Forefront Unified Access Gateway 2010

Infrastructure Design Guide

Microsoft® Corporation

Published: February, 2010

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

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

© 2009 Microsoft Corporation. All rights reserved.

Microsoft, and MS-DOS, Windows, Windows Server, and Active Directory are trademarks of the Microsoft group of companies. All other trademarks are property of their respective owners.

Contents

[Infrastructure design guide 5](#_Toc252835604)

[About this guide 5](#_Toc252835605)

[Introduction to infrastructure design 5](#_Toc252835606)

[Forefront UAG single server or array deployment 5](#_Toc252835607)

[Forefront UAG DirectAccess single server or array deployment 6](#_Toc252835608)

[Endpoint deployment 6](#_Toc252835609)

[Endpoint access control 6](#_Toc252835610)

[Application publishing 7](#_Toc252835611)

[Logging and monitoring 7](#_Toc252835612)

[Next steps in planning your infrastructure design 7](#_Toc252835613)

[Identifying your infrastructure design requirements 7](#_Toc252835614)

[Identifying design requirements for server installation and deployment 8](#_Toc252835615)

[Deployment scope 8](#_Toc252835616)

[DirectAccess requirements 8](#_Toc252835617)

[Network topology requirements 9](#_Toc252835618)

[Domain and workgroup requirements 10](#_Toc252835619)

[Network and routing requirements 10](#_Toc252835620)

[DNS requirements 11](#_Toc252835621)

[Identifying design requirements for client and endpoint deployment 11](#_Toc252835622)

[Identifying design requirements for endpoint access control 13](#_Toc252835623)

[Identifying design requirements for application publishing 14](#_Toc252835624)

[Identifying design requirements for logging and monitoring 15](#_Toc252835625)

[Next steps in planning your infrastructure design 15](#_Toc252835626)

[Identifying your infrastructure deployment goals 15](#_Toc252835627)

[Next steps in planning your infrastructure design 20](#_Toc252835628)

[Mapping your deployment goals to an infrastructure design 21](#_Toc252835629)

[Single server infrastructure design 22](#_Toc252835630)

[Selecting a topology location for the Forefront UAG server 22](#_Toc252835631)

[Behind a frontend firewall 22](#_Toc252835632)

[Between a frontend firewall and a backend firewall 23](#_Toc252835633)

[Configuring the backend firewall 23](#_Toc252835634)

[Joining the Forefront UAG server to a domain or a workgroup 24](#_Toc252835635)

[Configuring network addressing and routing 25](#_Toc252835636)

[Configuring DNS servers and settings 25](#_Toc252835637)

[Multiple server infrastructure design 25](#_Toc252835638)

[Selecting a topology location for the Forefront UAG server 26](#_Toc252835639)

[Behind a frontend firewall 26](#_Toc252835640)

[Between a frontend firewall and a backend firewall 26](#_Toc252835641)

[Configuring the backend firewall 27](#_Toc252835642)

[Joining the Forefront UAG server to a domain or workgroup 28](#_Toc252835643)

[Configuring network addressing and routing 28](#_Toc252835644)

[Configuring DNS servers and settings 28](#_Toc252835645)

[Configuring the array infrastructure 29](#_Toc252835646)

[Single Forefront UAG DirectAccess server infrastructure design 29](#_Toc252835647)

[Multiple Forefront UAG DirectAccess server infrastructure design 30](#_Toc252835648)

[Endpoint component infrastructure design 31](#_Toc252835649)

[Client authentication infrastructure design 31](#_Toc252835650)

[Endpoint health checking infrastructure design 32](#_Toc252835651)

[Application authorization infrastructure design 32](#_Toc252835652)

[Privileged (certified) endpoint infrastructure design 32](#_Toc252835653)

[Application publishing infrastructure design 33](#_Toc252835654)

[Logging and monitoring infrastructure design 33](#_Toc252835655)

# Infrastructure design guide

Forefront Unified Access Gateway (UAG) provides a gateway for remote employees, mobile workers, partners, and other third-parties, to access corporate applications and resources via a Forefront UAG Web portal.

## About this guide

This guide is intended for the system, network, and server administrators, who are responsible for the modifications that are required in your existing corporate infrastructure design in order to deploy Forefront UAG. It is assumed that the reader of this guide is familiar with network concepts, such as domain configuration, Certification Authority (CA) deployment, DNS configuration, network routing and protocols.

Infrastructure planning and designing consists of three phases: understanding the design requirements for Forefront UAG deployment, identifying your specific deployment goals, and understanding what changes are required in your infrastructure design in order to match those deployment goals.

The following steps will help you to plan and design your corporate infrastructure:

1. Understand the Forefront UAG features that will affect your corporate infrastructure. For information, see [Introduction to infrastructure design](#z4dd4276ecc33451ab0231994a599cfaa).

2. Understand the infrastructure considerations for Forefront UAG deployment. For information, see [Identifying your infrastructure design requirements](#z2003740048754fc482250a0c9e14acd7).

3. Identify your Forefront UAG deployment goals. For information, see [Identifying your infrastructure deployment goals](#zb11dbdc1079144e1986252ee6efb71a6).

4. Map each of your deployment goals to an infrastructure design that meets your deployment objectives. For information, see [Mapping your deployment goals to an infrastructure design](#zf8f7f8bb7239461c8ced914a6d6095b5).

# Introduction to infrastructure design

This topic provides an overview of the Forefront Unified Access Gateway (UAG) features that affect your infrastructure design.

## Forefront UAG single server or array deployment

Depending on your requirements, you can deploy a single Forefront UAG server, or an array of Forefront UAG servers. An array consists of multiple Forefront UAG servers that share the same configuration and provide scalability and high availability. You can implement load balancing among array members, using the Windows Network Load Balancing feature that is integrated into Forefront UAG or using a hardware load balancer.

For more information, see Introduction to array design. For more information about deploying Forefront UAG, see the Forefront UAG DirectAccess design guide.

## Forefront UAG DirectAccess single server or array deployment

Forefront UAG can be deployed as a DirectAccess server to extend the benefits of Windows DirectAccess across your infrastructure, enhancing scalability, simplifying deployment and management, and providing remote users the experience of being seamlessly connected to your internal network any time that they have Internet access. Depending on your requirements, you can deploy a single Forefront UAG DirectAccess server, or an array of servers to provide scalability and high availability. You can implement load balancing among array members, using the Windows Network Load Balancing feature that is integrated into Forefront UAG or using a hardware load balancer.

For more information, see Forefront UAG DirectAccess design guide, Configuring a network load balanced array for Forefront UAG DirectAccess, and Configuring an external load balanced array for Forefront UAG DirectAccess.

## Endpoint deployment

Forefront UAG deploys endpoint components on managed and unmanaged remote client endpoints connecting to Forefront UAG portals and published applications. These components are required to enable endpoints to access a number of Forefront UAG features. Components can only be installed on endpoints that comply with system requirements.

For more information, see System requirements for Forefront UAG endpoints, and Introduction to endpoint component deployment design.

## Endpoint access control

Forefront UAG provides a number of mechanisms for controlling and securing endpoint access to Forefront UAG portals and published applications including, client authentication, endpoint health checking, and application authorization.

1. Client authentication─You can require remote clients to authenticate in order to establish a session with a Forefront UAG portal. You can use a number of different client authentication mechanisms. In addition, you can implement single sign-on, so that client credentials that are provided during session logon are passed to backend published servers that require authentication, so clients only need to provide credentials once.

For more information, see Planning for client authentication.

2. Endpoint health checking─You can compare endpoint settings with Forefront UAG access policies. Only endpoints that comply with policies can access published resources. You can create inbuilt Forefront UAG access policies, or use Network Access Protection (NAP) policies that are downloaded from a Network Policy Server (NPS).

For more information, see Planning for endpoint health checking.

3. Portal application authorization─You can implement portal application authorization to limit access to portal applications to specific users and groups.

For more information, see Planning for portal application authorization.

## Application publishing

Forefront UAG allows remote endpoints to access internal corporate resources by publishing applications via one or more Forefront UAG trunks. Endpoints then access trunks via a Forefront UAG portal Web page.

For more information about Forefront UAG concepts such as trunks and portals, see Understanding Forefront UAG architecture. For more information about publishing, see the Application publishing design guide.

## Logging and monitoring

Forefront UAG can log to a variety of formats, including a syslog server, RADIUS accounting server, SMTP server, and SQL Server. In addition, you can monitor Forefront UAG using System Center Operations Manager (SCOM).

For more information, see Monitoring and logging.

## Next steps in planning your infrastructure design

[Identifying your infrastructure design requirements](#z2003740048754fc482250a0c9e14acd7).

# Identifying your infrastructure design requirements

This topic helps you to identify your infrastructure design requirements.

Identifying your infrastructure design requirements may require the following:

1. [Identifying design requirements for server installation and deployment](#z1)

2. [Identifying design requirements for client and endpoint deployment](#z2)

3. [Identifying design requirements for endpoint access control](#z3)

4. [Identifying design requirements for application publishing](#z4)

5. [Identifying design requirements for logging and reporting](#z5)

## Identifying design requirements for server installation and deployment

Consider the following design requirements for Forefront UAG installation and deployment:

 [Deployment scope](#z6)

 [DirectAccess requirements](#z7)

 [Network topology requirements](#z8)

 [Domain and workgroup requirements](#z9)

 [Network and routing requirements](#z10)

  [DNS requirements](#z11)

### Deployment scope

Identifying the deployment scope requires you to identify how many Forefront UAG servers you need, as follows:

1. How many endpoints need to be supported?─By grouping multiple Forefront UAG servers into an array with the same configuration, you increase Forefront UAG capacity for throughput and number of users. Endpoint requests are serviced by all servers in the array; thus, if you deploy an array with three servers, you can support three times as many endpoints as a single Forefront UAG server.

2. What are fault tolerance requirements?─A single Forefront UAG server does not provide fault tolerance. If the server is unavailable, client endpoints cannot connect to portals provided by Forefront UAG trunks. If fault tolerance is required, consider the deployment of a load balanced Forefront UAG array. In an array configuration, each Forefront UAG array member has the same configuration and provides the same service to client endpoints. If one array member fails, the remaining array members are still available and remote endpoints can continue to access sites and portals, via another array member. You can deploy arrays of Forefront UAG servers acting as VPN servers, to provide remote access to corporate applications via Forefront UAG trunks, or deploy arrays of Forefront UAG DirectAccess servers.

3. What are the specific requirements for the corporate access model?─For example, you might need multiple Forefront UAG servers if your organization devolves access management for distributed locations, or corporate policy requires that different groups of clients or applications need a separate access infrastructure.

### DirectAccess requirements

Forefront UAG DirectAccess extends the benefits of Windows DirectAccess across your infrastructure, enhancing scalability, and simplifying deployments and ongoing management. For a complete list of benefits, see Introduction to Forefront UAG DirectAccess design. There are a number of considerations that affect infrastructure design requirements, including:

1. Do you want to deploy Forefront UAG DirectAccess?─DirectAccess deployment requires a number of infrastructure design modifications, including configuration of infrastructure servers, a certification infrastructure, network adapter and routing requirements, and DNS configuration. For a complete list, see Forefront UAG DirectAccess prerequisites.

2. Do you need to use Forefront UAG DirectAccess in addition to publishing remote applications via Forefront UAG?─You can configure both Forefront UAG remote access publishing functionality, and DirectAccess on a single server. The only exception is that you cannot publish the legacy Network Connector application when Forefront UAG is configured as a DirectAccess server.

3. Do you want to deploy multiple DirectAccess servers?─There are a number of infrastructure requirements for deploying an array of DirectAccess servers. For more information, see Configuring a network load balanced array for Forefront UAG DirectAccess.

4. What are your DirectAccess client requirements?─DirectAccess clients must be managed domain computers with specific requirements. For more information, see Forefront UAG DirectAccess prerequisites.

### Network topology requirements

You can determine where Forefront UAG servers or Forefront UAG DirectAccess servers will be located within your organization, by considering the following:

1. Do you want to place Forefront UAG servers behind a frontend firewall?─In this configuration, the Forefront UAG server is placed in the internal network, behind a frontend firewall at the corporate edge. The Forefront UAG server has one network adapter that routes to the frontend firewall, and the other is in the internal network. The advantages and disadvantages are as follows:

a. It is the simplest solution, requiring the least amount of hardware and configuration.

b. It provides a single point of data, as the Forefront UAG server, published servers, and infrastructure servers, are all located within the internal network.

c. It provides a simple configuration for external users who connect via Forefront UAG, and internal users in the internal network can all view the same content.

d. The main disadvantage of this design is that the corporate internal network is separated from the Internet by a single firewall. Note that the Forefront UAG server itself is protected by Forefront TMG running as a firewall on the Forefront UAG server. Forefront TMG is installed by default during Forefront UAG setup.

2. Do you want to place Forefront UAG servers between a frontend firewall and a backend firewall?─In this configuration, the Forefront UAG server is placed in a perimeter network, between a frontend firewall protecting the edge, and a backend firewall protecting the internal network. The advantages and disadvantages are as follows:

a. Intranet content, such as servers published by Forefront UAG, can be isolated in the perimeter network and separated from corporate content that is intended for internal access only.

b. If content in the perimeter network is compromised or corrupted as a result of Internet access, the integrity of the content in the corporate network is retained.

c. If the Forefront UAG server is located in the perimeter network, and published servers or infrastructure servers are located in the internal network, the backend firewall must be configured to let the required protocols and ports through the firewall, so that Forefront UAG can effectively publish backend applications and access infrastructure servers, such as authentication servers, as required.

d. Are you deploying Forefront UAG as a DirectAccess server?─A Forefront UAG DirectAccess server can be located behind a firewall or between a frontend and backend firewall, but note that a public IPv4 address is required, and therefore the server should not be located behind a NAT (Network Address Translation) device.

### Domain and workgroup requirements

A Forefront UAG server can be joined to a domain or workgroup. Consider the following for a domain or workgroup deployment:

1. Do you want to configure Forefront UAG servers in an array?─Array servers must belong to a domain. A server must be joined to a domain before you can add it to an array.

2. Do you want to deploy one or more Forefront UAG DirectAccess servers?─This configuration requires servers to be domain-joined. For exact requirements, see Designing Active Directory for Forefront UAG DirectAccess.

3. Do you want to publish the File Access application via a Forefront UAG trunk?─The Forefront UAG server on which the trunk is configured must be a domain member.

4. Do you want to configure single sign on using Kerberos constrained delegation to forward session credentials to backend published servers requiring authentication?─ The Forefront UAG server must be a domain member.

5. Do you want to provide remote network access using SSTP?─The Forefront UAG server must be a domain member.

### Network and routing requirements

Forefront UAG deployment is highly dependent on correct network configuration, so you should consider the following:

1. Do you want to deploy Forefront UAG to publish remote applications to remote VPN clients?─A Forefront UAG server requires two network adapters, one connected to the internal network and the other connected to the external network (Internet). When you configure the internal network during deployment, it includes any subnets that are included in the internal network. When you define the internal network, you must include all subnets that are reachable from the adapter. Note that clients who connect to the internal network using Remote Network Access will be able to access all subnets reachable through the internal network adapter.

2. Do you want to deploy a Forefront UAG DirectAccess server?─Forefront UAG DirectAccess server requires a number of network adapter and routing prerequisites. For a full list, see Forefront UAG DirectAccess prerequisites.

3. Do you want to allow full VPN access to the internal corporate network?─If you allow client endpoints full VPN access to the internal network using SSTP, or the legacy Forefront UAG Network Connector, you can allocate IP addresses to endpoints from a static pool. You should plan this static pool range and ensure that its addresses are not included in the internal network address range.

###  DNS requirements

When planning for DNS requirements, consider the following:

1. Do you want to publish corporate applications via Forefront UAG trunks and a portal page?─A public DNS server must be able to resolve the portal’s public host name that is specified in the browser of remote endpoints to reach a Forefront UAG portal page.

2. Do you want to deploy a Forefront UAG DirectAccess server?─When deploying Forefront UAG DirectAccess there are a specific set of DNS requirements. For more information, see Designing a DNS infrastructure for Forefront UAG DirectAccess.

3. Do you want to use a specific public host name for an application published via a portal, in addition to the portal public host name?─Forefront UAG supports a new feature that allows you to publish an application using an application-specific host name instead of the portal host name. In order for remote endpoints to reach these applications, a public DNS server must be able to resolve each application-specific host name that you configure. Note that the application-specific host name must resolve to the same IP address as the portal host name.

4. Do you want to publish backend servers and applications via a trunk?─The Forefront UAG server requires internal name resolution to resolve the names and IP addresses of backend published servers, and infrastructure servers such as authentication servers.

5. Do you want to publish SharePoint via a trunk?─Forefront UAG supports alternate access mapping when publishing SharePoint. Alternate access mapping allows you to publish a single SharePoint Web server using multiple different host names. Each SharePoint application on the server is associated with a unique public host name, which is used for remote access to the application. Alternate access mapping requires a public DNS entry for each public host name that might be specified by client endpoints to reach published SharePoint applications.

## Identifying design requirements for client and endpoint deployment

When planning for client scope and endpoint requirements, consider the following:

1. Where are endpoints located?─Forefront UAG supports client access from a wide range of endpoint locations, including connections from managed corporate computers, and from non-managed locations such as partners, Internet kiosks, and mobile devices. The location of endpoints might influence your infrastructure and deployment design. For example, you might need more than one Forefront UAG server if your corporate policy requires endpoints in different locations to access servers in distributed locations, or if policy requires different types of endpoints to use a separate access infrastructure. In addition, if endpoints travel around, this might increase capacity requirements as endpoints appear in multiple locations.

2. What operating systems and browsers are endpoints running?─You must identity endpoint operating systems and browsers in order to know whether Forefront UAG servers support connections from the endpoint. Endpoints running unsupported operating systems and browsers will not be able to connect to Forefront UAG resources. For a list of supported clients, see System requirements for Forefront UAG endpoints.

3. What Forefront UAG features will endpoints access?─Forefront UAG installs endpoint components on endpoints connecting to Forefront UAG portals. Endpoint components are required if you want to implement any of the following:

a. Endpoint detection─Based on the detection results, endpoints are allowed access in line with access policies. Access policies can be inbuilt Forefront UAG access policies, or Network Access Protection (NAP policies downloaded from a Network Policy Server (NPS). Detection is provided by the Endpoint Detection component.

b. Endpoint session cleanup─Cleanup deletes persistent data that is downloaded to an endpoint from Forefront UAG, or created by a client endpoint browser, when a Forefront UAG session ends, when the user logs off, when a scheduled logoff occurs, or when an unscheduled power outage or computer restart occurs. Cleanup functionality is provided by the Endpoint Session Cleanup component.

c. Non-Web publishing─If you want to provide remote access to non-Web applications. Non-Web applications might require one or more of the following components: SSL Application Tunneling component, SSL Network Tunneling component, or Socket Forwarding component.

Endpoint components are not required for the following:

a. Remote access to Web applications.

b. Remote access to Outlook Anywhere (RPC-over\_HTTP).

c. Remote access to Exchange ActiveSync.

d. Remote access to Remote Desktop Services (RDS) RemoteApps.

e. Forefront UAG DirectAccess.

4. Are you deploying Forefront UAG DirectAccess?─You use Group Policy as an object-based method to create, distribute, and apply DirectAccess settings to DirectAccess clients. For a list of requirements for Forefront UAG DirectAccess client requirements, see Forefront UAG DirectAccess prerequisites. For information about client deployment, see Configuring clients for Forefront UAG DirectAccess.

## Identifying design requirements for endpoint access control

Depending on the client endpoint access mechanisms that you want to deploy, there are a number of infrastructure design considerations, as follows:

1. Do you want to authenticate clients before allowing them to access Forefront UAG portals?─When client authentication is required, Forefront UAG receives an authentication request from each Forefront UAG client that attempts to access the portal application. Forefront UAG then queries an authentication server to verify client credentials. Authenticating clients at the Forefront UAG gateway ensures that only authenticated client requests are passed to backend corporate servers and applications. Forefront UAG can use a variety of authentication mechanisms. For more information, see Planning for client endpoint authentication. Implementing client authentication requires you to set up an authentication infrastructure before deploying Forefront UAG. If you do not enable client authentication on the Forefront UAG server, Forefront UAG uses passthrough, and authentication takes place on backend servers only.

2. Do you want to pass client credentials to backend published applications that require authentication?─Forefront UAG allows you to implement a single sign-on mechanism that passes credentials provided during session authentication to backend servers using basic authentication (HTTP 401), an HTML form, Kerberos constrained delegation, or Active Directory Federation Services (ADFS).

To use Kerberos the following is required:

a. Forefront UAG servers must belong to a domain.

b. You must define at least one authentication server for the trunk to which the application belongs.

c. All domain controllers in the internal network must be computers running Windows Server 2008 or Windows Server 2003.

d. Authenticating clients must be part of the same Active Directory forest as the Forefront UAG server and the application servers.

e. Forefront UAG servers and the application servers must be part of the same domain.

To use ADFS the following is required:

a. Forefront UAG servers must belong to a domain.

b. An AD FS server must be deployed.

c. Active Directory must be used for authentication.

d. Forefront UAG requires a certificate that is trusted by endpoints because AD FS-enabled applications can only be published in an HTTPS trunk.

3. Do you want to verify the health of endpoints before allowing access to portals and published applications?─Using Forefront UAG, you can verify endpoint settings against predefined access policies, and allow or restrict access based on endpoint compliance. You can use predefined or custom inbuilt Forefront UAG access policies, or download Network Access Protection (NAP) policies. Setting up Forefront UAG access policies does not require any specific infrastructure changes. Setting up NAP policies requires the deployment of a Network Policy Server (NPS) in your corporate infrastructure. The NPS can be co-located on the Forefront UAG server.

4. Do you want to limit access to individual portal applications to specific users and groups?─Forefront UAG allows you to configure portal authorization to control access to portal applications. You use users and groups that are configured on authentication servers in order to implement authorization. An authentication server is required in the corporate infrastructure to do this.

5. Do you want to differentiate between endpoints and allow some endpoints privileged access?─Forefront UAG provides a certified endpoint feature for clients that connect over HTTPS to a portal. Certified endpoints are defined as privileged, and you can specify a more permissive access policy for these privileged endpoints. To deploy certified endpoints, a certification authority (CA) is required to issue client certificates to endpoints.

## Identifying design requirements for application publishing

Using Forefront UAG, you publish corporate applications and resources via a Forefront UAG trunk. Remote endpoints then access publishing applications and resources via a Forefront UAG portal Web page. The types of corporate applications that you want to publish will affect infrastructure planning, as follows:

1. Do you want to publish Web applications only?─If you want to publish Web applications only, endpoint components are not required for these applications. If you are publishing non-Web applications such as client/server and legacy applications, the File Access application, or Remote Network Access, endpoints require components to be installed in order to access these applications. Endpoints must meet system requirements for component installation. For more information, see System requirements for Forefront UAG endpoints.

2. Do you want endpoints to connect to portals over a secure HTTPS connection?─If endpoints connect using HTTPS, the Forefront UAG server must be able to present a server certificate that is trusted by connecting endpoints.

3. Do you want to publish the inbuilt File Access and Local Drive Mapping applications?─These applications provide remote access to internal file servers and shares. To publish these applications, Forefront UAG must be installed as a domain member.

4. Do you want to publish the inbuilt Remote Network Access application, in order to allow remote clients to access the entire internal network?─You can provide remote network access using the inbuilt Network Connector application, or SSTP.

a. To provide remote access using the inbuilt Network Connector application, you need a pool of IP addresses that are excluded from the internal network to assign to connecting VPN clients.

b. To use SSTP, you either need a pool of IP addresses that are excluded from the internal network to assign to connecting VPN clients, or a DHCP server set up to allocate addresses to connecting VPN clients. In addition, any clients must conform to SSTP requirements. For more information, see Setting up Remote Network Access.

5. Do you want to connect from the Forefront UAG server to backend published applications and servers over a secure connection?─If you want to use an HTTPS connection, the published server must have a server certificate that is trusted by the Forefront UAG server.

## Identifying design requirements for logging and monitoring

Forefront UAG can record system information and alerts, and user activity. These can be used proactively to ensure operations are running correctly, and during troubleshooting. Information can be logged in a number of formats, including logging to a built-in reporter that can be used with Forefront UAG Web Monitor, logging to a RADIUS accounting server, or a remote Syslog server. You can also use SMTP logging to send logged events to an email address. Forefront UAG can also use the Forefront TMG logging mechanism to log events to a SQL Server database. Events can be logged to a local SQL Server Express database running on the Forefront UAG server, or to a remote SQL Server.

Infrastructure design considerations include the following:

 What type of information do you want to log?─For information about SQL Server fields that can be logged, see SQL Server logging fields.

 Do you want to log to a remote SQL Server database?─You must configure a SQL Server database in your infrastructure. If fault tolerance is required, a remote SQL Server database can be placed in a Microsoft failover cluster.

 Do you want to monitor Forefront UAG activity with Systems Center Operations Manager (SCOM)?─You must have a SCOM server deployed in your organization, and you must deploy the Forefront UAG SCOM pack.

## Next steps in planning your infrastructure design

[Identifying your infrastructure deployment goals](#zb11dbdc1079144e1986252ee6efb71a6).

# Identifying your infrastructure deployment goals

After you have identified your infrastructure design requirements for each stage of the Forefront Unified Access Gateway (UAG) deployment, you must evaluate your specific deployment goals, and clearly pinpoint infrastructure modifications that are required to meet each goal. Depending on the size of your organization, this might involve multiple IT staff, in addition to the Forefront UAG administrator. Use this guide to help each person involved to identify the shifts that are required in the existing infrastructure, in order to deploy Forefront UAG successfully.

For information on identifying your infrastructure design requirements, see [Identifying your infrastructure design requirements](#z2003740048754fc482250a0c9e14acd7).

The following table summarizes the possible deployment goals and provides an overview of the infrastructure modifications required for each goal.

|  |  |
| --- | --- |
| Deployment goal | Infrastructure modifications |
| Deploy a single Forefront UAG server | This goal requires you to deploy and install a single Forefront UAG server in your existing network infrastructure. Infrastructure design modifications include:1. Placing the Forefront UAG server into your corporate topology, and configuring any corporate firewalls to allow traffic to and from the Forefront UAG server.2. Adding the Forefront UAG server to a domain or a workgroup.3. Configuring network addressing and routing.4. Configuring internal and external DNS servers. |
| Deploy multiple Forefront UAG servers | This goal requires you to deploy and install multiple Forefront UAG servers in your existing network infrastructure. Infrastructure design modifications include:1. Placing the Forefront UAG servers into your corporate topology, and configuring any corporate firewalls to allow traffic to and from the Forefront UAG server.2. Adding the Forefront UAG servers.3. Configuring network addressing and routing.4. Configuring internal and external DNS servers. |
| Deploy a single Forefront UAG DirectAccess server | This goal requires you to deploy and install a single Forefront UAG server in your existing network infrastructure, and configure the Forefront UAG server as a DirectAccess server. Infrastructure design modifications include:1. Placing the Forefront UAG DirectAccess server into your corporate topology, and configuring any corporate firewalls to allow traffic to and from the Forefront UAG DirectAccess server.2. Configuring domain settings.3. Configuring network addressing and routing.4. Deploying and configuring a certificate infrastructure.5. Configuring DNS servers.6. Setting up your infrastructure for a load balancing solution. |
| Deploy multiple Forefront UAG DirectAccess servers | This goal requires you to deploy and install multiple Forefront UAG servers in your existing network infrastructure, and configure the Forefront UAG server as a DirectAccess server. Infrastructure design modifications include:1. Placing the Forefront UAG DirectAccess server into your corporate topology, and configuring any corporate firewalls to allow traffic to and from the Forefront UAG DirectAccess server.2. Configuring domain settings.3. Configuring network addressing and routing for an array deployment.4. Deploying and configuring a certificate infrastructure.5. Configuring DNS servers.6. Setting up your infrastructure for a load balancing solution. |
| Deploy Forefront UAG Forefront UAG endpoints | This goal includes allowing remote endpoints to access corporate applications and resources via Forefront UAG. You can install Forefront UAG endpoint components online when clients connect to a trunk, or offline using the Forefront UAG Client Components installer or an installation file. Infrastructure design modifications include:1. Ensure that managed endpoints that will connect to Forefront UAG are running an operating system and browser that allows them to access published applications.2. Ensure that managed endpoints have the correct permissions, and Internet Explorer settings to enable the installation of components in online or offline mode. |
| Authenticate clients for access to Forefront UAG portals and published applications | This goal requires you to configure front end authentication to verify the credentials of clients connecting to Forefront UAG portal and site sessions. If the backend published servers require authentication, it also requires you to set up authentication mechanisms for verifying client credentials on backend servers. In addition, Forefront UAG supports single sign-on, allowing you to pass credentials supplied during session sign-on to backend servers, thus requiring clients to sign on only once. The following infrastructure design modifications are required:1. Set up a client authentication infrastructure.2. If you want to implement single sign-on using Kerberos constrained delegation, configure the Kerberos infrastructure.3. If you want to use Active Directory Federation Services (ADFS), deploy an ADFS server.  |
| Verify the health of endpoints connecting to Forefront UAG | Forefront UAG can verify the health of endpoints against inbuilt Forefront UAG access policies, or against Network Access Protection policies downloaded from a Network Policy Server (NPS). In addition to access policies, you can also implement granular authorization policies applications and resources published in a portal, by allowing only authorized users and groups to access specific portal applications. The following infrastructure design modifications are required:1. If you want to use NAP policies for endpoint health checking, set up and configure NPS servers.2. To set up certified endpoints, a certification authority (CA) is required to issue client certificates to endpoints. You can set up the CA remotely, or locally on the Forefront UAG server. |
| Limit application access to specific users and groups | This goal requires you to configure portal authorization to control access to portal applications. The following infrastructure design modifications are required:1. Set up an authentication server so that you can use users and groups for portal authorization.2. Set up users and groups on the authentication server. |
| Differentiate between different types of endpoints, and define some endpoints as privileged | This goal requires to configure endpoints as certified, and assign them a more permissive access policy. The following infrastructure design modifications are required: Certified endpoints use a client certificate for certification and identification. You must have a certification authority set up either locally on the Forefront UAG server, or remotely, in order to deploy certificates to clients. |
| Publish internal applications and resources via Forefront UAG | This goal requires you to set up Forefront UAG trunks. Using trunks, you can create a Forefront UAG portal or a Web site for accessing a single Web application. After creating a portal trunk, you add applications and resources to it, in order to publish them via the trunk. Infrastructure design modifications include:1. If you want endpoints to access Forefront UAG portals or sites over an HTTPS connection, the Forefront UAG server or array members hosting the site must have a server certificate to present to endpoints connecting over HTTPS.2. If there is an HTTPS connection between the Forefront UAG server and the backend published servers, server certificates are required on backend servers to authenticate the HTTPS connection.3. If you want to publish Remote Desktop Services (RDS), ensure that endpoints comply with system requirements.4. If you want to publish File Access and Local Drive Mapping applications, ensure that Forefront UAG servers belong to a domain. |
| Log Forefront UAG information | There are a number of logging options that include the following infrastructure modification: Set up a logging server. If you do not use the Forefront UAG inbuilt logging reporter, you can log to a Syslog server, a RADIUS accounting server, an SMTP server, or a local or remote SQL Server. |
| Monitor Forefront UAG activity | If you have Systems Center Operations Manager (SCOM) deployed in your organization, configure the Forefront UAG SCOM pack. |

## Next steps in planning your infrastructure design

[Mapping your deployment goals to an infrastructure design](#zf8f7f8bb7239461c8ced914a6d6095b5)

# Mapping your deployment goals to an infrastructure design

After you have planned your network infrastructure, and identified your deployment goals, use the following table to select an infrastructure design that meets each of your deployment objectives.

For information on planning your network infrastructure, see [Identifying your infrastructure design requirements](#z2003740048754fc482250a0c9e14acd7). For information on identifying your deployment goals, see [Identifying your infrastructure deployment goals](#zb11dbdc1079144e1986252ee6efb71a6).

|  |  |
| --- | --- |
| Deployment goal | Infrastructure design guide |
| Deploy a single Forefront UAG server | [Single server infrastructure design](#ze9a9d268d81541839708607afaa24c52) |
| Deploy multiple Forefront UAG servers | [Multiple server infrastructure design](#zc295f95b7e6c40efb4a285596df11029) |
| Deploy a single Forefront UAG DirectAccess server | [Single Forefront UAG DirectAccess server infrastructure design](#zbc185d2a10a6453ba5374a21315c8bdf) |
| Deploy multiple Forefront UAG DirectAccess servers | [Multiple Forefront UAG DirectAccess server infrastructure design](#z494bd341364047a18dfb24c28fddcf20) |
| Deploy Forefront UAG components on remote endpoints, so that endpoints can access Forefront UAG sites and resources and applications published via Forefront UAG | [Endpoint component infrastructure design](#za1f3c1eb29ea4d548d34e86aa86196e1) |
| Control endpoint access by authenticating clients connecting to Forefront UAG sites and published applications | [Client authentication infrastructure design](#za647039c8bb648739995774809bbb39d) |
| Control endpoint access by verifying the health of endpoints connecting to Forefront UAG, and ensure that endpoints comply with Forefront UAG access policies | [Endpoint health checking infrastructure design](#z3228e4a24c0442078eea7f5bb6af0841) |
| Control endpoint access by limiting application access to authorized users and groups | [Application authorization infrastructure design](#zb91e3fcbbf1f4fcfa4a34bee9c8ca0e1) |
| Control endpoint access by configuring some endpoints as privileged and allowing them a different level of access | [Privileged (certified) endpoint infrastructure design](#zb3cc82c80ce14550b51b40c9a3c39ff5) |
| Publish internal applications and resources via Forefront UAG, so that remote endpoints can access these applications and resources | [Application publishing infrastructure design](#zd777a6603f0941acb89141313d9dfed9) |
| Log and monitor Forefront UAG traffic | [Logging and monitoring infrastructure design](#z9f36e356ef554fa38d2a810b5f06d1ef) |

# Single server infrastructure design

This topic is designed to help you understand the infrastructure design required for deploying a single Forefront Unified Access Gateway (UAG) server.

This deployment has the following infrastructure design requirements:

 [Selecting a topology location for the Forefront UAG server](#z13)

 [Joining the Forefront UAG server to a domain or a workgroup](#z14)

 [Configuring network addressing and routing](#z15)

 [Configuring DNS servers and settings](#z16)

## Selecting a topology location for the Forefront UAG server

The most common topology locations for a Forefront UAG server are:

 Behind a frontend firewall─The Forefront UAG server is placed in the internal network, behind a frontend firewall at the corporate edge. The Forefront UAG server has one network adapter that routes to the frontend firewall, and the other is in the internal network.

 Between a frontend firewall and a backend firewall─The Forefront UAG server is placed in a perimeter network, between a frontend firewall protecting the edge, and a backend firewall protecting the internal network.

If Forefront UAG is located behind an edge or perimeter firewall, verify that the required ports and protocols are open on the firewall, as follows:

### Behind a frontend firewall

There are advantages and disadvantages to placing the Forefront UAG server behind the frontend firewall, as follows:

1. It is the simplest solution, requiring the least amount of hardware and configuration.

2. It provides a single point of data, as the Forefront UAG server, published servers, and infrastructure servers are all located within the internal network.

3. It provides a simple configuration for external users who connect via Forefront UAG, and internal users in the internal network can all view the same content.

4. The main disadvantage of this design is that the corporate internal network is separated from the Internet by a single firewall. Note that the Forefront UAG server itself is protected by Forefront TMG running as a firewall on the Forefront UAG server. Forefront TMG is installed by default during Forefront UAG setup.

If the Forefront UAG server is located behind a frontend firewall, the firewall must be configured to allow the following traffic through to the Forefront UAG server:

 HTTP traffic (port 80)

 HTTPS traffic (port 443)

### Between a frontend firewall and a backend firewall

There are advantages and disadvantages to placing the Forefront UAG server between a frontend and backend firewall, as follows:

1. Intranet content, such as servers published by Forefront UAG, can be isolated in the perimeter network and separated from corporate content intended for internal access only.

2. If content in the perimeter network is compromised or corrupted as a result of Internet access, the integrity of the content in the corporate network is retained.

3. If the Forefront UAG server is located in the perimeter network, and published servers or infrastructure servers are located in the internal network, the backend firewall must be configured to let the required protocols and ports through the firewall, so that Forefront UAG can effectively publish backend applications and access infrastructure servers, such as authentication servers, as required.

To allow remote endpoints to access the Forefront UAG server located in a perimeter network behind a frontend firewall, the following traffic must be allowed through the frontend firewall:

 HTTP traffic (port 80)

 HTTPS traffic (port 443)

#### Configuring the backend firewall

Configuration of the backend firewall depends upon where backend servers publishing via Forefront UAG are located, and on the location of infrastructure servers, such as Active Directory and authentication servers, used by Forefront UAG. If published backend servers are located in the internal network, allow the following traffic through the backend firewall:

 HTTP traffic (port 80)

 HTTPS traffic (port 443)

If infrastructure servers are located in the internal network, some of the following may be required, depending upon the authentication methods used by Forefront UAG:

|  |  |  |
| --- | --- | --- |
| Infrastructure server | Protocol | Port |
| Domain controller | Microsoft-DS traffic | TCP 445UDP 445 |
|  | Kerberos authentication | TCP 88UDP 88 |
|  | LDAP | TCP 389UDP 389 |
|  | LDAPS | TCP 636UDP 636 |
|  | LDAP to GC | TCP 3268UDP 3268 |
|  | LDAPS to GC | TCP 3269UCP 3269 |
|  | DNS | TCP 53UDP 53 |
| RADIUS server | RADIUS port | UDP 1645 or 1812 |
| SecureID ACE | SecurID ACE port | UJDP 5500 |

## Joining the Forefront UAG server to a domain or a workgroup

The Forefront UAG server can be configured as a member of a domain or a workgroup.

Forefront UAG must be a domain member in the following scenarios:

1. If you want to add the server to an array of Forefront UAG servers at a later date.

2. If you want to configure the server as a Forefront UAG DirectAccess server at a later date.

3. If you want to deploy single sign on using Kerberos constrained delegation to forward session credentials to backend published servers requiring authentication.

Forefront UAG can be deployed in a domain as follows:

1. In an existing domain.

2. Create a domain for the Forefront UAG server. Set up a one-way or two-way trust between the Forefront UAG server domain and the main corporate domain.

For information about joining a domain, see [How to join your computer to a domain](http://go.microsoft.com/fwlink/?LinkId=179039) (http://go.microsoft.com/fwlink/?LinkId=179039). For information about creating a domain, see [Creating a domain design](http://go.microsoft.com/fwlink/?LinkId=179040) (http://go.microsoft.com/fwlink/?LinkId=179040). For information about setting up trusts, see, [Checklist: Creating a forest trust](http://go.microsoft.com/fwlink/?LinkId=179041) (http://go.microsoft.com/fwlink/?LinkId=179041).

For all other scenarios, Forefront UAG can be installed as part of a workgroup. If the Forefront UAG server is a member of a workgroup, a DNS suffix must be defined for the workgroup.

## Configuring network addressing and routing

Network addressing and routing requirements for deploying a single Forefront UAG server include the following:

1. Forefront UAG deployment is highly dependent on correct network configuration. When you configure the internal network during deployment, it will include any subnets that are included in the internal network. When you define the internal network, you must include all subnets that are reachable from the adapter. Note that clients who connect to the internal network using a VPN client connection (Forefront UAG SSL network tunneling) will be able to access all subnets reachable through the internal network adapter.

## Configuring DNS servers and settings

DNS infrastructure requirements when deploying a Forefront UAG server include the following:

1. A public DNS server must be able to resolve the public host name specified by remote endpoints to reach Forefront UAG sites that you create on the Forefront UAG server.

2. The Forefront UAG server requires internal name resolution to resolve the names and IP addresses of backend published servers, and infrastructure servers such as authentication servers.

3. Forefront UAG supports alternate access mapping when publishing SharePoint. Alternate access mapping allows you to publish a single SharePoint Web server using multiple different host names. Each SharePoint application on the server is associated with a unique public host name, which is used for remote access to the application. Alternate access mapping requires a public DNS entry for each public host name that might be specified by client endpoints to reach published SharePoint applications.

4. Forefront UAG supports a new feature that allows you to publish an application using an application-specific host name instead of the portal host name. In order for remote endpoints to reach these applications, a public DNS server must be able to resolve each application-specific host name that you configure. Note that the application-specific host name must resolve to the same IP address as the portal host name.

# Multiple server infrastructure design

This topic is designed to help you understand the infrastructure design required for deploying multiple Forefront Unified Access Gateway (UAG) servers. Multiple Forefront UAG servers can be joined together into an array, in which all array members share the same configuration and settings. An array deployment allows you to scale Forefront UAG capacity and provide high availability to remote endpoints that connect to Forefront UAG portals and sites. In addition, you can load balance traffic between array members, thus providing failover for connecting endpoints.

This deployment has the following infrastructure design requirements:

 [Selecting a topology location for the Forefront UAG server](#z17)

 [Joining the Forefront UAG server to a domain or workgroup](#z18)

 [Configuring network addressing and routing](#z19)

 [Configuring DNS servers and settings](#z20)

 [Configuring the array infrastructure](#z21)

## Selecting a topology location for the Forefront UAG server

The most common topology locations for Forefront UAG servers are:

 Behind a frontend firewall─The Forefront UAG server is placed in the internal network, behind a frontend firewall at the corporate edge. The Forefront UAG server has one network adapter that routes to the frontend firewall, and the other is in the internal network.

 Between a frontend firewall and a backend firewall─The Forefront UAG server is placed in a perimeter network, between a frontend firewall protecting the edge, and a backend firewall protecting the internal network.

If Forefront UAG is located behind an edge or perimeter firewall, verify that the required ports and protocols are open on the firewall, as described in the table below.

### Behind a frontend firewall

There are advantages and disadvantages to placing the Forefront UAG server behind the frontend firewall, as follows:

1. It is the simplest solution, requiring the least amount of hardware and configuration.

2. It provides a single point of data, as the Forefront UAG server, published servers, and infrastructure servers are all located within the internal network.

3. It provides a simple configuration for external users who connect via Forefront UAG, and internal users in the internal network can all view the same content.

4. The main disadvantage of this design is that the corporate internal network is separated from the Internet by a single firewall. Note that the Forefront UAG server itself is protected by Forefront TMG running as a firewall on the Forefront UAG server. Forefront TMG is installed by default during Forefront UAG setup.

If the Forefront UAG server is located behind a frontend firewall, the firewall must be configured to allow the following traffic through to the Forefront UAG server:

 HTTP traffic (port 80)

 HTTPS traffic (port 443)

### Between a frontend firewall and a backend firewall

There are advantages and disadvantages to placing the Forefront UAG server between a frontend and backend firewall, as follows:

1. Intranet content, such as servers published by Forefront UAG, can be isolated in the perimeter network and separated from corporate content intended for internal access only.

2. If content in the perimeter network is compromised or corrupted as a result of Internet access, the integrity of the content in the corporate network is retained.

3. If the Forefront UAG server is located in the perimeter network, and published servers or infrastructure servers are located in the internal network, the backend firewall must be configured to let the required protocols and ports through the firewall, so that Forefront UAG can effectively publish backend applications, and access infrastructure servers, such as authentication servers, as required.

To allow remote endpoints to access the Forefront UAG server located in a perimeter network behind a frontend firewall, the following traffic must be allowed through the frontend firewall:

 HTTP traffic (port 80)

 HTTPS traffic (port 443)

#### Configuring the backend firewall

Configuration of the backend firewall depends upon where the backend servers publishing via Forefront UAG are located, and on the location of infrastructure servers, such as Active Directory and authentication servers, used by Forefront UAG. If published backend servers are located in the internal network, allow the following traffic through the backend firewall:

 HTTP traffic (port 80)

 HTTPS traffic (port 443)

If infrastructure servers are located in the internal network, some of the following may be required depending upon the authentication methods used by Forefront UAG:

|  |  |  |
| --- | --- | --- |
| Infrastructure server | Protocol | Port |
| Domain controller | Microsoft-DS traffic | TCP 445UDP 445 |
|  | Kerberos authentication | TCP 88UDP 88 |
|  | LDAP | TCP 389UDP 389 |
|  | LDAPS | TCP 636UDP 636 |
|  | LDAP to GC | TCP 3268UDP 3268 |
|  | LDAPS to GC | TCP 3269UCP 3269 |
|  | DNS | TCP 53UDP 53 |
| RADIUS server | RADIUS port | UDP 1645 or 1812 |
| SecureID ACE | SecurID ACE port | UJDP 5500 |

## Joining the Forefront UAG server to a domain or workgroup

Each Forefront UAG server that you want to join to an array must be installed as a domain member, as follows:

1. All array members must belong to the same domain.

2. You can install Forefront UAG servers in an existing domain.

3. Alternatively, you can create a domain for Forefront UAG servers. Then set up a one-way or two-way trust between the Forefront UAG server domain and the main corporate domain.

For information about joining a domain, see [How to join your computer to a domain](http://go.microsoft.com/fwlink/?LinkId=179039) (http://go.microsoft.com/fwlink/?LinkId=179039). For information about creating a domain, see [Creating a domain design](http://go.microsoft.com/fwlink/?LinkId=179040) (http://go.microsoft.com/fwlink/?LinkId=179040). For information about setting up trusts, see, [Checklist: Creating a forest trust](http://go.microsoft.com/fwlink/?LinkId=179041) (http://go.microsoft.com/fwlink/?LinkId=179041).

## Configuring network addressing and routing

Network addressing and routing requirements for deploying an array of Forefront UAG servers include the following:

1. Forefront UAG deployment is highly dependent on the correct network configuration. When you configure the internal network during deployment, it includes any subnets that are included in the internal network. When you define the internal network you must include all subnets that are reachable from the adapter. Note that clients who connect to the internal network using a VPN client connection (Forefront UAG SSL network tunneling) will be able to access all subnets reachable through the internal network adapter.

## Configuring DNS servers and settings

DNS infrastructure requirements when deploying a Forefront UAG server include the following:

1. A public DNS server must be able to resolve the public host name specified by remote endpoints to reach Forefront UAG sites that you create on the Forefront UAG server. If you are load balancing an array using a VIP, the public host name must resolve to the VIP.

2. The Forefront UAG server requires internal name resolution to resolve the names and IP addresses of backend published servers, and infrastructure servers, such as authentication servers.

3. Forefront UAG supports alternate access mapping when publishing SharePoint. Alternate access mapping allows you to publish a single SharePoint Web server using multiple different host names. Each SharePoint application on the server is associated with a unique public host name, which is used for remote access to the application. Alternate access mapping requires a public DNS entry for each public host name that might be specified by client endpoints to reach published SharePoint applications.

4. Forefront UAG supports a new feature that allows you to publish an application using an application-specific host name instead of the portal host name. In order for remote endpoints to reach these applications, a public DNS server must be able to resolve each application-specific host name that you configure. Note that the application-specific host name must resolve to the same IP address as the portal host name.

## Configuring the array infrastructure

The infrastructure requirements for deploying a Forefront UAG array include the following:

1. If you want to use a hardware load balancer for balancing endpoint requests to array members, ensure that it is set up before array deployment.

2. In a Forefront UAG array, one of the array members acts as the array manager and holds the configuration for all array members. The array manager requires a user account that is used when it communicates internally with array members. Before deploying an array, ensure you have a domain account that is recognized by all the Forefront UAG servers you will deploy in the array, and that it has local administrator permissions on all Forefront UAG computers that you will add to the array. It should be an account with a long expiry period.

# Single Forefront UAG DirectAccess server infrastructure design

Forefront Unified Access Gateway (UAG) DirectAccess extends the benefits of Windows DirectAccess across your infrastructure, enhancing scalability, and simplifying deployments and ongoing management. Forefront UAG DirectAccess gives remote users the experience of being seamlessly connected to your internal network any time you have Internet access. Following the installation of Forefront UAG, you can configure a Forefront UAG server to act as a Forefront UAG DirectAccess server.

The infrastructure design requirements for deploying Forefront UAG DirectAccess include the following:

1. A domain controller running Windows Server 2003 or Windows Server 2008.

2. A DNS server running Windows Server 2008 is recommended.

3. A certificate infrastructure.

4. Requirements for DirectAccess client deployment.

5. Active Directory group requirements.

6. Network and routing requirements, including IPv4 and IPv6 considerations.

7. Protocol and port configuration for firewalls located in front of DirectAccess servers.

For a detailed list of infrastructure requirements for deploying Forefront UAG DirectAccess, see Forefront UAG DirectAccess prerequisites.

# Multiple Forefront UAG DirectAccess server infrastructure design

Forefront Unified Access Gateway (UAG) DirectAccess extends the benefits of Windows DirectAccess across your infrastructure, enhancing scalability, and simplifying deployments and ongoing management. Forefront UAG DirectAccess gives remote users the experience of being seamlessly connected to your internal network any time you have Internet access. Following the installation of Forefront UAG, you can configure a Forefront UAG server to act as a Forefront UAG DirectAccess server. In addition, multiple Forefront UAG servers can be gathered into an array to provide scalability and high availability. Traffic can be load balanced across array members, providing failover for remote endpoint requests.

The infrastructure design requirements for deploying an array of Forefront UAG DirectAccess servers include the following:

1. A domain controller running Windows Server 2003 or Windows Server 2008.

2. A DNS server running Windows Server 2008 is recommended.

3. A certificate infrastructure.

4. Requirements for DirectAccess client deployment.

5. Active Directory group requirements.

6. Protocol and port configuration for firewalls located in front of DirectAccess servers.

7. Network and routing requirements for an array deployment.

For a detailed list of infrastructure requirements for deploying Forefront UAG DirectAccess, see Forefront UAG DirectAccess prerequisites.

For information about network and routing requirements for an array deployment, see Configuring a network load balanced array for Forefront UAG DirectAccess.

For information about infrastructure requirements for a hardware load balancer, see Configuring a network load balanced array for Forefront UAG DirectAccess.

# Endpoint component infrastructure design

In order for remote endpoints to connect to internal resources and applications published via Forefront Unified Access Gateway (UAG), Forefront UAG components must be installed on the endpoints, either offline or online via the client browser.

This deployment has the following infrastructure requirements:

1. Remote endpoints may be managed or unmanaged. Ensure that managed endpoints meet the operating system and browser requirements. For more information, see System requirements for Forefront UAG endpoints.

2. Ensure that managed endpoints have the correct permissions, and Internet Explorer settings in order to install components in online or offline mode. For more information, see Allowing Allowing remote client access.

# Client authentication infrastructure design

Forefront Unified Access Gateway (UAG) controls access to internal applications and resources that are published via Forefront UAG, using client authentication.

Client authentication requires you to configure frontend authentication to verify the credentials of clients that connect to Forefront UAG portal and site sessions. If backend published servers require authentication, you must also set up authentication mechanisms for verifying client credentials on the backend servers. In addition, Forefront UAG supports single sign-on, which allows you to pass credentials supplied during session sign-on to the backend servers.

1. You can implement frontend authentication to ensure that remote clients authenticate before establishing sessions to Forefront UAG sites and portal.

2. In addition, you can require client authentication to published backend servers as follows:

a. Use passthrough authentication so that clients authenticate on backend servers only.

b. You can implement single sign-on so that clients need only specify credentials once by passing session credentials to backend servers using basic authentication (HTTP 401), an HTML form, Kerberos constrained delegation, or Active Directory Federation Services (ADFS).

The following infrastructure design is required for client authentication:

1. Authentication servers, to verify client credentials during frontend and backend authentication. For more information, see the Endpoint access design guide.

2. If you want to implement single sign-on using Kerberos constrained delegation, a Kerberos infrastructure must be configured. For more information, see Configuring single sign-on with Kerberos constrained delegation.

3. If you want to use Active Directory Federation Services (ADFS), an ADFS server must be deployed. For more information, see Deploying federation with AD FS.

# Endpoint health checking infrastructure design

When remote endpoints request resources or applications that are published by Forefront Unified Access Gateway (UAG), Forefront UAG can verify the health of the endpoints against specific policies. These include:

1. Inbuilt policies─Inbuild Forefront UAG policies allow you to control endpoint access based on a wide range of compliance requirements, including the endpoint operating system or browser, and the endpoint location. Using these policies, you can control access to applications, application uploads and downloads, and restrictive application areas.

2. Network Access Protection (NAP) policies─You can check endpoint health against NAP policies downloaded from a Network Policy Server (NPS).

No infrastructure modifications are required to deploy inbuilt policies. To use NAP policies, you must set up an NPS in your network infrastructure. For more information, see Configuring NAP.

# Application authorization infrastructure design

When you create a Forefront Unified Access Gateway (UAG) trunk, by default all users that access the trunk successfully can access all applications published via the trunk. For more granular control, you can configure application authorization, which limits access to the application to specific users and groups. This design has the following infrastructure design requirements:

1. Set up an authentication server so that you can use its users and groups for portal authorization. For instructions, see Deploying frontend authentication servers.

# Privileged (certified) endpoint infrastructure design

Forefront Unified Access Gateway (UAG) provides a certified endpoint feature for clients that connect over HTTPS to a Forefront UAG site or portal. Certified endpoints are defined as privileged, and you can specify a more permissive access policy for them. This feature has the following infrastructure requirements:

1. Deploy a certification authority (CA) to issue client certificates to endpoints.

2. You can set up the CA remotely or locally on the Forefront UAG server. For information about setting up a CA, see Implementing certified endpoints.

# Application publishing infrastructure design

Using Forefront Unified Access Gateway (UAG), you publish internal applications and resources by means of Forefront UAG trunks. Each trunk has a portal Web page, and remote endpoints connect to the portal over an HTTP or HTTPS connection. The following infrastructure design tasks are required when setting up a trunk, and publishing applications via the trunk:

1. When you create a trunk, you specify whether remote endpoints should connect to the trunk site or portal over an HTTP or HTTPS connection. If you want a remote endpoint to connect to trunks over an HTTPS connection, you must have an infrastructure for requesting a server certificate from a public certification authority (CA). Usually a public certificate will be required because client endpoints might be managed or unmanaged, and the endpoint must trust the CA that issued the certificate.

2. In addition, when you create a trunk you specify whether the connection between the Forefront UAG server and backend published servers is over HTTP or HTTPS. If you want to use an HTTPS connection, the backend server must have a server certificate in order to authenticate the HTTPS connection to the Forefront UAG server. This will usually be a certificate issued by an internal CA, because only the Forefront UAG server is required to trust it.

# Logging and monitoring infrastructure design

Forefront Unified Access Gateway (UAG) can log to a number of formats, including an inbuilt reporter, a RADIUS server, a Syslog server, an SMTP server, and SQL Server. You can also monitor Forefront UAG events using Systems Center Operations Manager (SCOM). The following infrastructure modifications might be required.

1. If you want to log to RADIUS, you must deploy a RADIUS accounting server, either remotely or running on the Forefront UAG server.

2. To log to Syslog, you must have an industry-standard Syslog server deployed in your organization.

3. To send email messages, you must have an SMTP server deployed.

4. Forefront UAG uses Forefront TMG functionality to enable SQL Server logging (Forefront TMG is automatically installed during Forefront UAG setup). For local SQL Server logging, you can log to the local instance of SQL Server Express that is installed automatically during Forefront UAG setup. No infrastructure changes are required. To log to a remote SQL Server, you must have SQL Server deployed in your organization. For instructions on remote SQL Server deployment, see  [Setting up SQL Server for logging](http://technet.microsoft.com/en-us/library/bb794867.aspx), in the Forefront TMG TechNet library.

5. To monitor Forefront UAG using SCOM, you must have an Operations Manager 2007 server deployed in your organization. For more information, see Monitoring with System Center Operations Manager (SCOM)