

Infrastructure Planning
and Design

DirectAccess

Version 1.3

Published: October 2009

Updated: November 2011

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

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

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

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

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

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

Microsoft, Active Directory, Forefront, Hyper-V, Windows, Windows Server, and Windows Vista 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](#_Toc299515795)

[Introduction to the DirectAccess Guide 2](#_Toc299515796)

[Step 1: Define the Scope of the DirectAccess Project 6](#_Toc299515797)

[Step 2: Determine Network Requirements 8](#_Toc299515798)

[Step 3: Design DirectAccess Server Infrastructure 12](#_Toc299515799)

[Step 4: Design Web Servers and Certificate Infrastructure 15](#_Toc299515800)

[DirectAccess and Microsoft Forefront Unified Access Gateway 19](#_Toc299515801)

[Conclusion 20](#_Toc299515802)

[Appendix A: Job Aids 21](#_Toc299515803)

[Appendix B: DirectAccess Components at a Glance 23](#_Toc299515804)

[Appendix C: IPD in Microsoft Operations Framework 4.0 25](#_Toc299515805)

[Appendix D: DirectAccess in Microsoft Infrastructure Optimization 26](#_Toc299515806)

[Version History 27](#_Toc299515807)

[Acknowledgments 28](#_Toc299515808)

#

# The Planning and Design Series Approach

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

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

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

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

## Benefits of Using This Guide

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

Benefits for Business Stakeholders/Decision Makers:

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

Benefits for Infrastructure Stakeholders/Decision Makers:

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

**Benefits for** Consultants or Partners:

* Rapid readiness for consulting engagements.
* Planning and design template to standardize design and peer reviews.
* A “leave-behind” for pre-sales 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 DirectAccess Guide

This guide leads the reader step by step through the process of planning a DirectAccess infrastructure. The guide addresses the following fundamental decisions and tasks:

* Identifying the business and technical requirements for implementing DirectAccess.
* Identifying which resources on the corporate network should be accessible by users as well as which resources will be used to manage users’ devices.
* Determining the resources needed to employ DirectAccess to serve the selected user population.
* Designing the components, layout, and connectivity of the DirectAccess infrastructure.

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

## Assumptions

The content in this guide assumes that the reader has deployed or will be deploying Windows® 7 operating system clients; is familiar with IPv6, IPsec, and related networking technologies; and is planning an implementation of DirectAccess.

## DirectAccess Design Process

The goal of this guide is to present common scenarios, decisions, and practices for implementing a DirectAccess infrastructure. 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. Mobile computers can be managed any time the mobile computer has Internet connectivity, even if the user is not logged on. Data confidentiality and user authentication is ensured through the use of IPsec.

Using this guide, IT professionals can plan and design a DirectAccess infrastructure that ensures that critical phases are not left out of the plan and that a good foundation is established for future expansion.

The required components of a DirectAccess infrastructure include:

* **DirectAccess client.** A computer that is a member of the domain running Windows 7 Enterprise Edition (or later), Windows 7 Ultimate Edition (or later), or Windows Server® 2008 R2 Standard Edition (or later) that can automatically and transparently connect to an intranet through a DirectAccess server.
* **DirectAccess server.** A domain-joined computer running Windows Server 2008 R2 Standard Edition (or later) that may, depending on architecture, accept connections from DirectAccess clients and facilitates communication with intranet resources.
* **Network location server.** A Web server that a DirectAccess client accesses to determine whether it is located on the intranet or Internet.
* **Certificate revocation list (CRL) distribution points.** Servers that provide access to the CRL that is published by the certification authority (CA) issuing certificates for DirectAccess. This includes both internal and external CRL distribution points.

Additionally, a DirectAccess server must have access to:

* Active Directory® domain controllers.
* A Domain Name System (DNS) server with DNS dynamic updates enabled running Windows Server 2008 R2, Windows Server 2008 with the Q958194 hotfix, or Windows Server 2008 SP2 or later, or a third-party DNS server that supports DNS message exchanges over the Intra-site Automatic Tunnel Addressing Protocol (ISATAP).

Other network resources that must be used in a DirectAccess deployment:

* The organization’s public key infrastructure (PKI) for internally issued certificates.
* A Web server that hosts an HTTPS-based URL for network location detection.
* A Web or file server that hosts the CRL.

Other network resources that might be used in a DirectAccess deployment:

* System health validation systems like Network Access Protection (NAP) servers.
* IPv6/IPv4 translator with IPv6/IPv4 DNS gateway servers or devices. An example is NAT64 with DNS64.

Appendix B: “DirectAccess Components at a Glance” provides a tabular view of the required and optional infrastructure components.

This guide addresses the decisions and activities that need to occur in preparing for DirectAccess. The four steps below represent the most critical design elements in a well-planned DirectAccess design:

* Step 1: Define the Scope of the DirectAccess Project
* Step 2: Determine Network Requirements
* Step 3: Design DirectAccess Server Infrastructure
* Step 4: Design Web Servers and Certificate Infrastructure

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

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

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



Figure 1. The DirectAccess infrastructure decision flow

The primary components of a DirectAccess infrastructure are shown in Figure 2.



Figure 2. Example DirectAccess architecture

## Applicable Scenarios

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

* Organizations with mobile users who need to access resources on the intranet directly without the use of a virtual private network (VPN).
* Organizations with mobile users who operate beyond firewalls but must be managed centrally, with or without the users gaining access to intranet applications.
* Organizations that need to protect their roaming resources.

## Out of Scope

This guide concentrates on DirectAccess infrastructure design and planning exclusively. Solutions containing the following elements are considered outside the scope of this guide:

* Access to internal resources from non-domain member computers.
* Design of Microsoft Forefront® Unified Access Gateway (UAG).
* Design of other remote access solutions such as a VPN.
* Design of a new PKI for customers who do not yet have one.
* Design of NAP for validating system health and enforcing health policy compliance.
* The design of IPv6/IPv4 translator or IPv6/IPv4 DNS gateway devices.
* Interoperability with legacy or operating systems, other than Windows, for IPsec-protected communication.
* Moving an entire environment to IPv6.
* IPv6 application compatibility.

#

# Step 1: Define the Scope of the DirectAccess Project

The focus of this step is to define the scope of the project. This will then be applied to the design to ensure its applicability and success. There is opportunity throughout this guide to align business needs with the infrastructure design in order to meet the goals of the project.

To assist with the planning of this project, Table A-1 “Project Scope” in Appendix A: “Job Aids” has been provided to record the collected data.

The output from this step will be used in Steps 2, 3, and 4 to determine the network requirements and to design the DirectAccess infrastructure.

## Task 1: Determine the Scope of the Project

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.

Understanding the full extent of the work to be performed enables the designer to begin visualizing the tasks and roles that will be needed to successfully implement the infrastructure plan. The following list provides questions to ask to assist in gathering data:

* Which parts of the organization will be participating?
* Which geographic areas will be included?
* What are the number of users, access peak time, and maximum number of concurrent connections? A precise number is not needed, but an estimate will help define the hardware configuration needed to support the load.
* What internal resources will the users need to access? Is the target to have a single application, all applications, or differing levels of access to internal resources available through DirectAccess?
* What operating system is running on the domain controllers and DNS servers?
* What operating system is running on each internal resource that will be accessible to DirectAccess clients?
* Does the organization need to monitor all Web traffic of certain users or machines? If so, which ones?
* Will DirectAccess be used to manage remote computers?

Record the information that defines the overall scope of the project in Table A-1 in Appendix A. These requirements will drive the scalability and the IPv6 infrastructure design in later steps.

## Step Summary

In this step, the project scope and its attending goals were determined in order to clearly understand the motivation behind the DirectAccess project. Data gathered relative to which parts of the organization will be participating, which geographic areas will be included, and the number of users were recorded in Table A-1 in Appendix A.

The output of this step will be used to determine the network requirements in Step 2 and to design the DirectAccess infrastructure in Steps 3 and 4.

## Additional Reading

* “Next Generation Remote Access with DirectAccess and VPNs”: [www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=70723e47-3d57-415b-9182-744ceaf8c04a#tm](http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=70723e47-3d57-415b-9182-744ceaf8c04a#tm)
* “Technical Overview of DirectAccess in Windows 7 and Windows Server 2008 R2”: [www.microsoft.com/downloads/details.aspx?FamilyID=64966e88-1377-4d1a-be86-ab77014495f4&DisplayLang=en](http://www.microsoft.com/downloads/details.aspx?FamilyID=64966e88-1377-4d1a-be86-ab77014495f4&DisplayLang=en)
* Windows Server 2008 R2 site for DirectAccess: [www.microsoft.com/servers/directaccess.mspx](http://www.microsoft.com/servers/directaccess.mspx)

# Step 2: Determine Network Requirements

In this step, the project’s scope and business’s goals identified in Step 1 will be analyzed to determine the network requirements necessary to support DirectAccess clients’ connectivity to the corporate network. Additionally, how the DirectAccess server and remote clients will be provided access to internal resources will be determined.

All of the data gathered in this step will be recorded in Table A-2 “External Connectivity Methods” in Appendix A. The outputs for this step will be used in Steps 3 and 4 to design the DirectAccess infrastructure.

## Task 1: Determine Connectivity Needs for DirectAccess Clients

The first task in this step is to record which external client connectivity methods will be designed. The DirectAccess server sits between the corporate network and the Internet and provides a link for traffic to and from the corporate network. A DirectAccess client can connect to the DirectAccess server over the IPv6 Internet, or use 6to4, Teredo, or IP-HTTPS to send IPv6 packets across the IPv4 Internet. The selection of the appropriate connectivity model depends primarily on what type of IP address the DirectAccess client is currently assigned. If a client cannot connect over native IPv6, Teredo, or 6to4, the default behavior is to fall back to an IP-HTTPS connection.

IP-HTTPS–based connections could be used exclusively, but will have lower performance and higher overhead on the DirectAccess server than 6to4 and Teredo-based connections.

The following table shows a list of possible DirectAccess client networking configurations and the resulting primary IPv6 connectivity method.

Table 1. External Connectivity Methods

|  |  |  |
| --- | --- | --- |
| **DirectAccess client’s IP address type** | **Use case** | **Primary connectivity method** |
| Private (NAT) IPv4 address | At home | Teredo |
| Public IPv4 address  | Tethered cell phone  | 6to4 |
| 6to4 gateway address | Client has an IPv6 address, and is behind an Internet gateway device that is configured to act as a 6to4 router | 6to4 |
| Globally routable IPv6 address  | ISPs that use IPv6 | Globally routable IPv6 address (native IPv6) |
| If the client cannot connect via the previous methods | Behind a stringent firewall or Web proxy | IP-HTTPS |

Often, an organization will support all of these methods. Record which external connectivity methods will be supported in the organization’s infrastructure in Table A-2 in Appendix A. This will be used in Step 3 to determine which services to implement on the DirectAccess servers.

## Task 2: Determine Connectivity Needs for Internal Resources

This task focuses on determining how the DirectAccess server and remote clients will be provided access to internal resources. Refer to the list of internal resources the users will be accessing that was created in Step 1 to determine if any of these connectivity methods will be required.

If an internal resource has IPv6 connectivity with the DirectAccess server, no further connectivity method is needed. Where IPv6 connectivity is not available, consult the following table for the appropriate alternative internal connection methods.

Table 2. Internal Connectivity Methods for IPv4 Connections

|  |  |  |
| --- | --- | --- |
| **Operating system** | **Internal resource’s networking capability** | **Primary connectivity method** |
| Windows Server 2008 or later, Windows Vista® or later | ISATAP host | ISATAP |
| Windows Server 2003 and earlier, Windows XP and earlier | All others | IPv6/IPv4 translator |

Review each internal resource that will be accessible by DirectAccess clients, and determine the appropriate connectivity method. Note that the organization may use native IPv6, Intra-site Automatic Tunnel Addressing Protocol (ISATAP), and/or IPv6/IPv4 translators in any combination to achieve connectivity within the network. Windows Server 2008 or later, or Windows Vista or later, could be placed behind an IPv6/IPv4 translator device as well, but connectivity will be better with ISATAP.

If the organization does not have a native IPv6 infrastructure, ISATAP can be used to make IPv6-capable intranet servers and applications reachable by encapsulating IPv6 inside of IPv4. Infrastructure changes required to deploy ISATAP consist of setting up one or more ISATAP routers to provide address configuration and default routing for ISATAP hosts on the intranet. Infrastructure adjustments to allow IPv4 protocol 41 traffic may be required. Computers running Windows Server 2008 R2, including the DirectAccess server, support ISATAP host functionality and can be configured to act as ISATAP routers.

IPv6/IPv4 translator devices perform IPv6-to-IPv4 translation services for traffic between DirectAccess clients and IPv4-only intranet application servers, which include Windows Server 2003 and earlier, and Windows XP and earlier. Testing should be done of each application that is to be accessed by DirectAccess clients via an IPv6/IPv4 translator, native IPv6, or over ISATAP. Even though there may be general connectivity to a specific server, some applications on that server may not work as expected. For example, Session Initiation Protocol (SIP) applications such as VoIP solutions do not work when traffic crosses an IPv6/IPv4 translator device.

Microsoft Forefront UAG includes NAT64 functionality and can be used in conjunction with a DirectAccess deployment. For more information, see “Forefront UAG and DirectAccess” at <http://go.microsoft.com/fwlink/?LinkId=159955>. IPv6/IPv4 translator devices are also available from Layer 2 and Layer 3 switch and router vendors.

**Note**There cannot be full end-to-end IPsec protection to an internal Windows resource that is accessed via an IPv6/IPv4 translator device as the Microsoft implementation of IPsec cannot pass through these devices. If full end-to-end IPsec protection is required, the IPv4-only resources may need to be upgraded to Windows Server 2008 R2 or Windows 7 or later to support IPv6 or ISATAP.

Alternatively, a conventional remote access VPN (non-DirectAccess) connection can be used on the DirectAccess client to reach an IPv4-only resource.

Record whether an ISATAP router and/or IPv6/IPv4 translator device will be implemented to achieve connectivity for intranet resources in Table A-3 “Internal Connectivity Methods” in Appendix A. The IPv6/IPv4 translator device will be placed on the corporate network and logically resides, from a traffic standpoint, between the DirectAccess server and the internal resource.

## Step Summary

In this step, the project’s scope and business’s goals were analyzed to determine which services are needed to support DirectAccess clients’ connectivity to intranet resources. Additionally, it was determined how the DirectAccess server and remote clients will be provided access to internal resources. All of the data gathered in this step was recorded in Tables A-2 and A-3 in Appendix A.

The output of this step will be used in Steps 3 and 4 to design the DirectAccess infrastructure.

## Additional Considerations

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

* **IPsec policies in the form of Windows Firewall with Advanced Security connection security rules.** DirectAccess clients will access intranet resources over three tunnels. The first tunnel, also known as the infrastructure tunnel, connects to the Active Directory domain controllers and DNS servers. The second tunnel, also known as the intranet tunnel, allows the DirectAccess client to access intranet resources (for example, application servers or file shares) after the user has logged on. The third tunnel, also known as the management tunnel, allows management servers on the intranet to initiate connections with DirectAccess clients. The infrastructure and management tunnels use computer authentication, and the intranet tunnel uses both computer and user authentication.

Potential resources that might need to be accessible via the infrastructure and management tunnels include:

* Active Directory Domain Services (AD DS) domain controllers.
* NAP servers, including Health Registration Authorities (HRAs) and Remediation servers.
* DNS servers.
* Microsoft System Center Configuration Manager 2007 servers.
* Windows Server Update Services servers.
* Help desk department computers that use remote desktop connections to connect to and troubleshoot remote DirectAccess clients.
* Servers for anti-malware updates, such as antivirus servers.
* Corporate proxy servers to log and/or restrict Internet traffic.

All server endpoints that are accessible via the infrastructure and management tunnels must be specified in the IPsec policies.

* **DirectAccess force tunneling.** If the business requirements dictate that all Internet traffic should be sent through the tunnels to the DirectAccess server, force tunneling can be enabled via Group Policy and by adding a special entry in the Name Resolution Policy Table (NRPT). When force tunneling is configured, DirectAccess clients that detect that they are on the Internet modify their IPv4 default route so that, with the exception of local subnet traffic, all traffic sent by the DirectAccess client goes through tunnels to the DirectAccess server.

Enabling force tunneling has the following consequences:

* All Internet traffic forced over the tunnels will travel over the organization’s Internet connection four times (from client to corporate network, corporate network to Internet, Internet to corporate network, and corporate network to client), which may mean the size of the corporation’s Internet connection might need to be increased.
* DirectAccess clients use only IP-HTTPS to obtain IPv6 connectivity to the DirectAccess server over the IPv4 Internet. IP-HTTPS–based connections have lower performance and higher overhead on the DirectAccess server than 6to4-based and Teredo-based connections.
* The only locations that a DirectAccess client can reach by default with IPv4 traffic are those on its local subnet. All other traffic sent by the applications and services running on the DirectAccess client is IPv6 traffic sent over the DirectAccess connection. Therefore, IPv4-only applications on the DirectAccess client cannot be used to reach Internet resources, except those on the local subnet.

Connectivity to the IPv4 Internet must be done through servers and devices on the intranet that translate the IPv6 traffic from DirectAccess clients to IPv4 traffic for the IPv4 Internet. If the organization does not have the appropriate servers or translators, the DirectAccess clients will not have access to IPv4 Internet resources, even though they are directly connected to the IPv4 Internet.

## Additional Reading

* DirectAccess Design Guide: [www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=647222d1-a41e-4cdb-ba34-f057fbc7198f](http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=647222d1-a41e-4cdb-ba34-f057fbc7198f)
* *Intra-site Automatic Tunnel Addressing Protocol Deployment Guide*: [www.microsoft.com/downloads/details.aspx?familyid=0f3a8868-e337-43d1-b271-b8c8702344cd&displaylang=en](http://www.microsoft.com/downloads/details.aspx?familyid=0f3a8868-e337-43d1-b271-b8c8702344cd&displaylang=en)
* *Test Lab Guide: Demonstrate DirectAccess*: [www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=8d47ed5f-d217-4d84-b698-f39360d82fac](http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=8d47ed5f-d217-4d84-b698-f39360d82fac)
* Microsoft Internet Protocol Version 6 (IPv6) site: <http://technet.microsoft.com/en-us/network/bb530961.aspx>
* “IPv6 Transition Technologies”: <http://technet.microsoft.com/en-us/library/bb726951.aspx>
* “Support for IPv6 in Windows Server 2008 R2 and Windows 7”: <http://technet.microsoft.com/en-us/magazine/2009.07.cableguy.aspx>
* IPv6 Blog: <http://blogs.technet.com/ipv6/>

# Step 3: Design DirectAccess Server Infrastructure

Now that the project scope and the network requirements have been determined, the DirectAccess server infrastructure can be designed. The DirectAccess server configuration will be determined and, if desired, function separation will be performed. Additionally, fault tolerance and server placement will be decided. The decisions made in this step will be recorded in the job aids in Appendix A.

The DirectAccess server is a required component of any DirectAccess design.
A DirectAccess server must be running Windows Server 2008 R2 and be a member of the domain, but not be a domain controller.

## Task 1: Determine the Server Configuration

The DirectAccess server can perform the following functions:

* Teredo server and relay
* 6to4 relay
* IP-HTTPS server
* ISATAP router
* Native Internet Protocol version 6 (IPv6) router
* IPsec tunnel endpoint and gateway

DirectAccess can be installed in a virtual machine. It cannot be installed in a Microsoft failover cluster.

### Scaling

No information is available at the time of writing this guide on the core scaling metrics of a DirectAccess infrastructure. That is to say, there is no quantifiable data that can be presented to say that X servers should be deployed for Y users. The organization should gradually add users and monitor the server performance to identify the optimum number of users that the server can support.

DirectAccess is designed to be installed and managed as a single unit. Any splitting of the functions will inherently introduce additional complexity and potential for configuration problems. Additionally, fault tolerance, scaling, sizing, and connectivity will need to be determined for each server.

Some DirectAccess functions can be transferred to other servers. For example, one configuration that may increase scalability of DirectAccess connections is to configure the DirectAccess server to use the Teredo, 6to4, and IP-HTTPS functions on another server. The IPsec gateway and ISATAP router can be separated on to another physical computer with IPsec offload hardware, which can better handle the processor-intensive cryptographic operations and support many IPsec tunnels. If the organization already has one of the DirectAccess functions deployed separately on the network for other purposes (for example, a non-DirectAccess server 6to4 relay or Teredo server), the existing servers could also be used for the DirectAccess deployment.

Microsoft Forefront UAG can be used in conjunction with DirectAccess to create a load-balanced array to provide scalability. DirectAccess does not natively provide a mechanism to scale out. If it is determined that more than one DirectAccess entry point will be needed in the environment and if Forefront UAG is not available, distribution of the users across multiple DirectAccess servers via manual processes like Group Policy settings will therefore be required. However, no documentation is available from the product group at the time of this writing on the steps required to achieve this.

Record where each function will be placed in Table A-4 “Server Inventory” in Appendix A.

### Fault Tolerance

DirectAccess does not natively provide fault tolerance. To provide service redundancy for DirectAccess, use Microsoft Forefront UAG for scalability, high availability, and enhanced management for a DirectAccess deployment.

As a risk mitigation strategy to the specific scenario of hardware failure, DirectAccess can be installed in a VM that is then clustered via a Microsoft Hyper-V® failover cluster. The users on that DirectAccess server will experience session interruption in the event of a failover. This provides protection against hardware failure of the host machine only; it does not protect against service failure, operating system failure, or application-level failure. Nor does it provide protection against planned maintenance such as applying patches. Although the VM will be available, there is no guarantee on whether DirectAccess will be running.

Note   IPsec offload network adapters are not supported in a virtual machine. If the decision was made to separate the IPsec gateway service, it must be run on a physical machine to support the IPsec offload network adapters.

Record whether DirectAccess will be installed in a Hyper-V failover cluster in Table A-4 in Appendix A.

## Task 2: Determine Placement of Each Server

Because DirectAccess servers provide intranet connectivity to DirectAccess clients on the Internet, DirectAccess servers are typically installed in the perimeter network between an Internet-facing connection and the intranet, as indicated in the diagram below.



Figure 3. Placement of a DirectAccess server behind a firewall

The DirectAccess server must be joined to an Active Directory domain, must be running Windows Server 2008 R2, and must have at least two physical network adapters installed (one connected to the Internet side and the other one connected to the intranet side).

The DirectAccess server must have at least two consecutive public IPv4 addresses assigned to the interface that is connected to the perimeter network or, in the absence of an Internet firewall, connected directly to the Internet. Addresses in the ranges 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 are private IPv4 addresses and cannot be used.

**Note**   These addresses should be chosen with care since after they are used, the entire IPv6 internal corporate network is addressed using them. Changing them will necessitate reworking the ISATAP deployment. These issues decrease if the organization has already deployed native IPv6 and is not running ISATAP.

The DirectAccess server must be a member of the Active Directory domain, but cannot be a domain controller. Additionally, the same computer acting as a DirectAccess server and a remote access VPN server with Routing and Remote Access is not a supported configuration, except when used with Forefront UAG.

Determine the placement of each DirectAccess server and record this in Table A-4 in Appendix A.

## Additional Considerations

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

* **Active Directory Sites and Services and IPv6.** Active Directory Sites and Services will need additional configuration with the introduction of native IPv6 or transition technologies in the organization. For each IPv4 subnet object, an equivalent IPv6 subnet object will need to be configured in which the IPv6 address prefix for the subnet expresses the assigned IPv6 prefix or the same range of ISATAP, IP-HTTPS, 6to4, and Teredo host addresses as the IPv4 subnet. This should be a site with domain controllers and global catalog servers for all of the domains in the organization and have good connectivity to the DirectAccess server.
* **Active Directory domain controllers on the Internet.** An Active Directory domain controller cannot be reachable from the Internet interface of the DirectAccess server. (In other words, the Internet interface cannot be in the domain profile of Windows Firewall.) If this is true, the DirectAccess Setup Wizard cannot be run.

If an Active Directory domain controller must be on the perimeter network and is therefore reachable from the Internet interface of the DirectAccess server, the DirectAccess server can be prevented from reaching it by adding packet filters on the Internet interface of the DirectAccess server that prevent connectivity to the Internet Protocol (IP) address of the perimeter network domain controller.

Because the DirectAccess server is an IPv6 router, if the organization has a native IPv6 infrastructure, the Internet interface can also reach the domain controllers on the intranet. In this case, add packet filters to the Internet interface that prevent connectivity to the intranet domain controllers.

## Step Summary

In this step, the DirectAccess server infrastructure was designed. The DirectAccess server configuration was determined and, if function separation is desired, that was designed in this step. Additionally, fault tolerance was determined, as well as server placement. All data gathered and decisions made were recorded in Table A-4 in Appendix A.

## Additional Reading

* Microsoft Intelligent Application Gateway site for UAG and DirectAccess: <http://go.microsoft.com/fwlink/?LinkId=159955>
* “Teredo Overview”: <http://go.microsoft.com/fwlink/?Linkid=157322>
* “IP Security Features: Intel Ethernet Security Adapters and Microsoft Windows Server 2008”: [www.intel.com/assets/pdf/whitepaper/320172.pdf](http://www.intel.com/assets/pdf/whitepaper/320172.pdf)

# Step 4: Design Web Servers and Certificate Infrastructure

In the previous step, the DirectAccess server infrastructure was designed. In this step, the Web servers and certificate requirements for a DirectAccess deployment will be designed.

Web locations will be needed for the following resources:

* The network location server (an HTTPS-based URL).
* An HTTP-based intranet certificate revocation list (CRL) distribution point for the HTTPS certificate of the network location server.
* An HTTP-based Internet CRL distribution point for the IP-HTTPS certificate of the DirectAccess server, if IP-HTTPS connectivity will be supported.

## Task 1: Design the Computer Certificates

Computer certificates are required for the authentication of IPsec protection.

The infrastructure and management tunnels use a computer certificate for the first authentication and user (NTLMv2) with computer credentials for the second authentication. The intranet tunnel uses a computer certificate for the first authentication and user (Kerberos V5) with user credentials for the second authentication.

Issuing computer certificates through a public key infrastructure (PKI) via autoenrollment is the easiest way to get certificates installed on DirectAccess clients. Autoenrollment ensures that all domain members obtain a computer certificate from an enterprise certification authority (CA).

The computer certificates in the Enhanced Key Usage field should have the Client Authentication object identifier (OID).

No additional infrastructure is required for DirectAccess; however, ensure that the organization’s PKI is configured to support autoenrollment of certificates or that the PKI administrator is prepared to issue certificates manually.

## Task 2: Design the Network Location Servers

A network location server is an internal Web server that hosts an HTTPS-based uniform resource locator (URL). DirectAccess clients attempt to access the URL to determine whether they are located on the intranet; if the attempt fails, they conclude they are on the Internet and initiate the DirectAccess tunnels. The content of the HTTPS-based URL is not important—only the DirectAccess client’s ability to successfully access the page at the URL. The DirectAccess server can act as the network location server, or another Web server can be designated. The network location server could also be hosted on the same server as other services (for example, on a local branch file or print server). It does not need to be a Microsoft IIS server.

**Note**To ensure that clients can correctly detect when they are on the Internet, DirectAccess clients on the Internet must not be able to successfully access the network location URL. This is accomplished by ensuring that the fully qualified domain name (FQDN) in the URL cannot be resolved using Internet DNS servers, by configuring the Web server to deny connections from Internet-based clients, or by ensuring that the certificate validation process fails when DirectAccess clients are on the Internet.

It is recommended that the network location server be made highly available since all DirectAccess clients on the intranet will attempt to access it to determine their locations.
If the network location server is down, all internal clients will conclude they’re on the Internet and this can result in impaired intranet connectivity. Additionally, depending on the number of DirectAccess clients that are configured to use the URL for detecting their network locations, the server may need to be designed to support high capacities.

If a Microsoft IIS server will be used to host the network location server URL, refer to the *Infrastructure Planning and Design Guide for Microsoft Internet Information Services 7.0 and Internet Information Services 7.5*, available at <http://go.microsoft.com/fwlink/?LinkId=157703>, to design the IIS servers.

Determine the placement of the network location server and record the URL in Table A-5 “Network Location Server” in Appendix A.

## Task 3: Design the Network Location Server Certificates

The certificate for the network location server’s Web site must have the following properties:

* In the Subject field, either an IP address of the intranet interface of the network location server or the FQDN of the network location URL.
* For the Enhanced Key Usage field, the Server Authentication OID.

### Intranet CRL Distribution Point

Certificate revocation list (CRL) distribution points provide access to the CRL that is published by the certification authority (CA) issuing certificates for DirectAccess and are published by Web servers.

The DirectAccess client relies on an available CRL to determine if the network location server is using a valid certificate. The intranet CRL must be published using a domain name that is not included in the namespace defined by DirectAccess as the internal network; it should be hosted on an intranet Web, file, or Lightweight Directory Access Protocol (LDAP) server and can be published to multiple locations.

Without a reachable CRL distribution point on the intranet for the network location server certificate, intranet detection fails, which can impair intranet connectivity for DirectAccess clients.

Record the location of the intranet CRL distribution point in Table A-6 “CRL Distribution Points” in Appendix A.

## Task 4: Design the DirectAccess Server Certificates

If it was decided in Step 2 that IP-HTTPS connectivity will not be supported, this task should be skipped.

A separate certificate is required for IP-HTTPS connections between a DirectAccess client and the DirectAccess server. It is only used over IP-HTTPS connections, which will include clients that were unable to connect over native IPv6, Teredo, or 6to4.

The IP-HTTPS certificate for the DirectAccess server must have the following properties:

* In the Subject field, either an IP address of the Internet interface of the DirectAccess server or the FQDN of the IP-HTTPS URL.
* For the Enhanced Key Usage field, the Server Authentication OID.
* For the CRL Distribution Points field, a CRL distribution point that is accessible by DirectAccess clients that are connected to the Internet.

### Internet CRL Distribution Point

In order for DirectAccess clients to be able to connect to the DirectAccess server using IP-HTTPS, they must be able to access a valid CRL, which can be published to multiple locations. CRL distribution points can be accessed through either a Web server using an HTTP-based URL or a file server via a UNC path. This CRL distribution point must be resolvable and accessible from DirectAccess clients on the Internet. Without a reachable CRL distribution point on the Internet, all IP-HTTPS-based DirectAccess connections will fail.

External certificates are not required; however, if the certificate is purchased from a third-party CA, the CA is responsible for managing the CRL distribution points. If the business uses a certificate issued by its self-hosted CA, additional infrastructure may be required to ensure the CRL distribution point is available externally for DirectAccess clients. Refer to the *Infrastructure Planning and Design Guide for Microsoft Internet Information Services 7.0 and Internet Information Services 7.5*, available at <http://go.microsoft.com/fwlink/?LinkId=157703>, for more details on designing a highly available Web server.

**Note** If the DirectAccess server is also serving as the network location server, separate certificates will be needed for the IP-HTTPS and network location server HTTPS.

Record the location of the Internet CRL distribution point in Table A-6 in Appendix A.

## Validating with the Business

To ensure that the network location server will have enough capacity to support network traffic and that there will be a disaster recovery plan in place in case of server failure, ask business stakeholders the following questions:

* If using an existing IIS server for the network location server, does the server have enough capacity to support both existing Web application traffic and the DirectAccess clients on the intranet performing network location detection? DirectAccess clients will query the network location server on every network state transition, including DHCP renewals and link state changes.
* Is the network location server included in the Business Continuity Plan and/or Disaster Recovery Plan? Intranet connectivity for DirectAccess clients can be impaired if the network location server fails.

## Additional Considerations

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

* **Smart cards for additional authorization.** Smart cards are currently the only supported form of multi-factor authentication. To use smart cards with IPsec tunnel mode authorization, the organization must first have a PKI deployment and a smart card infrastructure. After the smart card deployment has been completed, smart card authorization can be enabled on the Connectivity page of Step 2 of the DirectAccess Setup Wizard.
* **Network Access Protection (NAP).** NAP enforces health requirements by monitoring and assessing the health of client computers when they attempt to connect or communicate on a network. No changes to the NAP infrastructure for the IPsec NAP enforcement method are required specifically for DirectAccess clients; however, the NAP servers should be listed in the infrastructure tunnel IPsec policy to properly validate and remediate the health of DirectAccess clients.

## Step Summary

The network location server is simply a Web server that the DirectAccess clients attempt to access to determine if they are on the intranet. In this step, it was determined how many servers are required, and the servers were designed by referencing the Infrastructure Planning and Design guide for Microsoft IIS. The requirements for certificates for the network location servers and DirectAccess clients and implications to the PKI infrastructure were also reviewed.

## Additional Reading

* *Infrastructure Planning and Design Guide for Microsoft Internet Information Services 7.0 and Internet Information Services 7.5*: <http://go.microsoft.com/fwlink/?LinkId=157703>
* DirectAccess Troubleshooting Guide: [http://technet.microsoft.com/en-us/library/ee624056(WS.10).aspx](http://technet.microsoft.com/en-us/library/ee624056%28WS.10%29.aspx)
* “AuthIP in Windows Vista”: <http://technet.microsoft.com/en-us/library/bb878097.aspx>
* Active Directory Certificate Services resources site: <http://technet.microsoft.com/en-us/windowsserver/dd448615.aspx>
* Active Directory Certificate Services Overview: <http://technet.microsoft.com/en-us/library/cc755071.aspx>

# DirectAccess and Microsoft Forefront Unified Access Gateway

To provide fault tolerance, scalability, and increased management, Microsoft Forefront Unified Access Gateway (Forefront UAG) can be used in conjunction with DirectAccess. This will allow multiple servers to be placed in a load-balanced array. For more information, see “Configuring NLB for a Forefront UAG DirectAccess array” at <http://go.microsoft.com/fwlink/?LinkId=160075>.

Note that an Infrastructure Planning and Design guide for Forefront UAG has been released; it is available at <http://go.microsoft.com/fwlink/?LinkId=169356>.

## Additional Reading

Microsoft Intelligent Application Gateway site for Forefront UAG and DirectAccess: [www.microsoft.com/forefront/edgesecurity/iag/en/us/UAG-DirectAccess.aspx](http://www.microsoft.com/forefront/edgesecurity/iag/en/us/UAG-DirectAccess.aspx)

# Conclusion

Microsoft DirectAccess is a new feature available in Windows 7 and Windows Server 2008 R2 that can make corporate network connectivity much simpler for remote clients, but the infrastructure requirements to make this happen involve technologies that are new to many experienced networking personnel. IPv6 is required, but IPv6 transition technologies can ease the pathway.

The implementation decisions in this guide are separated into actionable steps to make the process more straightforward. First, the scope of the project was decided. In the second step, the methods to enable connectivity from the DirectAccess clients to the corporate network were determined, and then support for intranet communication to both IPv6 and IPv4 resources was designed. This provided the information for the configuration of the DirectAccess server in Step 3. Lastly, the Web servers and certificate infrastructure were designed.

## Additional Reading

* DirectAccess Design Guide: [www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=647222d1-a41e-4cdb-ba34-f057fbc7198f](http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=647222d1-a41e-4cdb-ba34-f057fbc7198f)
* Windows Server 2008 R2 site for DirectAccess: [www.microsoft.com/servers/directaccess.mspx](http://www.microsoft.com/servers/directaccess.mspx)
* TechNet resources site for DirectAccess: <http://technet.microsoft.com/en-us/network/dd420463.aspx>

# Appendix A: Job Aids

Use the job aids in this appendix to enhance the success of the DirectAccess planning and design process.

Step 1. Use this job aid to record the project’s scope.

Table A-1. Project Scope

|  |  |
| --- | --- |
| Which parts of the organization will be participating? |  |
| Which geographic areas will be included? |  |
| What are the number of users, access peak time, and maximum number of concurrent connections? |  |
| What internal resources will the users need to access? Is the target to have a single application, all applications, or differing levels of access to internal resources available through DirectAccess? |  |
| What operating system is running on the domain controllers and DNS servers? | Resource | Operating system |
|  |  |
|  |  |
|  |  |
|  |  |
| What operating system is running on each internal resource that will be accessible to DirectAccess clients? | Resource | Operating system |
|  |  |
|  |  |
|  |  |
|  |  |
| Does the organization need to monitor all Web traffic of certain users or machines? If so, which ones? | User | Machine |
|  |  |
|  |  |
|  |  |
|  |  |
| Will DirectAccess be used to manage remote computers? |  |

Step 2. Use this job aid to record external connectivity methods for use in gathering DirectAccess network requirements.

Table A-2. External Connectivity Methods

| External connection method | Select |
| --- | --- |
| Teredo |  |
| 6to4 |  |
| Native IPv6 |  |
| IP-HTTPS |  |

Step 2. Use this job aid to record internal connectivity methods for use in gathering DirectAccess network requirements.

Table A-3. Internal Connectivity Methods

| Internal connectivity method | Select |
| --- | --- |
| ISATAP |  |
| IPv6/IPv4 translator |  |

Step 3. Use this job aid to record the DirectAccess server inventory.

Table A-4. Server Inventory

| Server function placement (if not all on same server) | Hyper-V failover cluster installation? | DirectAccess server placement |
| --- | --- | --- |
|  |  |  |
|  |  |  |

Step 4. Use this job aid to record the DirectAccess network location server.

Table A-5. Network Location Server

| Location | Server name | URL |
| --- | --- | --- |
|  |  |  |
|  |  |  |

Step 4. Use this job aid to record the CRL distribution points.

Table A-6. CRL Distribution Points

| CRL distribution point location | URLs or UNC paths |
| --- | --- |
| Intranet |  |
| Internet  |  |

# Appendix B: DirectAccess Components at a Glance

This table shows a snapshot view of the components of a DirectAccess infrastructure.

Table B-1. DirectAccess Components at a Glance

|  |
| --- |
| DirectAccess server-side components |
| Capability | Required | Optional | Needed when… |
| Teredo relay service |  | Yes1 | To support DirectAccess clients with private (NAT) IPv4 addresses |
| Teredo server service |  | Yes1 | To support DirectAccess clients with private (NAT) IPv4 addresses |
| 6to4 router service |  | Yes1 | To support DirectAccess clients with public IPv4 addresses |
| IP-HTTPS server service |  | Yes1 | To support DirectAccess clients where firewall or other restrictions prevent connectivity |
| Native IPv6  |  | Yes1,2 | To support DirectAccess clients with native IPv6 connections |
| ISATAP router service |  | Yes2 | Windows Server 2008 (or later) or Windows Vista (or later) internal servers need to be accessible to clients |
| IPsec DoS Protection Service | Yes |  | This provides denial of service (DoS) protection of the corporate IPv6 address space from unauthenticated users |
| IPsec gateway service |  | Yes | To support internal servers when end-to-end encryption cannot be supported OR when using smart-card authorization of connections  |
| Additional HTTPS certificates on DirectAccess server |  |  | Only if IP-HTTPS is supported or if the DirectAccess server is the network location server |
| **Yes 1**At least one of Teredo, 6to4, IP-HTTPS, or Native IPv6 must be enabled on the server to support connections from DirectAccess clients.**Yes 2**At least ISATAP or Native IPv6 must be enabled on the server to support connections to internal resources. |
| DirectAccess client-side components |
| Capability | Required | Optional | Needed when… |
| Teredo client |  | Yes1 | When connecting from a private (NAT) IPv4 address |
| 6to4 client |  | Yes1 | When connecting from a public IPv4 address |
| IP-HTTPS client |  | Yes1 | When connecting over IP-HTTPS |

|  |
| --- |
| DirectAccess client-side components |
| Capability | Required | Optional | Needed when… |
| Native IPV6 client connectivity to DirectAccess server |  | Yes3 | When connecting from a native IPv6 address |
| Client computer certificates | Yes |  | Used by the client to authenticate when negotiating IPsec-protected tunnels |
| **Yes 3**At least one of Teredo, 6to4, IP-HTTPS, or Native IPv6 must be enabled on the client to support connections to the DirectAccess server. |
| Supporting infrastructure components |
| Capability | Required | Optional | Needed when… |
| PKI to issue computer certificates to DirectAccess server and clients | Yes |  | Issue certificates to client and server systems in order to be able to create DirectAccess tunnels. See client computer certificates. |
| Network Location Server (an HTTPS URL on an internal Web server) | Yes |  | Used by client to detect if on intranet  |
| Network Location Server certificate | Yes |  | Prove identity of Network Location Server |
| Intranet CRL distribution point | Yes |  | Validate Network Location Server certificate |
| Internet CRL distribution point |  | Yes | Only if IP-HTTPS connections from clients are supported |
| ISATAP router |  | Yes | If native IPv6 is not deployed, then ISATAP will need to be used to enable IPv6 over an existing IPv4 infrastructure |
| ISATAP host |  | Yes | On each host on an IPv4-only intranet |
| IPv6/IPv4 translator and IPv6/IPv4 DNS gateway |  | Yes | To connect to IPv4-only resources, like Windows Server 2003 and earlier or Windows XP or earlier |
| NAP |  | Yes | Client health needs to be assessed |
| UAG |  | Yes | Scaling to multiple servers, fault tolerance |
| Hyper-V |  | Yes | When DirectAccess server is run in a VM |
| Hyper-V cluster |  | Yes | When DirectAccess VM needs to be fault tolerant |

# Appendix C: IPD in Microsoft Operations Framework 4.0

Microsoft Operations Framework (MOF) 4.0 offers integrated best practices, principles, and activities to assist an organization in achieving reliable solutions and services. MOF provides guidance to help individuals and organizations create, operate, and support technology services, while helping to ensure the investment in technology delivers expected business value at an acceptable level of risk. MOF’s question-based guidance helps to determine what is needed for an organization now, as well as providing activities that will keep the organization running efficiently and effectively in the future.

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

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



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

# Appendix D: DirectAccess in Microsoft Infrastructure Optimization

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

IO is structured around three information technology models: Core Infrastructure Optimization, Application Platform Optimization, and Business Productivity Infrastructure Optimization. According to the Core Infrastructure Optimization Model, implementing DirectAccess will help move an organization to the Rationalized level and, in some cases, even to the Dynamic level. On the path to the Rationalized level, organizations can use DirectAccess to give mobile users seamless access to corporate networks without the need to use a virtual private network (VPN) and allow IT to manage mobile computers any time the mobile computer has Internet connectivity.



Figure D-1. Mapping of DirectAccess technology into the Core Infrastructure Optimization Model

# Version History

| **Version** | **Description** | **Date** |
| --- | --- | --- |
| 1.3 | Minor updates. Put document in current template. | November 2011 |
| 1.2 | Minor changes to wording. | February 2010 |
| 1.1 | Minor changes to wording. | November 2009 |
| 1.0 | First release. | October 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 DirectAccess.* 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*
* Michael Kaczmarek – *Microsoft*
* Robin Maher – *Microsoft*
* Ryan Sokolowski – *GrandMasters*
* Jeromy Statia– *Microsoft*
* Fergus Stewart – *Microsoft*
* Melissa Stowe– *Microsoft*
* Kiyoshi Watanabe *– Microsoft*

**Reviewers:**

* Rajeev Agrawal– *Microsoft*
* Fernando Cima– *Microsoft*
* Joseph Davies – *Microsoft*
* Dan Griffin – *JW Secure, Inc.*
* Devrim Iyigun – *Microsoft*
* Michael Niehaus – *Microsoft*
* Christopher Palmer – *Microsoft*
* René Scholten – Capgemini
* Sean Siler– *Microsoft*
* Andy Tang– *Microsoft*
* Pat Telford – *Microsoft*

**Editors:**

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

## Feedback

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