

Infrastructure Planning
and Design

Microsoft® Forefront® Unified Access Gateway

Version 1.1

Published: December 2009

Updated: July 2010

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

Copyright © 2010 Microsoft Corporation. This documentation is licensed to you under the Creative Commons Attribution License.  To view a copy of this license, visit <http://creativecommons.org/licenses/by/3.0/us/> or send a letter to Creative Commons, 543 Howard Street, 5th Floor, San Francisco, California, 94105, USA.  When using this documentation, provide the following attribution: Infrastructure Planning and Design is provided with permission from Microsoft Corporation.

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 website references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, email addresses, logos, people, places and events depicted herein are fictitious.

Microsoft, ActiveSync, Active Directory, Forefront, Outlook, SharePoint, SQL Server, Windows, Windows Mobile, 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](#_Toc245634497)

[Introduction to the Microsoft Forefront Unified Access Gateway Guide 2](#_Toc245634498)

[Forefront Unified Access Gateway in Microsoft Infrastructure Optimization 5](#_Toc245634499)

[Forefront Unified Access Gateway Design Process 6](#_Toc245634500)

[Step 1: Define the Scope of the Forefront Unified Access Gateway Project 9](#_Toc245634501)

[Step 2: Determine the Number of Forefront Unified Access Gateway Instances Required 12](#_Toc245634502)

[Step 3: Design the Server Infrastructure 15](#_Toc245634503)

[Dependencies 19](#_Toc245634504)

[Conclusion 19](#_Toc245634505)

[Appendix A: Job Aids 21](#_Toc245634506)

[Appendix B: Using Forefront Unified Access Gateway with DirectAccess 23](#_Toc245634507)

[Appendix C: Certificates in Forefront Unified Access Gateway 24](#_Toc245634508)

[Version History 27](#_Toc245634509)

[Acknowledgments 28](#_Toc245634510)

#

# 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 Infrastructure Planning and Design (IPD) 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.

## 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 Forefront® Unified Access Gateway technology.

Benefits for Business Stakeholders/Decision Makers:

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

Benefits for Infrastructure Stakeholders/Decision Makers:

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

**Benefits for** Consultants or Partners:

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

Benefits for the Entire Organization:

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

# Introduction to the Microsoft Forefront Unified Access Gateway Guide

This guide leads the reader step by step through the process of planning a Forefront® Unified Access Gateway (Forefront UAG) infrastructure. The guide addresses the following fundamental decisions and tasks:

* Identifying the access functionality that will be provided by Forefront UAG—that is, identifying the users and client machines that will be able to access specific corporate resources including applications and servers.
* Deciding how many instances of Forefront UAG will be required in order to meet the business requirements.
* Designing the infrastructure needed for each instance of Forefront UAG.

Before starting the technical design, it’s very important to fully understand the business objectives for the project:

* What benefits does the business expect to achieve through the use of Forefront UAG?
* What is the value of those benefits and, therefore, the cost case for using Forefront UAG to deliver those benefits?
* Is the cost justification jointly entered into by more than one business group, and if so, do they depend on the success of the project for their relationship with each other?

The business objectives should be prioritized right at the start of the project so that they are clearly understood and agreed upon between IT and the business.

## Forefront UAG and DirectAccess

DirectAccess can provide seamless connectivity experiences for mobile workers when connected to the Internet. DirectAccess enables the mobile workforce to increase their productivity by providing them with the same connectivity experience—whether in or out of the office. Forefront UAG can be used in conjunction with DirectAccess to provide fault tolerance, scalability, and increased management for the DirectAccess infrastructure. In this case, the DirectAccess design should be completed at the same time as the Forefront UAG design, since both Forefront UAG and DirectAccess must be installed on the same server and are configured together using the same interface.

For more information, see:

* Infrastructure Planning and Design Guide for Direct Access: <http://go.microsoft.com/fwlink/?LinkId=164151>
* “Overview of Forefront UAG DirectAccess”: <http://technet.microsoft.com/en-us/library/ee406226.aspx>
* “Forefront UAG and DirectAccess”: <http://go.microsoft.com/fwlink/?LinkId=159955>

## Assumptions

To limit the scope of the material, the following assumption has been made:

* This design is for use in a production environment. It is expected that a test environment will also be created to mirror the configuration of the production environment.

## Feedback

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

We value your feedback on the usefulness of this guide. Please complete the following **Solution Accelerators Satisfaction Survey**, available at <http://go.microsoft.com/fwlink/?LinkID=132579>, and help us build better guidance and tools.

.

## IPD in Microsoft Operations Framework (MOF 4.0)

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

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

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



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

# Forefront Unified Access Gateway in Microsoft Infrastructure Optimization

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

IO is structured around three information technology models: Core Infrastructure Optimization, Application Platform Optimization, and Business Productivity Infrastructure Optimization. According to the Core Infrastructure Optimization Model, Forefront UAG can be used to move an organization from a Standardized to a Dynamic level of maturity, enabling dynamic application access and recovery for desktop applications in the process.

At a Standardized level, the enterprise may use Forefront UAG to assess client health before permitting any access to the corporate network.At the Rationalized level, providing a Virtual Private Network (VPN) is included so that users outside the corporate firewall can securely access different types of resources within the corporate firewall.
At the Dynamic level of maturity, only the functions and content for which clients have privileges is exposed, and the client’s health and location is used to dynamically modify those privileges.



Figure 2. Mapping of Forefront Unified Access Gateway technology into Core Infrastructure Model

# Forefront Unified Access Gateway Design Process

This guide addresses the most common scenarios, decisions, activities, options, tasks, and outcomes. Forefront UAG architecture has well-defined requirements and supported configurations; planning a Forefront UAG infrastructure that incorporates elements beyond this document should be carefully reviewed with Microsoft Support Services to ensure that it will be a supported scenario.

Figure 3 illustrates the relationship between the components that can work together to deliver an edge protection and access solution with Forefront UAG.



Figure 3. Forefront UAG Architecture

The components can be designed in many different ways; Figure 3 shows them in a particular implementation for illustrative purposes only.

## Decisions

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

* Step 1: Define the Scope of the Forefront Unified Access Gateway Project
* Step 2: Determine the Number of Forefront Unified Access Gateway Instances Required
* Step 3: Design the Server Infrastructure

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

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

## Decision Flow

The following figure provides a graphical overview of the steps in designing a Forefront UAG infrastructure.



Figure 4. The Forefront UAG infrastructure decision flow

## Applicable Scenarios

This guide addresses considerations that are related to planning and designing the following necessary components for a successful Forefront UAG infrastructure:

* Publishing Microsoft Outlook Web Access from Exchange Server to users on the Internet or extranets.
* Publishing SharePoint® services to users on the Internet or extranets.
* Publishing non-web applications such as client server applications over a secure SSL tunnel.
* Providing virtual private network (VPN) access to a corporate network.
* Providing scale out and fault tolerance for DirectAccess deployments.
* Providing NAT64 and DNS64 for DirectAccess deployments.
* Delivering secure edge protection and remote access control for corporate resources.

## Out of Scope

This guide does not address the following:

* Migration from Microsoft Intelligent Application Gateway (IAG).
* Migration from Microsoft Internet Security and Acceleration (ISA) Server.
* Infrastructure design of DirectAccess or Network Access Protection (NAP).
* Infrastructure design for a separate Forefront Threat Management Gateway (Forefront TMG) installation. A customized version of Forefront TMG is automatically installed by the Forefront UAG installation program.
* Design of a test environment. This document is intended to be used to design the production environment; however, the process could be adapted to separately design a limited scale test environment.

# Step 1: Define the Scope of the Forefront Unified Access Gateway Project

In this step, the scope of the Forefront Unified Access Gateway (Forefront UAG) project will be defined and the client requirements will be determined. This will be used to determine the requirements of the client populations that will be included. In addition, the service level expectations for Forefront UAG will be determined so that they can be used to appropriately size and place the infrastructure in later steps.

If an organization is considering multiple implementations of Forefront UAG, it can iterate through this guide for each instantiation.

The output of this step will be used in later steps to determine how many instances of Forefront UAG will be required, and then to design the infrastructure for each of those instances.

## Task 1: Define the Scope of the Project

Before designing a Forefront UAG infrastructure, an organization needs to determine which parts of its environment to include in the scope. This information will enable planners to know the boundaries for which they are building a solution and, in Step 2,
to determine how many instances of Forefront UAG will be required.

Start by defining the populations of clients for which Forefront UAG will provide access. These could be enterprise workstations used by travelling workers, workstations on a partner extranet that access corporate data for order fulfillment, or any client on the Internet if information or services are to be exposed publically.

This will be used to later determine:

* How many Forefront UAG client agents will be deployed.
* How many Forefront UAG server instances will be required.
* The size of the Forefront UAG server instances, and the server infrastructure in them.

Next, define the corporate resources that those client populations will access through Forefront UAG. The corporate resources may include specific applications, such as Exchange or SharePoint, or the clients may be provided access to the entire corporate network. This will be used to guide the placement of Forefront UAG instances in Step 3;
it will also determine which Forefront UAG client components must be installed on the client workstations, if any.

Finally, determine whether DirectAccess will be used by the client populations that are in scope. If so, determine whether the only role of Forefront UAG will be to provide scale out for a DirectAccess server infrastructure. In that use case, the Forefront UAG client code will not need to be deployed to the client workstations.

Record this information in Table A-1: “Project Scope” in Appendix A: “Job Aids.”

## Task 2: Determine the Client Requirements

Refer to Task 1 in which the scope of the project was determined in order to understand which populations of client workstations will be included. This will determine the location of the Forefront UAG client installations, the number of Forefront UAG instances in Step 2, and the design and placement of Forefront UAG servers in Step 3.

For each population of clients that is in scope, use Table A-1 in Appendix A to record the following information:

* **Where are the client machines located?** Record the name of each location and the number of users in it. This information will be used in Step2 to determine the Forefront UAG instance locations and in Step 3 to design the server infrastructure for each instance.
* **Will client machines and users travel between locations?** If so, this may require the design of additional instances in Step 2 and additional capacity in the server infrastructure in Step 3. Add the number of travelling machines to each of the locations to which they may travel, and record in Table A-1 in Appendix A the maximum number of machines that could be in the location. Note that travelling machines may appear in multiple locations.
* **What client operating systems and browsers are in use?** This information is required in order to determine whether the Forefront UAG client can be deployed there (for example, Windows®, Linux, Macintosh, Windows Mobile®, and iPhone).
If the client does not meet the Forefront UAG requirements, it will need to be removed from the project.
* **What Forefront UAG functionality will the client workstation use?** This will be used to determine what Forefront UAG client code must be installed on the client workstations. If endpoint detection and browser cache wiping are not required, no Forefront UAG code is required on the client workstation in the following scenarios:
* End-user authentication
* Web applications access through Forefront UAG
* Microsoft Outlook® Anywhere
* Microsoft Exchange ActiveSync®
* RemoteApps
* **Whether the client will use DirectAccess.** If the client is running one of the following operating systems:
* Windows 7 Enterprise edition
* Windows 7 Ultimate edition
* Windows Server® 2008 R2

and is domain-joined, it can use DirectAccess. Determine whether the client is included in the DirectAccess infrastructure design. This will be used in Step 2 to determine whether additional Forefront UAG instances must be designed for DirectAccess.

* **How users will be authenticated.** Determine what authentication methods will be used (such as passwords, tokens, or client certificates) and which identity providers will be used (Active Directory Domain Services, LDAP, RADIUS, ADFS, or others). This will be used to design the Forefront UAG servers’ connections to authentication services.
* **Fault-tolerance requirements**. It is important to understand whether continuous access to the infrastructure is required so that fault tolerance can be designed into the Forefront UAG infrastructure, if required.

Repeat this task for each group of client workstations and record the results in Table A-1 in Appendix A.

## Task 3: Determine the Endpoint Health Approach

If there is a requirement to evaluate client health prior to allowing access, there are two options:

* The Forefront UAG built-in access policies can be used to specify prerequisites that endpoints must meet for session access, such as having applied updates or running an antivirus program.
* Network Access Protection (NAP) policies can be downloaded from a Network Policy Server (NPS). For information on designing a NAP infrastructure, refer to [http://technet**.**microsoft.com/en-us/library/dd857268.aspx](http://technet.microsoft.com/en-us/library/dd857268.aspx).

Either option, or both of them, can be used to verify the health of client endpoints connecting to the Forefront UAG server.

If NAP is used, the Forefront UAG server will need to connect to the NPS where NAP policies are stored. This will be used to guide placement of the Forefront UAG server instances in Step 3.

Decide if NAP will be used and, if so, record that and the location of the NAP server in Table A-1 in Appendix A.

## Validating with the Business

Ask business stakeholders whether there are any future changes planned for the environment that may affect the Forefront UAG design. For example, are any acquisitions or divestitures planned for the environment in which Forefront UAG will be implemented? These could affect the size of the client population and, therefore, the infrastructure sizing.

## Step Summary

In this step, the scope of the Forefront UAG project was defined, and the client requirements were determined. This was used to understand the requirements of the
in-scope client populations. In addition, the service level expectations for Forefront UAG were determined in order to appropriately size and place the infrastructure in Step 3. Finally, the approach for evaluating endpoint health was decided. Data gathered in this step was recorded in Table A-1 in Appendix A.

## Additional Reading

* “Overview of Forefront UAG”: <http://technet.microsoft.com/en-us/library/dd857382.aspx>
* Microsoft Forefront Unified Access Gateway home page: <http://www.microsoft.com/forefront/prodinfo/roadmap/uag.mspx>
* Infrastructure Planning and Design Guide *for Direct Access*: <http://go.microsoft.com/fwlink/?LinkId=164151>
* “Configuring NAP”: [http://technet**.**microsoft.com/en-us/library/dd857268.aspx](http://technet.microsoft.com/en-us/library/dd857268.aspx)
* Infrastructure Planning and Design Guide for Selecting the Right NAP Architecture: <http://go.microsoft.com/fwlink/?LinkId=160981>
* “Endpoint system requirements”: <http://technet.microsoft.com/en-us/library/dd920232.aspx>

# Step 2: Determine the Number of Forefront Unified Access Gateway Instances Required

In Step 1, the project scope was defined and the user and client populations were identified for inclusion in the project.

This step will be used to decide how many instances of Forefront UAG are required in order to service the needs of the in-scope client population. Only one instance of Forefront UAG can be hosted on a server, so the output of this step will be used in the next step to design the server infrastructure for each instance.

A Forefront UAG instance includes the following:

* The Forefront UAG server, including associated services on which it depends, such as the customized version of Forefront TMG that is installed by the Forefront UAG installation program.
* A data store, which can be a file server, a Remote Authentication Dial-In User Service (RADIUS) accounting server, or a Microsoft SQL Server® database that stores events. The data store is optional and may be shared with other Forefront UAG instances.
* Workstations that access corporate resources through the Forefront UAG server. Note that a workstation may connect to different Forefront UAG instances, but not at the same time.
* If the instance will include an array of servers for scale or fault-tolerance reasons, one of the array servers, the array manager, will store the array configuration.
Note that the array manager cannot be made fault tolerant. If the array manager fails, clients can continue to use the remaining members of the array and, if necessary, one of those members can be configured as a replacement array manager.

Separate Forefront UAG instances cannot be integrated, so adding instances to the design decentralizes the infrastructure.

## Task 1: Decide the Number of Forefront UAG Instances Required

In this task, the number of Forefront UAG instances will be determined and the scope of each instance defined so that the design of the server infrastructure for each instance can be completed in the next step.

Begin with one Forefront UAG instance; then add more instances only if necessary for:

* **Servicing both DirectAccess clients and UAG Network Connector clients.** A Forefront UAG instance cannot serve both as a DirectAccess server and as a UAG Network Connector; so if both DirectAccess and the UAG Network Connector application are required, increment the number of instances by one.

In order to determine whether DirectAccess may be in use, refer to Table A-1 in Appendix A.

* **Aligning with the organization’s management model.** If the organization chooses to delegate access management, decide whether additional instances of Forefront UAG may be required in each of the distributed locations and, if so, add them to the design.
* **Separating client populations or server farms for regulatory reasons.** If regulations require that a group of clients or a set of applications use a separate infrastructure, add another Forefront UAG instance.
* **Isolating networks.** Refer to Table A-1 in Appendix A to identify where clients are located. Determine if any clients reside in networks that are isolated and therefore require a separate Forefront UAG instance. For example, organizations often isolate lab networks from production networks. Add a Forefront UAG instance to the design for each isolated network that will contain Forefront UAG clients.
* Connecting to services in domains beyond the trust boundary. A Forefront UAG server can be installed in an Active Directory® Domain Services (AD DS) domain or in a workgroup. The services to which it provides access must be within the trust boundary of the Forefront UAG server. Add one Forefront UAG instance to the design for each group of services that is beyond a trust boundary.

Note   If applications such as Exchange and SharePoint will be published using Kerberos constrained delegation, the Forefront UAG server and the published Web server must be members of the same domain.

In Table A-2: “Instance and Server Design” in Appendix A, record a name for each instance of Forefront UAG that will be designed, along with the reason for its inclusion in the architecture and the clients that will be assigned to it. This information will be used in Step 3 to design the server infrastructure for each instance.

## Step Summary

In this step, the number of Forefront UAG instances required to service the in-scope client population was decided. Only one instance of Forefront UAG can be hosted on a server, so the output of this step will be used in the next step to design the server infrastructure. The data gathered in this step was recorded in Table A-2 in Appendix A.

# Step 3: Design the Server Infrastructure

Now that the number of instances of Forefront UAG has been determined, the server infrastructure must be designed for each instance to meet the requirements for each group of clients listed in Step 1.The scale out and fault-tolerance design for the server infrastructure will be completed, if required, and the data store will be designed.

## Task 1: Design and Place the Forefront UAG Server

In this task, the Forefront UAG server will be designed and placed. To understand the load that will be placed on the server and the resources to which it must be connected,
it can be useful to review the functions that the server performs:

* Receives an authentication request from each Forefront UAG client when that Forefront UAG client attempts to access a service.
* Queries AD DS, or other authentication services, to authenticate clients’ access permissions.
* Stores access policy.
* Implements access policies by filtering traffic so that only authorized services are exposed to the Forefront UAG client.
* Logs events to a data store, which may be local on the same server, or remote.
* Provides scale, fault tolerance, and IPv6 to IPv4 conversion for DirectAccess when they are both installed on the same server. Further details are available in Appendix B: “Using Forefront Unified Access Gateway with DirectAccess.”

### Server Configuration

The Forefront UAG product group provides a recommended server configuration in “System requirements in Forefront UAG,” available at [http://technet.microsoft.com/en-us/library/dd903051.aspx](http://technet.microsoft.com/en-us/library/dd903051.aspx%20). However, there is no architectural guidance offered to support this recommendation. Performance test data, available in “Forefront UAG DirectAccess performance information,” at <http://technet.microsoft.com/en-us/library/ff723731.aspx> provides some guidance of hardware configuration.

The entire Forefront UAG server product is designed to be run on the same server, with the exception of the data store, which can be run on either the Forefront UAG server or a remote server. This is the only supported configuration. So roles cannot be split out across multiple servers. Forefront UAG is a 64-bit application, so it is able to take advantage of large memory.

The recommended server configuration assumes that the Forefront UAG server and the services on which it may depend (NLB, Forefront TMG, SQL Server, and DirectAccess) will run on a dedicated server since sharing the server with other workloads is not supported.

The Forefront UAG server can be run in a virtual machine (VM). If a VM will be used, ensure that it has access to CPU and memory resources equivalent to those specified for a physical machine.

The UAG product group recommended disk capacity is 2.5 GB, in addition to the requirements of the operating system. However, no architectural guidance is offered to support this recommendation. The number of access policies that must be stored will depend on how many different policies are required for different Forefront UAG clients using the same applications, as well as the number applications that will be accessed.

Record the server configuration that will be used, and then add it to the design in Table A-2 in Appendix A.

### Placing the Server

The server will typically be placed in the perimeter network. It should have high-speed network access to the endpoint machines for which it will provide access and to the identity repositories that will be used to authenticate users, such as AD DS, LDAP, and RADIUS. If client certificates will be used, the Forefront UAG server should have access to the certificate revocation information provider.

If Forefront UAG will be used with DirectAccess, both must be installed on the same server. As stated in the previous step, the UAG Network Connector application cannot co-exist with DirectAccess, so plan to implement them on separate servers.
In addition, when using DirectAccess, the Forefront UAG server will require public IP addresses and cannot be placed behind a NAT firewall. Refer to the *Infrastructure Planning and Design Guide for Direct Access*, available at <http://go.microsoft.com/fwlink/?LinkId=164151>, for further information on these requirements.

Record the location of the Forefront UAG server in Table A-2 in Appendix A.

## Task 2: Design Fault Tolerance and Scale Out

Refer to the requirements that were determined in Step 1 for fault tolerance and performance of the Forefront UAG instance being planned. Use these requirements to determine whether fault tolerance or additional scale may be required within the instance.

Load balancing of incoming requests can be performed by either of the following:

* **Windows Network Load Balancing (NLB).** Up to eight Forefront UAG servers can be placed into an array to load balance VPN or DirectAccess traffic.
* **Hardware load balancer**. The hardware load balancer must use IP affinity. Note that if Forefront UAG is used to provide an array for DirectAccess, use of a hardware load balancer is not supported.

Note that Forefront UAG is not compatible with failover clustering provided by Windows Server 2008 R2.

No architectural guidance is available for determining the number of servers that will be required in the array, so plan to deploy an initial set of users, monitor performance, and use that as the performance baseline for their workload; then plan the number of servers accordingly.

The array function is implemented by Forefront TMG, which is installed by the Forefront UAG installer. The array members share the same configuration and provide the same set of services. If an array node fails, services can be accessed from another array member. One of the array members is configured as the array manager and holds the configuration for the entire array.

There is no fault-tolerance solution for the array manager. If the array manager fails, clients can continue to use the remaining members of the array, and if necessary, one of those members can be configured as a replacement array manager.

To deploy multiple Forefront UAG servers in an array, all the servers must be domain members.

If fault tolerance will be needed, add it to the design, and record it in Table A-2 in Appendix A.

## Task 3: Design the Data Store

Decide what type of data store will be used if logging will be enabled. The Forefront UAG server can record information about system usage, user activities, and alerts about security risks. These can be used to troubleshoot Forefront UAG issues, to assist remote users if they encounter problems while accessing the internal resources published by Forefront UAG, and to provide an audit log.

Forefront UAG can log events in the following ways:

* **Built-in Forefront UAG reporter.** The Forefront UAG built-in reporter is enabled by default to allow events to be saved to a log file. The Forefront UAG Web Monitor console can then be used to query this event log and to filter events according to type, time, and other parameters. The product group recommends that these logs be saved on the Forefront UAG server.

If fault tolerance is required, the log files can instead be placed on a clustered file server.

* **RADIUS accounting server.** Microsoft’s implementation of a RADIUS accounting server is in the NPS role in Windows Server 2008. NPS logs data either in text format or database format, or to a stored procedure in a SQL Server database. The NPS role may be installed on the Forefront UAG server or on a remote server.
* **Remote syslog server.** Events can be sent using the syslog protocol to a third-party server where they can be logged by the syslog daemon.
* Simple Mail Transfer Protocol (**SMTP) mail server.** Events can be sent to one or more email addresses.
* **SQL Server database.** Forefront UAG can log events to a SQL Server database using the Forefront TMG logging mechanism. It’s possible to specify which log fields should be written to the SQL Server log when configuring SQL Server logging in the Forefront TMG Management console. Events can be logged to a local SQL Server Express database running on the Forefront UAG server or to a remote SQL Server database. If fault tolerance is required, a remote SQL Server database can be placed in a Microsoft failover cluster.

If logging will be enabled, decide what type of data store will be used, and record that in Table A-2 in Appendix A.

### Size and Place the Data Store

No guidance is available from the Forefront UAG product group to determine the size of the data store. The data that can be logged is listed in “SQL Server logging fields”at <http://technet.microsoft.com/en-us/library/ee441342.aspx> and in “Web proxy log fields” at <http://technet.microsoft.com/en-us/library/cc441708.aspx>. However, the fields that are actually logged will usually be a subset of these, based on the features of Forefront UAG that are in use.

If the available disk space is exhausted, notification of that will depend on the logging mechanism in use. If the Forefront UAG built-in logging process is used, logs are no longer written to the disk without notification.

A cleanup process is available that can be used to prune the Forefront UAG logs when they reach a configurable size. This is described in “Cleaning up log files” at <http://technet.microsoft.com/en-us/library/ee406237.aspx>.

Design the Forefront UAG log space to be as large as possible; then monitor the size of the log files that are written during typical use to determine the required space.

Record the size and location of the data store in Table A-2 in Appendix A.

## Step Summary

The server infrastructure for each instance was designed in this step. This included determining whether the Network Policy Server and data store will exist on the Forefront UAG server or on a remote server, as well as the type and size of the data store. In addition, the fault-tolerance and scale out design for the server infrastructure was completed in this step. Data gathered in this step was recorded in Table A-2 in Appendix A.

## Additional Reading

* “System requirements in Forefront UAG”: <http://technet.microsoft.com/en-us/library/dd903051.aspx>
* “NLB Fundamentals – FAQ”: [http://technet.microsoft.com/en-us/library/cc738464(WS.10).aspx](http://technet.microsoft.com/en-us/library/cc738464%28WS.10%29.aspx)
* “Comparing UAG and TMG arrays”: <http://blogs.technet.com/edgeaccessblog/archive/2009/07/20/comparing-uag-and-tmg-arrays.aspx>
* “UAG Array and Network Load Balancing”: <http://blogs.technet.com/edgeaccessblog/archive/2009/06/29/array-and-network-load-balancing.aspx>
* “Configuring a network load balanced array for Forefront UAG DirectAccess”: [http://technet.microsoft.com/en-us/library/ee191502(printer).aspx](http://technet.microsoft.com/en-us/library/ee191502%28printer%29.aspx)
* “SQL Server logging fields”: <http://technet.microsoft.com/en-us/library/ee441342.aspx>
* “Web proxy log fields”: <http://technet.microsoft.com/en-us/library/cc441708.aspx>
* Network Policy Server page: <http://technet.microsoft.com/en-us/network/bb629414.aspx>
* Infrastructure Planning and Design Guide for Microsoft SQL Server 2008: <http://go.microsoft.com/fwlink/?LinkId=160982>
* “Planning for load balancing”: <http://technet.microsoft.com/en-us/library/dd861441.aspx>
* Microsoft Forefront Unified Access Gateway (UAG) 2010 Best Practices Analyzer Tool: <http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=d24994ef-8670-4324-957a-805d35f1244e>

# Dependencies

The Forefront UAG installation program automatically installs a customized version of Forefront TMG. Forefront UAG utilizes many functions that are in Forefront TMG, including the array and the firewall. It also stores the publishing rules for the Forefront UAG portal. If Forefront TMG is uninstalled from a Forefront UAG server, this creates a configuration that Microsoft does not support.

Note that Forefront UAG does not support the stand-alone version of Forefront TMG;
the only supported configuration is where Forefront UAG automatically installs its own version of Forefront TMG.

Further information about Forefront TMG’s role when used with Forefront UAG is available at <http://technet.microsoft.com/en-us/library/ee522953.aspx>.

# Conclusion

This guide has summarized the critical design decisions, activities, and tasks required to enable a successful design of Microsoft Forefront Unified Access Gateway. It focused on decisions involving:

* Defining the scope of the Forefront UAG project.
* Determining how many Forefront UAG instances will be required.
* Designing the Forefront UAG instances and the server infrastructure in them.

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

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 the architecture has been designed, a pilot should be conducted before a major rollout begins so that lessons learned can be incorporated back into the design. Refer to the Forefront UAG TechNet library at <http://technet.microsoft.com/en-us/library/dd861463.aspx> to proceed with the installation.

This guide, when used in conjunction with product documentation, allows organizations to confidently plan the implementation of Forefront UAG.

##  Feedback

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

We value your feedback on the usefulness of this guide. Please complete the following **Solution Accelerators Satisfaction Survey**, available at <http://go.microsoft.com/fwlink/?LinkID=132579>, and help us build better guidance and tools.

#

# Appendix A: Job Aids

This section provides job aid examples to record data while planning the Forefront UAG infrastructure.

Step 1. Use the table below to record information relative to the Forefront UAG project scope.

A-1. Project Scope

| Client population and location | Corporate resources in-scope | Will clients use DirectAccess? (Task 1) | Will Forefront UAG be used ONLY to provide server scale out for DirectAccess? |
| --- | --- | --- | --- |
| Fulfillment partners – North America | North America networkExchange AA01 - AA07SharePoint tracking system | Y | N |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

A-1. Project Scope (continued)

| Max # clients in location | Will clients travel between locations? | OS in use | Forefront UAG functionality |
| --- | --- | --- | --- |
| 700 | Y | Windows 7 | RemoteApps |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

A-1. Project Scope (continued)

|  |  |  |  |
| --- | --- | --- | --- |
| Authentication method and identity provider | Will client use DirectAccess? (Task 2) | Fault tolerance | NAP enforcement and NAP server location |
| AD DS | Y | Y | Y, New Jersey site  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Steps 2 and 3. Use the table below to record information relative to the Forefront UAG server instances and the design of each instance.

A-2. Instance and Server Design

| Forefront UAG instance name | Reason for design | Clients assigned | Forefront UAG servers in instance | Forefront UAG server configuration |
| --- | --- | --- | --- | --- |
| Forefront UAG-11 | Exchange publishing | Boise call center | Forefront UAG-11-1 | 2.66 GHz Dual core, 8 GB of RAM |
| Boise call center | Forefront UAG-11-2 | 2.66 GHz Dual core, 8 GB of RAM |
| Boise call center | Forefront UAG-11-3 | 2.66 GHz Dual core, 8 GB of RAM |
|  |  |  |  |  |
|  |  |  |  |  |

A-2. Instance and Server Design (continued)

| Forefront UAG server location | Fault tolerance and scale out | Data store type, size, and location |
| --- | --- | --- |
| Boise | NLB | SQL-11, 60 GB, Boise |
| Boise | NLB | SQL-11, 60 GB, Boise |
| Boise | NLB | SQL-11, 60 GB, Boise |
|  |  |  |
|  |  |  |

# Appendix B: Using Forefront Unified Access Gateway with DirectAccess

Forefront UAG complements DirectAccess when they are both installed on the same server. Forefront UAG can provide the following services to DirectAccess:

* NAT64 and DNS64 translation. Provides DirectAccess clients with access to IPv4-only resources. The NAT64 function in Forefront UAG allows IPv6 traffic to be initiated toward the organization’s IPv4 intranet and for the responses to return properly. It does not work in reverse; so if traffic needs to be initiated outbound to the DirectAccess-enabled clients, this capability is not available with NAT64.
* Fault tolerance and scale. The Forefront UAG server running DirectAccess can be placed into an array to load balance client requests. Forefront UAG DirectAccess works with NLB; so if one of the servers in the array fails, it’s removed from the array and requests are sent to the remaining servers. Note that a hardware load balancer is not supported for Forefront UAG when it is used to provide an array for DirectAccess.
* Simplified configuration tools. These support additional items including NAP integration, third-party load balancers, and flexible server selection.
* Forefront TMG. Provides the underlying hardening and firewall functions of Forefront TMG.

# Appendix C: Certificates in Forefront Unified Access Gateway

When workstations access the Forefront UAG server using the VPN configuration, by default, communications between clients and the Forefront UAG server are encrypted with Transport Layer Security (TLS), using 128-bit encryption. TLS is an updated version of Secure Sockets Layer (SSL), and both are sometimes referred to as “SSL encryption.” This requires that the Forefront UAG server has a server certificate that can be used for TLS/SSL, and that the client computers trust the certification authority (CA) that has issued the server certificate.

When workstations use DirectAccess with Forefront UAG, in addition to a server certificate on the Forefront UAG server, both the Forefront UAG server and all clients will require certificates for the IPsec security associations (SAs). The SAs are created by using Authenticated Internet Protocol (AuthIP), an enhancement of the Internet Key Exchange (IKE) protocol. AuthIP requires both peers (the client and the Forefront UAG server) to have trusted certificates.

Some applications may have additional certificate requirements—for example, publishing Outlook Anywhere by using Forefront UAG requires that the Exchange Client Access Server (CAS) server certificate be installed on the Forefront UAG server.

## Trusting Certificates

It is beyond the scope of this guide to fully describe the roles and relationships between all elements of a public key infrastructure (PKI), but in order to determine the strategy for the certification authority, a few key elements must be fully understood.

Each certificate is associated with a public key and a private key. In the case of a server certificate, the server holds the private key and keeps it secret, while the public key is available with the certificate and is provided to the client. The client uses the server’s public key to encrypt a small packet and then sends the packet to the server. The server can decrypt this packet using its own private key. This provides the basis for a key exchange in which the two computers securely exchange new, symmetric encryption keys that will be used to encrypt data for the connection.

Before creating and exchanging session keys, the client must trust the server. In order to determine the validity of the server certificate, the client can examine the certificate for a signature. Each certificate has been signed by its issuer (usually a CA, as described below). The CA signs the certificate by encrypting a small attribute by using its secret, private key and including that in the certificate. The client can use the public key of the issuer to decrypt that signature. If the decryption fails, the certificate is fraudulent or damaged.

Each client maintains its own list of trusted issuers. If a certificate signature decrypts properly, it is a valid certificate, but it is only trusted if the issuer is in the list of trusted issuers maintained on the client. (Certificates may also be chained. A root CA issues a certificate to an intermediate CA, which in turn issues one to a server, for example.
The root CA must be trusted for any certificate in the chain to be trusted.)

## Choosing the Certification Authority

There are three ways to provide certificates to the Forefront UAG server and to enable the client workstations to trust them:

* **Self-signed certificates.** Certificates are generated locally by the Forefront UAG server and are placed on the Forefront UAG server. As with all self-signed certificates, the issuer is not a CA, but the server itself. In other words, the server says “Hello, I’m the Forefront UAG server. Trust me. That’s who I am.”

This requires no infrastructure setup and there is no additional cost for the certificates, but every client machine must be configured to trust these certificates. This configuration can require significant work. Each client downloads a copy of the certificate and an administrator adds it to the trusted certificate store.

Due to the administrative overhead, this is usually only a recommended solution in test environments or for very small deployments.

* **Trusted third party.** There are a number of trusted CAs, including VeriSign, Thawte, Entrust, Equifax, Cybertrust, and others that provide certificate services for a fee. These organizations are pre-loaded into the Trusted Root CA certificate store in the operating system, after having been vetted by Microsoft. Each CA also follows strict and known processes before issuing server certificates to its customers. The operator of the Forefront UAG server requests a server certificate for the Forefront UAG server from the CA of choice and installs the certificate on the Forefront UAG server. In this case, the server says “Hello, I’m the Forefront UAG server, and our mutual friend the CA (who can be trusted) vouches for me.”

Since the client and the server both already trust the CA, there is no need to manually place a certificate on the client or to change the client’s configuration, which can be very convenient. There will normally be a fee for the server certificate.

This approach is often used if unmanaged clients (that is, non-domain–joined clients) will connect to the Forefront UAG environment, and DirectAccess is not used.

* **Operate a certificate server.** In this case, a certificate server is set up for the corporate network. Usually, this will be part of a PKI rollout that supports many enterprise functions. Rather than using a trusted third-party CA, the organization acts as its own CA. Generally, the issuing CA will be an Enterprise CA that is integrated with Active Directory Domain Services (AD DS). This CA issues a server certificate to the Forefront UAG server. In this design, the server says “Hello, I’m the Forefront UAG server, and here is proof that I am a member of our organization.”

Clients, however, must be configured to trust this CA. By default, members of the AD DS forest will automatically trust the Enterprise CA since domain policies will force the root certificate into the Trusted Root CA store on all domain members.
If the CA is a stand-alone CA (not part of the AD DS infrastructure), Group Policy can be used to configure domain members to trust the CA. Non-domain members, such as non-managed computers will need to be configured manually.

If DirectAccess will be used, an Enterprise CA should be designed for the organization. This CA can also issue the client certificates required for DirectAccess and IPsec. The domain can be configured so that domain members automatically receive all required certificates.

## Additional References:

* “Deep dive into UAG DirectAccess (Certificates)”: <http://blogs.technet.com/edgeaccessblog/archive/2009/10/27/deep-dive-into-uag-directaccess-certificates.aspx>
* “The Authenticated Internet Protocol”: <http://207.46.16.252/en-us/magazine/2007.10.cableguy.aspx>
* “Authenticating Exchange Mail Applications using UAG RC0”: <http://blogs.technet.com/edgeaccessblog/archive/2009/10/12/authenticating-exchange-mail-applications-using-uag-rc0.aspx>
* “PKI Enhancements in Windows 7 and Windows Server 2008 R2”: <http://technet.microsoft.com/en-us/magazine/2009.05.pki.aspx?pr=blog>
* Windows Server 2008 PKI and Certificate Security: <http://search.barnesandnoble.com/Windows-Server-2008-PKI-and-Certificate-Security/Brian-Komar/e/9780735625167>

# Version History

|  |  |  |
| --- | --- | --- |
| **Version** | **Description** | **Date** |
| 1.1 | Minor updates to this guide to reflect current IPD template. | July 2010 |
| 1.0 | Original release. | December 2009 |

# 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 Forefront Unified Access Gateway*. The following people were either directly responsible for or made a substantial contribution to the writing, development, and testing of this guide.

**Contributors:**

* Jude Chosnyk – GrandMasters
* Joe Coulombe – *Microsoft*
* Byron P. Hynes – Xtreme Consulting
* Michael Kaczmarek – *Microsoft*
* Robin Maher – *Microsoft*
* Fergus Stewart *– Microsoft*
* Melissa Stowe – *Microsof*t

**Reviewers:**

* Fernando Cima – *Microsof*t
* Philip Derbeko – *Microsof*t
* Devrim Iyigun – *Microsof*t
* Steve Jones – *Microsof*t
* Udo Karten – *Capgemini*
* Bert Kruizenga – *Capgemini*
* Uri Lichtenfeld – *Microsof*t
* Meir Mendelovich – *Microsof*t
* Sean Siler – *Microsof*t
* Pat Telford – *Microsof*t

**Editors:**

* Laurie Dunham – *Microsoft*
* Pat Rytkonen – *Volt Technical Services*