files that will be delivered over the network, weigh the characteristics above to determine whether to design a primary site, a secondary site, or a BDP in the location. If the requirement was for a different Configuration Manager function, primary sites will be required**.**

## Task 6: Determine Whether Native Mode Is Required

A Configuration Manager site can operate in either native mode or mixed mode. It is important to determine whether native mode is required, because a native mode site cannot report up to a mixed mode site in a site hierarchy, so another hierarchy might need to be added to the design. Alternatively, all the sites above this one in the hierarchy must be converted to native mode.

Forefront Endpoint Protection is site mode-neutral. It can be implemented in either mixed or native mode site hierarchies.

### Option 1: Native Mode

In native mode, trust is established between clients and servers by exchanging certificates using a public key infrastructure (PKI) for authentication. The PKI can be complex to set up and maintain, but it enables secure management of devices outside the enterprise, such as smart phones.

#### Benefits

The benefits of deploying a Configuration Manager hierarchy in native mode are:

* Higher level of security by integrating with a PKI to help protect client-to-server communication.
* Enables the management of clients that are connected to the Internet, such as portable computers used by mobile workers, computers used from an employee’s home, and smart phones.

#### Challenges

The limitations of deploying Configuration Manager sites in native mode are:

* A PKI is required.
* It is estimated that native mode site operations are 10–15 percent slower in overall performance compared to sites configured to operate in mixed mode because of the added load of encryption and signing.
* Cannot interoperate with Systems Management Server 2003.
* All parent locations up to and including the central site must be in native mode.

### Option 2: Mixed Mode

In mixed mode, a trust relationship exists between clients and servers. Mixed mode enables integration of devices that will not be upgraded from the Systems Management Server 2003 client. It is also easier to set up, but it does not offer secure communications beyond the trust boundary.

#### Benefit

The benefit of deploying a Configuration Manager hierarchy in mixed mode is that it enables integration with Systems Management Server 2003 infrastructure.

#### Challenge

The limitation of deploying Configuration Manager sites in mixed mode is that clients on the Internet are not supported. If native mode is required, a PKI must be in place because native mode must use a PKI as part of the authentication process. If a PKI is not in place, it will need to be designed. In that case, determine whether the effort required to design and implement the PKI will be justified for the native mode requirements of the Configuration Manager project.

Review the benefits and limitations of native mode compared to mixed mode to decide whether the use of native mode is required. Record the mode for each site in Appendix B. Repeat this step for the next Configuration Manager hierarchy.

## Task 7: Assign Clients to Sites

Now that the site hierarchy and site locations have been decided, clients must be assigned to the primary sites. Note that clients cannot be assigned to secondary sites; secondary sites are used only to store content and (if a PMP is in place) to store policy. This is done by defining the site boundaries to include the appropriate clients, making sure to avoid any ambiguity about which site a client is in. When a client is placed within the boundary of a secondary site, it will report up to the parent primary site. Site boundaries can be defined using the following criteria, either alone or in combination:

* **Internet Protocol (IP) subnets**. Enable granularity in designing Configuration Manager sites, which can span AD DS sites.
* **AD DS site names.** Enable a logical site to be created from a number of physical network segments. However, it does create a dependency on AD DS administration.
* **IP version 6 (IPv6) prefix.** Using IPv6 prefixes provides granularity in administration over a large address range, but it may create a significant administrative burden. IP version 4 (IPv4)-only systems cannot communicate directly with IPv6-based computers and may require IP translation, such as Network Address Translation, to communicate.
* **IP address range.** IP address ranges are most useful for clients that access Remote Access Service (RAS) or VPN servers. Because clients connecting to RAS and VPN servers typically have an IP subnet mask of 255.255.255.255, every address is equivalent to a subnet.

FEP clients depend on the Configuration Manager client for policy updates, management tasks, and software distribution and therefore have the same site requirements. FEP clients respond in the same manner as Configuration Manager clients to changes in the network and have the same site-based operational constraints.

Decide how to implement site boundaries, and then assign the clients to their respective sites. Record the decision for each site in Appendix B.

## Task 8: Design the Boundaries of Protected Distribution Point Systems

A distribution point can be protected to limit the load on the server and content acquisition by clients. This is done by restricting access to that distribution point to only certain clients within a site. A special boundary is set up for the protected distribution point within the site boundary. Review the site boundaries that were designed in the previous task to determine whether a distribution point must be protected and, if so, design additional distribution points in the next task to service the site clients that will be beyond its boundaries.

Where client populations within a site are separated by lower-speed WAN links, it may appear attractive to design a protected distribution point in each of the separated populations to service just that population. This has the advantage that the protected distribution point is local to its clients, but such distribution points must themselves be populated with packages, which would then flow across the WAN links within the site. Because it is not possible to throttle the bandwidth on intrasite links, a better design would be to place each of these groups of clients in a separate site, as described in
Step 3.

FEP relies on Configuration Manager’s DPs for storage of antimalware software definition updates, which should be taken into account when planning DPs.

## Task 9: Design the Site Systems

Now that the demand on the required roles has been determined, the roles can be mapped onto one or more site servers. Working within the support limits shown above, start by reviewing the product group’s recommendations so that these can be applied to the design as appropriate.

### Product Group Recommendations

There is no architectural guidance available for designing the site systems, so the Configuration Manager product group recommendations for site infrastructure design are provided here:

* For site servers that manage a large number of assigned clients, use an eight-core computer with the fastest possible CPU and 16 gigabytes (GB) of memory.
* Configuration Manager is a 32-bit application, and 64-bit hardware does not deliver additional benefits.
* Configuration Manager has been designed to effectively maximize overall CPU processing. It is not unusual to see 85 percent or greater CPU usage on Configuration Manager site servers.
* The use of virtual computer site systems for Configuration Manager sites that must process a large amount of data is not recommended.
* Use separate storage volumes on the site server for:
* Operating system
* Configuration Manager installation directory
* Site and site database backup storage
* Volume Shadow Copy Service storage association for shadow copy temporary storage of the site and site database backup snapshots
* Separate the site server and the site server database roles onto different computers.
* Use separate storage volumes on the site server for:
* The SQL Server tempdb database
* SQL Server database logs
* SQL Server database
* For best performance, the SQL Server tempdb database should be divided into a number of files corresponding to half the number of processors installed on the SQL Server-based computer. When the tempdb SQL Server database is installed using only one file, collisions with multiple processors might occur.
* If the MP has been set up in an NLB configuration, it should be configured to access a replicated site database hosted by a different SQL Server instance than the actual site database. Using NLB site systems to access a replicated SQL Server site database reduces the load on the site database and improves site performance. If the default management point is configured as an NLB and configured to access the site database directly, it will cause degraded site server performance.
* All the roles can co-exist on the site server, but that may not be the best design. The FSP role always uses unauthenticated HTTP in clear text to communicate with clients, even if the site is in native mode. For this reason, the FSP role represents a security exposure. The Configuration Manager product group recommends that if used, it should be hosted on a separate server that does not host any other roles to reduce the potential attack surface.

It also makes sense to separate the fallback status point from the MP. Clients contact the FSP if they are unable to contact the MP. When both roles are on the same server, failure of that server may orphan the client without recording any troubleshooting data.

The Forefront Endpoint Protection product group states that, when integrated into a Configuration Manager design, FEP components do not significantly add to the server capacity and performance requirements of Configuration Manager, and no additional planning is required.

Details of the implementation on which these recommendations are based are available in the following performance white papers:

* “System Center Configuration Manager 2007: Sample Configurations and Common Performance Related Questions,” available at <http://download.microsoft.com/download/4/b/9/4b97e9b7-7056-41ae-8fc8-dd87bc477b54/Sample%20Configurations%20and%20Common%20Performance%20Related%20Questions.pdf>
* “Configuring Configuration Manager Sites for Best Performance,” available at <http://technet.microsoft.com/en-us/library/bb892809.aspx>
* FEP “Performance and Scalability,” available at <http://technet.microsoft.com/en-us/library/gg710930.aspx>

### Size and Place the Site Server

The site server defines the site. It is the first server that is instantiated in the site and may be the only server in the site. If all the required roles will be hosted on the site server, proceed to the next section to design the form factor of the server. If some of the roles will be offloaded onto different servers within the site, add those to the site design and proceed to design the form factor for those servers. Because no architecture guidance is available on the performance characteristics of each role, proceed with caution and ideally set up a test environment in which the performance of the site can be modeled.

### Form Factor

The System Center Configuration Manager product group has completed performance testing for a number of sample configurations. The results are available at <http://download.microsoft.com/download/4/b/9/4b97e9b7-7056-41ae-8fc8-dd87bc477b54/Sample%20Configurations%20and%20Common%20Performance%20Related%20Questions.pdf>.

However, many variables can affect the required size of the server and its performance, including options to throttle the rate at which packages are distributed to clients and the rate at which inventory information is collected from the clients. In the absence of architectural guidance, proceed with caution, selecting a form factor that is initially small and can grow. If possible, set up a test environment on a small scale to model the site’s behavior in the production environment. If System Center Operations Manager is available, use the Management Pack for System Center Configuration Manager to monitor the performance of this test environment. Then, deploy on an increasingly larger scale and measure, learn, and adjust at each deployment.

## Task 10: Determine the Fault-Tolerance Approach

Refer to the requirements for availability and performance that were determined in Step 1. Performance is important here, just on a different scale, because response time can be measured in days. Use these requirements to first determine whether fault tolerance is required at all and, if so, what level of fault tolerance should be planned.

The following fault-tolerance options are available within sites:

* The SQL Server database can be clustered.
* Management points can use NLB.
* The SUP can use NLB, with either an active or non-active (warm spare) SUP.
* WSUS can use NLB.

Availability in FEP relies on the fault-tolerance design of Configuration Manager; if the FEP architecture requires high availability, Configuration Manager must be designed to provide fault tolerance. In addition, the only fault-tolerance option supported for the Forefront Endpoint Protection reporting database is SQL Server failover clusters.

Record the roles for which fault tolerance will be used in Appendix B.

## Step Summary

In Step 4, the sites were designed. The output of Step 4 is:

* The required roles were designed and placed in primary and secondary sites.
* The optional and feature-specific roles were designed and placed.
* A determination was made about where to place hierarchy roles.
* A determination was made for each site’s security mode.
* The site boundaries were designed to assign clients to their sites.
* The boundaries of protected distribution point systems were designed.
* The site systems were then designed.
* The fault-tolerance approach was determined.

This step must be repeated for each site required. This information will be used in Step 5 to determine the number of hierarchies.

## Additional Reading

* Configuration Manager 2007 R3 Supported Configurations: <http://technet.microsoft.com/en-us/library/ff977062.aspx>
* Configuration Manager Site Capacity Planning: <http://technet.microsoft.com/en-us/library/bb680869.aspx>
* Configuring Configuration Manager Sites for Best Performance: <http://technet.microsoft.com/en-us/library/bb892809.aspx>
* Performance Configuration Recommendations: <http://technet.microsoft.com/en-us/bb932186.aspx>
* Best Practices for Central and Primary Site Hardware and Software Configuration: <http://technet.microsoft.com/en-us/bb932180.aspx>
* Troubleshooting Configuration Manager Performance: <http://technet.microsoft.com/en-us/bb932206.aspx>
* System Center Configuration Manager 2007: Sample Configurations and Common Performance Related Questions: <http://download.microsoft.com/download/4/b/9/4b97e9b7-7056-41ae-8fc8-dd87bc477b54/Sample%20Configurations%20and%20Common%20Performance%20Related%20Questions.pdf>
* Understanding Mobile Device Management: <http://technet.microsoft.com/en-us/library/bb632613.aspx>
* Performance Considerations When Designing Configuration Manager Sites: <http://technet.microsoft.com/en-us/library/bb932210.aspx>
* Expected Server Resource Usage for Configuration Manager Sites: <http://technet.microsoft.com/en-us/bb932128.aspx>
* Determine Whether a Proxy Management Point is Needed at a Secondary Site: <http://technet.microsoft.com/en-us/library/bb693472.aspx>
* Determine If You Should Install a Fallback Status Point for Configuration Manager Clients: <http://technet.microsoft.com/en-us/library/bb632756.aspx>
* Understanding Configuration Manager Sites: <http://technet.microsoft.com/en-us/library/bb632547.aspx>
* Configuration Manager Site Capacity Planning: <http://technet.microsoft.com/en-us/library/bb680869.aspx>
* Choose Configuration Manager Boundaries: <http://technet.microsoft.com/en-us/library/bb633084.aspx>
* Choose between Native Mode and Mixed Mode: <http://technet.microsoft.com/en-us/library/bb632431.aspx>
* FAQs for Branch Distribution Points: <http://blogs.technet.com/wemd_ua_-_sms_writing_team/archive/2008/07/27/faqs-for-branch-distribution-points.aspx>
* Deploying by Using Configuration Manager Packages: <http://technet.microsoft.com/en-us/library/ff823885.aspx>
* Forefront Endpoint Protection 2010: <http://technet.microsoft.com/en-us/library/gg412484.aspx>
* About Configuration Manager Site Topologies and FEP 2010: <http://technet.microsoft.com/en-us/library/gg412503.aspx>
* Client Deployment: <http://technet.microsoft.com/en-us/library/ff823762.aspx>
* Assigning a Policy to Endpoint Computers: <http://technet.microsoft.com/en-us/library/ff823839.aspx>
* Performance and Scalability: <http://technet.microsoft.com/en-us/library/gg710930.aspx>

# Step 5: Determine the Number of Hierarchies Required

A Configuration Manager hierarchy consists of a central site and, optionally, one or more primary and secondary sites. A hierarchy also includes all the clients within the boundaries of those sites. In this step, the number of hierarchies is determined so that the required sites can be placed into the appropriate hierarchies in Step 6.

## Task 1: Determine the Number of Hierarchies

Start with one hierarchy and add more hierarchies only if necessary. Additional hierarchies could be required in the following scenarios:

* **Size**. The maximum size of a Configuration Manager hierarchy is 200,000 clients, or 300,000 clients with System Center Configuration Manager 2007 R3. Refer to Step 1, where the number of clients included in the scope of the project was determined. Compare the number of clients with the scale limit. Add more hierarchies if the limit is exceeded.
* **Central site is mixed mode, and native mode is required**. When the central site will be mixed mode, perhaps because a PKI cannot easily be implemented there but one or more native mode sites are required, an additional Configuration Manager hierarchy will be required. A native mode site cannot report up to a mixed mode site. Remember that native mode is a requirement for Internet-based client management.
* **Isolated networks**. Networks in which clients need to be managed but cannot be connected to any of the planned sites will require an additional Configuration Manager hierarchy. For example, when a client is on an isolated lab network and requires software updates, an additional hierarchy is required. Examine each location that is in scope for the project to identify any isolated networks there.
* **Politics**. Different groups within the organization might each require their own hierarchies. For each location, record any requirement for a separate hierarchy driven by political considerations.
* **Regulatory requirements**. Regulatory requirements can require total separation of an environment from other environments. Examine each location and record any regulatory requirements that will require the design of additional hierarchies.

Record the hierarchies required in Appendix B.

## Step Summary

This step explained that a Configuration Manager hierarchy consists of a central site and, optionally, one or more primary and secondary sites, and that a hierarchy also includes all the clients within the boundaries of those sites. The scenarios that require more than one hierarchy were listed.

The output of Step 5 is the number of Configuration Manager hierarchies required for this project, recorded in Appendix B.

This information will be used in Step 6 to design each site hierarchy.

# Step 6: Design Each Hierarchy

In Step 5, the number of hierarchies was determined. Configuration Manager has three types of sites: central, primary, and secondary. A primary site reports up to a central site or another primary site; if secondary sites are required, they will report up to a primary site or the central site.

In this step, the site hierarchy is designed. There are no published limits to the number of sites that can be in one hierarchy. Refer to Figure 1 earlier in this guide to see one possible site hierarchy implementation.

## Task 1: Determine Where to Place the Central Site

If there is only one site in the hierarchy, it is a central site. A central site requires a site server and a site database. It replicates much of the data from the primary sites that are below it. Place the central site in the location where the best administrative skills and network connections are available.

When there are more than 100,000 clients in the hierarchy, the Configuration Manager product group recommends that clients not be assigned to the central site. Assign them instead to primary or secondary sites so that the central site can provide better performance for centralized administration as well as rollup and reporting of inventory, status, and compliance data.

## Task 2: Plan the Site Hierarchy

All the sites have been defined, along with their locations. Next, the site connections must be designed within the hierarchy. The hierarchy can be deep or wide. Try to limit the depth of the hierarchy to as few tiers as possible because each parent site will hold a replica of much of the data in the databases for all its children. In a deep hierarchy with grandchildren or even great-grandchildren, this will create significant duplication of data in databases that are likely already under heavy load. Record the relationships between sites in the hierarchy in Appendix B.

## Step Summary

In this step, each hierarchy was designed. The location of the central site was determined, and the remaining sites were connected to each other. Repeat this entire step for each hierarchy.

# Step 7: Design the Forefront Endpoint Protection Integration

In previous steps, the complete Configuration Manager hierarchical site structure that supports the organization’s business objectives was designed. This structure includes the placement of services and servers across sites that were identified as being in scope for the project.

This step is only required if it was determined that FEP will be implemented.

In this step, FEP is integrated into the design by mapping the required FEP components to each Configuration Manager site hierarchy. FEP instances are tied to hierarchies, and only one FEP instance can be implemented per hierarchy. The result will be a fully functional FEP design tailored to the Configuration Manager infrastructure for the project.

This step must be performed once per Configuration Manager hierarchy.

## Task 1: Determine Forefront Endpoint Protection Management and Reporting Design

Determining the placement of the Forefront Endpoint Protection database components based on management and reporting requirements is the focus of this task. Each FEP instance requires that FEP management extensions be implemented into Configuration Manager site servers along with two databases: the FEP database, which supports the FEP management services by storing near-term data on the last time each endpoint client reported into the system, and the FEP Reporting database, which contains a historical record of all endpoint client events. FEP databases cannot be federated or consolidated.

Placement of the FEP components into the Configuration Manager hierarchy will determine the FEP management and reporting boundaries. Centralization of all tasks is possible by implementing FEP at the highest level (primary parent site), while the distribution of tasks is achieved by deploying FEP throughout the child sites. A hybrid model is possible that supports centralized reporting and distributed administration.

Two distinct types of management tasks are available: policy control and administration. These can be implemented individually at the level required of the specific function.

Reporting services is independent of the management functionality and can thus also be deployed at the level that meets the business requirements on the reporting services. For example, FEP reporting can be implemented for a centralized view of all resources in the FEP instance while management tasks are distributed at a team level.

Table 7 describes each possible deployment type and the level at which management and reporting tasks will be possible under the deployment. Table 8 further describes the effects of centralization and decentralization in relation to what specific tasks will be possible under each type. These tables should be used with the business functionality requirements that were identified in Step 1 and recorded in Table A-1 in Appendix A to determine which centralization model should be used for the project.

Table 7. FEP Centralization Model–Based Levels of Control

|  |  |
| --- | --- |
|  | Level of control |
| Deployment type | Policies | Administration | Reporting |
| FEP deployed in primary parent site only | C | C | C |
| FEP deployed in parent site and child sites | C | D | D |
| FEP deployed in child sites only | D | D | D |
| FEP deployed in child sites only, with FEP reporting deployed in primary parent site | D | D | C |

C = centralized, D = decentralized

Table 8. FEP Tasks Allowed Based on Managed Client Connection

|  |  |  |
| --- | --- | --- |
|  | Clients connected to parent site | Clients connected to child sites |
| Policy/admin model | C/C | C/D | D/D | D/C | C/C | C/D | D/D | D/C |
| Task |  |  |  |  |  |  |  |  |
| Deploy FEP clients to collections | Y | Y | N | N | Y | Y | Y | Y |
| Create or modify FEP policies | Y | Y | N | N | N | N | Y | Y |
| Assign FEP policies to collections | Y | Y | N | N | Y | Y | Y | Y |
| Monitor FEP client deployment and policy deployment progress | Y | Y | N | N | L | Y | Y | Y |
| Monitor FEP via the FEP dashboard | Y | Y | N | N | N | Y | Y | Y |
| FEP reporting | Y | Y | N | Y | N | Y | Y | Y |
| Configure FEP alerts | Y | Y | N | Y | N | Y | Y | Y |
| FEP Operations | Y | Y | N | N | L | Y | Y | Y |
| Centralized Reporting | N | N | N | Y | N | N | N | Y |

C = centralized, D = decentralized, L = limited support

Record the FEP centralization model and placement of FEP components in Configuration Manager sites in Table C-1 in Appendix C.

## Task 2: Determine SQL Server Requirements

Determining the requirements of the SQL Server instances that host the FEP databases is the focus of this task. Microsoft SQL Server 2005 Standard or Enterprise Edition with SP3 (x86 or x64), Microsoft SQL Server 2008 Standard or Enterprise (x86 or x64), or Microsoft SQL Server 2008 R2 Standard or Enterprise (x86 or x64) is required for hosting the Forefront Endpoint Protection databases. The *Infrastructure Planning and Design Guide for Microsoft SQL Server 2008 and SQL Server 2008 R2* at <http://go.microsoft.com/fwlink/?LinkId=160982> may assist in the design of the SQL Server instances.

Each FEP instance must have a minimum of one SQL Server instance that can host these databases. A single SQL Server computer can host multiple SQL Server instances if needed. More instances and servers can be added for isolation, performance, scalability, and fault tolerance. The FEP database must reside on the same SQL Server instance as the Configuration Manager site database.

The Forefront Endpoint Protection reporting database can be implemented on any available instance of SQL Server that meets the capacity and performance requirements of the database and does not need to be in the same instance that hosts the site database or other FEP components. SQL Server Analysis Services (SSAS), SQL Server Integration Services (SSIS), and SQL Server Reporting Services (SSRS) are required on the server that hosts the FEP Reporting database.

The Forefront Endpoint Protection product group has no prescriptive guidance on capacity and performance planning for the FEP Reporting database. There is, however, a limited amount of storage estimation planning information available in the “FEP 2010 Datawarehouse Space Capacity Planner” worksheet found at <http://go.microsoft.com/fwlink/?LinkId=210853>.

Record the SQL Server name and instance for each FEP site database and reporting database in Table C-2 in Appendix C.

## Task 3: Determine the Fault-Tolerance Approach

Refer to the requirements for availability and performance that were determined in Step 1, and determine the correct fault-tolerance approach to take to meet the stated business requirements. Fault tolerance for the Configuration Manager infrastructure was designed in Step 4, with the exception of the FEP Reporting database. The reporting database is stored inside a SQL Server data warehouse. FEP supports all SQL Server–supported methods of providing fault tolerance.

If this instance of FEP requires high availability, the SQL Server instance that hosts the reporting database as well as the dependent SQL Server data warehouse services (SSIS, SSRS, SSAS) must be made fault tolerant. See Step 3, Task 4 of the *Infrastructure Planning and Design Guide for Microsoft SQL Server 2008 and SQL Server 2008 R2* for help on determining the right fault-tolerance mechanism.

## Step Summary

In this step, the type of FEP deployment and a list of the Configuration Manager sites requiring FEP components were determined. The location of each FEP site and reporting database was determined. This information was recorded in Tables C-1 and C-2 in Appendix C. Repeat this entire step once for each hierarchy.

## Additional Reading

* Infrastructure Planning and Design (IPD) Guide for Microsoft SQL Server 2008 and SQL Server 2008 R2: <http://go.microsoft.com/fwlink/?LinkId=160982>
* About Configuration Manager Site Topologies and FEP 2010: <http://technet.microsoft.com/en-us/library/gg412503.aspx>

# Conclusion

This guide has summarized the critical design decisions, activities, and tasks required to enable a successful design of System Center Configuration Manager and Forefront Endpoint Protection. It focused on decisions involving:

* Which Configuration Manager and FEP roles will be required.
* The server roles, role placement, databases, and connectivity of the Configuration Manager and FEP infrastructure.
* The number of Configuration Manager hierarchies required, and how many sites are required within each hierarchy.
* The integration of FEP through the process of mapping FEP components into the Configuration Manager hierarchies.

This process was accomplished by leading the reader through the seven steps in the decision flow to arrive at a successful design. Where appropriate, the decisions and tasks have been illustrated with typical usage scenarios.

As stated in the introduction, it is important at the start of a Configuration Manager or Forefront Endpoint Protection project to have a full understanding of the business objectives for the project by answering the following questions:

* What benefits does the business expect to achieve through the use of Configuration Manager and FEP?
* What is the value of those benefits and, therefore, the cost case for using Configuration Manager and FEP to deliver those benefits?

The business objectives should be prioritized at the start of the project so that they are clearly understood and agreed upon between IT and the business. When an architecture has been drafted, limited pilot tests should be conducted before a major rollout begins so that lessons learned can be incorporated into the design.

This guide, when used in conjunction with product documentation, allows organizations to confidently plan the implementation of Configuration Manager and Forefront Endpoint Protection.

# Appendix A: Client Population Job Aid

Use Table A-1 to record the parts of the organization that are in scope for the project.

Table A-1. Deployment Scope

|  |  |  |  |
| --- | --- | --- | --- |
| Entire enterprise, hub, or satellite? | Is FEP in scope? | List hub or satellite sites | List sites that require FEP |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Use Table A-2 to record the connection characteristics of clients that are in scope for the project.

Table A-2. Client Population Assessment

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Client location | Device type | Security bound-ary | Connec-tion type (LAN/ WAN dial-up/ VPN) | Always connect-ed | Some-times connect-ed | Never connect-ed | FEP required? |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

Use Table A-3 to record stakeholders’ expectations of the service levels to be delivered by the infrastructure.

Table A-3. Service Expectations

|  |  |  |
| --- | --- | --- |
| Stakeholder | Function | Agreed-on service expectation |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Use Table A-4 to record the FEP integration with Configuration Manager requirements.

Table A-4. FEP Integration with System Center Configuration Manager Requirements

|  |  |  |
| --- | --- | --- |
| Database | Location in the Configuration Manager hierarchy | Fault-tolerance requirements |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Appendix B: Number of Configuration Manager Sites and Hierarchies Requirements Job Aid

Use a table such as Table B-1 to design each required hierarchy.

Table B-1. Required Sites and Hierarchies

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Site | Reason required | Site mode | Roles and whether fault tolerant | Boundary type | Clients | Hierarchy | Reason required |
|  |  |  |  |  |  |  |  |
|  |
|  |
|  |
|  |
|  |
|  |  |  |  |  |  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# Appendix C: Forefront Endpoint Protection Integration Job Aid

Use Table C-1 to record the component locations required for FEP integration with the Configuration Manager site design.

Table C-1. FEP Mapping to System Center Configuration Manager Sites

|  |  |  |
| --- | --- | --- |
| FEP deployment type | Configuration Manager sites where FEP will be deployed | Configuration Manager sites where FEP reporting will be deployed |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Use Table C-2 to record the placement of the FEP site and reporting databases in the Configuration Manager site design.

Table C-2. FEP Database Placement

|  |  |  |
| --- | --- | --- |
| FEP database (site/reporting) | SQL Server instance name | SQL Server instance |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Appendix D: Forefront Endpoint Protection Fringe Scenarios

This guide presents the most commonly used FEP deployment scenarios, which involve a tight integration with Configuration Manager. Other types of deployment scenarios are possible, including options that allow for the deployment of FEP without a Configuration Manager infrastructure. These are described in limited detail here.

* **The use of WSUS to manage FEP clients.** It is possible to use FEP without implementing Configuration Manager by using WSUS alone. This method provides an automatic updating of the client software but does not provide any management, monitoring, or reporting functionality. In addition, in this scenario, all FEP clients must initially be installed manually.
* **FEP policies managed through Group Policy settings.** In this scenario, AD DS group policies are used to manage the FEP client policies. These policies can be used either in place of or in addition to FEP’s standard client policy management, which is done through Configuration Manager. This option only provides management of FEP policy settings that are exposed in Group Policy. Caution should be used when using both methods, as results are unpredictable—particularly when settings conflict between the two sets of settings.
* **Unmanaged FEP clients.** In this scenario, all clients are installed manually and definition updates retrieved directly from the Microsoft repository or an internal file share. There is no centralized collection of FEP client events, no centralized management of FEP settings, and no centralized reporting. All management and changes to the installed client must be performed manually for each machine on which FEP is used.
* **FEP client installation and use on servers.** The FEP client can be implemented on a computer running a Windows Server operating system to provide the same endpoint security as traditional client computers. Servers have different operational metrics and are typically managed differently than client computers; therefore, planning and design for this scenario is not provided.
* **The use of System Center Operations Manager for monitoring.** System Center Operations Manager is typically used to monitor high-valued assets (such as servers) and not client computers, as each monitored device requires a dedicated Operations Manager agent and software license. Operations Manager can, however, be used in addition to or as a replacement for Configuration Manager for monitoring FEP clients in the organization. Although the FEP management interface provides a concise, detailed view of all endpoint security items, the results are not returned in real time: there is a 15-minute or greater delay in the data reported. In contrast, the Operations Manager platform provides near–real-time status of events (less than 1-minute response), which can include FEP clients. Operations Manager only supports monitoring and alerting of FEP events: all other management must be performed either through Configuration Manager or manually.
* The use of non–System Center Configuration Manager–integrated definition update methods. It is possible to use a different definition update process, such as having clients download their updates directly from FTP servers or by using scripting to “automate” a manual copy process instead of relying on Configuration Manager’s Software Update Manager functionality.

# Appendix E: IPD in Microsoft Operations Framework 4.0

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

# Appendix F: System Center Configuration Manager and Forefront Endpoint Protection in Microsoft Infrastructure Optimization

The Infrastructure Optimization (IO) Model groups IT processes and technologies across a range 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 IO Model was to develop a simple way to use a maturity framework that is flexible and that 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 IO Model, Configuration Manager can move an organization from a basic to a dynamic level of maturity. At a standardized level, the environment distributes software packages using manual processes. A rationalized level includes fully automatic software updates. A dynamic level of maturity requires asset management that includes automated compliance. This guide will assist you in planning and designing the infrastructure for a Configuration Manager and FEP implementation.



Figure F-1. Mapping Configuration Manager and FEP technology into the Core IO Model

# Version History

|  |  |  |
| --- | --- | --- |
| **Version** | **Description** | **Date** |
| 2.0 | Added the “What’s New in System Center Configuration Manager 2007 R3 and Forefront Endpoint Protection” section.Added “Appendix C: Forefront Endpoint Protection Integration Job Aid.”Added “Appendix D: Forefront Endpoint Protection Fringe Scenarios.”Updated verbiage throughout the guide to add details about Forefront Endpoint Protection. | July 2011 |
| 1.0 | Original release. | October 2008 |

# Acknowledgments

The Solution Accelerators–Management and Infrastructure (SA-MI) team acknowledges and thanks the people who produced the Infrastructure Planning and Design Guide for Microsoft System Center Configuration Manager 2007 R3 and Forefront Endpoint Protection. 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
* Karl Grunwald – Microsoft
* Michael Kaczmarek – Microsoft
* Robin Maher – *Microsoft*
* Terry Matthews – GrandMasters
* Eric Orman – Microsoft
* Fergus Stewart – Microsoft
* Melissa Stowe – *Microsoft*
* Henry Webb – Microsoft

Reviewers:

* Bill Anderson – *Microsoft*
* Yumin Guo – *Microsoft*
* Edo Jorritsma – Capgemini
* Adwait Joshi – *Microsoft*
* Udo Karten – Capgemini
* Wally Mead – *Microsoft*
* Michael Niehaus – *Microsoft*
* Abhishek Pathak – *Microsoft*
* Josh Pointer – *Microsoft*
* Przemek (Shem) Radzikowski – *Microsoft*
* Martin Ruiter – Capgemini
* Rob Stack – *Microsoft*
* Ron Thomas – GrandMasters
* Arthur van den Berg – Capgemini
* Jeroen van Reijmersdaal – Capgemini

Editors:

* Michelle Anderson – *Xtreme Consulting Group*
* Laurie Dunham – *Xtreme Consulting Group*
* Pat Rytkonen – *Volt Technical Services*

## Feedback

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