Lotus® Domino®

Version 7

Installing Domino Servers

G210-1993-00

Second Edition (October, 2005)

This edition applies to IBM® Lotus® Domino^{TM} and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Deploying Domino

This chapter outlines the steps required to deploy IBM® Lotus® Domino(TM) 7 successfully and introduces important concepts that you need to know before you install Domino servers.

Guidepost for deploying Domino

Whether you're setting up IBM Lotus Domino 7 and IBM Lotus Notes® 7 for the first time or adding to an established Domino environment, planning is vital. Along with determining your company's needs, you need to plan how to integrate Domino into your existing network. After planning is complete, you can begin to install and set up Domino servers and the Domino Administrator and build the Domino environment. The following list describes, in order, the process to use to deploy Domino.

1. Determine your company's server needs. Decide where to locate each server physically, taking into consideration local and wide-area networks and the function of each server.
2. Develop a hierarchical name scheme that includes organization and organizational unit names.
3. Decide whether you need more than one Domino domain.
4. Understand how server name format affects network name-to-address resolution for servers. Ensure that the DNS records for your company are the correct type for the server names.
5. Determine which server services to enable.
6. Determine which certificate authority -- Domino server-based certification authority, Domino 5 certificate authority, third-party -- to use.
7. Install and set up the first Domino server.
8. Install and set up the Domino Administrator on the administrator's machine.
9. Complete network-related server setup.
10. If the Domino server is offering Internet services, set up Internet site documents. There are some instances where Internet Site documents are required.
11. Specify Administration Preferences.
12. Create additional certifier IDs to support the hierarchical name scheme.
13. Set up recovery information for the certifier IDs.
14. Add the administrator's ID to the recovery information for the certifier IDs and then distribute the certifier IDs, as necessary, to other administrators.
15. Register additional servers.
16. If you did not choose to do so during first server setup, Create a group in the Domino Directory for all administrators, and give this group Manager access to all databases on the first server.
17. Install and set up additional servers.
18. Complete network-related server setup for each additional server.
19. Build the Domino environment.

Functions of Domino servers

Before you install and set up the first Domino server, consider the function and physical location of the servers that your company needs and determine how to connect the servers to each other. The current configuration of local and wide-area networks affects many of these decisions.

Consider your company's need for:

- Servers that provide Notes and/or browser users with access to applications
- Hub servers that handle communication between servers that are geographically distant
- Web servers that provide browser users with access to Web applications

- Servers that manage messaging services
- Directory servers that provide users and servers with information about how to communicate with other users and servers
- Passthru servers that provide users and servers with access to a single server that provides access to other servers
- Domain Search servers that provide users with the ability to perform searches across all servers in a Domino domain
- Clustered servers that provide users with constant access to data and provide load-balancing and failover
- Partitioned servers that run multiple instances of the Domino server on a single computer
- Firewall servers that provide Notes users with access to internal Domino services and protect internal servers from outside users
- xSP servers that provide users with Internet access to a specific set of Domino applications

Your decisions help determine which types of Domino servers your require. When you install each server, you must select one of the following installation options:

- Domino Utility Server -- Installs a Domino server that provides application services only, with support for Domino clusters. The Domino Utility Server is a new installation type for Lotus Domino 7 that removes client access license requirements. Note that it does NOT include support for messaging services. See full licensing text for details.
- Domino Messaging Server -- Installs a Domino server that provides messaging services. Note that it does NOT include support for application services or Domino clusters.
- Domino Enterprise Server -- Installs a Domino server that provides both messaging and application services, with support for Domino clusters.

Note: All three types of installations support Domino partitioned servers. Only the Domino Enterprise Server supports a service provider (xSP) environment.

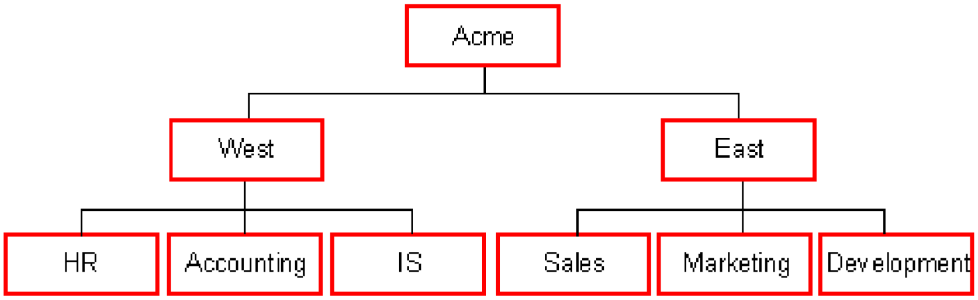
Hierarchical naming for servers and users

Hierarchical naming is the cornerstone of Domino security; therefore planning it is a critical task. Hierarchical names provide unique identifiers for servers and users in a company. When you register new servers and users, the hierarchical names drive their certification, or their level of access to the system, and control whether users and servers in different organizations and organizational units can communicate with each another.

Before you install Domino servers, create a diagram of your company and use the diagram to plan a meaningful name scheme. Then create certifier IDs to implement the name scheme and ensure a secure system.

A hierarchical name scheme uses a tree structure that reflects the actual structure of a company. At the top of the tree is the organization name, which is usually the company name. Below the organization name are organizational units, which you create to suit the structure of the company; you can organize the structure geographically, departmentally, or both.

For example, the Acme company created this diagram for their servers and users:



Looking at Acme’s diagram, you can see where they located their servers in the tree. Acme decided to split the company geographically at the first level and create certifier IDs for the East and West organizational units. At the next level down, Acme made its division according to department.

For more information on certifier IDs, see the topic ″Certifier IDs and certificates″ in this chapter.

Components of a hierarchical name

A hierarchical name reflects a user’s or server’s place in the hierarchy and controls whether users and servers in different organizations and organizational units can communicate with each another. A hierarchical name may include these components:

- Common name (CN) -- Corresponds to a user’s name or a server’s name. All names must include a common name component.
- Organizational unit (OU) -- Identifies the location of the user or server in the organization. Domino allows for a maximum of four organizational units in a hierarchical name. Organizational units are optional.
- Organization (O) -- Identifies the organization to which a user or server belongs. Every name must include an organization component.
- Country (C) --Identifies the country in which the organization exists. The country is optional.

An example of a hierarchical name that uses all of the components is:

Julia Herlihy/Sales/East/Acme/US

Typically a name is entered and displayed in this abbreviated format, but it is stored internally in canonical format, which contains the name and its associated components, as shown below:

CN=Julia Herlihy/OU=Sales/OU=East/O=Acme/C=US.

Note: You can use hierarchical naming with wildcards as a way to isolate a group of servers that need to connect to a given Domino server in order to route mail.

For more information, see the chapter ″Setting Up Mail Routing.″

Domino domains

A Domino domain is a group of Domino servers that share the same Domino Directory. As the control and administration center for Domino servers in a domain, the Domino Directory contains, among other documents, a Server document for each server and a Person document for each Notes user.

Planning for Domino domains

There are four basic scenarios for setting up Domino domains. The first scenario, which many small- and medium-size companies use, involves creating only one Domino domain and registering all servers and users in one Domino Directory. This scenario is the most common and the easiest to manage.

The second scenario is common when a large company has multiple independent business units. In this case, one organization spread across multiple domains may be the best scenario. Then all servers and users are members of the same organization, and each business unit administers its own Domino Directory.

For more information on administering multiple Domino directories, see the chapter ″Planning Directory Services.″

A third scenario is common when multiple companies work closely together yet want to retain individual corporate identities. Then one domain and multiple organizations may work best.

Finally, the fourth scenario involves maintaining multiple domains and multiple organizations. This scenario often occurs when one company acquires another.

Sometimes the decision to create multiple Domino domains is not based on organizational structure at all. For example, you may want to create multiple Domino domains if you have slow or unreliable network connections that prohibit frequent replication of a single, large directory. Keep in mind that working with multiple domains requires additional administrative work and requires you to set up a system for managing them.

Domains can be used as a broad security measure. For example, you can grant or deny a user access to servers and databases, based on the domain in which the user is registered. Using an extended ACL is an alternative to creating multiple domains, because you can use the extended ACL to specify different levels of access to a single Domino Directory, based on organization name hierarchy.

For more information on extended ACLs, see the chapter ″Setting Up Extended ACLs.″

Partitioned servers

Using Domino server partitioning, you can run multiple instances of the Domino server on a single computer. By doing so, you reduce hardware expenses and minimize the number of computers to administer because, instead of purchasing multiple small computers to run Domino servers that might not take advantage of the resources available to them, you can purchase a single, more powerful computer and run multiple instances of the Domino server on that single machine.

On a Domino partitioned server, all partitions share the same Domino program directory, and thus share one set of Domino executable files. However, each partition has its own Domino data directory and NOTES.INI file; thus each has its own copy of the Domino Directory and other administrative databases.

If one partition shuts down, the others continue to run. If a partition encounters a fatal error, Domino’s fault recovery feature restarts only that partition, not the entire computer.

For information on setting up fault recovery, see the chapter ″Transaction Logging and Recovery.″

Partitioned servers can provide the scalability you need while also providing security. As your system grows, you can migrate users from a partition to a separate server. A partitioned server can also be a member of a cluster if you require high availability of databases. Security for a partitioned server is the same as for a single server.

When you set up a partitioned server, you must run the same version of Domino on each partition. However, if the server runs on UNIX®, there is an alternative means to run multiple instances of Domino on the server: on UNIX, you can run different versions of Domino on a single computer, each version with its own program directory. You can even run multiple instances of each version by installing it as a Domino partitioned server.

For more information on installing Domino on UNIX, see the chapter ″Installing and Setting Up Domino Servers.″

Deciding whether to use partitioned servers

Whether or not to use partitioned servers depends, in part, on how you set up Domino domains. A partitioned server is most useful when the partitions are in different Domino domains. For example, using a partitioned server, you can dedicate different Domino domains to different customers or set up multiple Web sites. A partitioned server with partitions all in the same Domino domain often uses more computer resources and disk space than a single server that runs multiple services.

When making the decision to use partitioned servers, remember that it is easier to administer a single server than it is to administer multiple partitions. However, if your goal is to isolate certain server functions on the network -- for example, to isolate the messaging hub from the replication hub or isolate work groups for resource and activity logging -- you might be willing to take on the additional administrative work. In addition, running a partitioned server on a multiprocessor computer may improve performance, even when the partitions are in the same domain, because the computer simultaneously runs certain processes.

To give Notes users access to a Domino server where they can create and run Domino applications, use a partitioned server. However, to provide customers with Internet access to a specific set of Domino applications, set up an xSP server environment.

For more information about using Domino in an xSP environment, see the chapter ″Planning the Service Provider Environment.″

Deciding how many partitions to have

How many partitions you can install without noticeably diminishing performance depends on the power of the computer and the operating system the computer uses. For optimal performance, partition multiprocessor computers that have at least one, and preferably two, processors for each partition that you install on the computer.

Certifier IDs and certificates

Certifier IDs and certificates form the basis of Domino security. To place servers and users correctly within your organization’s hierarchical name scheme, you create a certifier ID for each branch on the name tree. You use the certifiers during server and user registration to ″stamp″ each server ID and user ID with a certificate that defines where each belongs in the organization. Servers and users who belong to the same name tree can communicate with each other; servers and users who belong to different name trees need a cross-certificate to communicate with each other.

Note: You can register servers and users without stamping each server ID and user ID if you have migrated the certifier to a Domino server-based certification authority (CA).

For more information about server-based CAs, see the chapter ″Setting Up a Domino Server-based Certification Authority.″

Each time you create a certifier ID, Domino creates a certifier ID file and a Certifier document. The ID file contains the ID that you use to register servers and users. The Certifier document serves as a record of the certifier ID and stores, among other things, its hierarchical name, the name of the certifier ID that issued it, and the names of certificates associated with it.

Note: During server setup, you can use an existing certifier ID instead of creating a new one. The certifier ID that you specify cannot have multiple passwords assigned to it. Attempting to user a certifier ID with multiple passwords generates an error message and causes server setup to halt.

There are two types of certifier IDs: organization and organizational unit.

Organization certifier ID

The organization certifier appears at the top of the name tree and is usually the name of the company -- for example, Acme. During first server setup, the Server Setup program creates the organization certifier and stores the organization certifier ID file in the Domino data directory, giving it the name CERT.ID. During first server setup, this organization certifier ID automatically certifies the first Domino server ID and the administrator's user ID.

If your company is large and decentralized, you might want to use the Domino Administrator after server setup to create a second organization certifier ID to allow for further name differentiation -- for example, to differentiate between company subsidiaries.

For more information on working with multiple organizations, see the topic ″Domino domains″ earlier in this chapter.

Organizational unit certifier IDs

The organizational unit certifiers are at all the branches of the tree and usually represent geographical or departmental names -- for example, East/Acme or Sales/East/Acme. If you choose to, you can create a first-level organizational unit certifier ID during server setup, with the result that the server ID and administrator's user ID are stamped with the organizational unit certifier rather than with the organization certifier. If you choose not to create this organizational unit certifier during server setup, you can always use the Domino Administrator to do it later -- just remember to recertify the server ID and administrator's user ID.

For information on recertifying user IDs, see the chapter ″Setting Up and Managing Notes Users.″ For information on recertifying server IDs, see the chapter ″Maintaining Domino Servers.″

You can create up to four levels of organizational unit certifiers. To create first-level organizational unit certifier IDs, you use the organization certifier ID. To create second-level organizational unit certifier IDs, you use the first-level organizational unit certifier IDs, and so on.

Using organizational unit certifier IDs, you can decentralize certification by distributing individual certifier IDs to administrators who manage users and servers in specific branches of the company. For example, the Acme company has two administrators. One administers servers and users in West/Acme and has access to only the West/Acme certifier ID, and the other administers servers and users in East/Acme and has access to only the East/Acme certifier ID.

Certifier security

By default, the Server Setup program stores the certifier ID file in the directory you specify as the Domino data directory. When you use the Domino Administrator to create an additional organization certifier ID or organizational unit certifier ID, you specify where you want the ID stored. To ensure security, store certifiers in a secure location -- such as a disk locked in a secure area.

User ID recovery

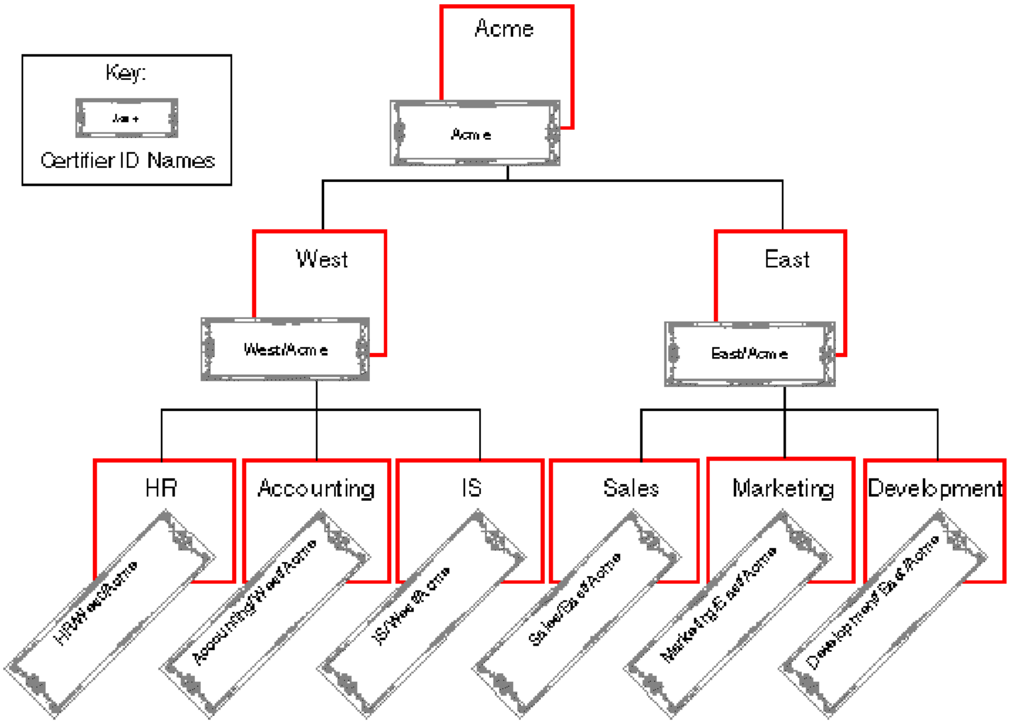
To provide ID and password recovery for Notes users, you need to set up recovery information for each certifier ID. Before you can recover user ID files, you need access to the certifier ID file to specify the recovery information, and the user ID files themselves must be made recoverable. There are three ways to do this:

- At user registration, create the ID file with a certifier ID that contains recovery information.
- Export recovery information from the certifier ID file and have the user accept it.
- (Only for servers using the server-based certification authority) Add recovery information to the certifier. Then, when existing users authenticate to their home server, their IDs are automatically updated.

For more information, see the chapter ″Protecting and Managing Notes IDs.″

Example of how certifier IDs mirror the hierarchical name scheme

To implement their hierarchical name scheme, the Acme company created a certifier ID at each branch of the hierarchical name tree:



To register each server and user, Acme does the following:

- Creates /Acme as the organization certifier ID during first server setup.
- Uses the /Acme certifier ID to create the /East/Acme and /West/Acme certifier IDs.
- Uses the /East/Acme certifier ID to register servers and users in the East coast offices and uses the /West/Acme certifier ID to register servers and users in the West coast offices.
- Uses the /East/Acme certifier ID to create the /Sales/East/Acme, /Marketing/East/Acme, and /Development/East/Acme certifier IDs.
- Uses the /West/Acme certifier ID to create the /HR/West/Acme, /Accounting/West/Acme, and IS/West/Acme certifier IDs.
- Uses the /Sales/East/Acme, /Sales/Marketing/Acme, and Development/East/Acme certifier IDs to register users and servers in the East coast division.
- Uses the /HR/West/Acme, /Accounting/West/Acme, and IS/West/Acme certifier IDs to register users and servers in the West coast division.

For more information on hierarchical name schemes, see the topic ″Hierarchical naming for users and servers″ earlier in this chapter.

Domino server services

Before you start the Server Setup program, decide which services and tasks to set up on the server. If you don’t select the services during the setup program, you can later enable them by editing the ServerTasks setting in the NOTES.INI file or by starting the server task from the server console.

Internet services

The Domino Server Setup program presents these selections for Internet services:

- Web Browsers (HTTP Web services)

- Internet Mail Clients (SMTP, POP3, and IMAP mail services)
- Directory services (LDAP)

Advanced Domino services

These Domino services, which are necessary for the proper operation of the Domino infrastructure, are enabled by default when you set up a Domino server:

- Database Replicator
- Mail Router
- Agent Manager
- Administration Process
- Calendar Connector
- Schedule Manager
- DOLS (Domino Off-Line Services)

These are optional advanced Domino server services that you can enable:

- DIIOP CORBA Services
- DECS (Domino Enterprise Connection Services)
- Billing
- HTTP Server
- IMAP Server
- ISpy
- LDAP Server
- POP3 Server
- Remote Debug Server
- SMTP Server
- Stats
- Statistic Collector
- Web Retriever

Note: It is best to use activity logging instead of the billing service.

For more information on activity logging, see the chapter ″Planning the Service Provider Environment.″

Table of Domino naming requirements

Consider these guidelines when naming parts of the Domino system.

Name	Characters	Tips
Domino domain	31 maximum	• This is usually the same as the organization name. • Use a single word, made up of only alpha (A-Z) or numeric (0-9) characters.
Notes named network	31 maximum	• By default, the Server Setup program assigns names in the format *port name* network -- for example, TCP/IP network. • Edit Notes named network names to use an identifier such as the location of the Notes named network and the network protocol -- for example, TCPIP-Boston.

Name	Characters	Tips
Organization	3-64 maximum*	• This name is typically the same as the Domino domain name. • The organization name is the name of the certifier ID and is appended to all user and server names.
Organizational unit	32 maximum*	• There can be up to four levels of organizational units.
Server	79 maximum	• Choose a name you want to keep. If you change a server name, you must recertify the server ID. • Choose a name that meets your network's requirements for unique naming. On TCP/IP, use only the characters 0 through 9, A through Z, and - (dash). On NetBIOS, the first 15 characters must be unique. On SPX, the first 47 characters must be unique. • Keep in mind that Domino performs replication and mail routing on servers named with numbers before it does those tasks on servers named with alphabetic characters.
User	79 maximum*	• Use a first and last name. A middle name is allowed, but usually not needed.
Alternate user	No minimum	• Can have only one alternate name
Group	62 maximum	• Use any of these characters: A - Z, 0 - 9, & - . _ ' / (ampersand, dash, period, space, underscore, apostrophe, forward slash). The only characters that are expressly prohibited are @ and //. **Note:** You can create groups with hierarchical distinguished names (DN). However, you must surround the forward slash (/) in a component value of a DN by surrounding it with double quotes. For example, 24″/″7 Support. **Note:** Do not create group names containing a / (slash) unless you are working in a hosted environment. Using the / in group names in a non-hosted environment causes confusion with hierarchical naming schemes. Hierarchical names are required in a hosted environment. • For mail routing, you can nest up to five levels of groups. For all other purposes, you can nest up to six levels of groups.
Port	No maximum	• Do not include spaces
Country code	0 or 2	• Optional

* This name may include alpha characters (A - Z), numbers (0 - 9), and the ampersand (&), dash (-), period (.), space ( ) , and underscore (_).

For more information on network name requirements and the effect that server name format has on network name-to-address resolution, see the chapter ″Setting Up the Domino Network.″

Building the Domino environment

After installing the first Domino server and any additional servers, you configure the servers and build the environment.

This overview lists the features that you may want to include in your Domino environment.

1. Create Connection documents for server communication.

2. If you have mobile users, set up modems, dialup support, and RAS.
3. Set up mail routing
4. Establish a replication schedule.
5. Configure incoming and outgoing Internet mail (SMTP).
6. Customize the Administration Process for your organization.
7. Plan and create policies before you register users and groups.
8. Register users and groups.
9. Determine backup and maintenance plans and consider transaction logging.
10. Consider remote server administration from the Domino console or Web Administrator console. Also consider the use of an extended administration server.
11. Set up a mobile directory catalog on Notes clients to give Notes users local access to a corporate-wide directory.
12. Consider implementing clustering on servers.

    For information about clustering, see the book *Administering Domino Clusters.*

Chapter 2. Setting Up the Domino Network

This chapter describes planning concepts and presents protocol-specific procedures required to run Domino on a network. The chapter describes using network protocols from a Domino perspective and does not provide general network information.

Lotus Domino and networks

A variety of client systems can use wireless technology or modems to communicate with Domino servers over local area networks (LANs), wide area networks (WANs), and metropolitan area networks (MANs). To govern how computers share information over a network, they use one or more protocols, which are sets of rules. For example, Notes workstations and Domino servers use the Notes remote procedure call (NRPC) protocol running over the LAN's network protocol to communicate with other Domino servers. Other client systems, such as Web browsers, Internet mail clients, wireless application protocol (WAP) devices, and personal information management (PIM) devices, can also communicate with Domino servers.

Isolated LANs can be connected by WANs. A WAN is either a continuous connection -- such as a frame-relay, leased telephone line, or digital subscriber line (DSL) -- or a dialup connection over a modem or Integrated Services Digital Network (ISDN) line. Dialup connections are either to an individual server or to a LAN (through a provider network or your company's own communications server).

Buildings or sites that are geographically close to each other can use a MAN, which is a continuous, high-speed connection that can connect corporate LANs or connect a LAN to the WAN. Like a WAN, a MAN is usually shared by multiple organizations.

Wireless technology that works with Domino ranges from localized transmission systems (802.11a or 802.11b) to national or international satellite transmission systems that are geostationary, mid-orbit, or tracked orbit.

If you are planning a network for geographically dispersed locations, consider how to achieve a cost-effective infrastructure. Placing servers in one location requires that users in other locations access the Domino server across WAN connections, which can be slow and expensive. Placing servers in every location and replicating databases to make the same information available on several LANs requires attention to administration at each location. One effective way to set up a network is to use a hub server at each location to handle communication with hub servers in other locations. Then, only the hub servers, not every server in the network, use WAN connections.

The functionality of Notes workstations and Domino servers depends on the effectiveness and capacity of networks. To plan a Domino network with sufficient capacity, you must consider not only the traffic to and from Domino servers but also any other traffic on the network.

NRPC communication

Domino servers offer many different services. The foundation for communication between Notes workstations and Domino servers or between two Domino servers is the Notes remote procedure call (NRPC) service.

Network protocols for NRPC communication

To communicate, two computers must run the same network protocol and software driver. For dialup connections, Lotus Domino uses its own X.PC protocol natively; Notes and Domino also support PPP using either Microsoft Dialup Networking (DUN) or Remote Access Service (RAS) for network dialup. In addition, you can use any IETF-compliant PPP communications server to dial into the network on which the Domino server resides or though which the server can be accessed.

For more information on dialup connections, see the chapter ″Setting Up Server-to-Server Connections.″

On LANs, Lotus Domino is compatible with the TCP/IP and NetBIOS over the lower transport IP For NetBIOS connections to work, both Notes workstations and Domino servers must use the same lower transport.

For detailed information on which protocols are compatible with Lotus Domino for each supported operating system, see the*Release Notes*.

Notes network ports

During the Server Setup program, Domino provides a list of Notes network ports based on the current operating system configuration. If these ports are not the ones you want to enable for use with the Domino server, you can edit the list during setup.

Because each network protocol consumes memory and processing resources, you might want to exclude one or more ports and later remove the associated protocol software from the system.

In TCP/IP and NetBIOS, you can install multiple network interface cards (NICs) and enable additional Notes network ports for each protocol, using the NOTES.INI file to bind each port to a separate IP address or NetBIOS LANA number.

For more information, see the topic ″Adding a network port on a server″ later in this chapter.

Notes named networks

Consider Notes named networks in your planning. A Notes named network (NNN) is a group of servers that can connect to each other directly through a common LAN protocol and network pathway -- for example, servers running on TCP/IP in one location. Servers on the same NNN route mail to each another automatically, whereas you need a Connection document to route mail between servers on different NNNs.

When you set up Server documents, be sure to assign each server to the correct NNN. Lotus Domino expects a continuous connection between servers that are in the same NNN, and serious delays in routing can occur if a server must dial up a remote LAN because the remote server is inadvertently placed within the NNN. Also bear in mind that the Notes Network field for each port can contain only one NNN name, and no two NNN names can be the same.

NNNs affect Notes users when they use the Open Database dialog box. When a user selects Other to display a list of servers, the servers displayed are those on the NNN of the user’s home server for the port on which the Notes workstation communicates with the home server. Also, when users click on a database link or document link, if a server in their home server’s NNN has a replica of that database, they can connect to the replica.

Note: If a server is assigned to two NNNs in the same protocol, as in the case where the server has two Notes network ports for TCP/IP, a Notes workstation or Domino server connecting to that server uses the NNN for the port listed first in the Server document.

Resolving server names to network addresses in NRPC

Communications between Lotus Notes and Lotus Domino run over the NRPC protocol on top of each supported LAN protocol. When a Notes workstation or Domino server attempts to connect to a Domino server over a LAN, it uses a combination of the built-in Notes Name Service and the network protocol’s name-resolver service to convert the name of the Domino server to a physical address on the network.

The Notes Name Service resolves Domino common names to their respective protocol-specific names. Because the Notes Name Service resolves common names by making calls to the Domino Directory, the service becomes available to the Notes workstation only after the workstation has successfully connected to its home (messaging) server for the first time. (The protocol name-resolver service normally makes the first connection possible.) When the Notes workstation makes a subsequent attempt to connect to a Domino server, the Notes Name Service supplies it with the Domino server's protocol-specific name -- that is, the name that the server is known by in the protocol's name service -- which is stored in the protocol's Net Address field in the Server document. The protocol's name-resolver service then resolves the protocol-specific name to its protocol-specific address, and the workstation is able to connect to the server.

Note: When resolving names of Domino servers that offer Internet services, Lotus Notes uses the protocol's name-resolver service directly.

How name resolution works in NRPC

A Notes workstation or Domino server follows these steps to resolve the name of the Domino server to which it is trying to connect over NRPC.

Note: If the Net Address field in the Server document contains a physical address -- a practice that is not recommended in a production environment-- the Notes Name Service performs the resolve directly, thus placing the burden of maintaining physical address changes on the Domino administrator.

1. If the workstation/server has a Connection document for the destination server that contains the protocol-specific name, the workstation/server passes the protocol-specific name to the protocol's name-resolver service. If the Connection document contains a physical address, the Notes Name Service performs the resolve directly. Normal-priority Connection documents are checked first, and then low-priority Connection documents.

   Note: Unlike in Server documents, adding physical addresses in Connection documents is not discouraged, since only the local workstation/server uses the Connection document.
2. To determine if the destination server's protocol-specific name is cached, the workstation checks the Location document and the server checks its own Server document. If the name is cached, the workstation/server uses the last-used Notes network port to determine the protocol and passes this value to the protocol's name-resolver service.
3. If the protocol-specific name is not cached, one of the following occurs, based on the list order of enabled Notes network ports:
   - For a Notes workstation connected to the home (messaging) server, Notes gives the common name of the destination Domino server to the home server, which looks in the Domino Directory for the Server document of the destination server. The home server locates the contents of the Net Address field for the Notes named network that the Notes workstation has in common with the destination server and passes this name to the protocol's name-resolver service. If the workstation and the destination server are in the same Domino domain but not in the same Notes named network, the home server locates the names of each protocol that the workstation has in common with the destination server and passes each to the appropriate protocol until a resolve is made. If the Notes workstation can't access its home server, it connects to its secondary Notes name server, which carries out the same actions as the home server.
   - For a Domino server, Domino checks the Server document for the destination server, locates the contents of the Net Address field for the Notes named network that the Domino server has in common with the destination server, and passes this name to the protocol's name-resolver service. If the destination server is in the same Domino domain as the Domino server, but not in the same Notes named network, the Domino server locates the protocol name of each protocol that it has in common with the destination server and passes each to the appropriate protocol until a resolve is made.
4. If Steps 1 through 3 do not produce the server's network address, the workstation/server offers the Domino common name of the destination server to the name-resolver service of each protocol, based on the order of the enabled network ports in the Server document.

Network security

Physical network security is beyond the scope of this book, but you must set it up before you set up connection security. Physical network security prevents unauthorized users from breaking through the network and using one of the operating system's native services -- for example, file sharing -- to access the server. Physical network security also comes into play when any data is exposed, as the potential exists for malicious or unauthorized users to eavesdrop both on the network where the Domino system resides and on the system you are using to set up the server.

Network access is typically controlled using network hardware -- such as filtering routers, firewalls, and proxy servers. Be sure to enable rules and connection pathways for the services that you and others will access.

Newer firewall systems offer virtual-private-network (VPN) services, which encapsulate the TCP/IP packet into another IP wrapper where the inner TCP/IP packet and its data are encrypted. This is a popular way to create virtual tunnels through the Internet between remote sites. If you want to have the Domino server access both a private VPN and the Internet for SMTP mail, make sure your solution is able to handle full TCP data packets and that it allows dual connections. If not, the Domino server system may require a second NIC to work around limitations of the VPN solution.

For more information, see the chapter ″Controlling Access to Domino Servers.″

NRPC and Internet connection security

To control connection access, you typically use a network hardware configuration, such as a firewall, reverse proxy, or Domino passthru server, to which you can authorize connections and define access to network resources.

In addition, you can encrypt all connections by service type. Encrypting connections protects data from access by malicious or unauthorized users. To prevent data from being compromised, encrypt all Domino and Notes services that connect to public networks or to networks over which you have no direct control. Encrypting the connection channel prevents unauthorized users from using a network protocol analyzer to read data.

To encrypt NRPC network traffic, use the Notes port encryption feature. For traffic over Internet protocols, use SSL. For both NRPC and Internet protocols, you can enforce encryption at the server for all inbound and outbound connections. In the case of the Notes client, you can also enforce encryption on all outbound connections, even if the server to which you are connecting allows unencrypted connections.

Because encryption adds additional load to the server, you may want to limit the services for which the server uses encryption. Other ways to minimize the load that encryption puts on the system include:

- Using an additional Domino server acting as a passthru server for NRPC connections
- Using a reverse proxy to manage authentication and encryption outside of Domino servers when using SSL
- Removing unnecessary or unused protocols or services on the server system as well as Domino server services

For more information, see the chapters ″Installing and Setting Up Domino Servers″ and ″Setting Up SSL on a Domino Server.″

Using a Domino passthru server as a proxy

A proxy is a system that understands the type of information transmitted -- for example, NRPC or HTTP-format information -- and controls the information flow between trusted and untrusted clients and servers. A proxy communicates on behalf of the requester and also communicates information back to the requester. A proxy can provide detailed logging information about the client requesting the information and the information that was transmitted. It can also cache information so requesters can quickly retrieve information again.

A proxy stops direct access from an untrusted network to services on a trusted network. If an application proxy is in use, then application-specific heuristics can be applied to look at the connections from the untrusted networks and determine if what is being requested is legal or safe.

An application proxy resides in the actual server application and acts as an intermediary that communicates on behalf of the requester. An application proxy works the same as a packet filter, except the application proxy delivers the packet to the destination. An application proxy can be used with any protocol, but it is designed to work with one application. For example, an SMTP proxy understands only SMTP.

A circuit-level proxy is similar to an application proxy, except that it does not need to understand the type of information being transmitted. For example, a SOCKS server can act as a circuit-level proxy. You can use a circuit-level proxy to communicate using Internet protocols with TCP/IP -- that is, IMAP, LDAP, POP3, SMTP, IIOP, and HTTP, as well as Internet protocols secured with SSL.

HTTP is a special case. In Domino, when the HTTP Connect method is used by an HTTP proxy, applications using other protocols can also use the HTTP proxy, but they use it as a circuit-level proxy, not as an application proxy. SSL uses the HTTP Connect method to get through an application proxy because the data is encrypted and the application proxy cannot read the data. HTTPS (HTTP and SSL) use both the HTTP proxy and the Connect method, which implies that the HTTP proxy is a circuit-level proxy for HTTPS. The same method is used to get NRPC, IMAP, and other protocols through the HTTP proxy.

You can set up a Domino passthru server as an application proxy for NRPC. A passthru server provides all levels of Notes and Domino security while allowing clients who use dissimilar protocols to communicate through a single Domino server. The application proxy does not allow Internet protocols -- for example, HTTP, IMAP, and LDAP -- to use a Domino passthru server to communicate, however. For Internet protocols, you can use an HTTP proxy with the HTTP Connect method to act as a circuit-level proxy.

A Notes client or Domino server can also be a proxy client and interoperate with either passthru (NRPC protocol only) or as a SOCKS or HTTP tunnel client (for NRPC, POP3, LDAP, IMAP, and SMTP protocols). You set this up in the Proxy setting in the client Location document.

To set up a Domino passthru server as an application proxy

When you set up an application proxy, make sure the following Domain Name System (DNS) services are correctly configured:

- The databases db.DOMAIN and db.ADDR, which DNS uses to map host names to IP addresses, must contain the correct host names and addresses.
- Hosts files must contain the fully qualified domain name of the servers.

If you are using the Network Information Service (NIS), you must use the fully qualified domain name and make sure NIS can coexist with DNS.

For information on configuring these settings, see the documentation for your network operating system.

You must first connect the server to the untrusted network -- for example, the Internet -- and then set up Notes workstations and Domino servers to use the passthru server as a proxy when accessing services outside the trusted network.

To set up a workstation or server to use the passthru server, you must specify the passthru server in the Location document for a workstation and in the Server document for a server.

For more information on connecting a server to the Internet and passthru servers, see the chapter ″Setting Up Server-to-Server Connections.″

TCP/IP security considerations

In a TCP/IP network, configure all Domino servers to reject Telnet and FTP connections. Furthermore, do not allow file system access to the Domino server or the operating system on which it runs, unless you are sure you can properly maintain user access lists and passwords and you can guarantee a secure environment.

If you use the Network File System (NFS) without maintaining the password file, users can breach security by accessing files through NFS instead of through the Domino server. If this ″back door″ access method is needed, isolate the network pathway on a LAN NIC and segment, and make sure that the ability to access files through NFS is exclusive to this isolated secure network.

Mapped directory links and Domino data security

To ensure data security, do not create a mapped directory link to a file server or shared Network Attached Storage (NAS) server for a Domino server. These links can cause both database corruption and security problems.

Database corruption

If the network connection fails while the Domino server is writing to a database on the file server or shared NAS server, the database can become corrupted. In addition, the interdependence of the file sharing protocols -- Server Message Block (SMB), Common Internet File System (CIFS), and Network File System (NFS) -- and the remote file system can affect the Domino server's performance. Domino sometimes needs to open large numbers of remote files, and low latency for read/write operations to these files is desirable.

To avoid these problems on Domino servers, consider doing one or more of the following:

- Create an isolated network and use cut-through (non-buffering) layer-2 switches to interconnect the Domino server to the NAS system.
- Limit access to the NAS system to the Domino server.
- Reduce the number of hops and the distance between hops in the connection pathways between the Domino server and the storage system.
- Use a block protocol instead of a file protocol.
- Use a private storage area network (SAN) instead of a shared NAS system.
- Avoid creating any file-access contention between Domino and other applications.

To avoid problems with Notes workstations, consider doing the following:

- Locate Notes workstations so that they are not accessing a remote file server or NAS system over a WAN.
- To minimize the risk of database corruption because of server failure when a Notes client's Domino data directory is on a file server or NAS server, evaluate the reliability of the entire network pathway as well as the remote system's ability to maintain uninterrupted sessions to the Notes client over the file sharing protocols it is using (SMB, CIFS, NFS, NetWare Core Protocol, or AppleShare).
- If a Notes client's Domino data directory is on a file server or NAS server, remember that only one user (user session) can have the user data directory files open a time. Lotus Notes does not support concurrent access to the same ″local″ database by two clients.

Security problems

When ″Encrypt network data″ is enabled, all Domino server and Notes workstation traffic is encrypted. However, the file I/O between the Domino server and the file server or shared NAS server is not encrypted, leaving it vulnerable to access by unauthorized users.

Planning the TCP/IP network

The default TCP/IP configuration for a Domino server is one IP address that is globally bound, meaning that the server listens for connections at the IP addresses of all NICs on the computer. Global binding works as long as the computer does not have more than one IP address offering a service over the same assigned TCP port.

For operating system requirements, see the *Release Notes*.

The default configuration

Use these topics to plan how to integrate Lotus Domino with the TCP/IP network when the Domino server has one IP address and is not partitioned:

- NRPC name-to-address resolution over TCP/IP
- Ensuring DNS resolves in TCP protocols

Advanced configurations

Use these topics to plan how to integrate Lotus Domino with the TCP/IP network when the Domino server has more than one IP address or is partitioned:

- Advanced Domino TCP/IP configurations
- Partitioned servers and IP addresses
- Ensuring DNS resolves in advanced TCP/IP configurations

Changing a server's IP address

Use this topic to change a server's IP address:

- Changing a server's IP address

Moving to IPv6

This topic provides the information you need if your company is migrating to the IPv6 standard:

- IPv6 and Lotus Domino

NRPC name-to-address resolution over TCP/IP

In the TCP/IP protocol, the method most commonly used to resolve server names to network addresses is the Domain Name System (DNS), an Internet directory service developed both to allow local administrators to create and manage the records that resolve server names to IP addresses and to make those records available globally. While the POP3, IMAP, LDAP, and HTTP services use DNS directly, the NRPC service uses a combination of the Notes Name Service and DNS to resolve server names to network addresses.

For background information on how the Notes Name Service works with name-resolver services such DNS, see the topic ″Resolving server names to network addresses in NRPC″ earlier in this chapter.

Within DNS, ″domain″ refers to a name space at a given level of the hierarchy. For example, the .com or .org in a Web URL represents a top-level domain. In a domain such as acme.com, a DNS server -- that is, a server running DNS software -- in the Acme company stores the records for all Acme servers, and an administrator at Acme maintains those records.

When you set up a Notes workstation on the TCP/IP network, you normally rely on DNS to resolve the name of the workstation's Domino home server the first time the workstation tries to connect to it. As long as the Notes workstation and Domino home server are in the same DNS domain level, DNS can accomplish the resolve.

When to edit the Net Address field in the Server document

The default format for a server's TCP/IP network address in Lotus Domino is its fully qualified domain name (FQDN) -- for example, app01.acme.com -- based on the DNS record and the IP address references in the system's TCP/IP stack. When a Notes workstation or Domino server requests this name, the TCP/IP resolver passes it to DNS, and DNS resolves the name directly to the IP address of the destination server, regardless of the DNS domain level of the requesting system.

If you do not want to enter the FQDN in the Net Address field, you can change it to the simple IP host name -- for example, app01 -- either during server setup or later by editing the Server document. For example, you might use the simple IP host name if you are setting up multiple TCP ports for NRPC, a configuration in which using the FQDN for each network address can cause connection failures if the Notes Name Service returns the FQDN for the wrong TCP port. In this case, using the simple IP host name ensures that DNS does a lookup in *all* domain levels within the scope of the domains defined in the requesting system's TCP/IP stack settings.

CAUTION:
In a production environment, do not use IP addresses in Net Address fields. Doing so can result in serious administrative complications if IP addresses change or if Network Address Translation (NAT) connections are used, as the values returned by the Notes Name Service will not be correct.

Secondary name servers

To ensure that the Notes Name Service is always available over TCP/IP, when you set up a Notes user, you can designate a Domino secondary name server that stands in for the home server in these situations:

- The user's home server is down.
- The user's home server is not running TCP/IP.
- The user's home server cannot be resolved over TCP/IP.

Note: In companies using multiple DNS domains, a Domino secondary name server ensures that a Notes workstation can connect with its home server even when the home server is in a different DNS domain. You can use policies to automate the setup of secondary name servers.

For more information, see the topic ″Ensuring DNS resolves in NRPC -- Best practices″ later in this chapter. For information on policies, see the chapter ″Using Policies.″

Special case: The passthru server

By connecting to a passthru server, Notes users can access servers that do not share a network protocol with their systems. If both the Notes workstation and destination server are in a different Domino domain from the passthru server, it may not be possible for the passthru server to resolve the name of the destination server. In this case, do one of the following:

- On the Notes workstation, create a Connection document that includes the IP address of the destination server.
- On the passthru server, create a Connection document to the destination server.

For more information on passthru servers, see the chapter ″Setting Up Server-to-Server Connections.″

Internal alternatives to DNS

If you don't use DNS at your site or if a Domino server is not registered with DNS (as is sometimes the case if the server offers Internet services), use one of these methods to enable each Notes workstation and Domino server to perform name resolution locally. Keep in mind that the upkeep required for both of these approaches is considerable.

- Place a hosts file, which is a table that pairs each system name with its IP address, on every system that needs private access. Set up each system so that it accesses the hosts file before accessing DNS.

- Create a Connection document that contains the destination server's IP address on every Notes workstation and Domino server that needs to access that server.

  Tip: Use policies to automate the setup of Connection documents for Notes users. Even if you use DNS, you should set up Connection documents for Notes users in locations from which they have difficulty accessing the DNS server.

  For more information on policies, see the chapter ″Using Policies.″

Alternative IP name services

Microsoft networking services offers four additional methods of IP address resolution. These methods are not as reliable as traditional DNS and hosts files and can cause name and address confusion. For best results, do not use these methods when also using the Notes network port for TCP/IP.

- Direct NetBIOS broadcast -- The system sends out a name broadcast message so that all of the systems on the local network segment can register the name and IP address in their name cache. If you must use NetBIOS over IP and use Domino with both the NetBIOS and TCP/IP port drivers, avoid name-resolution problems by giving the Domino server and the system different names.

Master Browser cache (for NT domains or SAMBA servers) -- Collects broadcasted names and IP addresses and publishes them across the NT domain to other Master Browser systems for Windows ® systems to access in their name lookups.

- Windows Internet Name Service (WINS) -- Uses NetBIOS broadcasts. Unlike DNS, which is static in nature, WINS is dynamic. Note that the TCP/IP stacks of Macintosh and UNIX client systems may not be able to access the WINS server.
- LAN Manager Hosts (LMHosts) -- A static hosts file method.

CAUTION:
On a Windows system, the combination of the system's native NetBIOS over IP name-resolver service and DNS can cause name resolution failure for the Domino server name.

For information on avoiding this problem, see the topic ″Server name-to-address resolution over NetBIOS″ later in this chapter.

Ensuring DNS resolves in TCP protocols

When you register a new Domino server, you specify a common name for it. Within a Domino hierarchical name, the common name is the portion before the leftmost slash. For example, in the name App01/East/Acme, the common name is App01. The common name, not the hierarchical name, is the name that the Domino server is known by in DNS.

Note: When you choose a common name for a Domino server that uses DNS, use only the characters 0 through 9, A through Z, and the dash (-). Do not use spaces or underscores.

Note: The DNS names held in Lotus Notes and Lotus Domino are not case sensitive; Notes workstations and Domino servers always pass DNS names to DNS in lowercase.

You can avoid problems and extra work if you consider the DNS configuration, as well as the effect of other protocol name-resolver services, when you choose the format for the common name of the Domino server.

To avoid name-resolution problems that affect all TCP services on Windows systems, see the topic ″Ensuring DNS resolves on Windows systems -- All TCP protocols.″

For procedures to help you avoid DNS problems in NRPC, see these topics:

- Ensuring DNS resolves in NRPC -- Best Practices
- Ensuring DNS resolves in NRPC -- Alternative practices

- Ensuring DNS resolves in NRPC -- A practice to use with caution

Note that these procedures apply only to servers handling communications between Lotus Notes and Lotus Domino (NRPC services). If you administer servers that provide Internet services such as HTTP, SMTP, POP3, or LDAP, you can skip these topics, as these services use DNS directly.

For naming requirements when using Domino Off-Line Services (DOLs) or Domino Web Access, see the chapter ″Installing and Setting Up Domino Servers.″

Ensuring DNS resolves on Windows systems -- All TCP protocols

If a Domino server is a Windows system, often two name services exist on the system -- NetBIOS over IP and DNS. If you assign the same name to both the Domino server and the system, client applications that use either the Notes Name Service or DNS can encounter name-space ghosting between the two names. In other words, because the NetBIOS record for a system's host name has already been found, the name resolving process ends and the DNS record for the Domino server on that system is never found.

Note: For a Domino server on Windows 2000, problems occur only if you enable name services for NetBIOS over IP in order to join an NT domain using Server Message Blocks (SMB).

To prevent this problem:

1. Add a preface such as W2K- to the system name, using the Network Identification tab on the System Properties dialog box.
2. Create an A record (or, for IPv6, AAAA record) in DNS for the system name. The IP address is the same as the one for the Domino server.
3. Create a CNAME record in DNS for the Domino server's name, linking it to the system name.

For example, for the Domino server BosMail02/Acme, the common name is BosMail02. You name the system NT-BosMail02. You create an A record in DNS for NT-BosMail02.acme.com and a CNAME record for BosMail02.acme.com, linking it with NT-BosMail02.acme.com.

Ensuring DNS resolves in NRPC -- Best practices

The following procedures provide the best name-resolution practices for a Domino server using the default NRPC configuration on a TCP/IP network (one Notes network port for TCP/IP). These procedures address the following DNS configurations:

- One DNS domain
- Multiple DNS domain levels

If your TCP/IP configuration has multiple Notes network ports for TCP/IP, see the topic ″Ensuring DNS resolves in advanced TCP/IP configurations″ later in this chapter.

When you have one DNS domain: If your company uses only one DNS domain, doing the following eliminates the need for CNAME records in DNS:

1. Assign the same name as both the Domino server common name and the simple IP host name registered with DNS.
2. Make sure the Net Address field on the Server document contains the server's FQDN.
3. Create an A record (or, for IPv6, AAAA record) in DNS.

For example, you set up the Domino server App01/Engr/Acme. Thus, you register the server with DNS as app01, the server's common name. The Net Address field in the Server document contains app01.acme.com (the server's FQDN), and the A record is: app01.acme.com IN A 192.168.10.17.

When you have multiple DNS domain levels: If your company uses multiple DNS domain levels -- for example, when each country in which a multinational company has offices is a subdomain in DNS --

doing the following eliminates the need for multiple CNAME records in DNS and ensures that DNS lookups always work, regardless of the DNS domain level of the user's system:

1. Assign the same name as both the Domino server common name and the simple IP host name.
2. Make sure the Net Address field on the Server document contains the server's FQDN.
3. Create an A record (or, for IPv6, AAAA record) in DNS.
4. If users' systems are in a different DNS domain than that of their home server or in a DNS subdomain of their home server's domain, set up a secondary name server. Place this secondary name server on the same physical network as the users' systems or on a network that the users can access.

   Note: Register the secondary name server in the root of the company's DNS domain.
5. Set up all Notes users or a subset of users affected by Step 4, or set up an individual Notes user.

   For more information on setting up groups of users, see the chapter ″Using Policies.″ For more information on setting up an individual Notes user, see the topic ″Setting up a secondary name server″ later in this chapter.

For example, you register the Domino server ParisMail01/Sales/Acme with DNS as parismail01.france.acme.com. Parismail01 is the home server for some users in the DNS subdomain spain.acme.com. You set up a secondary name server, Nameserver/Acme, register it with DNS as nameserver.acme.com, and ensure that the Location documents of users who need a secondary name server point to this server.

When a user in spain.acme.com attempts a first connection with the home server (parismail01.france.acme.com), the connection fails because the DNS subdomain for spain.acme.com has no records for the subdomain france.acme.com. Notes then connects successfully with the secondary name server (nameserver.acme.com), since the DNS subdomain for spain.acme.com does include the records for acme.com. When the secondary name server supplies the Notes workstation with the FQDN from the Net Address field in the Server document for ParisMail01, DNS resolves the FQDN to an IP address, and the user can access mail.

As long as all Server documents in the Domino domain have the TCP/IP network address in FQDN format, this approach allows any Notes workstation or Domino server to locate any Domino server, regardless of its DNS domain level.

Ensuring DNS resolves in NRPC -- Alternative practices

The following procedures provide alternative name-resolution practices for a Domino server using the default NRPC configuration on a TCP/IP network (one Notes network port for TCP/IP).

Domino server names that differ from their DNS names: When your name scheme for Domino servers is different than that for DNS, use one of the following methods to translate the Domino server's name to the host name:

- Create a local Connection document on each Notes client and Domino server that needs to connect to the Domino server, and enter the FQDN for the system that hosts the Domino server in the Net Address field. For example, for the Domino server named App01/Sales/Acme on the system registered with DNS as redflier, enter redflier.acme.com in the Net Address fields of the Connection documents.
- Use an alias (CNAME) record in DNS to link the Domino server common name to the simple IP host name. For example, for the Domino server App01/Sales/Acme on the system registered with DNS as redflier, use a CNAME record to link the name App01 to the name redflier. When a Notes workstation first accesses this server, it obtains the host name from the Net Address field of the Server document and caches it, thereby making future connections faster.

IP addresses in Connection documents: In situations in which you don't want to use any name-resolver service -- such as bringing up a new server system that you don't want known yet, or having a server on the Internet that you want accessible but for which you can't use DNS -- create Connection documents that directly tell Notes workstations or Domino servers how to access this Domino server by using the server's IP address in the documents' Net Address fields.

Network Address Translation (NAT): NAT is a method of translating an IP address between two address spaces: a public space and a private space.

Public addresses are assigned to companies by the Internet Corporation of Assigned Names and Numbers (ICANN) or leased from the company's ISP/NSP. Public addresses are accessible through the Internet (routable) unless firewalls and isolated networks make them inaccessible.

Private addresses are IP address spaces that have been reserved for internal use. These addresses are not accessible over the Internet (non-routable) because network routers within the Internet will not allow access to them.

The following address spaces have been reserved for internal use. It is best to use these IP addresses and not make up your own.

- Class A: 10.0.0.0 to 10.255.255.255
- Class B: 127.16.0.0 to 172.31.255.255
- Class C: 192.168.0.0 to 192.168.255.255

For example, users inside a company access the Domino server based on its assigned IP address, which is a private address (192.168.1.1). Internet users must access the Domino server through a NAT router, which converts the private address to one of its static public addresses (130.20.2.2). Therefore, a Notes client accessing the server from the Internet uses the public address.

Ensuring DNS resolves in NRPC -- A practice to use with caution

The following practice, if followed precisely, should ensure good DNS resolves in NRPC for companies with multiple DNS domain levels, but might result in extra work if the infrastructure changes. Using this practice has the following disadvantages:

- You can never assign more than one IP address in DNS to the Domino server.
- If the FQDN changes, the Domino server name will not match the FQDN, thus invalidating the DNS resolve. You will then need to create a new server and migrate users to it.
- If you use network address translation (NAT), the server's FQDN must be identical in both instances of DNS (internal and external shadow DNS).
- You cannot use other network protocols, as many of them use flat network name services, and those that use hierarchical name systems will not function unless the name hierarchy is exactly the same.
- Diagnosing connectivity issues can be much harder.

When you have multiple DNS domain levels: If your company uses multiple DNS domain levels -- for example, when each country in which a multinational company has offices is a subdomain in DNS -- do the following:

1. Use the server's FQDN as the Domino server common name.
2. Create an A record (or, for IPv6, AAAA record) in DNS.

For example, if you register a server with DNS as app01.germany.acme.com, you can also assign the Domino server's common name as app01.germany.acme.com. In this case, the server's Domino hierarchical name might be app01.germany.acme.com/Sales/Acme.

Changing a server's IP address

Before changing a server's IP address, consider the following potential problems:

- Problem 1: If the server's previous IP address is stored in any Server Connection documents or Server documents, when that server's IP address is changed in DNS and on the server itself, these old Server Connection documents or Server documents will cause connection failures.

Solution: Use the DNS fully-qualified domain name, not the IP address, as the network address stored in the Server Connection documents and Server documents. You can then change the server's IP address in DNS without having to change the Server Connection documents or Server documents. Changing the network address from the IP address to the DNS name can be done at any time.

To modify the Server Connection document, open the Server Connection document. On the Basics tab, if Local Area Network is chosen in the Connection Type field, click the Advanced tab and check the entry in the Destination server address field. If the field contains the server's IP address, delete the IP address and enter the fully-qualified domain name. Remember, both the server-based Domino Directory and the client-based Address Book can have this problem.

To modify the Server document, click the Ports tab for the Net Address for TCP ports. If the field contains the IP address, change the entry to the proper fully-qualified domain name.

- Problem 2: The algorithm that all Notes clients and Domino servers use to connect to a Domino server can cache the IP address that was used to successfully connect to a server. If this cache entry exists, when the server's IP address is changed, the old cached address may be used causing the connection to fail.

  It is important to understand why this caching is performed. Notes supports a wide range of networking technologies implemented as Notes ports. If Notes attempts to connect to a server that is down, and tries every possible technology (Notes port) using every possible Name to Address resolution tool until each one fails, the connection attempt takes a long time. To prevent the long delay that would occur in reporting the error when the server goes down, Notes has implemented two server connection algorithms. One algorithm is fast, using cached addresses, and the other is slower, using the complete algorithm which bypasses the cache when it fails.

  The following solutions can resolve this problem. Solutions are listed in the order in which they should be used.

  Solution 1: The fast connection algorithm is only used if the client or server had successfully connected to the same server earlier in the day. If a successful connection has not yet occurred today, the slower algorithm is used and the cache is bypassed. To avoid this problem, change a server's IP address late in the evening, but before midnight. This is the easiest solution because it is transparent to the user and involves no help desk calls or any action on the user's part.

  Solution 2: The cache is rewritten following successful connection to the server. The cached address is the address entered by the user, not the resolved IP address. Therefore, if users have the habit of connecting to servera/acme by entering servera.acme.com, the cached address will be servera.acme.com, not 1.2.3.4 and the problem will not occur.

  Solution 3: The cache is rewritten following any successful connection to the server. If a user tries to connect to the server by its Notes name, for example, servera/acme, the stale cache entry is used. If the user tries to connect using the server's fully-qualified domain name, for example, servera.acme.com, then the cache will not be used, the new address will be fetched from DNS and the correct new address entered in the cache. To make this successful connection using the fully-qualified domain name of the server, use the File - Database - Open menu command or the File - Preferences - User Preferences - Ports - Trace service menu selections.

  Solution 4: The cache is stored in the following Notes fields in the Location documents for the client and in the Server document for the server:

  - $Saved Addresses
  - $SavedDate
  - $SavedPorts
  - $SavedServers
  - $SavedTriedDate

  If these fields are deleted from the Location or Server document, for example, using a formula agent, the old IP addresses in the cache cannot be used. This method can be confusing because the Notes items are rewritten when the client or server exists from an in-memory copy. Therefore, to use this method to clear the cache for the client, create the agent in the Local Address Book, and then switch to the Island Location document and exit the client. Restart the client, and then run the agent to clear the cache for all other locations. Switch to your normal location.

Sample agent formula language code to clear the cache:

– FIELD $SavedAddresses:=@DeleteField;

– FIELD $SavedDate:=@DeleteField;

– FIELD $SavedPorts:=@DeleteField;

– FIELD $SavedTriedDate:=@DeleteField;

– FIELD $SavedServers:=@DeleteField;

– SELECT @All

Solution 5: Disable the use of the cached addresses by using the following NOTES.INI setting:

DONT_USE_REMEMBERED_ADDRESSES=1

If the client uses multiple or slow port technologies, we discourage the use of this technique because it can cause a long delay in reporting that a server is down.

IPv6 and Lotus Domino

Because support for IPv6 by hardware and operating system suppliers and the Internet is still in the early stages, moving to the IPv6 standard will be a gradual process for most organizations. In Lotus Domino, you can enable IPv6 support for SMTP, POP3, IMAP, LDAP, and HTTP services on AIX®, Solaris®, and Linux systems.

Domino supports both IPv6 and IPv4. Thus, if an IPv6-enabled Domino server encounters an IP address in IPv4 format, the Domino server can still make the connection to that address. When attempting to connect to a server, Domino tries to resolve all IP addresses for a server until one works. This allows a server to have both an IPv4 address and an IPv6 address. Domino caches the last successful address for a server and uses only the cached address to quickly search for a server. If you do not want to use only the cached address, enter the NOTES.INI setting DONT_USE_REMEMBERED_ADDRESSES=1.

In DNS, records that store IPv6 addresses are called AAAA records. After you enable IPv6 on a Domino server and add the server's AAAA record to DNS, another IPv6-enabled Domino server can connect to it *only* over IPv6. Servers that don't support IPv6 can run Domino with IPv6 support disabled, which is the default. These servers can successfully connect to IPv6-enabled Domino servers only if the DNS for the IPv6 servers contain A records.

Using IPv6 in a Domino network

For best results when using IPv6 with Domino servers, set up network devices in the network pathway to connect directly with native IPv6, rather than tunnel through the IPv4 network.

Enabling IPv6 on Notes and Domino 7

To enable IPv6 on Notes and Domino 7, add the setting TCP_ENABLEIPV6=1 to the NOTES.INI file on both the Notes client and the Domino server.

How Lotus Domino decides whether to connect over IPv6 or IPv4

A Domino server evaluates the address format and then, based on that information, makes an IPv4 or an IPv6 connection.

Address format	**Server response**
IPv4	Makes an IPv4 connection.
IPv4 address mapped to IPv6	Attempts to make an IPv6 connection and waits for the TCP/IP software to make either an IPv6 or IPv4 connection, depending on the remote system's TCP/IP stack.
IPv6	Makes an IPv6 connection.

Address format	Server response
Server name	Uses DNS to resolve the name: • If only an A record is found, connects over IPv4. • If only an AAAA record is found, connects over IPv6 or waits for the TCP/IP software to make the connection. • If both an A record and AAAA record are found, uses the AAAA record.

Using IPv6 address formats with Domino and Notes

You can use an IPv6 address as a string anywhere that an IPv4 address as a string can be used; however, IPv4 addresses with port numbers are supported by the Notes client and the Web server in the following format:

```
1.2.3.4:1352
```

IPv6 addresses contain a varying number of colons; therefore, the syntax shown above can not be used with IPv6 addresses. To be consistent with a proposed format for Web servers, if the port number is included with an IPv6 address, the address must be enclosed in square brackets.

The following address formats can be used wherever address strings are supported, for example, in Server documents, in the Open Database dialog box, or in the Port Trace dialog box.

```
9.95.77.78
9.95.77.78:1352
[9.95.77.78]
[9.95.77.78]:1352
fe80::290:27ff:fe43:16ac
[fe80::290:27ff:fe43:16ac]
[fe80::290:27ff:fe43:16ac]:1352
```

Installing the IPv6 stack

Install the IPv6 stack before IPv6 will work for any software. To install the IPv6 stack, follow the instructions provided for by your platform's vendor. The instructions in this section contain general guidelines for many platforms, but you need to follow the instructions provided by the manufacturer of your platform.

Prior to installing the IPv6 stack, check to see if IPv6 is configured on your system by using the following commands according to platform:

Platform	Commands
Microsoft Windows platforms	ipconfig /all
All other platforms	ifconfig -a

After installing IPv6, use that same command to verify that IPv6 is available.

Microsoft Windows 2003 server platform: To enable IPv6 on the Microsoft Windows 2003 server platform, use

```
netsh interface ipv6 install
```

Link local address automatically assigned

Microsoft Windows XP client: To enable IPv6 on the Microsoft Windows XP client, use

```
netsh interface ipv6 install
```

Link local address automatically assigned

AIX platform: To enable IPv6 on the AIX platform, enter

```
ifconfig le0 inet6 plumb up
```

Link local address automatically assigned

Solaris platform: To enable IPv6 on the Solaris platform, enter

```
ifconfig le0 inet6 plumb up
```

Link local address automatically assigned

United Linux platform: IPv6 is enabled by default on the United Linux platform.

Zones: In the IPv6 standard, when link local address and site local address are used, an additional parameter is required to specify the interface on which the address is valid. In the API, this additional parameter is called the scope_id; in user documentation, the parameter is called the zone. In Notes and Domino 7, use the format address string followed by the percent sign (%) followed by the zone.

On Microsoft Windows, the zone is an integer index into the interface list with the first interface being zone one.

Note the following information regarding zones:

- Zones are mandatory on Windows for link local addresses.
- Zones are mandatory on Linux for link local addresses.
- Zones are not required on AIX and Solaris.
- A zone is NOT a characteristic of the target system, but rather a characteristic of the source system; therefore, never attempt to put a zone into DNS, in a hosts file, or in a global data store such as the Domino Directory.
- If a computer has only a single network interface, you can use the NOTES.INI variable TCP_DEFAULTZONE to provide a default zone for all link local addresses.

Receiving incoming connections on IPv6 sockets or IPv4 sockets

UNIX platforms receive both IPv4 and IPv6 incoming connections on the same socket. Microsoft Windows is not capable of receiving both incoming IPv4 and IPv6 connections on the same socket. If IPv6 is disabled, Microsoft Windows only receives IPv4 connections. If IPv6 is enabled and the port is not bound to an address, only IPv6 connections are received. To receive both IPv4 and IPv6 connections, define two ports -- one bound to an IPv4 address and one bound to an IPv6 address. This is easily done for NRPC, but until now, Internet servers only provided support for a single Notes port.

Domino 7 supports two Notes ports for Internet servers. The user interface specifies two Notes port names in the NOTES.INI variable SMTPNotesPort. For example,

```
SMTPNotesPort=TCPIP,TCPIP6
```

There is one restriction. If either of the ports is shut down (stop port tcpip) the Internet servers momentarily shut down both ports and restart listening on the one remaining port. Also, outbound connections for any address will succeed on any TCP port. For outbound connections, Domino creates the proper socket to handle the attempted target address.

Making outbound connections with a TCP port bound to an IP address: When a client or a server making outbound connections has a TCP port bound to a specific IP address, using the NOTES.INI setting SMTPNotesPorts= <TCPIPAddress>, the bound port can only make outbound connections of the type of the bound IP Address. For example, if a server binds the Notes Port TCPIP to an IPV4 address and the Notes Port TCPIP6 to an IPV6 address, then port TCPIP can only make outbound connections to IPV4 addresses and port TCPIP6 can only make outbound connections to IPV6 addresses.

In a configuration that includes IPV4 and IPV6 Notes ports bound to IP addresses, the ports listed in the Connection documents must include all TCP ports over which the connection can possibly be made. For example, if you create a Server Connection document from serverA to serverB, and serverB's DNS name can resolve to both an IPV4 address and an IPV6 address, and you want the connection to work over IPV4 or IPV6, you must include both ports in the Connection document.

When an IPv4 or an IPv6 socket is created and used: Use the following set of rules to determine whether to use an IPv4 or IPv6 socket:

- When connecting or listening, if IPv6 is not enabled, always create an IPv4 socket.
- If connecting or listening with a bound address, use a socket that matches the address type.
- If listening and no address is bound, and if IPv6 is enabled, use an IPv6 socket.
- If listening and no address is bound, and if IPv6 is disabled, use an IPv4 socket.

Note: The address 0 indicates that a listener is willing to listen to any address. Applying the above set of rules, note the following:

- To create an IPv6 socket that listens to any IPv6 address, do not bind to an address.
- To create an IPv4 socket that listens to any IPv4 address, bind it to address ::ffff:0.0.0.0

On UNIX servers, an IPv6 socket bound to any address accepts all incoming connections, but on Windows the same socket only listens to incoming IPv6 connections.

On Linux, if one port binds to the ″any″ address and IPv6 is enabled, a second port cannot bind to a specific IPv4 or IPv6 address. If this is attempted, an ″Address is already in use″ error is returned.

Examples of using NOTES.INI variables with IPv6

This section contains examples of how to set NOTES.INI variables to support various platforms and configurations when using IPv6. In these examples, support for NRPC and SMTP is configured. The other Internet servers are configured similarly to SMTP.

Example 1-- No IPv6 support (Applies to all platforms): No change required. IPv6 is off by default.

Example 2 -- UNIX platform supporting all valid IPv4 and IPv6 addresses: TCP_EnableIPv6=1

Example 2 assumes that no ports are bound to any addresses. By default, on UNIX, the single unbound listening socket is IPv6. The IPv6 socket can receive connections from any IPv4 or IPv6 address.

Example 3 -- Microsoft Windows platform supporting all valid IPv4 and IPv6 addresses:
TCP_EnableIPv6=1

TCPIP=TCP, 0, 15, 0

TCPIP6=TCP, 0, 15, 0

PORTS=TCPIP,TCPIP6

TCPIP_TCPIPADDRESS=0,[::ffff:0.0.0.0]:1352

SMTPNotesPort=TCPIP,TCPIP6

Example 3 assumes that no ports are bound to any addresses. On Microsoft Windows, by default, the TCPIP6 port is an IPv6 socket because IPv6 is enabled. The TCPIP port is an IPv4 socket, because its bound address has the IPv4 format. Both listen to all addresses because the bound address is 0. The SMTPNotesPort variable is required to force the SMTP listener to listen on two sockets -- one for IPv4 and one for IPv6.

Example 4 -- UNIX (but not Linux 2.4) partitioned servers. Each server listens to its assigned IPv4 and IPv6 addresses only: Each Server:

```
TCP_EnableIPv6=1

TCPIP=TCP, 0, 15, 0

TCPIP6=TCP, 0, 15, 0

PORTS=TCPIP,TCPIP6

TCPIP_TCPIPADDRESS=0,9.33.162.84:1352

TCPIP6_TCPIPADDRESS=0,[fe80::209:6bff:fecd:5b93]:1352

SMTPNotesPort=TCPIP,TCPIP6
```

Example 5 -- Microsoft Windows (and Linux 2.4) partitioned servers. Each server listens to its assigned IPv4 and IPv6 addresses only: Each Server:

```
TCP_EnableIPv6=1

TCPIP=TCP, 0, 15, 0

TCPIP6=TCP, 0, 15, 0

PORTS=TCPIP,TCPIP6

TCPIP_TCPIPADDRESS=0,9.33.162.84:1352

TCPIP6_TCPIPADDRESS=0,[fe80::209:6bff:fecd:5b93%4]:1352

SMTPNotesPort=TCPIP,TCPIP6
```

The difference here is that Microsoft Windows and Linux 2.4 require the use of the zone in the address even for addresses bound to listeners if the address is a link local address. The same effect can also be achieved as shown in Example 5A.

Examle 5A -- Microsoft Windows and Linux 2.4 partitioned servers. Each server listens to its assigned IPv4 and IPv6 addresses only: For each server:

```
TCP_EnableIPv6=1

TCP_DefaultZone=4

TCPIP=TCP, 0, 15, 0

TCPIP6=TCP, 0, 15, 0

PORTS=TCPIP,TCPIP6

TCPIP_TCPIPADDRESS=0,9.33.162.84:1352

TCPIP6_TCPIPADDRESS=0,[fe80::209:6bff:fecd:5b93]:1352

SMTPNotesPort=TCPIP,TCPIP6
```

Example 6 -- Any client wants to make outbound IPv4 connections: No change required

Example 6A -- A UNIX client (not Linux 2.4) wants to make an outbound IPv6 connection: TCP_EnableIPv6=1

Connect to an IPv6 address, or to a DNS or hosts file resident name that resolves to an IPv6 address.

Example 7 -- Microsoft Windows/Linux 2.4 client wants to make outbound connection via IPv6: TCP_EnableIPv6=1

Connect to an IPv6 address, or to a DNS or hosts file resident name that resolves to an IPv6 address. If the address is a link local address, it must include the zone, such as fe80::209:6bff:fecd:5b93%4, or the local NOTES.INI file must contain a default zone, or the zone must be included in the local bound address. Such addresses must NEVER be stored in DNS, in Server documents, or Connection documents. If an IPv6-capable computer running Windows XP enables IPv6 and it is DHCP, it will automatically have its QUAD A record stored in DNS and it is stored without a zone, because the zone is a local construct. Therefore, the ONLY way to use such a DNS entry is to have a default zone in NOTES.INI.

Example 7A -- Microsoft Windows / Linux 2.4 client wants to make outbound connection via IPv6: TCP_EnableIPv6=1

TCP_DefaultZone=4

Connect to an IPv6 address, or to a DNS or hosts file resident name that resolves to an IPv6 address. If the address is a link local address, it need not include the zone, such as fe80::209:6bff:fecd:5b93 because the zone is defaulted by the NOTES.INI variable.

Example 7B -- Microsoft Windows / Linux 2.4 client wants to make outbound connection via IPv6: TCP_EnableIPV6=1

TCPIP=TCP, 0, 15, 0

PORTS=TCPIP

TCPIP_TCPIPADDRESS=0,[fe80::209:6bff:fecd:5b93%4]:1352

Connect to an IPv6 address, or to a DNS or hosts file resident name that resolves to an IPv6 address. If the address is a link local address, it need not include the zone, such as fe80::209:6bff:fecd:5b93 because it is defaulted by the bound address's zone.

Enabling Internet protocols on both TCP/IP and TCP/IPV6 ports: Add the following settings to the file, NOTES.INI:

- ldapnotesport=tcpip,tcpipv6
- imapnotesport=tcpip,tcpipv6
- smtpnotesport=tcpip,tcpipv6
- pop3notesport=tcpip,tcpipv6

Connecting a Notes client to a Domino server via IPv6

1. Install the Domino 7 server and Notes 7 client.
2. Enable IPv6 on both the client and the server by adding the NOTES.INI setting, TCP_ENABLEIP6=1, to the NOTES.INI files on the Notes client and Domino server:
3. Configure a zone on both the Notes client and the Domino server.
4. On the Domino server, configure the port for IPv4 and the port for IPv6.
5. Launch the Notes client.

6. Connect from the Notes client using IPv6 address-NRPC. Optionally, you can enter the zone if you want to.
7. A low priority Connection document is added to the local Domino Directory (NAMES.NSF). This Connection document and IPv6 are used during future connection attempts initiated with File -- Database -- Open.

Connecting from a Notes client using IPv6 address-NRPC: Use this procedure to connect from the Notes client to a server using an IPv6 address.

1. Choose File -- Database -- Open.
2. In the Server field, enter the IPv6 address. Optionally, you can enter a server name that resolves to an IPv6 address instead of entering the IPv6 address in the Server field.

   A low-priority Connection document is added to your local Domino Directory (NAMES.NSF).

Advanced Domino TCP/IP configurations

A single Domino server can have multiple IP addresses if you use multiple NICs, each offering an address, or if one NIC offers multiple addresses. Having multiple IP addresses allows the server to listen for connections at more than one instance of the TCP port assigned to NRPC (1352) or at TCP ports that are assigned to other services such as LDAP or HTTP. Both individual Domino servers and partitioned Domino servers can have multiple NICs, each with its own IP address.

Multiple IP addresses and NICs on a Domino server

Set up a Domino server with multiple IP addresses, each with its own NIC, if you want to:

- Split the client load for better performance
- Split client-to-server access from server-to-server communication
- Set up mail routing, replication, or cluster replication on an alternate path (private network)
- Partition a Domino server so that more than one partition offers the same Internet service (SMTP, POP3, IMAP, LDAP, or HTTP).
- Allow access to the Domino server via a TCP/IP firewall system over a different network segment, a configuration known as a demilitarized zone (DMZ)
- Use a Domino passthru server as an application proxy
- Provide network/server failover, used in mission-critical resource access
- Set up alternate window and/or maximum transmission unit (MTU) settings for satellite uplink and downlink connections isolated from local access connections

For a configuration with multiple IP addresses, you must bind each listening port to the appropriate IP address to ensure that each TCP service receives the network connections intended for it.

For more information, see the topics ″Binding an NRPC port to an IP address″ and ″Binding an Internet service to an IP address″ later in this chapter. For more information on private networks for cluster replication, see the book *Administering Domino Clusters.*

Note: A configuration with multiple NICs does not increase the number of Domino sessions you can have on a server. In TCP/IP, machine capacity depends on processors and memory.

Multiple IP addresses with one NIC

Reasons to use one NIC to serve multiple IP addresses include:

- Isolating local versus WAN Notes named networks so local users can see only local Domino servers
- Preventing independent remote access dialup connections (ISDN dialup router) from being arbitrarily accessed
- When setting up redundant WAN path connections for server to server access
- When the use of a different TCP/IP port map is needed for firewall connections

- When offering HTTP services to a different group than NRPC connections
- As a service provider when offering Domino server access for either Notes or Web clients to different groups/companies

For a configuration with multiple addresses and one NIC, you must configure the TCP/IP stack and bind each listening port to an IP address.

Partitioned servers and IP addresses

When you set up a Domino partitioned server, it is usually best to assign a separate IP address to each partition and use a separate NIC for each. Using a separate NIC for each address can make the computer's I/O much faster.

Lotus Domino is designed to listen for TCP/IP connections on all NICs in a computer system. If more than one partition is hosting the same service (NRPC, SMTP, POP3, IMAP, LDAP, or HTTP), fine-tune which partitions listen for which connections by associating each service's TCP port with a specific IP address.

For more information on associating services with IP addresses, see the topics ″Binding an NRPC port to an IP address″ and ″Binding an Internet service to an IP address″ later in this chapter.

As an alternative to using a separate NIC for each IP address, you can use a single NIC and still assign a separate IP address to each partition.

For more information, see the topic ″Assigning separate IP addresses to partitions on a system with a single NIC″ later in this chapter.

If you are unable to assign a separate IP address to each partition, you can use port mapping.

For more information on port mapping, see the topic ″Configuring a partitioned server for one IP address and port mapping″ later in this chapter.

Note: As an alternative to port mapping, you can use port address translation (PAT), in which a firewall redirects the TCP port connection to a different TCP port. Both port mapping and PAT require advanced skills to implement correctly.

Ensuring DNS resolves in advanced TCP/IP configurations

When you have Domino servers with multiple Notes network ports for TCP/IP, follow these procedures to ensure server name-to-address resolution by DNS. This topic covers the following configurations:

- Users in different DNS subdomains accessing one Domino server
- User-to-server access and server-to-server access via different DNS subdomains

For information on servers accessing a private LAN in a Domino cluster, see the book *Administering Domino Clusters.*

Users in different DNS subdomains accessing one Domino server: If users are on two isolated networks and the Domino server has a NIC for each network, use DNS to direct the users to the NIC the server shares with them.

1. Assign an IP address to each NIC by creating A records (or, for IPv6, AAAA records) in DNS. Use the ping command and the IP address to test the responsiveness of the NIC.

   Note: If the Domino server is running Windows and there is a route between the two networks, prevent the NetBIOS broadcasts from exiting from both adapters by using the Windows Control Panel to disable one instance of the WINS client. Use the Bindings tab of the Network dialog box, select All Adapters, and select the name of the NIC for which you want to disable WINS.

2. Create two CNAME records in DNS for the Domino server, linking the server’s common name to each NIC name in the A records. (Using CNAME records for the Domino server provides diagnostic fidelity to test the network pathway independently of the server’s name resolve.)
3. Add a second Notes network port for TCP/IP in Domino.

   For more information, see the topic ″Adding a network port on a server″ later in this chapter.
4. Bind each TCP/IP port to the IP address of the appropriate NIC. On the server console, verify that both TCP/IP ports are active and linked to the correct IP address.

   For more information on binding ports to IP addresses, see the topic ″Binding an NRPC port to an IP address″ later in this chapter.
5. In the Server document’s Net Address field for each TCP/IP port, use the server’s common name only, not its FQDN.
6. On each Notes workstation, set the user’s DNS name lookup scope to the correct DNS subdomain.

Example: At the Acme company, some users connect to the Domino server Chicago/Sales/Acme over an Ethernet network, others over a Token Ring network. Register the Domino server with DNS as chicago.east.acme.com for the users on the Ethernet network and as chicago.west.acme.com for users on the Token Ring network.

1. Create start of authority (SOA) table entries in DNS for the subdomain east.acme.com, as follows:

chi-ethernet	**A**	**10.20.20.2**
chicago	CNAME	chi-ethernet

2. Create SOA table entries in DNS for the subdomain west.acme.com, as follows:

chi-tokenring	**A**	**10.10.10.1**
chicago	CNAME	chi-tokenring

3. Change the name of the original Notes network port for TCP/IP to TCPIP1, and name the second port TCPIP2.
4. Use the NOTES.INI file to bind TCPIP1 to the IP address for the Ethernet network and to bind TCPIP2 to the IP address for the Token Ring network.
5. In the Server document’s Net Address field for each TCP/IP port, enter chicago.
6. On the Ethernet users’ workstations, set the DNS name lookup scope to east.acme.com, and on the Token Ring users’ workstations, set it to west.acme.com.

User-to-server access and server-to-server access via different DNS subdomains: If users need to access a Domino server over the LAN and other Domino servers need to access the same server over the WAN, add a second NIC to the server. Then use DNS to direct the users to the NIC for the LAN and to direct other servers to the NIC for the WAN.

1. Assign an IP address to each NIC by creating an A record (or, for IPv6, AAAA record) in DNS. Use the ping command and the IP address to test the responsiveness of the NIC.

   Note: If the Domino server is running Windows and there is a route between the two networks, prevent the NetBIOS broadcasts from exiting from both adapters by using the Windows Control Panel to disable one instance of the WINS client. Use the Bindings tab of the Network dialog box, select All Adapters, and select the name of the NIC for which you want to disable WINS.
2. Create two CNAME records in DNS for the Domino server, linking the server’s common name to each NIC name in the A records. (Using CNAME records for the Domino server provides diagnostic fidelity to test the network pathway independently of the server’s name resolve.)
3. Add a second Notes network port for TCP/IP in Domino.

   For more information, see the topic ″Adding a network port on a server″ later in this chapter.

4. Bind each TCP/IP port to the IP address of the appropriate NIC. On the server console, verify that both TCP/IP ports are active and linked to the correct IP address.

   For more information on binding ports to IP addresses, see the topic "Binding an NRPC port to an IP address" later in this chapter.

5. To direct the Domino server's first outbound connection to the server-to-server network, edit the PORT setting in the NOTES.INI file to read as follows:

   ```
   PORT=serverportname, userportname
   ```

   Where *serverportname* is the name of the Notes network port for TCP/IP that other Domino servers will use to connect to this server, and *userportname* is the name of the Notes network port for TCP/IP that users will use to connect to this server.

6. In the Server document's Net Address field for the first TCP/IP port (the port that users will use), enter the FQDN, using the server's common name and the users' DNS subdomain.

   Note: Listing the port that users will use first is important, as the Notes Name Service cannot distinguish which NIC a user is accessing and makes the connection based on the content of the Net Address field for the first TCP/IP port listed in the Server document.

7. In the Server document's Net Address field for the second TCP/IP port (the port that servers will use), enter the FQDN, using the server's common name and the servers' DNS subdomain.

   An initiating server uses its local Domino Directory to detect the Notes named network it has in common with this server.

8. Set each user's DNS name lookup scope to the correct DNS subdomain.
9. In each server's TCP/IP stack, set the DNS name lookup scope to the correct DNS subdomain.

Example: At the Acme company, users connect to the Domino server BostonApp04/Sales/Acme over the LAN, and other Domino servers access it privately over the WAN. You register the server with DNS as bostonapp04.boston.acme.com for the LAN users and as bostonapp04.domino.acme.com for the server-to-server network over the WAN.

1. Create the following SOA table entries in DNS for the subdomain boston.acme.com, as follows:

usr-bostonapp04	**A**	**103.210.20.2**
bostonapp04	CNAME	usr-bostonapp04

2. Create the following SOA table entries in DNS for the subdomain domino.acme.com, as follows:

srv-bostonapp04	**A**	**103.210.41.1**
bostonapp04	CNAME	srv-bostonapp04

3. Change the name of the original Notes network port for TCP/IP to TCPIP1, and name the second port TCPIP2.
4. Use the NOTES.INI file to bind TCPIP1 to the IP address for the user network, to bind TCPIP2 to the IP address for the server-to-server network, and to add the setting PORT=TCPIP2, TCPIP1.
5. In the Server document's Net Address field for port TCPIP1, enter bostonapp04.boston.acme.com. For port TCPIP2, enter bostonapp04.domino.acme.com.
6. On each user's workstation, set the DNS name lookup scope to boston.acme.com. In the TCP/IP stacks of the servers that need to connect to this server, set the name lookup scope to domino.acme.com.

Planning the NetBIOS network

The Domino network is compatible with NetBIOS, a set of IBM session-layer LAN services that has evolved into a standard interface that applications use to access transport-layer network protocols. Domino supports the NetBIOS interface on Windows systems over the following transport protocols: TCP/IP (on systems running TCP/IP) and NetBEUI (supplied with all Microsoft network products).

Note: Although you can add some NetBIOS services to Linux and UNIX systems, NRPC communication does not use them.

For detailed system requirements for using NetBIOS with Lotus Domino, see the *Release Notes*.

Deciding whether to use NetBIOS services

Including NetBIOS in the Domino network has both benefits and risks. The benefits are as follows:

- NetBIOS has low overhead relative to other protocol suites. NetBIOS over NetBEUI has the least overhead; and NetBIOS over TCP/IP has the most.
- Because it is not directly routable, NetBIOS over NetBEUI can provide a secure means to access your server for administration within a flat network. To access the server over a routed IP network, you can create a data-link switching (DLSw) tunnel to limit the administration access with NetBIOS over NetBEUI.
- Because NetBIOS name-to-address resolution services offer dynamic registration by name broadcasts, you can use NetBIOS to build a mobile Domino network for temporary or emergency use.

The risks of using NetBIOS involve the security of the file system on Domino servers. Depending on the access permissions of the operating system and on the transport protocol being used, NetBIOS name and file services might allow users to see or access the server's file system. When a server provides NRPC services, mitigate this risk by disabling the NetBIOS name and file services (SMB/CIFS) on the system so that the system's name cannot be seen over the network. Other Notes/Domino systems can still find the Domino server because Lotus Domino has its own NetBIOS name service to propagate and register the Domino server's NetBIOS name, but access is secure because it is controlled by the authentication and certification features in NRPC.

If the system on which you run Domino requires NetBIOS name or authentication services, mitigate the security risk by isolating the NetBIOS services. Install an additional NIC on the system for NetBIOS over a private administration network, and disable NetBIOS on the NIC that the Domino server uses.

How to tell if NetBIOS is active on a system

The following are indications that NetBIOS is active:

- On Windows systems, you can see or access another Windows system's file system through the Network Neighborhood (indicates Server Message Block/NetBIOS).
- You can register with an NT domain (indicates Server Message Block/NetBIOS).
- On Windows 2000 or XP systems, ″NetBIOS over IP″ is selected in the system's TCP/IP protocol settings.

Note: On Linux and UNIX systems, the SAMBA server service (Windows file server) can offer Server Message Block/NetBIOS or Common Internet File System/IP access, or both.

Server name-to-address resolution over NetBIOS

When a Notes workstation or Domino server running NetBIOS tries to connect to a Domino server, the initiating system offers the destination server's common name to the NetBIOS name service, which then broadcasts that name and its associated network address over the NetBIOS network.

For background information on how the Notes Name Service works with name-resolver services such as the NetBIOS name service, see the topic ″Resolving server names to network addresses in NRPC″ earlier in this chapter.

When you use the Notes Name Service with the NetBIOS name service, only a Notes or Domino system using the same NetBIOS transport protocol as the destination Domino server can see the destination server’s NetBIOS name. If the Notes or Domino system has more than one NIC for which the NetBIOS transport protocol is enabled, only the NetBIOS port with the same LANA binding as that of the destination server can see the destination server’s name.

Which physical address is registered for a Domino server depends on the transport protocol:

- For NetBIOS over NetBEUI, the NIC’s 32-bit MAC address is used.
- For NetBIOS over TCP/IP, the system’s IP address is used.

Ways to ensure successful NetBIOS resolves

Because NetBIOS broadcasting has a limited range, you may need to create a Connection document that includes the physical address of the destination server. This process works as long as the network pathway can carry the given lower transport protocol.

For NetBIOS over TCP/IP, you can also do one of the following:

- Use a WINS server with a static entry.
- In the initiating system’s TCP/IP stack settings, enable NetBIOS name lookup by DNS. This works even if you are not using any NRPC services; however, the destination server must be registered with DNS.

Note: NetBIOS name space is flat, even with TCP/IP. If the client is not within the same DNS domain level, access by name may not be possible.

Naming Domino servers on NetBIOS

NetBIOS names are limited to 15 characters. If the common name of the Domino server is longer than 15 characters, NetBIOS truncates the name.

CAUTION:
The resolution of a Domino server name can be adversely affected if the server name is the same as the NetBIOS name for a Windows system.

To prevent this problem without making it difficult to manage system files remotely, do the following:

- On Windows 2000, add a preface such as W2K- to the system name, using the Network Identification tab on the System Properties dialog box.

For more information on the NetBIOS name service, see Microsoft’s resource kit documentation for the Windows 2000 operating systems.

Setting up Domino servers on the network

Before installing a Domino server, make sure you have done the following:

- Installed one or more NICs on the system.
- Installed protocol software if necessary.
- Installed all network drivers in the correct directories.
- Installed any network software required for the protocols. For more information, see the vendor’s documentation.

After you install the server, you use the Domino Server Setup program to accept network defaults or customize network settings.

For more information, see the chapter ″Installing and Setting Up Domino Servers.″

After you run the setup program, you may need to complete one or more of these tasks to finish setting up Lotus Domino on the network:

- Change the default names assigned to Notes named networks to make them consistent with actual network topography.
- Fine-tune network port setup by adding, enabling, renaming, reordering, disabling, or deleting ports or by enabling network encryption or compression on a port.
- Complete tasks specific to the TCP/IP, or NetBIOS, protocol.

For information on connecting Notes workstations to the network, see Lotus Notes 7 Help.

Setting up Notes named networks

The Domino Server Setup program automatically places all servers that are in a Domino domain and that run the same network protocol in the same Notes named network (NNN). In the Server document, the setup program assigns each NNN a default name in the format *portname* network.

After you complete the Server Setup program, rename the NNN for each network port in the Server document. It is useful if the name reflects both the location of the network and its protocol. For example, if your company has a TCP/IP network and has LANs in Boston and San Francisco, change the name of the NNN in Boston to ″TCPIP Boston network,″ and change the name of the NNN in San Francisco to ″TCPIP SF network.″

CAUTION:
Domino assumes that all servers in a NNN have a continuous LAN or WAN connection. If this is not the case, serious delays in mail routing between servers can occur. Be careful not to include servers with only dialup connections in an NNN.

To change the name of a Notes named network

1. From the Domino Administrator, select the server you just set up.
2. Click the Configuration tab.
3. Expand the Server section in the view pane.
4. Click Current Server Document.
5. Click Edit Server, and then click the Ports - Notes Network Ports tab.
6. In the Notes Network field for each port, enter a new name for the server's Notes named network. The name can include space characters.
7. Click Save and Close.

Fine-tuning network port setup on a server

After you install and set up a Domino server, review the list of network ports that were enabled by the Server Setup program. Unless you customize network settings during setup, Domino enables ports based on the current operating system configuration. To conserve system resources, disable the ports for protocols that you don't need.

For information on configuring a communication port for a dialup modem, see the chapter ″Setting Up Server-to-Server Connections.″

Use Domino Administrator to make these changes to a server's network port setup:

- Disable a network port
- Enable a network port
- Add a network port
- Rename a network port

- Reorder network ports
- Delete a network port
- Encrypt network data on a port
- Compress network data on a port

Note: On a Notes workstation, you use the User Preferences dialog box to change port setup.

For more information on changing port preferences on a workstation, see Lotus Notes 7 Help.

Disabling a network port on a server

Even after you disable a port, it still appears in the list of available ports so that you can later enable it.

1. From the Domino Administrator or Web Administrator, click the server on which you want to disable a port.
2. Click the Configuration tab.
3. Do one of these:
   - From the Domino Administrator’s Tools pane, choose Server - Setup Ports.
   - From the Web Administrator’s Port tool, choose Setup.
4. Select the port you want to disable, and then deselect ″Port enabled.″
5. Click OK.
6. Click the Server - Status tab.
7. Do one of these so that the change takes effect:
   - From the Domino Administrator’s Tools pane, choose Restart Port. (If you can’t see the Tools pane, make sure you are in the Server Tasks view.)
   - From the Web Administrator’s Ports tool, choose Restart.
8. In the Server document, on the Ports - Notes Network Ports tab, specify Disabled next to the name of the port you are disabling.
9. Save the Server document.

Enabling a network port on a server

If the server port you want to enable will be the Notes workstation’s only means of connecting with the server, do not use this procedure. Instead, use the Ports setting in the server’s NOTES.INI file.

For more information, see the appendix ″NOTES.INI File.″

For information on creating a Connection document on a Notes workstation, see Lotus Notes 7 Help.

To enable a network port

1. From the Domino Administrator or Web Administrator, click the server on which you want to enable a port.
2. Click the Configuration tab.
3. Do one of these:
   - From the Domino Administrator’s Tools pane, choose Server - Setup Ports.
   - From the Web Administrator’s Port tool, choose Setup.
4. Select the port you want to enable, and then select ″Port enabled.″
5. Click TCP/IP Options, LANx Options, or COMx Options, and specify information as appropriate.

   For more information on TCP/IP and LAN*x* options, see the topics ″Changing the TCP/IP connection time-out interval,″ ″Defining a NetBIOS LANA number for a Notes network port,″ and ″Defining a server’s NetWare name service in Lotus Domino″ later in this chapter.

   For more information on COM*x* options, see the chapter ″Setting Up Server-to-Server Connections.″

6. Click OK.
7. Click the Server - Status tab.
8. Do one of these so that the change takes effect:
   - From the Domino Administrator's Tools pane, choose Restart Port. (If you can't see the Tools pane, make sure you are in the Server Tasks view.)
   - From the Web Administrator's Ports tool, choose Restart.
9. In the Server document, click the Ports - Notes Network Ports tab, and edit these fields as necessary:

Field	Action
Port	Enter the port name. Lotus Domino assigns a default port name to each network protocol detected on the system.
Notes Network	Enter the name of the Notes named network for the group of Domino servers that are in this location and run on a particular protocol -- for example, Boston TCPIP. Space characters are allowed in a Notes network name.
Net Address	Enter the protocol-specific name of the server -- for example, sales.acme.com. The name you use depends on the convention of the network protocol. This field is used to determine the address that other servers use to access this server.
Disabled/Enabled	Choose Enabled so that other servers will know the port is enabled.

10. Save the Server document.
11. Make sure that this server is set up to replicate its Domino Directory to other servers, or enter the preceding changes into the Server document on a server that is set up to do the replication, or other servers will not know that they can connect to this server over the newly enabled port.

Adding a network port on a server

If the server port you want to add will be the Notes workstation's only means of connecting with the server, do not use this procedure. Instead, use the Ports setting in the server's NOTES.INI file.

For more information, see the appendix ″NOTES.INI File.″

For information on creating a Connection document on a Notes workstation, see Lotus Notes 7 Help.

To add a network port

1. From the Domino Administrator or Web Administrator, click the server on which you want to add a port.
2. Click the Configuration tab.
3. Do one of these:
   - From the Domino Administrator's Tools pane, choose Server - Setup Ports.
   - From the Web Administrator's Port tool, choose Setup.
4. Click New.
5. Specify the port name and driver, and click OK.
6. Click TCP/IP Options, LANx Options, or COMx Options, and specify information as appropriate.

   For more information on TCP/IP and LAN*x* options, see the topics ″Changing the TCP/IP connection time-out interval,″ ″Defining a NetBIOS LANA number for a Notes network port,″ and ″Defining a server's NetWare name service in Lotus Domino″ later in this chapter.

   For more information on COM*x* options, see the chapter ″Setting Up Server-to-Server Connections.″
7. Click OK.
8. Click the Server - Status tab.
9. Do one of these so that the change takes effect:

- From the Domino Administrator's Tools pane, choose Restart Port. (If you can't see the Tools pane, make sure you are in the Server Tasks view.)
- From the Web Administrator's Ports tool, choose Restart.

10. In the Server document, click the Ports - Notes Network Ports tab, and edit these fields as necessary:

Field	Action
Port	Enter the port name. Lotus Domino assigns a default port name to each network protocol detected on the system.
Notes Network	Enter the name of the Notes named network for the group of Domino servers that are in this location and run on a particular protocol -- for example, Boston TCPIP. Space characters are allowed in a Notes network name.
Net Address	Enter the protocol-specific name of the server -- for example, sales.acme.com. The name you use depends on the convention of the network protocol. This field is used to determine the address that other servers use to access this server.
Disabled/Enabled	Choose Enabled so that other servers will know the port is enabled.

11. Save the Server document.
12. Make sure that this server is set up to replicate its Domino Directory to other servers, or enter the preceding changes to the Server document on a server that is set up to do the replication, or other servers will not know that they can connect to this server over the newly enabled port.
13. If you are adding an additional TCP/IP port on a computer with multiple NICs, see these topics:
    - Binding an NRPC port to an IP address
    - Binding an Internet service to an IP address.
14. If you are adding an additional NetBIOS port on a computer with multiple NICs, see the topic Creating additional network ports for NetBIOS.

Renaming a network port on a server

You might want to rename a port to reflect its function. For example, suppose you add a second TCP/IP port named SRV-TCP so that clustered servers can communicate over a private network. Then you might want to might want to rename the original TCP/IP port through which users will communicate with the server USR-TCP.

1. From the Domino Administrator or Web Administrator, click the server on which you want to rename a port.
2. Click the Configuration tab.
3. Do one of these:
    - From the Domino Administrator's Tools pane, choose Server - Setup Ports.
    - From the Web Administrator's Port tool, choose Setup.
4. Select the port you want to rename.
5. Click Rename, and then enter the new name. Do not use spaces in the port name.
6. Click OK.
7. Click the Server - Status tab.
8. Do one of these so that the change takes effect:
    - From the Domino Administrator's Tools pane, choose Restart Port. (If you can't see the Tools pane, make sure you are in the Server Tasks view.)
    - From the Web Administrator's Ports tool, choose Restart.
9. In the server document, on the Ports - Notes Network Ports tab, change the name of the port to the new name and save the document.
10. If this server is the source server for any Connection documents in the Domino Directory, click Server - Connections.

11. Select a Connection document and click Edit Connection.
12. On the Basics tab, enter the new port name in the ″Use the port(s)″ field.
13. Save and close the Connection document.
14. Repeat steps 10 to 13 for each Connection document for which this server is the source.

Reordering network ports on a server

Changing the order in which ports are listed in the Setup Ports dialog box also changes the Ports setting in the NOTES.INI file. List the ports in the order in which you want them to be used -- for example, list nearest or fastest connections first. Then when a server uses a Notes named network or a Connection document to locate another server, the port with a close or fast connection will be used as the preferred path.

If the Domino server has multiple TCP/IP ports, see the topic ″Reordering multiple server ports for TCP/IP″ later in this chapter.

To reorder network ports

1. From the Domino Administrator or Web Administrator, click the server on which you want to reorder ports.
2. Click the Configuration tab.
3. Do one of these:
   - From the Domino Administrator’s Tools pane, choose Server - Setup Ports.
   - From the Web Administrator’s Port tool, choose Setup.
4. Select the port that you want to relocate in the list.
5. Click the up and down arrows, as necessary to relocate the port.
6. Click OK.
7. Click the Server - Status tab.
8. Do one of these so that the change takes effect:
   - From the Domino Administrator’s Tools pane, choose Restart Port. (If you can’t see the Tools pane, make sure you are in the Server Tasks view.)
   - From the Web Administrator’s Ports tool, choose Restart.
9. In the Server document, on the Ports - Notes Network Ports tab, change the port order to the new order by cutting and pasting all the necessary fields.
10. Save the Server document.

Note: When you create a Connection document on a server, the Connection document takes the port order from the order in the Setup Ports dialog box. Then, whenever the server connects with the destination server, the server obtains the port order directly from the Connection document. If you change the port order after you create Connection documents, you must save each Connection document again. To have different Connection documents reflect different port orders, change the port order, save a Connection document, change the port order again, save another Connection document, and so on.

Deleting a network port on a server

If you delete a port, it no longer appears in the list of available ports in the Setup Ports dialog box.

1. From the Domino Administrator or Web Administrator, click the server on which you want to delete a port.
2. Click the Configuration tab.
3. Do one of these:
   - From the Domino Administrator’s Tools pane, choose Server - Setup Ports.
   - From the Web Administrator’s Port tool, choose Setup.

4. Select the port you want to delete.
5. Click Delete.
6. Click OK.
7. Click the Server - Status tab.
8. Do one of these so that the change takes effect:
   - From the Domino Administrator's Tools pane, choose Restart Port. (If you can't see the Tools pane, make sure you are in the Server Tasks view.)
   - From the Web Administrator's Ports tool, choose Restart.
9. In the Server document, on the Ports - Notes Network Ports tab, delete the contents of all the fields next to the name of the port you are deleting.
10. Save the Server document.

Encrypting NRPC communication on a server port

You can encrypt network data on a server's Notes network ports to prevent the network eavesdropping that's possible with a network protocol analyzer. Network encryption occurs at the application layer of a given protocol and is independent of other forms of encryption. Network data is encrypted only while it is in transit. After the data is received and stored, network encryption is no longer in effect.

Network data encryption occurs if you enable network data encryption on either side of a network connection. For example, if you enable encryption on a server's Notes network port for TCP/IP, you don't need to enable encryption on the TCP/IP ports of workstations or servers that connect to the server.

If you want the server to have one TCP/IP port for Notes traffic over the Internet and another TCP/IP port for internal traffic over NRPC, you can encrypt the port for Internet traffic and leave the port for internal traffic unencrypted.

Be aware that multiple high-speed encrypted connections to a server can affect server performance adversely. Encrypting network data has little effect on client performance. For protocols other than NRPC, you use SSL for encryption.

For more information, see the chapter ″Setting Up SSL on a Domino Server.″

To encrypt NRPC communication

1. From the Domino Administrator or Web Administrator, choose the server for which you want to encrypt network data.
2. Click the Configuration tab.
3. Do one of these:
   - From the Domino Administrator's Tools pane, choose Server - Setup Ports.
   - From the Web Administrator's Port tool, choose Setup.
4. Select the port you want to encrypt.
5. Select ″Encrypt network data.″
6. Click OK.
7. Click the Server - Status tab.
8. Do one of these so that the change takes effect:
   - From the Domino Administrator's Tools pane, choose Restart Port. (If you can't see the Tools pane, make sure you are in the Server Tasks view.)
   - From the Web Administrator's Ports tool, choose Restart.

Compressing network data on a server port

To reduce the amount of data transmitted between a Notes workstation and Domino server or between two Domino servers, enable network compression for each enabled network port. Whether you should enable compression on a network port depends on the type of network connection and the type of data being transmitted.

For compression to work, enable it on both sides of a network connection. To enable compression for a network port on a server, use the Server tab in the Domino Administrator. To enable compression on network ports on Notes workstations, from the Domino Administrator, use a setup or desktop policy settings document or from a workstation, use the User Preferences dialog box.

For information on policy settings, see the chapter ″Using Policies.″

WAN connections

Enabling network compression on X.PC ports can significantly reduce the time it takes to send and receive data over a remote connection between a Notes workstation and a Domino server or between two Domino servers.

You benefit from using network compression only if the data being transmitted is not already compressed. In the case of a network dialup service such as Microsoft's Remote Access Service (RAS) which includes built-in compression, enabling compression on Notes network ports does not provide any additional benefit. The same is true of tasks involving data that was compressed using the Lempel-Ziv algorithm (LZ1 compression) -- such as replicating a mail file with a large number of compressed attachments.

LAN connections

While compression decreases bandwidth use on a LAN, you must weigh this gain against increased memory and processor use, since network compression works by buffering data before compressing it. The cost of compression might be worth it only for a heavily loaded network.

To compress data on a server port

1. From the Domino Administrator or Web Administrator, click the server for which you want to turn on network compression.
2. Click the Configuration tab.
3. Do one of these:
   - From the Domino Administrator's Tools pane, choose Server - Setup Ports.
   - From the Web Administrator's Port tool, choose Setup.
4. Select the port for which you want to turn on compression.

   Note: Make sure ″Port enabled″ is selected for that port.
5. Select ″Compress network data.″
6. Click OK.
7. Click the Server - Status tab.
8. Do one of these so that the change takes effect:
   - From the Domino Administrator's Tools pane, choose Restart Port. (If you can't see the Tools pane, make sure you are in the Server Tasks view.)
   - From the Web Administrator's Ports tool, choose Restart.

Server setup tasks specific to TCP/IP

After you run the Domino Server Setup program, complete these procedures:

1. Set up a secondary name server for Notes clients.
2. Change the server’s connection-time-out interval.
3. For servers that provide services to Internet clients, enable Domino support for IPv6.
4. For configurations involving multiple NICs on a server or partitioned server:
   - Reorder multiple Notes network ports for TCP/IP.
   - Bind an NRPC port to an IP address.
   - Bind an Internet service to an IP address.
5. For a partitioned server with a single NIC for the entire computer, assign an IP address to each server partition
6. Change a default TCP or SSL port number.
7. Confirm that TCP/IP is configured properly.

Setting up a secondary name server

To ensure that the Notes Name Service is always available to Notes workstations, assign a secondary name server in users’ Location documents. You can specify a different secondary name server for each LAN location defined. The secondary name server is used when:

- The user’s home server is down.
- The user’s home server is not running TCP/IP.
- The name of the user’s home server cannot be resolved over TCP/IP.

For examples of situations in which the name of a home server cannot be resolved, see the topic ″Ensuring DNS resolves in advanced TCP/IP configurations″ earlier in this chapter.

Note: You can use setup or desktop policy settings to assign secondary name servers to groups of users.

For more information, see the chapter ″Using Policies.″

To set up a secondary name server

1. On the Notes workstation, choose File - Mobile - Locations, and open the location for which you want to designate a secondary name server.
2. Click ″Edit Location.″
3. Click the Advanced - Secondary Servers tab. (The Advanced tab appears only if you have a location defined as ″Local Area Network″ or ″Both Dialup and Local Area Network.″)
4. In the ″Secondary TCP/IP Notes server name″ field, enter one of the following:
   - The common name of the Domino server -- for example, Notesserver1
   - The hierarchical name of the Domino server -- for example, Notesserver1/Acme
5. In the ″Secondary TCP/IP host name or address″ field, enter one of the following:
   - IP address -- for example, 197.114.33.22
   - The fully qualified domain name -- for example, notesserver1.acme.com
   - The simple host name -- for example, notesserver1

     If you specify only the host name in this field, the workstation must use the Domain Name System (DNS) or local hosts file to locate the secondary name server. When you specify the IP address in this field, Lotus Domino resolves the host’s IP address without having to perform a DNS or hosts file lookup.
6. Click ″Save and Close.″

Changing the TCP/IP connection-time-out interval

You might want to increase the number of seconds that Lotus Domino waits before terminating a connection attempt. For example, increasing the time-out interval is often necessary on a server that dials up other Domino servers. The default time-out interval is 5 seconds.

1. From the Domino Administrator or Web Administrator, click the server for which you want to change the time-out interval.
2. Click the Configuration tab.
3. Do one of these:
   - From the Domino Administrator's Tools pane, choose Server - Setup Ports.
   - From the Web Administrator's Port tool, choose Setup.
4. Select the TCP/IP port.
5. Click ″TCPIP Options,″ and enter a number.

   Note: Unless the connection is over a dial-on-demand ISDN modem, remote bridge, or router, it is best to enter a number no greater than 10, as the Notes client or Domino server won't retry the connection until the timer has expired.
6. Click OK.

Enabling support for IPv6 on a Domino server

You can enable support for IPv6 on a Domino server that runs the IMAP, POP3, SMTP, LDAP, or HTTP service.

To enable IPv6, add this NOTES.INI setting to the server's NOTES.INI file:

```
TCP_EnableIPV6=1
```

Reordering multiple server ports for TCP/IP

If a Domino server has multiple Notes network ports for TCP/IP, the order in which these ports are listed in the NOTES.INI file and the Server document affects how other servers and workstations connect to this server. The Ports setting in the NOTES.INI file determines which port a workstation or server tries first. In the absence of other settings that bind an NRPC, POP3, IMAP, SMTP, or LDAP service to an IP address, all of these services will try to use the port listed first in the NOTES.INI file.

Server-to-server communication

If you add a second Notes network port for TCP/IP in order to isolate server-to-server communication -- for example, a private network for cluster replication -- list this port first in the NOTES.INI file so that server-to-server traffic will tend to occur over this connection, thus decreasing the data flow on the port for the user network. To change the port order in the NOTES.INI file, use the Port Setup dialog box.

For more information, see the topic ″Reordering network ports on a server″ earlier in this chapter.

Note: If you are setting up a private cluster network and do not list the server port first, you must add the setting Server_Cluster_Default_Port to the NOTES.INI file. The disadvantage of adding this setting is that if the server encounters a problem connecting over this port, it will not try another port, and replication will not occur.

For more information on the Server_Cluster_Default_Port setting, see the appendix ″NOTES.INI File.″

Workstation-to-server communication

If a Domino server has a port for workstations to connect on -- for example, over a LAN -- and another port for servers to connect on -- for example, over a WAN -- list the workstation port first in the Server document so that users see only servers on the LAN when they choose File - Database - Open.

To reorder the ports in the Server document, click the Ports - Notes Network Ports tab, and edit the fields in the table.

Binding an NRPC port to an IP address

By default, all TCP/IP-based services on a Domino server listen for network connections on all NICs and on all configured IP addresses on the server. If you have enabled more than one Notes network port for TCP/IP (TCP port for NRPC) on either a single Domino server or a Domino partitioned server, you must associate the NRPC ports and IP addresses by binding each port to an address.

For background information on Domino server setups with multiple IP addresses, see the topic ″Advanced Domino TCP/IP configurations″ earlier in this chapter.

To bind an NRPC port to an IP address

When setting the NOTES.INI variables for port mapping, do not include a zone in a port mapped address. The zone is only valid locally.

1. For each IP address, make sure you have added a Notes port for TCP/IP. Also make sure that each port has a unique name.

   For information on adding a Notes port, see the topic ″Adding a network port on a server″ earlier in this chapter.
2. In the NOTES.INI file, confirm that these lines appear for each port that you added:
   ```
   Ports=TCPIPportname
   TCPIPportname=TCP, 0, 15, 0
   ```
   Where *TCPIPportname* is the port name you defined.
3. For each port that you want to bind to an IP address, add this line to the NOTES.INI file:
   ```
   TCPIPportname_TCPIPAddress=0,IPaddress
   ```
   Where *IPaddress* is the IP address of the specific NIC.

   For example:
   ```
   TCPIP_TCPIPAddress=0,130.123.45.1
   ```
   Note: For IPv6, enclose the address in square brackets, as it contains colons. For example:
   ```
   TCPIP_TCPIPAddress=0,[fe80::290:27ff:fe43:16ac]
   ```
4. (Optional) To help you later remember the function of each port, add the default TCP port number for NRPC to the end of the line you entered in Step 3, as follows:
   ```
   :1352
   ```
   CAUTION:
   Do not change the assigned TCP port number unless you have a way to redirect the inbound connection with Domino port mapping or a firewall that has port address translation (PAT).

   In a situation where you must change the default NRPC port number, see the topic ″Changing a TCP or SSL port number″ later in this chapter.

Binding an Internet service to an IP address

If the Domino server has multiple Notes network ports for TCP/IP (NRPC ports) and the server is also hosting the SMTP, POP3, IMAP, LDAP, or Internet Cluster Manager (ICM) service, you must specify the NRPC port that you want the service to use in the NOTES.INI file. If you do not specify an NRPC port for an Internet service, by default the service will use the port listed first in the Ports setting in the NOTES.INI file. You can specify the same NRPC port for multiple Internet services.

For the Domino Web server (HTTP service), you use the Server document to bind HTTP to a host name IP address.

To bind the SMTP, POP3, IMAP, LDAP, or ICM service

1. Bind each NRPC port to an IP address.
2. In the NOTES.INI file, specify the appropriate NRPC port for each Internet service as follows:

   Note: If you don't know the port name to enter for an NRPC port, open the Server document, click the Ports - Notes Network Ports tab, and look at the ports associated with the TCP protocol.

Service	Action
POP3	Enter POP3NotesPort=*port name*where *port name* is the name of the NRPC port that you want to link the service to.
IMAP	Enter IMAPNotesPort=*port name*where *port name* is the name of the NRPC port that you want to link the service to.
SMTP	Enter SMTPNotesPort=*port name*where *port name* is the name of the NRPC port that you want to link the service to.
LDAP	Enter LDAPNotesPort=*port name*where *port name* is the name of the NRPC port that you want to link the service to.
ICM	Enter ICMNotesPort=*port name*where *port name* is the name of the NRPC port that you want to link the service to.

Example

The following example shows the lines (in bold) to add to the Ports section of the NOTES.INI file to bind two NRPC ports to their IP addresses and to specify the second NRPC port for the SMTP service.

```
Ports=TCPIP, TCP1P2
TCPIP=TCP, 0, 15, 0
TCPIP_TCPIPAddress=0,10.33.52.1
TCPIP2=TCP, 0, 15, 0
TCPIP2_TCPIPAddress=0, 209.98.76.10
SMPTNotesPort=TCPIP2
```

Note: Domino adds the lines that are not bold when you use either the Domino Server Setup program or the Domino Administrator's Setup Ports dialog box to enable a port.

To bind the HTTP service

1. On the Internet Protocols - HTTP tab of the Server document, enter one or more IP addresses or FQDNs for the server in the ″Host name(s)″ field.
2. Select Enabled in the ″Bind to host name″ field.

Note: If the server is a partitioned server and has Web sites configured with separate IP addresses, or has virtual servers (Domino 5) configured for one or more partitions, enter the partition's IP address, and each Web site or virtual server's IP address in the ″Host name(s)″ field, separated by semicolons. Alternatively, you can use FQDNs in this field. Do not list additional Web sites and virtual hosts that have IP addresses that are already listed in this field.

Example 1 -- Server partition with Web sites

The partition's host name is app01 and there are two Web sites configured for it: sales.acme.com and accounting.acme.com. The Web site sales.acme.com uses the same IP address as the partition, and the Web site accounting.acme.com has its own IP address. Enter the following in the ″Host name(s)″ field:

```
9.88.43.113;9.88.46.110
```

where 9.88.43.113 is the IP address for both the partition and the Web site sales.acme.com and 9.88.46.110 is the IP address for the Web site accounting.acme.com.

Example 2 -- Server partition with virtual servers

The partition's host name is app01 and there are two virtual servers (9.88.46.114 and 9.88.46.115) and one virtual host configured for it. Enter the following in the ″Host name(s)″ field:

```
9.88.43.113;9.88.46.114;9.88.46.115
```

where 9.88.43.113 is the IP address for both the partition and the virtual host sales.acme.com, 9.88.46.114 is the IP address for virtual server 1 (accounting.acme.com), and 9.88.46.115 is the IP address for virtual server 2 (northeastsales.acme.com).

For information on Web sites and Internet Site documents, see the chapter ″Installing and Setting Up Domino Servers.″

Assigning separate IP addresses to partitions on a system with a single NIC

If you use a single NIC with multiple IP addresses, you must complete additional configuration instructions, which are based on your operating system, for each server partition.

Note: Using separate IP addresses with a single NIC can have a negative impact on the computer's I/O performance.

For background information on partitioned servers and the TCP/IP network, see the topic ″Partitioned servers and IP addresses″ earlier in this chapter.

IBM AIX or Linux

You must be logged on as root.

To enable an IP address in IBM AIX

1. Add one entry in the local host names file /etc/hosts for each server partition. The entry for the partition that uses the computer host name should already exist.
2. To enable an IP address, enter this command under the heading ″Part 2 -Traditional Configuration″ in the startup file (etc/rc.net). Do not enter this command for the partition that uses the computer host name.

   ```
   /usr/sbin/ifconfig interface alias server_name
   ```

   where *interface* is the name of the network interface, and *server_name* is the name of the partitioned server -- for example:

   ```
   /usr/sbin/ifconfig en0 alias server2
   ```

3. Restart the system if necessary, and test the configuration. From another computer, use the ping command with the server names. To show the network status, use the netstat command.

To disable an IP address in IBM AIX or Linux

Do not remove the IP address of a server partition that uses the computer host name as its server name.

1. Enter this command at the console:

   ```
   /usr/sbin/ifconfig interface delete server_name
   ```

   where *interface* is the name of the network interface, and *server_name* is the name of the partitioned server.

2. Remove the partition's name entry from the local host names /etc/hosts file.
3. Remove the corresponding ifconfig command from the system startup /etc/rc.net file.

Sun Solaris

This procedure is for Sun Solaris 2.6. You must have superuser privileges to configure the NIC.

To enable an IP address in Sun Solaris

1. Add one entry in the local host names /etc/hosts file for each server partition. The entry for the partition that uses the computer host name should already exist.
2. For each partition, create a file named:

   ```
   /etc/hostname.device:n
   ```

   where *device* is the device name of the NIC, and *n* is a number that increments for each file name. The /etc/hostname.hme0 file should already exist and contain the computer host name.

   For example, if /etc/hostname.hme0 contains the name Server1, create:

   ```
   /etc/hostname.hme0:1
   ```

   which contains the name Server2. and

   ```
   /etc/hostname.hme0:2
   ```

   which contains the name Server3.
3. Create the alias for each IP address that goes to the NIC which is hme0. At the console, enter:

   ```
   /sbin/ifconfig hme0 plumb
   ```

   ```
   /sbin/ifconfig hme0:
   n IP_address
   ```

   where *n* is the number you created in Step 2 for each file name, and *IP_address* is the address assigned to the corresponding server in Step 1. For example:

   ```
   /sbin/ifconfig hme0 plumb
   /sbin/ifconfig hme0:1 111.123.11.96
   /sbin/ifconfig hme0:2 111.123.11.22
   ```
4. To verify the IP addresses that you configured, enter:

   ```
   /sbin/ifconfig -a
   ```
5. To enable each IP address that you configured in Step 3, enter:

   ```
   /sbin/ifconfig hme0:n up
   ```

   where *n* is the number assigned to the file that contains the server name. For example:

   ```
   /sbin/ifconfig hme0:1 up
   /sbin/ifconfig hme0:2 up
   ```

   To disable an IP address, enter:

   ```
   /sbin/ifconfig hme0:n down
   ```
6. To configure the NIC to support multiple IP addresses at system startup, add this ifconfig command to the startup file (probably /etc/rc2.d/S30sysident):

   ```
   /sbin/ifconfig hme0 plumb
   /sbin/ifconfig hme0:n IP_address
   /sbin/ifconfig hme0:n up
   ```

   where *n* corresponds to the number you created in Step 2 for each file name, and *IP_address* is the address assigned to the corresponding server in Step 1.
7. Test the configuration. From another computer, use the ping command with the server names. To show the network status, use the netstat command.

To disable an IP address in Sun Solaris

Do not remove the IP address of the server partition that uses the computer host name as its server name.

1. To disable the IP address, type:

   ```
   /sbin/ifconfig hme0:n down
   ```

   where *n* is the number assigned to the file that contains the server name. For example:

   ```
   /sbin/ifconfig hme0:1 down
   ```
2. Remove the corresponding /etc/hostname.hme0:*n* file. For example, to remove Server2, remove the /etc/hostname.hme0:1 file, which contains the name Server2.

3. Remove the partition's server name entry from the local host names /etc/hosts file.

Windows

To configure a single NIC for multiple IP addresses on Windows systems, do the following:

- For Windows 2000, use the Network and Dial-up Connections icon on the Control Panel , and then the Local Area Connection icon. Click the Properties button. For more information, see the Windows 2000 documentation.

Configuring a partitioned server for one IP address and port mapping

To configure server partitions to share the same IP address and the same NIC, you use port mapping. With port mapping, you assign a unique TCP port number to each server partition and designate one partition to perform port mapping. The port-mapping partition listens on port 1352 and redirects Notes and Domino connection requests to the other partitions.

If the port-mapping partition fails, existing sessions on the other partitions remain connected. In most cases, Notes clients will not be able to open new sessions on any of the partitions. However, because each Notes client maintains information in memory about recent connections, including those redirected by the port-mapping partition, a client may be able to connect to a partition even when the port-mapping partition is not running. A client or remote server that has a Connection document containing both the IP address and the assigned port can always access the port-mapping partition.

Because the port-mapping partition requires extra system resources, consider dedicating the partition to this task only. To do this, remove all other server tasks, such as mail routing and replication, from the partition's NOTES.INI file.

Port mapping works for NRPC communication only. However, you can use the Server document in the Domino Directory to configure IMAP, LDAP, and POP3 services and Domino Web servers to use unique ports for communication. When you do, you must make the port number available to users when they try to connect to the servers.

Note: Because Internet protocols carry a large amount of data, you may encounter I/O bottlenecks if you use a single NIC with too many server partitions. Consider adding additional NICs and isolating the data by protocol.

To configure for one IP address and port mapping

When you set up port mapping, the port-mapping partition automatically routes NRPC communication requests to the other server partitions.

Note: When setting the NOTES.INI variables for port mapping, do not include a zone in a port mapped address. The zone is only valid locally.

1. Decide which server partition will perform port mapping.
2. Choose a unique TCP/IP port number for each server partition on the computer. The port-mapping partition uses the assigned port, 1352. It is best to use port numbers 13520, 13521, 13522, 13523, or 13524 for the additional server partitions.
3. In the NOTES.INI file of the port-mapping partition, include one line for the port-mapping partition and one line for each of the other partitions. For the port-mapping partition, enter:

   ```
   TCPIP_TcpIpAddress=0,IPAddress:1352
   ```

   where *TCPIP* is the port name, and *IPAddress* is the IP address of the port-mapping partition.

   For each of the other partitions, enter:

   ```
   TCPIP_PortMappingNN=CN=server_name/O=org,IPaddress:TCP/IP port number
   ```

   where *TCPIP* is the port name, *NN* is a number between 00 and 04 assigned in ascending sequence, *server_name* is the server name of the partition, *org* is the organization name, *IPAddress* is the shared IP address, and *TCP/IP port number* is the unique port number you chose for the partition.

Note: You must assign the numbers for *NN* in ascending order beginning with 00 and ending with a maximum of 04. If there is a break in the sequence, Domino ignores the subsequent entries.

4. In the NOTES.INI file of each of the other partitions, include this line:

   ```
   TCPIP_TcpIpAddress=0, IPAddress:IPport_number
   ```

   where *TCPIP* is the port name, *IPAddress* is the shared IP address, and *IPport_number* is the unique port number you chose for the partitioned server.
5. In the Net Address field on the Ports - Notes Network Ports tab in the Server document for each partition, enter the fully qualified domain name -- for example, sales.acme.com -- or enter the common server name -- for example, Sales.
6. Create an IP address entry for the port-mapping partition in the DNS, NIS, or the local hosts file.
7. Include each partition name as a separate CNAME entry in the DNS, NIS, or the local hosts file.
8. If you also plan to set up the partitions for IMAP, LDAP, and POP3 services and Web server communication, assign to each protocol a unique port number in the "TCP/IP port number" field on the appropriate subtabs (Web, Directory, and Mail) on the Ports - Internet Ports tab of the Server document.

   Note: You must make these port numbers available to users when they try to connect to these servers. For example, if you assign port 12080 to the Web server acme.com, users must include acme.com:12080 in the URL in order to connect to the server, unless they have a means to redirect the connection to this port assignment.

Example

This example shows the lines you add to the NOTES.INI files of the server partitions to set up port mapping for six partitions.

Partition 1 (the port-mapping partition)

```
TCPIP_TcpIpAddress=0,192.94.222.169:1352
TCPIP_PortMapping00=CN=Server2/O=Org2,192.94.222.169:13520
TCPIP_PortMapping01=CN=Server3/O=Org3,192.94.222.169:13521
TCPIP_PortMapping02=CN=Server4/O=Org4,192.94.222.169:13522
TCPIP_PortMapping03=CN=Server5/O=Org5,192.94.222.169:13523
TCPIP_PortMapping04=CN=Server6/O=Org6,192.94.222.169:13524
```

Partition 2

```
TCPIP_TcpIpAddress=0,192.94.222.169:13520
```

Partition 3

```
TCPIP_TcpIpAddress=0,192.94.222.169:13521
```

Partition 4

```
TCPIP_TcpIpAddress=0,192.94.222.169:13522
```

Partition 5

```
TCPIP_TcpIpAddress=0,192.94.222.169:13523
```

Partition 6

```
TCPIP_TcpIpAddress=0,192.94.222.169:13524
```

Changing a TCP or SSL port number

The following sections describe the TCP ports that Domino services use and provide guidelines should you ever need to change these ports.

Default port for NRPC

By default, all NRPC connections use TCP port 1352. Because the Internet Assigned Number Authority (IANA) assigned Lotus Domino this port number, non-Domino applications do not usually compete for this port.

Do not change the default NRPC port unless:

- You can use a NAT or PAT firewall system to redirect a remote system's connection attempt.
- You are using Domino port mapping.
- You create a Connection document that contains the reassigned port number.

To change the default NRPC port number, use the NOTES.INI setting *TCPIPportname*_TCPIPAddress and enter a value available on the system that runs the Domino server. TCP ports with numbers less than 5000 are reserved for application vendors. You may use any number from 1024 through 5000, as long as you don't install a new application that requires that number.

Note: When setting the NOTES.INI variables for port mapping, do not include a zone in a port mapped address. The zone is only valid locally.

Default ports for Internet services

You may occasionally need to change the number of the TCP or SSL port assigned to an Internet service. Lotus Domino uses these default ports for Internet services:

Service	Default TCP port	Default SSL port
POP3	110	995
IMAP	143	993
LDAP	389	636
SMTP inbound	25	465
SMTP outbound	25	465
HTTP	80	443
IIOP	63148	63149
Server Controller	N/A	2050

Server setup tasks specific to NetBIOS

After you run the Domino Server Setup program, complete these procedures:

1. Use the Domino Administrator to define a NetBIOS LANA number for the NetBIOS port.
2. If you want the server to connect to different segments of a NetBIOS network, create one or more additional Notes network ports for NetBIOS.

Defining a NetBIOS LANA number for a Notes network port

To run NetBIOS on a server, after you complete the Server Setup program, you must determine the NetBIOS LANA number to which the Notes network port will be bound. The NetBIOS LANA number is a logical number that represents a NetBIOS transport protocol stack on a NIC. You must know which transport protocol Notes workstations and other Domino servers are using for NetBIOS within your workgroup or company.

If the computer running the Domino server has more than one NIC running the same protocol stack, you must define a different NetBIOS LANA number for each Notes network port for NetBIOS.

NetBIOS systems using the same transport protocol should be in the same Notes named network. If you create Connection documents on the server, the LAN port you select must also be for the same transport protocol.

To define a LANA number in Lotus Domino

1. From the Domino Administrator or Web Administrator, click the server for which you want to define a LANA number.
2. Click the Configuration tab.
3. Do one of these:
   - From the Domino Administrator’s Tools pane, choose Server - Setup Ports.
   - From the Web Administrator’s Port tool, choose Setup.
4. Select the *Portname* port, where *Portname* is the name of the NetBIOS port for which you are defining a LANA number.
5. Click "*Portname* Options," and choose Manual.
6. Enter the correct LANA number.
7. Click OK.

To find the LANA number for a NetBIOS protocol on a Windows XP or 2000 system

A Windows XP or 2000 system does not have a direct means to see the LANA associations. For Windows XP or 2000 systems you can either review the system’s registry bindings or use a Microsoft tool called LANACFG to see and change the LANA number assignments.

The following is an example of the tool’s output from a Windows 2000 server.

```
lanacfg [options]
showlanapaths - Show bind paths and component descriptions for each exported lana
setlananumber - Change the lana number of a bind path
rewritelanainfo - Verify and write out lana info to the registry
showlanadiag - Show lana diagnostic info
```

From the DOS prompt, enter

```
C:\>lanacfg showlanapaths
```

You see the following:

```
Lana:   4
-->NetBEUI Protocol-->3Com EtherLink III ISA (3C509/3C509b) in Legacy mode
Lana:   7
-->NetBEUI Protocol-->WAN Miniport (NetBEUI, Dial Out)
Lana:   3
-->NWLink NetBIOS
Lana:   0
-->WINS Client(TCP/IP) Protocol-->Internet Protocol (TCP/IP)-->3Com EtherLink III ISA (3C509/3C509b) in Legacy mode
```

Creating additional network ports for NetBIOS

After you run the Domino Server Setup program, you can create network segments for multiple NetBIOS interfaces on the same computer by adding a Notes network port for NetBIOS for each additional NIC.

In addition to adding each port for NetBIOS, do the following:

- Associate each Notes network port for NetBIOS with a specific NetBIOS interface by defining a LANA identifier for each port.
- Make sure that all Domino servers that will access each other have an interface that uses a common transport protocol. It is best if they are also in the same Notes named network.

- Make sure that the network segments to which the server system’s NICs are attached do not have a pathway in common. The NetBIOS name service (NetBIOS over IP) can fail if it detects the same system name or Domino name echoing back between the pathways. If you are using both the NetBIOS name service and DNS or a hosts file for name resolution, make sure that the server name in DNS or the hosts file is different from the system name.

Chapter 3. Installing and Setting Up Domino Servers

This chapter describes how to plan a hierarchical name tree and how to install, set up, and register Domino servers.

Installing and setting up Domino servers

Before you install and set up the first Domino server, you must plan server and organizational naming and security. In addition, you must understand your existing network configuration and know how Domino will fit into the network. If you are adding an additional server to an existing Domino infrastructure, you must have already registered the server and its server ID and password must be available.

Note: If you plan to run multiple language versions of Domino with Web browsers, install the International English version of the Domino server as the base Domino installation. Next, install other language packs. Installing the Domino server in English first prevents error messages from displaying in other languages, even when you have selected English as the language preference in your Browser options.

For information on system requirements, see the *Release Notes.*

To install and set up a server

Installing a Domino server -- that is, copying the server program files onto the designated machine -- is the first part of deploying a server. The second part is using the Domino Server Setup program to configure the server.

1. Choose a name for the server. Refer to the hierarchical name scheme that you created based on your company's structure.
2. Identify the function of the server -- for example, will it be a mail server or an application server? The function of the server determines which tasks to enable during configuration.
3. Decide where to locate the server physically and decide who administers it.
4. Decide whether the server is part of an existing Domino domain or is the first server in a new Domino domain.

   For more information on Steps 1 through 4, see the chapter ″Deploying Domino.″
5. If this is the first server in a Domino domain, do the following:
   a. Install the server program files.
   b. Use the Domino Server Setup program to set up the server.
   c. Complete network-related setup.
   d. Create organization certifier IDs and organizational unit certifier IDs, as required by the hierarchical name scheme.
   e. Distribute certifier IDs to administrators.
   f. Implement Domino security.
6. If this server is part of an existing Domino domain, do the following:
   a. Use the Domino Administrator to register the server.
   b. Install the server program files on each additional server.
   c. Use the Domino Server Setup program to set up each additional server.

   For more information on Steps 5 and 6, see the procedures that follow and the chapters ″Setting Up the Domino Network″ and ″Planning Security.″

7. Perform additional configuration procedures, based on the type of services, tasks, and programs that you want to run on this server.

Entering system commands correctly

Some of the procedures that follow include instructions for entering commands at the system command prompt. The instructions tell you to enter the command from the ″Domino program directory″ or ″Notes program directory,″ depending on whether you are performing the procedure on a Domino server or a Notes workstation. Before entering commands, make sure you understand the following definitions of these terms as they apply to your operating system.

Windows operating systems

On a Domino server, the Domino program directory is c:\lotus\domino, unless you installed the program files to a different location. On a Notes workstation, the Notes program directory is c:\lotus\notes, unless you installed the program files to a different location.

UNIX operating systems

For Domino on a UNIX® server, the actual location of the server program files is different from the directory you use for entering commands. Always use the following path for entering commands:

```
lotus/bin/server
```

The ″server′″ portion of the path is a script that initializes a UNIX shell so that Domino programs can run on UNIX.

While by default the actual location of the lotus directory is /opt/ibm/lotus, you can change it to any location, for example, /local/lotus or /usr/lotus.

Server installation

The first step in deploying a Domino server is installation, or copying the program files to the system's hard drive.

To install Domino, see the following procedures:

Installing Domino on Windows systems

Installing Domino on UNIX and on Linux on zSeries systems

For information on installing servers for hosted environments, see the chapter ″Setting Up the Service Provider Environment.″

Installing Domino on Windows systems

You can install Domino on a Windows system by following this procedure, or you can perform a silent install of a local server.

For information about installing the xSP server, see the topic Installing the first server or additional servers for hosted environments.

For information about silent server installation, see ″Using silent server installation to install Domino on Windows systems″ in this chapter.

1. Before you install the Domino server program files on a Windows system, do the following:
   - Make sure that the required hardware and software components are in place and working.
   - Read the *Release Notes* for operating system and network protocol requirements and for any last-minute changes or additions to the documentation.
   - Temporarily disable any screen savers and turn off any virus-detection software.

- Before running any Domino setup command, be sure to complete any pending reboot actions you may have from installing other applications.
- Make sure that all other applications are closed. Otherwise, you may corrupt any shared files, and the Install program may not run properly.
- If you are upgrading to Domino from a previous release, see the book *Upgrade Guide.*

2. Run the install program (SETUP.EXE), which is on the installation CD.
3. Read the Welcome screen, and click Next. Then read the License Agreement and click I accept the terms in the license agreement, and then click Next.
4. Choose the program directory, and choose whether you are installing partitioned servers. Click Next.
5. Specify the data directory in which to copy the software. If you are installing a partitioned server, If you are installing partitioned servers, specify a data directory for each partition.

   Note: For partitions, use the Add button to add each of the data directories to the list. If they are not added to the list they will not be installed.
6. Select the server type you acquired:
   - Domino Utility Server -- Installs a Domino server that provides application services only, with support for Domino clusters. The Domino Utility Server removes client access license requirements. Note that it does NOT include support for messaging services. See full licensing text for details.
   - Domino Messaging Server -- Installs a Domino server that provides messaging services. Note that it does NOT include support for application services or Domino clusters.
   - Domino Enterprise Server -- Installs a Domino server that provides both messaging and application services, with support for Domino clusters.
   - Customize - Allows you to select the features you want to install.

     Note: All installation types support Domino partitioned servers. Only the Domino Enterprise Server supports a service provider (xSP) environment.
7. If you are installing partitioned servers, specify a data directory for each partition.
8. Review the summary information, and then select Next to begin installing files.
9. Click Finish to complete the install program.
10. Choose Start - Programs - Lotus Applications - Lotus Domino Server, or use the icons on your Desktop to start the Server Setup program.

Using silent server installation to install Domino on Windows systems

Use Domino's silent server installation to install servers without any intervention during the installation process. The silent server installation suppresses the wizard and the launcher user interface. There is no need to monitor the installation or to provide additional input through the typical installation dialog boxes.

Before running Domino's silent server install on a Windows system, do the following:

- Make sure that the required hardware and software components are in place and working.
- Read the Lotus Domino Release Notes for operating system and network protocol requirements. Check the Release Notes for last-minute changes or additions that may impact the silent server install.
- Temporarily disable screen savers and turn off virus-detection software.
- Before running any Domino setup command, complete any pending reboot actions you may have from installing other applications.
- Make sure that all other applications are closed; otherwise, you may corrupt shared files, and the Install program may not run properly.
- If you are upgrading from a previous Domino release, see the book *Upgrade Guide*.

Customized silent server install on Win32 systems: There are two steps to running a customized silent server install.

1. Create or record the response file, which contains the installation configuration information.
2. To create the response file, you can use the template file, sample_response.txt, located on the CD with the other installation files. Modify the template file and save it to a new response file name.
3. Run the silent install referencing the response file.

Creating the response file for silent server installation: A typical (non-silent) install uses dialog boxes to receive input from you during installation. The silent (automated) server install does not prompt you for input. Instead, response files are used to provide the detail information for the install process. There are two methods of generating response files, the template and record methods.

A response file created using the template method contains the literal values that are used during the install process. It is generated prior to the execution of the installation and contains all of the default installation options and paths. You can manually customize this file by editing options. The benefit of using a template file is that you do not need to install a server in order to create the file.

A response file created using the record method is generated after the server install completes, at the time the wizard exits and stores the values of the applicable wizard properties in the file. The recorded response file is useful for saving a record of a specific wizard execution session which can later be reused in a silent or modified installation. When you install a server, your customizations are saved to the resulting response file, eliminating the need to edit the response file. This is the ″safer″ method because you do not create issues caused by typos or incorrect entries and values.

Creating a response file based on a template: Use this procedure to create a response file that is based on the template, sample_response.txt. Response files contain installation configuration information. The template file, sample_response.txt, is located on the CD with the other installation files.

Note: It takes several minutes for the response file to be created. When the SETUP.EXE file and the JAVA.EXE file have finished running, the new response file is ready for use. To determine whether SETUP.EXE and JAVA.EXE have finished running, check the Task Manager.

1. To create the response file, do one of these:
   - Open the template file, modify the file as necessary, and then save the file to a new name.
   - Save the file to a new file name, modify the file, and then save the file again.
2. Run the silent install referencing the response file.

To use a response file: To use a response file, specify the -options parameter and the exact path to the response file on the command line. Enter the command in the format shown in the example:

```
setup.exe -silent -options c:\temp\file.txt
```

For additional examples, see the table.

Installation activity	**Example**
Silent install with default selections and options	setup.exe - silent
Creating a Response File:	setup -options-template c:\temp\file.txt
Recording a response file	setup -options-record c:\temp\file.txt
Silent install using response files	setup.exe -silent -options c:\temp\file.txt

Running the Silent Server Install on Win32 Systems

To create a response file for automating the Lotus Domino installation, you must pass command line parameters to SETUP.EXE. The command line parameters are listed and explained in the table in Step 2.

When the response file has been created, perform the silent install of the Domino server.

1. Launch the server install with any of the command line parameters shown in the table below.

Parameter	Description and example
-silent	Runs the basic silent server install. For example, setup.exe -silent
-options-record filename	Records in a response file, all of the installer selections you use. For example, setup -option-record C:\temp\file.txt

Installing Domino on UNIX and on Linux on zSeries systems

Before you install the Domino program files on a UNIX system, do the following:

- Make sure that the required hardware and software components are in place and working.
- Read the *Release Notes* for operating system and network protocol requirements and for any last-minute changes or additions to the documentation.
- Temporarily disable any screen savers and turn off any virus-detection software.
- Make sure that all other applications are closed. Otherwise, you may corrupt any shared files, and the Install program may not run properly.
- If you are upgrading to Domino from a previous release, read the *Upgrade Guide.*
- For Domino for Linux, you must install the sysstat package containing iostat in order to obtain platform statistics.
- If you are using Linux on zSeries, do the following:

1. Copy the Domino installation tar file, ZLINUX.TAR.GZ, from the CD ROM at your workstation to a Linux on zSeries file system where it can be expanded and utilized for the installation steps. Be sure to transfer the file using a binary method. For example, for FTP, set the transfer mode to ″binary″. Neither the tar file nor its contents are required after installation has completed.
2. Expand the tar file by issuing the following shell command on Linux for zSeries:

   ```
   tar -xzvf ZLINUX.TAR.GZ
   ```

   Note: It could take a minute or two for this process to complete. Once complete, the subdirectories ″zlinux/domino″ should exist.
3. (Optional) Delete the tar file to save disk space.
4. Change to the directory containing the Domino install script:

   ```
   cd zlinux/domino
   ```

When the installation is complete (interactive mode or script mode), both the tar file and the ″zlinux″ subdirectory created by its expansion can be deleted.

You can install multiple instances of the Domino server on a single system. The instances can be the same release of Domino or different releases. If you install different releases, only one instance can be earlier than Domino 7.

If you want all instances to be the same release, it is best to install a Domino partitioned server because all Domino partitions then share one program directory and, by doing so, conserve system resources. If you install a single Domino server and later want to make it a partitioned server, you can do so without removing the initial installation. When you have multiple instances of the Domino server, each with a separate program directory, one or more of the instances may be a partitioned server.

To install the Domino program files on a UNIX system, you can use either interactive mode or script mode.

To use interactive mode

You use interactive mode to install the Domino program and data files on the local machine or to use a Telnet connection to install the Domino program and data files on specified remote systems.

During the interactive mode installation, you can use these keys at the UNIX command prompt:

- Type h for help
- Type e to exit the Install program
- Press ESC to return to the previous screen
- Press the spacebar to change the setting until you get the one you want
- Press TAB to accept a setting and continue to the next screen

1. Make sure the Domino server kit is available from your network or CD ROM drive.

   Note: If you are using Linux on zSeries, be sure the Install files are located in your local file system. For information on transferring the files to your local file system, see the procedure at the beginning of this topic.
2. Log in to the root account for Domino Server installation.
3. Change to the directory containing the ″install″ script.
4. Enter the following at the root command prompt to run the script:
   ```
   ./install
   ```
5. Follow the on-screen instructions and specify these options:

Option	Action
Add data directories only	Choose one: • Yes to change a single Domino server into a partitioned server or add data directories to an existing partitioned server • No to keep a single Domino server
Domino Server installation type	Choose the server type that you acquired. For an xSP server, you must have the Domino Enterprise Server.
Install template files	Choose one: • Yes to install new templates • No to retain templates from a previous release
Install xSP server (for Domino Enterprise Server only)	Choose one: • Yes if this is an xSP server • No if this is not an xSP server
Program directory	Specify the directory in which Domino will store program files.
Create /opt/ibm/lotus soft link	Choose one: • Yes if this system will have only one Domino installation (program directory) • No if this system will have multiple Domino installations (multiple program directories)
Data directory	Specify the directory in which Domino will store data files. If you are installing a partitioned server, indicate that and specify multiple data directories.
UNIX User name	Specify the person who will own the server configuration data. If you are installing a partitioned server, you may specify a different person for each data directory.
UNIX Group name	Specify the group to which the UNIX User belongs. If you are installing a partitioned server, you may specify a different group for each data directory.

To use script mode

Script mode installation provides silent install functionality for UNIX platforms and allows you to install saved installation settings to a local server or remote servers.

SCRIPT.DAT, the default sample script file, contains information you need to install the Domino server program files, including descriptions of each parameter and instructions for using the -script option to install partitioned servers.

1. Change the directory to the kit's install directory on either the CD-ROM or network drive.
2. Copy SCRIPT.DAT from the kit's install directory to your local system as

   ```
   filename.dat
   ```

   Where *filename* is the name you want to give to the local script file that will contain the installation settings.
3. Open the local script file, *filename.dat*, and set the parameters as needed. It is usually best to use the default settings, as follows:
   - Install target host name -- parameter = target_hosts
   - Domino server installation type --Choose the server type that you acquired.
   - Install template files -- template_install_option = 1
   - Add data directories only -- add_data_directories_only = 0
   - Install xSP server -- asp_install_option = 0
   - Program directory -- Use the directory where Domino stores program files.
   - Create /opt/ibm/lotus soft link -- opt_lotus_softlink = 0
   - Data directory -- Use the directory where Domino stores data files.
   - UNIX User name -- Person who will own the server configuration data
   - UNIX Group name -- The group to which the UNIX User belongs
4. Save the local file, *filename.dat.*
5. Log in to the root account from your local system.
6. Switch back to the kit's install directory (CD-ROM or network).
7. To install using the local script file, enter this command at the UNIX console prompt:

   ```
   install -script filename.dat
   ```

Using silent server install on UNIX systems

These instructions apply only to UNIX systems. Before running a silent server install, read all of the installation information in this chapter.

Running a silent server install on UNIX:

1. Make a local copy of the file SCRIPT.DAT. The SCRIPT.DAT file is located in the install directory.
2. Edit the new copy of SCRIPT.DAT. The step-by-step instructions for editing the file are in the SCRIPT.DAT file.
3. Run the install program by entering this command:

   ```
    ./install -script /tmp/script.dat
   ```

Note: The command shown above uses the directory name ″tmp″ but you may name this directory according to your own naming conventions.

Using Domino's express install

Note: Before running any Domino setup command, be sure to complete any pending reboot actions you may have from installing other applications.

Express install is similar to a regular server install except that you have the additional option of launching the server from the last window displayed during express install. During the express install, you are presented with various dialog boxes and informational messages, as you would be during the standard Domino server install; however, during express install, many of the options presented on the dialog boxes are selected for you, resulting in a faster install process.

To run Domino's Express Install, from the Installer command line, enter the following command:

```
setup -express
```

Note: Run Domino express server install from the full installation kit. It is not available for installation from a Web kit.

Concurrent I/O and Direct I/O not supported on Domino servers on AIX

Concurrent I/O (CIO) and Direct I/O (DIO) are not supported with Lotus Domino servers. CIO is a file system feature introduced in AIX 5.2.0.10, also known as maintenance level 01, in the Enhanced Journaling File system (JFS2). This feature improves performance for many environments, particularly for relational databases.

Because the CIO feature is not supported for use with Domino servers, do not enable this option on file systems that Domino accesses. If this option is enabled, Domino data may be corrupted which can causes server crashes or performance issues.

Certain core file system items, such as file buffer cache, per-file lock or inode lock, and sync daemon, are managed differently by the operating system with the CIO option enabled. Domino is not coded to address these changes in behavior.

The CIO option is typically enabled as a flag when a file system is mounted. Use these steps to disable the mount option:

1. Run this command for each file system mounted with CIO:

   ```
   chfs -a options=rw /FS_NAME
   ```

   Where /FS_NAME is the name of the mount point.
2. Unmount and remount each file system, or reboot, which has the same effect when done after running the chfs commands.
3. To verify that the change was applied, run 'mount' and verify that you do not see "cio" in the mount options column, as shown in the examples.

Example of output with CIO disabled

```
/dev/test05lv     /test05 jfs2   Oct 04 23:13 rw,log=INLINE
```

Example of output with CIO enabled:

```
/dev/test03lv /test03  jfs2   Sep 19 19:25 rw,cio,log=INLINE
```

For more information on the CIO feature, see the AIX whitepaper "Improving Database Performance With AIX Concurrent I/O" at http://www-1.ibm.com/servers/aix/whitepapers/db_perf_aix.pdf

The Domino Server Setup program

The Domino Server Setup program guides you through the choices you make to configure a Domino server. Setting up the first Domino server in a domain establishes a framework that consists of the Domino Directory, ID files, and documents. When you set up additional servers, you build upon this framework.

Note: Domino first server setup creates IDs with a default public key width of 1024 bits. If a different key width is required, run SETUP.EXE to install the Domino files but before starting the server, open the server’s NOTES.INI file, and then set SETUP_FIRST_SERVER_PUBLIC_KEY_WIDTH to the desired key width. For example, for Domino R5-compatible keys, install the files for the Domino server by running SETUP.EXE, but before starting the server, open the NOTES.INI file and then set SETUP_FIRST_SERVER_PUBLIC_KEY_WIDTH=630. The public key width can be set to either 630 or 1024 when using the NOTES.INI variable.

Setting up the first Domino server does the following:

- Creates a Domino domain.
- Creates the certification log file, names it CERTLOG.NSF, and saves it in the Domino data directory.
- Uses the PUBNAMES.NTF template to create the Domino Directory for the domain, names the directory NAMES.NSF, and places it in the Domino data directory.
- Creates an organization certifier ID, names it CERT.ID, and saves it in the Domino data directory.
- Optionally creates an organizational unit certifier ID, names it OUCERT.ID, and stores it in the Domino Directory.
- Creates a Certifier document, which describes the organization certifier ID, in the Domino Directory.
- Creates a server ID, names it SERVER.ID, and saves it in the Domino data directory.
- Uses the organization certifier ID to certify the server ID.
- Creates a Server document in the Domino Directory and includes in it information that you specified during the setup program.
- Creates a Person document in the Domino Directory for the Domino Administrator that you specified during the setup program.
- Creates a user ID and password for the Domino Administrator and attaches it as a file named USER.ID to the administrator’s Person document in the Domino Directory.
- Uses the organization certifier ID to certify the administrator’s user ID.
- Gives the administrator and the server Manager access in the ACL of the Domino Directory.
- Adds the server name to the LocalDomainServers group in the Domino Directory.
- Creates the log file, names it LOG.NSF, and saves it in the Domino data directory.
- Enables the appropriate network and serial ports.
- Creates a mail directory in the Domino data directory and creates a mail file in that directory for the Domino Administrator.
- Creates the Reports file, names it REPORTS.NSF, and saves it in the Domino data directory.
- Updates network settings in the Server document of the Domino Directory.
- Configures SMTP, if selected during the setup program.
- If ″DOLS Domino Off Line Services″ was selected during the setup program, creates the Off-Line Services file, names it DOLADMIN.NSF, and saves it in the Domino data directory,.
- Updates the Access Control List in all databases and templates in the Domino data directory tree to remove Anonymous access and/or add LocalDomainAdmin access, depending on the selections made during the setup program.
- Configures xSP Service Provider information, if selected during the install program.

Setting up an additional Domino server does the following:

- Copies the Domino Directory, if a file location was specified during the setup program, names it NAMES.NSF, and saves it in the Domino data directory.
- Dials the existing Domino server if the connection is made through a modem (possible only on Windows systems).
- Copies the server’s ID from the location specified during the setup program, either from a file, a copy of the directory, or the existing Domino server’s directory; names it SERVER.ID; and saves it in the Domino data directory.

- Retrieves the Domain name and Administrator name from the Server document in the Domino Directory.
- Creates the log file, names it LOG.NSF, and saves it in the Domino data directory.
- Copies or replicates the Administration Requests file, names it ADMIN4.NSF, and saves it in the Domino data directory.
- Copies or replicates the Monitoring Configuration file, names it EVENTS4.NSF, and saves it in the Domino data directory.
- Replicates the Domino Directory, if it doesn't already exist, names it NAMES.NSF, and saves it in the Domino data directory.
- Creates a Connection document to the existing Domino server in the Domino Directory.
- Creates the Reports file, names it REPORTS.NSF, and saves it in the Domino data directory.
- Updates network settings in the Server document of the Domino Directory.
- Configures SMTP, if selected during the setup program.
- If ″DOLS Domino Off-Line Services″ was selected during the setup program, creates the Off-Line Services file, names it DOLADMIN.NSF, and saves it in the Domino data directory.
- Updates the Access Control List in all databases and templates in the Domino data directory tree to remove Anonymous access and/or add LocalDomainAdmin access, depending on the selections made during the setup program.
- Configures xSP Service Provider information, if selected during the install program.
- Replicates changes made to the Server document with the existing server, if any.
- Removes the SERVER.ID attachment from the Domino Directory, if applicable.

Using Domino Off-Line Services (DOLS) and Domino Web Access

To provide Domino Web Access users with the ability to work off line, you must enable DOLS when you set up the server. DOLS enables users to work off line, disconnected from the network, and provides many replication features that Notes users expect when working in the Notes client.

Users require a Notes ID so that DOLS can synchronize the offline mail file with the server. The default DOLS configuration will prompt the user for a Notes ID the first time they go offline with Domino Web Access.

If you rename a user, the user must reinstall the DOLS offline subscription in order for the offline mail file to synchronize with the server. After a name change, the user must wait for the old Notes ID and password to stop working, accept the name change using a Notes client, then log on to Domino Web Access with the new Notes ID and password.

Setting up DOLS on a server

Domino Off-Line Services (DOLS) must be configured on the Domino server for users to be able to take applications off-line and use only a browser to work with them. You can enable any application for DOLS. The following templates are enabled for DOLS by default:

- Domino Web Access (DWA7.NTF, iNOTES6.NTF and iNOTES5.NTF)
- Extended Mail (MAIL7EX.NTF)
- Discussion - Notes and Web (R7) database (DISCSW7.NTF)

To configure DOLS during Domino Server Setup

1. Under ″Setup Internet services for,″ select ″Web Browsers (HTTP services),″ and then click Customize.
2. In the ″Domino tasks″ list, select ″DOLS Domino Off-Line Services.″
3. At the end of setup, when you have the option to create an access control list entry, add the group LocalDomainAdmins to all databases and templates.

4. Accept the default option ″Prohibit Anonymous access to all databases and templates.″ If you deselect this option, you must open the ACL for each DOLS application and assign No Access to Anonymous.
5. Make sure the following names are identical:
   - The TCP/IP DNS host name -- In Windows, choose Start - Programs - Windows Explorer. Then choose Network Neighborhood properties - TCP/IP properties. On the DNS Configuration tab, look at the Host field.
   - The server name -- Open the Server document and look at the Server name field.
   - The Internet host name -- Open the Server document and look at the ″Fully qualified Internet host name″ field.

Note: DOLS runs on Domino servers configured to work through a Microsoft IIS server.

To configure DOLS manually

If you do not configure DOLS during Domino Server Setup, you can configure DOLS manually by editing the Server document.

1. Open the Server document.
2. Click Internet Protocols - HTTP.
3. In the ″DSAPI filter file names″ field, enter the DSAPI filter file name that corresponds to the operating system that the server is running, and then restart the server:
   - Win32 - ndolextn
   - Linux - libdolextn
   - AIX® - libdolextn
   - Solaris/Sparc - libdolextn
   - S390® - libdolextn
   - iSeries® - libdolextn

     Note: On the iSeries platform, the Server document is updated when a new server is configured or an existing server is modified using the CFGDOMSVR or CHGDOMSVR CL command with DOLS(*YES) specified.

   For more information on configuring an iSeries server with DOLS, see the *Lotus Domino 7 for iSeries Release Notes*.
4. Create a DOLADMIN.NSF database from the template DOLADMIN.NTF.
5. After the database is created, restart the Domino administrator and click the Configuration tab. The name of the DOLADMIN.NSF is an option in the Navigation pane.

To set up DOLS on clustered servers

Before using DOLS on a clustered Domino 7 server, make sure that:

- The Domino server is either a Domino Utility Server or Domino Enterprise Server.
- All servers in the cluster run the same release of Domino with DOLS
- Clustered server management is running to handle both failover of replication and HTTP
- Internet Cluster Manager is running
- Subscription directories must have the same name on every clustered server. For example, if a subscription is under \data\Webmail user\7CD5957CB669AE2285256BDF00567AD8\, this name cannot be different on a different server in the cluster.

To configure DOLS on a server that uses Web Site documents

If you create a Web Site Document (a type of Internet Site document) on the Domino server, you must add the appropriate DOLS DSAPI filter filename to the DSAPI field in the Web Site document for DOLS to be enabled. If there are several Web Site documents, you must add the DSAPI filter filename to each one. To add the DOLS DSAPI filter filename to a Web Site document:

1. Open the Web Site document.

2. Click the Configuration tab.
3. In the ″DSAPI filter″ field, enter the DSAPI filter file name that corresponds to the operating system that the server is running, and then restart the server:
   - Win32 - ndolextn
   - Linux - libdolextn
   - AIX - libdolextn
   - Solaris/Sparc - libdolextn
   - S390 - libdolextn
   - iSeries - libdolextn

For more information on Internet Site documents, see the topic ″Configuring Internet sites with Web Site and Internet Site documents.″

Setting up Domino Web Access on a server

Domino Web Access provides Notes users with browser-based access to Notes mail and Notes calendar and scheduling features. Using Domino Web Access, a user can send and receive mail, view the calendar, invite people to meetings, create to do lists, keep a notebook, and work off line.

To set up Domino Web Access, choose ″Web Browsers (HTTP Web services)″ during Server Setup. If you want to give users the ability to work off line, also choose Domino Off-Line Services (DOLS). DOLS is not required to run Domino Web Access.

Note: When providing a Domino domain name, do not use a period. For example, use AcmeProduction as a domain name instead of Acme.Production.

In the Domino Administrator, make sure that the Fully Qualified Domain name (FQDN) (such as acme.lotus.com) is specified on the Basics tab of the Server document.

Setting up Domino Web Access with IBM Lotus Sametime

Domino Web Access (DWA) integrates an instant messaging (IM) capability so that users can chat with their co-workers online and maintain an instant messaging list that shows the online status of other users. The instant messaging awareness feature also displays online status next to the names of people in mail messages, views and folders.

There are two versions of Sametime available for Domino 7.0, however these instruction apply to both version. References to the Sametime server also apply to installing the limited use version. The two versions are:

- IBM Lotus Instant Messaging Limited Use -- the default instant messaging capability that is included in Domino 7.0.
- IBM Lotus Sametime® -- the full instant messaging product that includes Web conferencing capabilities. It is available only if your organization purchased it.

For complete information on installing IBM Lotus Sametime, see the *IBM Lotus Sametime 7.0 Installation Guide* for your operating system, and the *IBM Lotus Sametime 7.0 Administrator's Guide.* To view or download the Sametime documentation, go to http://www.lotus.com/LDD/doc.

Configuration Notes

- For Mozilla, you must have at least Sametime 3.1 to run instant messaging integration. Previous versions of Lotus Sametime are not supported in Domino Web Access on Mozilla.
- When you install Domino 7.0, the stlinks files that are installed in the stlinks directory (for example, C:\st\domino\Data\domino\html\sametime\stlinks), are overwritten. If you have modified stlinks files (for example, if the Sametime server is configured for tunneling) these files will be replaced. When

you are upgrade to 7.0, these files are backed up in a file called stlinks.sav. For additional information, see the topic Customizing STLinks files for tunneling or reverse proxy servers.

- To access the Sametime server using a protocol that is different from the current Web page's protocol, use the NOTES.INI configuration setting iNotes_WA_SametimeProtocol.
- Sametime integration with Domino Web Access is not supported with JRE 1.4.1.

Part 1 - Set up Domino Web Access on a Domino server

1. Set up Domino Web Access on a server by making the appropriate selections during server setup.
2. Register users with the Domino Web Access (DWA7.NTF) mail template.

Part 2 - Set up the Sametime server

If possible, the Sametime server should be in the same Domino domain as the Domino Web Access server. Follow the instructions in the *IBM Lotus Sametime 7.0 Installation Guide* to install and configure instant messaging on a dedicated Domino server in the same Domino domain as the Domino Web Access server.

If the Sametime server is in a different domain than your Domino Web Access server, follow the instructions in Setting up Sametime and Domino Web Access in different domains.

Make sure the Sametime server is functioning properly before proceeding. If you have multiple Sametime servers in a single community, also make sure that Domino single sign-on (SSO) is functioning properly between the servers. For complete information on working with multiple Sametime servers, see the *IBM Lotus Sametime 7.0 Administrator's Guide*, available on http:\\www.lotus.com/ldd/doc.

Part 3 - Create Connection documents

You need Connection documents for the Domino Web Access and the Sametime server if the Sametime server is not in the same domain as the Domino Web Access server. Also, if the Sametime server is in the same domain as the Domino Web Access server, but is not clustered with the registration server, you need a Connection document in order to replicate the Domino Directory.

Create Connection documents using the standard procedure, and include the information below:

On the Domino Web Access server:

- Enter the Sametime server's name in the ″Destination server″ field. For example: Sametime/Acme.
- Enter the Domino Web Access server's name in the ″Source domain″ field.
- Enter the Sametime server's name in the ″Destination domain″ field.

On the Sametime server:

- Enter the Domino Web Access server's name in the ″Destination server″ field.
- Enter the Sametime server's name in the ″Source domain″ field.
- Enter the Domino Web Access server's name in the ″Destination domain″ field.

Part 4 - Specify the Sametime server for Domino Web Access users

There are two ways to specify a Sametime server for Domino Web Access users. You can edit the Configuration Settings document for the Domino Web Access server, or you can edit the person document for each user who uses instant messaging.

Method 1

To enable instant messaging and set the Sametime server for all Domino Web Access users at one time, use the Instant Messaging settings in the Configuration Settings document, Domino Web Access tab. After you have done this, individual users can enable or disable instant messaging on their local Domino Web Access clients by setting a User Preference.

Method 2

If you choose not to enable instant messaging for all users, then you must edit the person document for each user who will use instant messaging:

1. From the Domino Administrator, click the People & Groups tab.
2. Select the Domino Web Access Domino directory, then click People.
3. Double-click a name to open the user's Person document.
4. Click Edit.
5. Enter the name of the Sametime server in the ″Sametime server″ field. For example, Sametime/Sales/Acme/UK.
6. Click ″Save & Close.″
7. Repeat Steps 3 though 6 for each person.

Part 5 - Set up Domino Web SSO authentication between the DWA server and IM server

Domino single sign-on (SSO) authentication allows Web users to log in once to a Domino or WebSphere server, and then access any other Domino or WebSphere server in the same DNS domain that is enabled for single sign-on (SSO) without having to log in again. In a multiple server environment, it is possible that one or more servers in your Domino domain are already configured for Domino SSO, and the Domino Directory already contains a Domino Web SSO configuration document. When you install Sametime, it creates a Web SSO configuration document called LtpaToken unless one already exists in the Domino directory. If an LtpaToken configuration document already exists, Sametime does not attempt to alter it.

For more information about Domino Web SSO authentication, see the topic Multi-server session-based name-and-password authentication for Web users (single sign-on).

Configure the Domino Web Access server for Web SSO

Complete the steps in this section if your DWA server is not configured for Web SSO, and you want to use the Web SSO document that Sametime created to configure it.

1. Ensure that the Domino Directory has replicated throughout the Domino domain since you installed Sametime.
2. Update the Web SSO Configuration document that was created when you installed Sametime (LtpaToken):
   a. Open the Domino Directory and select the Configurations - Web - Web Configurations view.
   b. From within this view, expand the list of Web SSO Configurations.
   c. Open the ″Web SSO Configuration for LtpaToken″ document in edit mode. (If you are unable to edit the document, record the settings in the document, and then delete it and create a new one.)
   d. Update these fields if necessary:

      Domino Server Names -- make sure this field contains the name of all of the DWA servers and Sametime servers that should participate in Single Sign-on.

      DNS Domain -- make sure this is the fully-qualified domain name of the DWA and Sametime server.
   e. Click Save & Close.
3. Enable single sign-on and basic authentication in the Server document for the DWA server as described in Enabling single sign-on and basic authentication. When you update the Web SSO Configuration field, select LtpaToken from the list.
4. Ensure that the updates replicate to all of the servers in the domain.

Update Domino Web Access server Web SSO configuration

Complete the steps in this section if your DWA server is already configured for Domino Web SSO. You must add the Sametime server to your configuration:

1. Update your existing Domino Web SSO Configuration document.
   a. Open the Domino Directory and select the Configurations - Web - Web Configurations view.
   b. From within this view, expand the list of Web SSO Configurations.
   c. Open the Domino Web SSO document that you are using for your DWA server in edit mode.
   d. Update these fields if necessary:

      Domino Server Names -- make sure this field contains the name of all of the DWA servers and Sametime servers that should participate in Single Sign-on.

      DNS Domain -- make sure this is the fully-qualified domain name of the Sametime server.
   e. Click save & Close.
2. Update the Server document for the Sametime server.
   a. Open the server document.
   b. Click Internet Protocols - Domino Web Engine, and select the Web SSO Configuration field.
   c. From the drop-down list, select the Web SSO Configuration that you are using for the DWA server.
   d. Click Save & Close.
3. Ensure that the updates replicate to all of the servers in the domain.

Although Domino SSO is the preferred authentication method, you can continue to use secrets and tokens authentication databases, if you are already using them. For example, if any of the servers in your domain is configured for something other than multiple server SSO, (single server SSO for example) you must use secrets and tokens authentication. For information on setting up Secrets and Tokens authentication, see the topic Setting up Secrets and Tokens authentication for instant messaging in Domino Web Access.

Part 6 - (for mixed environments only) Copy the SametimeApplet folder on the Domino Web Access server to the Sametime server

For a mixed environment, in which the users' mail files are based on the INOTES5.NTF mail template, and they are using Domino Web Access Chat, you must copy the SametimeApplet folder from the Domino Web Access server to the same location on the Sametime server. On the Domino Web Access server, the applets are located in the <data directory>\domino\html directory.

Note: Chat is the Domino Web Access feature that provided awareness and allowed people to chat with co-workers in Domino Web Access prior to 6.5.2. To use Chat, you must also lower the value of the instant messaging security setting in the SAMETIME.INI file to allow a connection from an older client. For iNotes5 and iNotes6 mail templates, use VP_SECURITY_LEVEL=20. For more information on specifying the minimum security level, see the *IBM Lotus Sametime 7.0 Installation Guide* (available on http://www.lotus.com/LDD/doc), which details this setting.

Part 7 - Verify that instant messaging works with Domino Web Access

1. Make sure that replication is complete, the Person documents exist on the Sametime server, and that the updated Web SSO document exists on all of the servers that will participate in single sign-on..
2. If you have not already done so, follow the instructions in the *IBM Lotus Sametime 7.0 Installation Guide* to verify that instant messaging is working properly before you test whether it is working with Domino Web Access clients.
3. Launch Domino Web Access in a browser. In any view or document in which online awareness appears, click the Active status icon of the person you want to chat with to test the instant messaging connection.

Note: If the instant messaging status does not appear next to the Welcome *username* text in Domino Web Access, check the user's Person document in the Domino directory. If you configured the Sametime server by populating this document, make sure the ″Sametime server″ field is correct (Basics tab, under Real-Time Collaboration).

Setting up Secrets and Tokens authentication for instant messaging in Domino Web Access

If you want to use Secrets and Tokens authentication databases for your instant messaging security instead of Domino Single Sign-On (SSO) Authentication, you must Create a one-time replica of the Tokens database on the Domino Web Access server. When you do this, remember that file names are case sensitive on UNIX, so the Secrets database name must be entered exactly as STAuthS.nsf.

To replicate STAuthS.nsf from the Sametime server to the Domino server directory:

1. Using a Notes client, choose File - Database - Open.
2. Enter the name of the Sametime server (for example, Sametime/Acme).
3. Enter the Secrets database filename: STAuthS.nsf
4. Click Open.
5. Choose File - Replication - New Replica.
6. Enter the name of the Domino Web Access server (for example, iNotes/Acme)
7. Ensure that the database is replicated to the data directory: ...\domino\data\stauths.nsf.
8. Click OK to create the replica.

Note: After you have replicated stauths.nsf from your Sametime server to your Domino server, open the Replication Settings dialog box for the database, click Other, and check the ″Temporarily disable replication for this replica″ box. This will prevent another version of the database from a Windows system from overwriting your name change (using uppercase and lowercase letters) for the UNIX server.

Setting up Sametime and Domino Web Access in different domains

If you prefer to use Web single sign on (SSO) authentication, see the topic Setting up the Web SSO Configuration document for more than one Domino Domain.

To set up a cross-domain configuration when the Sametime server and the Domino Web Access server are located in different domains:

1. Cross certify both domains with each other.
2. Configure Directory Assistance on the Sametime server.
3. If you have set up single sign on (SSO), go to Step 4. If you do not have SSO set up, replicate STAuthS.nsf to the Domino Web Access Server (file name is case sensitive on UNIX servers).
4. Create a server document for the Sametime server in the Domino Directory of the Domino Web Access server, completing the fields below. Another way to do this is to edit Configuration Settings document, Domino Web Access tab, and enter the Sametime server name in the in the field ″Set an instant messaging server hostname for all DWA users.″ If you use this setting, you do not need to complete Step 5.
   - Server name
   - Domain name
   - Fully qualified Internet host name
   - Is this a Sametime server?
5. Enter the Sametime server name in the Sametime Server field of each Domino Web Access user's Person document.

Note: If the Sametime server is configured using a port other than the default port, then the ″Fully Qualified Hostname″ field must contain hostname:port.

For complete information on working with multiple Sametime servers, see the *IBM Lotus Sametime 7.0 Administrator's Guide*, available on http://www.lotus.com/LDD/doc.

Troubleshooting Sametime in Domino Web Access

If instant messaging icons do not display in Domino Web Access mail and the Contact List, check the following:

- The Sametime server is up running. To make sure stlinks is running normally, you can check the Sametime server directory \trace\stlinks.txt log file.
- All the ST**** services are up running. Check the control panel - services; all ST**** services should be running when the Sametime server has fully started. If there are ST**** services not running, start STCommunity server first. If this service cannot be started, check the network connections and the Sametime server log file.
- Make sure the \stlinks directory and the files are on both the Sametime server and application server directories.
- When you update the level of Sametime by installing a newer release of Sametime or applying a fix pack, it is possible that you will also need to update the stlinks files on your DWA server. Make sure you check the documentation that accompanies the Sametime update.
- If you had previously customized the STLinks files and have recently upgraded either your Sametime server or your Domino Web Access server to a new version of Domino, the customized files may have been replaced. See the topic Customizing STLinks files for tunneling or Reverse Proxy servers.
- Make sure the user has enabled Instant Messaging in Preferences.
- Make sure the user's Person document has been set up with the Sametime server names.
- Use the http:// protocol only for the Sametime server.

To identify the current Sametime server version:

1. Type the following URL: http://<Sametime server hostname>/stcenter.nsf if the Sametime server is running on a Windows platform. To avoid case sensitive issues on other platforms, search for the file under <Sametime server directory>/stcenter.nsf and use the file name case as it shown there.
2. At the bottom of the page, click Administer the Server.
3. Login to Instant Messaging, and then click Help - About Sametime.

Browser Address: The instant messaging integration features rely on the ability of the browser to directly communicate with the Sametime server. This means that the fully-qualified Internet hostname of the Sametime server must be resolvable from the browser (for example, the fully qualified Internet hostname for a Domino server named IM/Acme might be im.acme.com).

Therefore, either DNS must be able to resolve this address or it must be resolved to the proper IP address by some other mechanism (such as editing of the local operating system's hosts file).

Using the Domino Server Setup program

The following procedures describe the ways you can use the Server Setup program.

- Use the Server Setup program on the server you are setting up
- Use the Server Setup program from a client system or from another server
- Create a setup profile by recording your choices during the Server Setup program
- Use a setup profile to set up multiple servers with the same requirements
- Use a setup profile without viewing the setup screens (″silent″ setup)
- Using automatic server setup on Linux on zSeries and on UNIX

Indic language support in the Domino Server Setup program

You can change both the font and the alphabet that displays when you enter text in a field on a Server Setup program screen. Normally, the alphabet that displays is that of the default language.

The Domino Server Setup program supports the following alphabets:

Bengali

Devanagari

Gujarati

Gurmukhi

Kannada

Malayalam

Oriya

Tamil

Telugu

To change the font

Note: Changing the font is required for the Devanagari alphabet, as the default font does not work with it.

1. Start the setup program by starting the Domino server.
2. On the Welcome screen, click Font.
3. Select a font that will work with the alphabet you plan to use.
4. To select an alphabet different from that of the default language, see the following procedure.

To change the alphabet

Changing the alphabet is supported for the Windows, AIX, and Linux operating systems only.

1. Start the setup program by starting the Domino server.
2. Right-mouse click on the title bar of the screen in which you want to enter text that uses an alphabet different than that of the default language.
3. Select ″Select Input Method.″
4. Select the alphabet that you want to use.
5. Enter text in one or more fields on the screen.

Note: Clicking Next to go to the next screen restores the alphabet to that of the default language. Repeat the preceding procedure for each screen on which you want to use a different alphabet.

Using the Domino Server Setup program locally

After installing the Domino server program files on a server, you can run the Domino Server Setup program locally by starting the server. The Server Setup program asks a series of questions and guides you through the setup process. Online Help is available during the process.

Note: During server setup, you can use an existing certifier ID instead of creating a new one. The certifier ID that you specify cannot have multiple passwords assigned to it. Attempting to use a certifier ID with multiple passwords generates an error message and causes server setup to halt.

If you are using Linux on zSeries, you cannot use the Domino Server Setup program locally. You must use the Domino Server Setup program remotely, as described in the next section.

Note: Before running any Domino setup command, be sure to complete any pending reboot actions you may have from installing other applications.

Using the Domino Server Setup program remotely

After you install the program files for a Domino server on a system, you can use either a Windows client system or another Domino server to run the Server Setup program remotely. Running the Server Setup program from a Windows client is easier if the client has Domino Administrator installed -- to run the program from a client without Domino Administrator, you need the Java runtime environment plus some files from the program directory of an installed Domino server.

Note: During server setup, you can use an existing certifier ID instead of creating a new one. The certifier ID that you specify cannot have multiple passwords assigned to it. Attempting to user a certifier ID with multiple passwords generates an error message and causes server setup to halt.

For more information, see the topic ″Entering system commands correctly″ earlier in this chapter.

To run the Server Setup program from a Windows client with Domino Administrator

Note: Before running any Domino setup command, be sure to complete any pending reboot actions you may have from installing other applications.

1. Make sure that you:
   - Selected ″Remote Server Setup″ when you installed Domino Administrator on the client system (on the Windows desktop, choose Start - Programs - Lotus Applications and see if Remote Server Setup appears in the list)
   - Know the host name or network address of the remote system
2. Install the Domino server program files on a server system, but do not run the Domino Server Setup program.
3. At the command prompt on the server system, from the Domino program directory, do one of the following:
   - On a Windows server, enter
     ```
     nserver -listen
     ```
   - On a UNIX server, enter
     ```
     server -listen
     ```
4. On the client system, choose Start - Programs - Lotus Applications - Remote Server Setup.
5. In the Connect to Remote Domino Server dialog box, click Ping to ensure that you can connect to the remote server.
6. Enter the host name or network address of the remote server.
7. Click OK to start the Domino Server Setup program.

To run the Server Setup program from a Windows client without Domino Administrator, or from a UNIX workstation

Note: Before running any Domino setup command, be sure to complete any pending reboot actions you may have from installing other applications.

1. Make sure that you know the host name or network address of the remote system.
2. Install the Domino server program files on a server system, but do not run the Domino Server Setup program.
3. At the command prompt on the server, from the Domino program directory, do one of the following:

- On a UNIX server, enter

  ```
  /lotus/bin/server -listen
  ```

- On a Windows server, enter

  ```
  nserver -listen
  ```

4. On the client system, install the Java runtime environment.
5. Create a temporary directory on the client system. For example, enter the following at the command prompt:
   - On a Windows client:

     ```
     mkdir c:\temp
     ```

   - On a UNIX workstation:

     ```
     mkdir /temp
     ```

6. Do one of the following:
   - From a Windows client, copy the remote setup files CFGDOMSERVER.JAR, JHALL.JAR, and REMOTESETUP.CMD from the server to the directory you created on the client system. These files are in C:\Domino program directory on the server.
   - From a UNIX workstation, copy the remote setup files CFGDOMSERVER.JAR, JHALL.JAR, and REMOTESETUP from the server to the directory you created on the workstation. These files are in */Domino program directory/*lotus/notes/latest/ibmpow/ on an AIX server, */Domino program directory/lotus/notes/latest/zlinux/*on a Linux on zSeries server, */Domino program directory*/lotus/notes/latest/linux/ on a Linux server, and */Domino program directory*/lotus/notes/latest/sunspa/ on a Solaris server.

     Note: Linux on zSeries and z/OS ship tar files on the cd which contain all the files needed for remote server setup.
   - On Linux on zSeries -- ZLINUX_CLIENT.TAR
   - On z/OS -- ZOS_CLIENT.TAR
7. At the command prompt on the client system, from the directory you created, do one of the following:
   - On a Windows client, enter remotesetup.cmd
   - On a UNIX workstation, enter remotesetup
8. In the Connect to Remote Domino Server dialog box, click Ping to ensure that you can connect to the remote server.
9. Enter the host name or network address of the remote server.
10. Click OK to start the Domino Server Setup program.

To run the Server Setup program from another server system

1. Install the Domino server program files on both server systems, but do not run the Domino Server Setup program.
2. Make sure that you know the host name or network address of the remote system.
3. At the command prompt on the local server system, from the Domino program directory, do one of the following:
   - On a Windows server, enter

     ```
     nserver -listen
     ```

   - On a UNIX server, enter

     ```
     server -listen
     ```

4. Do one of the following:
   - On a Windows server, enter

     ```
     nserver -remote
     ```

   - On a UNIX server, enter

```
server -remote
```

Note: For Linux on zSeries and z/OS, set the DISPLAY environment variable so that the setup program is directed to a workstation supporting X-Window.

Tip: Entering nserver -help or server -help displays all parameters available for working with remote server setups.

5. In the Connect to Remote Domino Server dialog box, click Ping to ensure that you can connect to the remote server.
6. Enter the host name or network address of the remote server.
7. Click OK to start the Domino Server Setup program.

Creating a server setup profile

A server setup profile is a file that you use to quickly configure servers. To create a server setup profile, you run the Server Setup program in record mode, either at the server you are setting up or from a Windows client. Creating a server setup profile from a Windows client is easier if the client has Domino Administrator installed -- to create a profile from a client without Domino Administrator, you need the Java runtime environment plus some files from the program directory of an installed Domino server.

For more information, see the topic ″Entering system commands correctly″ earlier in this chapter.

To create a setup profile at a server

1. Install the Domino server program files on the server system, but do not run the Domino Server Setup program.
2. At the command prompt on the server, from the Domino program directory, do one of the following:
   - On a Windows server, enter
     ```
     nserver -record
     ```
   - On a UNIX server, enter
     ```
     server -record
     ```

   Note: For Linux on zSeries and z/OS, set the DISPLAY environment variable so that the setup program is directed to a workstation supporting X-Window.

   Tip: Entering nserver -help or server -help displays the parameters available for working with server setup profiles.
3. Enter a name and description for the profile.
4. Continue through the setup program.

   Domino saves your selections in a file with the name you specified in Step 3. By default this file is created in the Domino program directory.

To create a setup profile from a Windows client with Domino Administrator

1. Make sure that you selected ″Remote Server Setup″ when you installed Domino Administrator on the client system.
2. Install the Domino server program files on the server system, but do not run the Domino Server Setup program.
3. At the command prompt on the client system, from the Notes program directory, enter
   ```
   serversetup -record
   ```
4. Enter a name and description for the profile.
5. Continue through the setup program.

   Domino saves your selections in a file with the name you specified in Step 4 and stores the file in the Notes program directory on the client system.

To create a setup profile from a Windows client without Domino Administrator or from a UNIX workstation

1. Install the Domino server program files on the server system, but do not run the Domino Server Setup program.
2. On the client system, install the Java runtime environment.
3. Create a temporary directory on the client system. For example, enter the following at the command prompt:
   - On a Windows client:
     ```
     mkdir c:\temp
     ```
   - On a UNIX workstation:
     ```
     mkdir /temp
     ```
4. Do one of the following:
   - From a Windows client, copy the remote setup files CFGDOMSERVER.JAR, JHALL.JAR, and REMOTESETUP.CMD from the server to the directory you created on the client system. These files are in C:\Domino program directory on the server.
   - From a UNIX workstation, copy the remote setup files CFGDOMSERVER.JAR, JHALL.JAR, and REMOTESETUP from the server to the directory you created on the workstation. These files are in */Domino program directory*/lotus/notes/latest/ibmpow/ on an AIX server, */Domino program directory/lotus/notes/latest/zlinux/*on a Linux on zSeries server, */Domino program directory*/lotus/notes/latest/linux/ on a Linux server, and */Domino program directory*/lotus/notes/latest/sunspa/ on a Solaris server.

     Note: Linux on zSeries and z/OS ship tar files on the CD that contains the files needed for remote server setup.
   - On Linux on zSeries -- ZLINUX_CLIENT.TAR
   - On z/OS -- ZOS_CLIENT.TAR
5. At the command prompt on the client system, from the directory you created, enter:
   ```
   remotesetup -record
   ```

   Note: For Linux on zSeries and z/OS, Set the DISPLAY environment variable so that the setup program is directed to a workstation supporting X-Window.
6. Enter a name and description for the profile.
7. Continue through the setup program.

   Domino saves your selections in a file with the name you specified in Step 6 and stores the file in the client-system directory that you created in Step 3.

Using a server setup profile

You can use a server setup profile at the server you are setting up or from a client system. Using a server setup profile from a Windows client is easier if the client has Domino Administrator installed -- to use a profile from a Windows or UNIX client without Domino Administrator, you need the Java runtime environment plus some files from the program directory of an installed Domino server.

When you use a setup profile, you choose whether or not to view the setup screens as you run the profile. Running a profile without viewing the screens is sometimes referred to as a ″silent″ setup.

For more information, see the topic ″Entering system commands correctly″ earlier in this chapter.

To use a setup profile at the server

1. Install the Domino server program files on a server system, but do not run the Domino Server Setup program.
2. At the command prompt on the server, from the Domino program directory, do one of the following:

- On a Windows server, enter

  ```
  nserver -playback
  ```

- On a UNIX server, enter

  ```
  server -playback
  ```

  Tip: Entering nserver -help or server -help displays the parameters available for working with server setup profiles.

3. Choose the profile to use. If you don’t see the profile you want in the list, click Browse to locate the directory that contains the profile.
4. To change the existing profile, select ″Modify selected profile.″ Click OK to start the server setup.

To use a setup profile from a Windows client with Domino Administrator

1. Make sure that you selected ″Remote Server Setup″ when you installed Domino Administrator on the client system.
2. Install the Domino server program files on a server system, but do not run the Domino Server Setup program.
3. At the command prompt on the server system, from the Domino program directory, do one of the following:
   - On a Windows server, enter

     ```
     nserver -listen
     ```

   - On a UNIX server, enter

     ```
     server -listen
     ```

4. At the command prompt on the Windows client, from the Notes program directory, enter:

   ```
   serversetup -playback
   ```

5. In the Connect to Remote Domino Server dialog box, click Ping to ensure that you can connect to the server.
6. Enter the host name or network address of the server.
7. Click OK.
8. Choose the profile to use. If you don’t see the profile you want in the list, click Browse to locate the directory that contains the profile.
9. To change the existing profile instead of running it to set up a new server, select ″Modify selected profile.″
10. Click OK to start the server setup.

To use a setup profile from a Windows client without Domino Administrator or from a UNIX workstation

1. Install the Domino server program files on a server system, but do not run the Domino Server Setup program.
2. At the command prompt on the server system, from the Domino program directory, do one of the following:
   - On a Windows server, enter

     ```
     nserver -listen
     ```

   - On a UNIX server, enter

     ```
     server -listen
     ```

3. On the client system, install the Java runtime environment.
4. Create a temporary directory on the client system. For example, enter the following at the command prompt:
   - On a Windows client:

     ```
     mkdir c:\temp
     ```

- On a UNIX workstation:

  ```
  mkdir /temp
  ```

5. Do one of the following:
   - From a Windows client, copy the remote setup files CFGDOMSERVER.JAR, JHALL.JAR, and REMOTESETUP.CMD from the server to the directory you created on the client system. These files are in C:\Domino program directory on the server.
   - From a UNIX workstation, copy the remote setup files CFGDOMSERVER.JAR, JHALL.JAR, and REMOTESETUP from the server to the directory you created on the workstation. These files are in */Domino program directory*/lotus/notes/latest/ibmpow/ on an AIX server, */Domino program directory/lotus/notes/latest/zlinux/*on a Linux on zSeries server, */Domino program directory*/lotus/notes/latest/linux/ on a Linux server, and */Domino program directory*/lotus/notes/latest/sunspa/ on a Solaris server.

     Note: Linux on zSeries and z/OS ship tar files on the CD that contains the files needed for remote server setup.
   - On Linux on zSeries -- ZLINUX_CLIENT.TAR
   - On z/OS -- ZOS_CLIENT.TAR
6. At the command prompt on the client system, from the directory you created, enter:

   ```
   remotesetup -playback
   ```

   Note: For Linux on zSeries and z/OS, set the DISPLAY environment variable so that the setup program is directed to a workstation supporting X-Window.
7. In the Connect to Remote Domino Server dialog box, click Ping to ensure that you can connect to the server.
8. Enter the host name or network address of the server.
9. Click OK.
10. Choose the profile to use. If you don't see the profile you want in the list, click Browse to locate the directory that contains the profile. To change the existing profile, select ″Modify selected profile.″
11. Click OK to start the server setup.

Using silent server setup

A ″silent″ setup is one in which you do not view the setup screens as you run the server setup profile. You can do a silent setup at the server you are setting up or from a client system. Doing a silent setup from a Windows client is easier if the client has Domino Administrator installed -- to do a silent setup from a Windows or UNIX client without Domino Administrator, you need the Java runtime environment plus some files from the program directory of an installed Domino server.

Tip: When doing a silent setup, display a progress bar (Windows) or have percent-complete written to the command line (UNIX) by adding the -pb parameter to the end of the command.

For more information, see the topic ″Entering system commands correctly″ earlier in this chapter.

To do a silent setup at the server

Note: Before running any Domino setup command, be sure to complete any pending reboot actions you may have from installing other applications.

1. Install the Domino server program files on a server system, but do not run the Domino Server Setup program.
2. At the command prompt on the server, from the Domino program directory, do one of the following:
   - On a Windows server, enter

     ```
     nserver -silent c:\myprofile.pds
     ```

- On a UNIX server, enter

  ```
  server -silent  /myprofile.pds
  ```

  where *myprofile* is the name you gave to the profile file.

  Note: If the profile file is not in the root directory, use the profile's full path in the command.

  Tip: Entering nserver -help or server -help displays the parameters available for working with server setup profiles.

3. If the profile uses existing server, certifier, or administrator IDs that require passwords, do the following:
   a. Create a text file that contains the passwords for the existing IDs. The keywords in this are:

      Server=

      AddServer=

      Certifier=

      OUCertifier=

      Administrator=

   b. Add a parameter in the command line for the name of the password file. For example, on Windows enter:

      ```
      nserver -silent c:\myprofile.pds c:\passwd.txt
      ```

4. If this is a partitioned server setup, add the = parameter to the command line to specify the NOTES.INI file in this partition's Domino data directory. For example, on Windows enter:

   ```
   nserver -silent c:\myprofile.pds =c:\lotus\domino\data2\notes.ini
   ```

5. Check the ERRORLOG.TXT file in the Domino data directory to confirm that the setup is complete, or to view any error messages that were generated during setup.

To do a silent setup from a Windows client with Domino Administrator

1. Make sure that you selected ″Remote Server Setup″ when you installed Domino Administrator on the client system.
2. Install the Domino server program files on a server system, but do not run the Domino Server Setup program.
3. At the command prompt on the server system, from the Domino program directory, do one of the following:
   - On a Windows server, enter

     ```
     nserver -listen
     ```

   - On a UNIX server, enter

     ```
     server -listen
     ```

4. At the command prompt on the client system, from the Notes program directory, enter:

   ```
   serversetup -silent c:\myprofile.pds -remote serveraddress
   ```

   Where *myprofile* is the name you gave the setup profile and *serveraddress* is the host name or network address of the server you are setting up.

   Note: If the profile file is not in the root directory, use the profile's full path in the command.

5. If the profile uses existing server, certifier, or administrator IDs that require passwords, do the following:
   a. Create a text file that contains the passwords for the existing IDs. The keywords in this are:

      Server=

      AddServer=

      Certifier=

      OUCertifier=

Administrator=

b. Add a parameter in the command line for the name of the password file. For example, on Windows enter:

```
serversetup -silent c:\myprofile.pds c:\passwd.txt -remote serveraddress
```

6. If this is a partitioned server setup, add the = parameter to the command line to specify the NOTES.INI file in this partition's Domino data directory. For example, on Windows enter:

```
serversetup -silent c:\myprofile.pds -remote serveraddress =c:\lotus\domino\data2\notes.ini
```

7. Check the ERRORLOG.TXT file in the Notes data directory to confirm that the setup is complete, or to view any error messages that were generated during setup.

To do a silent setup from a Windows client without Domino Administrator or from a UNIX workstation

1. Install the Domino server program files on a server system, but do not run the Domino Server Setup program.
2. At the command prompt on the server system, from the Domino program directory, do one of the following:
   - On a Windows server, enter

     ```
     nserver -listen
     ```
   - On a UNIX server, enter

     ```
     server -listen
     ```

   Note: For Linux on zSeries and z/OS, set the DISPLAY environment variable so that the setup program is directed to a workstation supporting X-Window.
3. On the client system, install the Java runtime environment.
4. Create a temporary directory on the client system. For example, enter the following at the command prompt:
   - On a Windows client:

     ```
     mkdir c:\temp
     ```
   - On a UNIX workstation:

     ```
     mkdir /temp
     ```
5. Do one of the following:
   - From a Windows client, copy the remote setup files CFGDOMSERVER.JAR, JHALL.JAR, and REMOTESETUP.CMD from the server to the directory you created on the client system. These files are in C:\Domino program directory on the server.
   - From a UNIX workstation, copy the remote setup files CFGDOMSERVER.JAR, JHALL.JAR, and REMOTESETUP from the server to the directory you created on the workstation. These files are in */Domino program directory*/lotus/notes/latest/ibmpow/ on an AIX server, */Domino program directory/lotus/notes/latest/zlinux/*on a Linux on zSeries server, */Domino program directory*/lotus/notes/latest/linux/ on a Linux server, and */Domino program directory*/lotus/notes/latest/sunspa/ on a Solaris server.

     Note: Linux on zSeries and z/OS ship tar files on the CD that contains the files needed for remote server setup.
   - On Linux on zSeries -- ZLINUX_CLIENT.TAR
   - On z/OS -- ZOS_CLIENT.TAR
6. At the command prompt on the client system, from the Notes program directory, enter:

   ```
   remotesetup -silent c:\myprofile.pds -remote serveraddress
   ```

   Note: For Linux on zSeries and z/OS, set the DISPLAY environment variable so that the setup program is directed to a workstation supporting X-Window.

Where *myprofile* is the name you gave the setup profile and *serveraddress* is the host name or network address of the server you are setting up.

Note: If the profile file is not in the root directory, use the profile's full path in the command.

7. If the profile uses existing server, certifier, or administrator IDs that require passwords, do the following:
   a. Create a text file that contains the passwords for the existing IDs. The keywords in this are:

      Server=

      AddServer=

      Certifier=

      OUCertifier=

      Administrator=

   b. Add a parameter in the command line for the name of the password file. For example, on Windows enter:

      remotesetup -silent *c:\myprofile*.pds c:\*passwd*.txt -remote *serveraddress*
8. If this is a partitioned server setup, add the = parameter to the command line to specify the NOTES.INI file in this partition's Domino data directory. For example, on Windows enter:

```
remotesetup -silent c:\myprofile.pds -remote serveraddress =c:\lotus\domino\data2\notes.ini
```
9. Check the ERRORLOG.TXT file to confirm that the setup is complete, or to view any error messages that were generated during setup.

Using automatic server setup on Linux on zSeries and on UNIX

Automatic server setup is a UNIX and Linux on zSeries feature for single local Domino servers. When automatic server setup is used for new server installations, server setup runs automatically after the server installation is complete. For server upgrades, the server is restarted automatically after the installation is complete.

Automatic server setup does not apply to partitioned servers or to remote servers.

By default, server setup is set to manual so that the server setup does not automatically run for new server installs, and server restart does not automatically run for server upgrades.

You can enable this feature from the script file containing all of the user configuration parameters for UNIX script installation. In the UNIX kit directory, the sample script file is SCRIPT.DAT.

Note: Before running any Domino setup command, be sure to complete any pending reboot actions you may have from installing other applications.

Enabling automatic server setup from the script file

To enable the automatic server setup feature from the script file, complete the following steps.

1. Open your script file.
2. Locate the variable, start_server_setup =

   Note: The default is start_server_setup = 0, which is the manual setting. When the manual setting (0) is active, you must manually initiate the server setup or server restart.
3. Enter one of these values according to when you want automatic setup to run:
   - 0 -- To disable automatic server setup and enable manual setup. You have to manually start the server after a new server installation or restart the server after an upgrade when you use this setting.
   - 1 -- To automatically launch server setup after installation or to automatically restart the server after a server upgrade.

Note: For Linux on zSeries and z/OS, set the DISPLAY environment variable so that the setup program is directed to a workstation supporting X-Window.

When the Install program starts, it asks for the password of the ID that owns the Notes data directory.

- 2 -- To automatically launch server setup in listen mode after installing a new server. You can then connect to the server using the Remote Server Setup tool. To automatically restart the server after installing a server upgrade.

  Note: When the Install program starts on a Linux on zSeries system, the program asks for the password of the ID that owns the Notes data directory.

Enabling automatic server setup from the user interface

To enable the automatic server setup feature from the UNIX or Linux on zSeries user interface, complete the following steps.

1. Locate the option ″Select server setup method.″

   Note: The default is Manual Server Setup. When the manual setting (0) is active, you must manually initiate the server setup or server restart.
2. Press the Spacebar until you see the setting you want to use. You can use one of the following settings:
   - Local Server Setup -- To automatically launch server setup after installation or to automatically restart the server after a server upgrade.

     Note: For Linux on zSeries and z/OS, set the DISPLAY environment variable so that the setup program is directed to a workstation supporting X-Window.

   When the Install program starts, it asks for the password of the ID that owns the Notes data directory.
   - Remote Server Setup -- To automatically launch server setup in listen mode after installing a new server. You can then connect to the server using the Remote Server Setup tool. To automatically restart the server after a server upgrade.

     Note: When the Install program starts on a Linux on zSeries system, the program asks for the password of the ID that owns the Notes data directory.
   - Manual Server Setup -- To disable automatic server setup and enable manual setup. You have to manually start the server after a new server installation or restart the server after an upgrade when you use this setting.
3. Press Tab to accept the setting.

The Certification Log

When you set up the first Domino server in a domain, the Server Setup program creates the Certification Log. If you delete the log, you can recreate it, but be aware that the new log will not contain the information it previously stored.

The Certification log records information related to recertification and name changes. When you add servers and users to Domino, the Certification Log maintains a record of how you registered them. For each registered server and user, the Certification Log stores a document containing the following information:

- Name and license type
- Date of certification and expiration
- Name, license type, and ID number of the certifier ID used to create or recertify the ID

Create a replica of the Certification Log on every server that is a registration server and on every server that stores a Domino Directory that is used for user management -- for example, renaming and recertifying users. If the server whose Domino Directory replica you are using does not have a Certification Log, user-management actions will fail.

Server registration

Before you install and set up additional servers, you must register them. In effect, registering a server adds the server to the system. The server registration process creates a Server document for the server in the Domino Directory and creates a server ID. After registering and installing a server, you use the Server Setup program to obtain a copy of the Domino Directory for the new server and to set up the server to run particular services and tasks -- for example, the HTTP service, the Mail Router, and so on.

The server registration user interface automatically removes leading spaces and trailing spaces from passwords. Passwords cannot begin or end with a space. This also applies to certifier registration and user registration.

Note: When setting up an additional server, obtaining the Domino Directory from the registration server via dialup over a modem is possible for Windows systems only. For other operating systems, the additional server must be on the network in order to communicate with the registration server.

Before you register servers, plan and understand your company's hierarchical name scheme. The name scheme defines which certifier ID to use when you register each new server. In addition, make sure that you have access to each certifier ID, know its password, and have created ID recovery information for it.

If you have decided to use the Domino server-based certification authority (CA), you can register servers without access to the certifier ID file and its password.

For more information on the hierarchical name scheme, see the chapter ″Deploying Domino.″ For information on ID recovery, see the chapter ″Protecting and Managing Notes IDs.″ For more information on using the Domino server-based CA, see the chapter ″Setting Up a Domino Server-based Certification Authority.″

The registration server, which is the server that initially stores changes to documents in the Domino Directory until the Domino Directory replicates with other servers, must be up and running on the network. To register servers from your workstation, you must have access to the registration server and have at least Author access with the Server Creator and Group Modifier roles in the ACL of the Domino Directory.

When you register a server, Domino does the following:

- Creates a server ID for the new server and certifies it with the certifier ID
- Creates a Server document for the new server in the Domino Directory
- Encrypts and attaches the server ID to the Server document and saves the ID on a disk or in a file on the server
- Adds the server name to the LocalDomainServers group in the Domino Directory
- Creates an entry for the new server in the Certification Log (CERTLOG.NSF)

If you have a Domino server-based CA for issuing Internet certificates, you can choose to configure the new server to support SSL connections by providing a server key ring password and the server's host name. Then, Domino does the following:

- The registration process creates a certificate request in the Administration Requests database (ADMIN4.NSF) to be processed by the server's Internet CA
- The registration process creates a ″create SSL key ring″ request in ADMIN4.NSF

- Once you set up and start the new server and the ″create SSL keying″ request has replicated to it, the ″create SSL key ring″ request creates the server key ring file and an ″enable SSL ports″ request for the administration server of the Domino Directory
- The ″enable SSL ports″ request enables all the SSL ports on the new server and creates a ″monitor SSL status″ request for the new server
- The ″monitor SSL status″ request restarts all of the Internet tasks currently running on the new server so that the tasks will accept SSL connections

Note: You must use the Domino Administrator if you want to use this server registration process to configure a new server for SSL.

For more information on these requests, see the appendix ″Administration Process Requests.″

Registering a server

Note: If you have not specified a registration server in Administration Preferences, this server is by default:

- The server specified in the NewUserServer setting in the NOTES.INI file
- The Administration server

1. If you are supplying the certifier ID, make sure that you have access to it and that you know its password.
2. If you are using the Domino Administrator and would like the new server to support SSL, make sure that you have an Internet CA configured.
3. From the Domino Administrator or Web Administrator, click the Configuration tab.
4. From the Tools pane, click Registration - Server.
5. If you are using the Domino Administrator, do the following:
   a. If you are using the CA process, click Server and select a server that includes the Domino Directory that contains the Certificate Authority records, and the copy of the Administration Requests database (ADMIN4.NSF) that will be updated with the request for the new certificate. Then click ″Use the CA Process,″ select a CA-configured certifier from the list, and click OK.
   b. If you are supplying the certifier ID, select the registration server. Then click ″Certifier ID″ and locate the certifier ID file. Click OK, enter the password for the certifier ID, and click OK.
   c. In the Register Servers dialog box, click Continue if you want to apply the current settings to all servers registered in this registration session; otherwise, complete these fields:

Field	Action
Registration Server	Click Registration to specify the registration server.
Certifier	If the certifier ID displayed is NOT the one you want to use for all servers registered in this session, or if you want to use the Domino server-based CA instead of a certifier ID, click Certifier and you return to Step 4.
Public key specification	The public key specification that you use impacts when key rollover is triggered. Key rollover is the process used to update the set of Notes public and private keys that is stored in user and server ID files. Choose one: • Compatible with all releases (630 bits) • Compatible with Release 6 and later (1024 bits) **Note:** For information about the significance of the public key specification and key rollover, see the topic User and server key rollover.
License type	Choose either North American (default) or International. In practice, there is no difference between a North American and an International ID type.

Field	Action
Expiration date	(Optional) To change the expiration date of the Server Certificate, enter the date in *mm-dd-yyyy* format in the Certificate Expiration Date box. The default date is 100 years from the current date, minus allowances for leap years.
Certificate Authority	If you want the server to support SSL, select an Internet CA from the list.

d. Click Continue.

6. If you are using the Web Administrator, do the following:
   a. Select a registration server that includes the Domino Directory that contains the Certificate Authority records, and the copy of the Administration Requests database (ADMIN4.NSF) that will be updated with the request for the new certificate.
   b. Select a CA-configured certifier from the list, and click OK.
7. In the Register New Server(s) dialog box, complete these fields for each server that you want to register:

Field	Action
Server name	Enter the name of the new server.
Server title	Enter the server title, which appears on the Configuration tab in the All Server Documents view and in the Server Title field of the Server document.
Domino domain name	The default domain name is usually the same as the name of the organization certifier ID.
Server administrator name	Enter the name of the person who administers the server.
ID file password	Required if you are going to store the server ID in the Domino Directory. Optional if you store the server ID in a file. The password is case-sensitive and characters you use will depend on the level you set in the Password quality scale.
Password Options	Click Password Options. Specify a password quality scale by choosing the level of complexity for the password. By default, the level is 0, where 16 is the highest. Click OK.
Location for storing server ID	• Select ″In Domino Directory″ to store the server ID in the Domino Directory. • Select ″In File″ to store the server ID file in a file. Then click ″Set ID File,″ select the name and path for the file, and click Save. **Note:** You don't see this field from the Web Administrator, as the server ID is stored in the Domino Directory.

8. (Domino Administrator only) If you chose an Internet CA in the Register Servers dialog box and you want the server to support SSL connections, click Advanced, select ″Enable SSL ports,″ and complete the following fields:
   - Server key ring password -- Enter a password for the server key ring
   - Server host name -- Enter the fully qualified domain name of the server, for example, app01.acme.com
9. Do one:
   - Click the green check box to add the server to the registration queue.
   - Click the red X to clear the fields.
10. The server registration queue displays the servers ready to be registered. To display the settings for a server, select the server name in the queue.
11. Click one:

- New Server -- To clear fields in the Register New Server(s) dialog box
- Register All -- To register all servers in the registration queue
- Register -- To register the highlighted server in the registration queue
- Remove -- To remove the highlighted server from the registration queue
- Done -- To close the Register Server(s) dialog box. Any servers remaining in the registration queue will not be registered.

12. After you register a server, install it and then run the Server Setup program to configure it.

Optional tasks to perform after server setup

After running the Server Setup program, you may want to perform one or more of the following tasks, depending on the needs of your company:

- Create an additional organization certifier ID.
- Create an organizational unit certifier ID.
- Use Internet Site documents to configure Internet protocol server tasks:
  - Enable the Internet Sites view
  - Create an Internet Site document
  - Set up security for Internet Site documents

Creating an additional organization certifier ID

When you set up the first server in a domain, you create an organization certifier. If your hierarchical name scheme calls for having multiple organizations but only one Domino Directory, you must create an additional organization certifier ID.

For more information on organization certifier IDs, see the chapter ″Deploying Domino.″

1. From the Domino Administrator, click the Configuration tab.
2. From the Tools pane, choose Registration - Organization.
3. (Optional) To change the registration server, which is the server that initially stores the Certifier document until the Domino Directory replicates, click Registration Server, select the correct server, and then click OK. If you have not specified a registration server in Administration Preferences, the registration server is by default:
   - The local server, if there is one and it contains a Domino Directory
   - The server specified in the NewUserServer setting in the NOTES.INI file
   - The Administration server
4. (Optional) Click Set ID file to change the location where Domino stores the certifier ID. Be sure to keep the certifier ID file in a secure place so that it is readily accessible to register new servers and users, but safe from misuse. By default, the certifier ID is stored in C:\.
5. Complete these fields:

Field	Action
Organization name	Enter the name of the organization. Enter a name different from the one used on the organization certifier ID created when you set up the first Domino server.
Country code	(Optional) Adding an organizational country or region code for the country or region where the organization’s corporate headquarters are located minimizes the chance that another organization has the same organization name as yours. Enter the country or region code only if you have registered your organization name with a national or international standards body. For multinational companies, you can enter a country or region in which the company has offices, as long as the organization name is registered there.

Field	Action
Certifier password	Enter a case-sensitive password for the certifier. The characters you use for this password depend on the level set in the ″Password quality scale″ field.
Password quality scale	Choose the level of complexity for the password. By default, the level is 8, where 16 is the highest.
Security type	Choose either North American (default) or International. In practice, there is no difference between a North American and an International ID type.
Mail certification requests to (Administrator)	Enter the name of the administrator who handles recertification requests. The name specified here appears in the Certifier document in the Domino Directory. If you are creating a certifier ID for an off-site administrator, enter that administrator's name in this field.
Location	(Optional) Enter text that appears in the Location field of the Certifier document.
Comment	(Optional) Enter text that appears in the Comment field of the Certifier document.

6. Click Register.

Creating an organizational unit certifier ID

You can create up to four levels of organizational unit (OU) certifiers. To create first-level OU certifier IDs, you use the organization certifier ID. To create second-level OU certifier IDs, you use the first-level OU certifier IDs, and so on.

For background information on OU certifier IDs, see the chapter ″Deploying Domino.″

For background information on OU certifier IDs, see the topic ″Certifier IDs and certificates.″

Note: The registration server is the server that initially stores the Certifier document until the Domino Directory replicates. If you have not specified a registration server in Administration Preferences, the registration server is by default:

- The local server if there is one and it contains a Domino Directory
- The server specified in NewUserServer setting of NOTES.INI
- The Administration server

To create an organizational unit certifier ID

1. From the Domino Administrator, click the Configuration tab.
2. From the Tools pane, select Registration - Organizational Unit.
3. (Optional) To change the registration server, click Registration Server, select the correct server, and then click OK.
4. Do one:
   - Select ″Supply certifier ID and password.″ Click Certifier ID, select the certifier ID, click Open, and click OK. Enter the ID password, and click OK.
   - Select ″Use the CA Process″ and then choose a CA certifier from the list.
5. Click OK. If you are supplying the certifier ID, enter its password and click OK.
6. (Optional) To change the registration server, click Registration Server, select the correct server, and then click OK.
7. (Optional) To change which certifier ID to use to register the new certifier ID:
   a. Click Certifier ID.
   b. Select the certifier ID, click Open, and click OK.
   c. Enter the ID password and click OK.

8. (Optional) Click ″Set ID File″ if you want to change the location where Domino stores the certifier ID. Be sure to keep the certifier ID file in a secure place so that it is readily accessible to register new servers and users, but safe from misuse. By default the ID is stored in C:\.
9. Complete these fields:

Field	Action
Organizational Unit	Enter a name for the new organizational unit.
Certifier password	Enter a case-sensitive password for the certifier. The characters you use for this password depend on the level set in the ″Password quality scale″ field.
Password quality scale	Choose the level of complexity for the password. By default, the level is 8, where 16 is the highest.
Security type	Choose either North American (default) or International. In practice, there is no difference between a North American and an International ID type.
Mail certification requests to (Administrator)	Enter the name of the administrator who handles recertification requests. The name specified here appears in the Certifier document in the Domino Directory. If you are creating a certifier ID for an off-site administrator, enter that administrator's name in this field.
Location	(Optional) Enter text that appears in the Location field of the Certifier document.
Comment	(Optional) Enter text that appears in the Comment field of the Certifier document.

10. Click Register.

Internet Site documents

Internet Site documents are used to configure the Internet protocols supported by Domino servers. A separate Internet Site document is created for each protocol -- Web (HTTP), IMAP, POP3, SMTP Inbound, LDAP, and IIOP -- which is then used to provide protocol configuration information for a single server, or for multiple servers in a Domino organization. Specifically, you can create:

- **Web Site documents.** You create a Web site document for each Web site hosted on the Domino server.
- **LDAP Site documents.** You create an LDAP site document for LDAP protocol access to an organization in a directory.
- **IMAP, POP3, and SMTP Site documents.** You create an individual Internet Site document for each mail protocol for which you enter an IP address.
- **IIOP Site documents.** You create an IIOP Site document to enable the Domino IIOP (DIIOP) task on the server. This task allows Domino and the browser client to use the Domino Object Request Broker (ORB) server program.

Internet Site documents make it easier for administrators to configure and manage Internet protocols in their organizations. For example, prior to Domino 6, if you wanted to set up a Web site in your organization, it was necessary to configure each Domino server in the domain with Mapping documents, Web realms, and File Protection documents. If you had virtual servers and virtual hosts, you had to do the same thing for them. In Domino 6, you can configure a Web Site document so that all servers and hosts use it to get configuration information for a Web site, including mapping information, file protection information, and Web realm authentication information.

You must use Internet Site documents if you:

- Want to use Web-based Distributed Authoring and Versioning (WebDAV) on a Domino Web server.
- Have enabled SSL on your server and want to use Certificate Revocation Lists to check the validity of Internet certificates used to authenticate with the server.
- Are using a service provider configuration on your server (see ″For service providers only″ below).

The Domino server is configured to use Internet Site documents if the option ″Load Internet configurations from Server\Internet Sites documents″ is enabled on the Basics tab on Server document. If the option is not enabled, the server defaults to Server document settings to obtain configuration information for Internet protocols.

Internet Site documents are designed to be used as follows:

- For any incoming connection, Internet Site documents, Certifier documents and Global Domain documents are used to determine which organization (certifier) is associated with the target IP address. In the xSP configuration, this is important because the Site document determines the hosted organization. In a non-xSP Domino configuration, all incoming IP addresses usually map to the top level certifier.
- For a specific organization and a specific protocol and a specific server, the Internet Site document is used to determine which authentication controls are to be applied.

When you enter a Host name or IP address in an Internet Site document, you do not gain control over which authentication controls are applied according to the IP address the user connects to. Instead, the first Internet Site document located for the server and the organization is used. As a result, except for Web Site documents, you should have only one Internet Site document for each organization, protocol, and server combination.

For example, do not do the following:

Server A has two IP addresses and you create the following two Internet Site documents for POP3:

- One Internet Site document for one IP address with no SSL allowed
- One Internet Site document for another IP address, with SSL allowed.

The IP address is used to determine the organization and both Internet Site documents apply to the same organization. The first Internet Site document that matches the server and the organization is used, in this case, the Internet Site document that does not allow SSL.

Modifications to Internet Site documents (including the creation of new Site documents) are dynamic. The server or protocol does not need to be restarted after you create a new Site document, or after you modify or delete an existing one. Changes generally take effect minutes after the change is made. The ability to dynamically create, modify, or delete Internet Site documents is especially valuable in service provider environments, so that existing hosted organizations are not interrupted when a new hosted organization is configured.

Internet Site documents are created in the Internet Sites view, which is used to help manage Internet protocol configuration information by listing the configured Internet Site documents for each organization in the domain.

CAUTION:
If you use an Internet site document to configure one Internet protocol on a server, you must also use Internet site documents for all Internet protocols on that server. For example, you cannot set up an LDAP Internet Site document and, on the same server, use the Server document to configure HTTP.

While most protocol settings are configured in Internet Site documents, there are some settings that need to be configured in the Server document to support Internet protocol configurations. These include settings for:

- Enabling and configuring the TCP/IP port.
- Enabling and configuring the SSL port (including redirecting TCP to SSL).
- Accessing the server -- such as who can access the server and how.

For more information on server access settings, see the chapter ″Controlling Access to Domino Servers.″

Setting up Internet Site documents on a Domino server

Do the following to set up basic Internet Site functionality on a Domino server.

1. Create Internet Sites document for the Internet protocols you want to use.
2. Set up security for each Internet Site document.
3. Enable Internet Site documents on the server.

For service providers only

Internet Site documents are required for hosted organizations. These documents control each hosted organization's use of Internet protocols. A hosted organization can only use an Internet protocol if the hosted organization has an Internet site document for that protocol. A shared IP address may be used for all hosted organizations, or unique IP addresses may be set up for each hosted organization. Internet Site documents link IP addresses to the individual hosted organizations for each Internet protocol.

When registering hosted organizations, you have the option to create Internet Site documents during hosted organization registration, or you can choose to create them later.

Service providers need to consider the following when using Internet Site documents:

- Each hosted organization has one Web Site document that can be created during hosted organization registration. You must create this initial Web Site document to activate the HTTP protocol. If you have multiple Web sites, you need one individual Web Site document for each additional Web site for each organization. If the hosted organization supports DOLS, the Web Site document must contain the name of the DSAPI filter file name. For more information, see the topic To configure DOLS on a server that uses Web Site documents in this chapter.
- You must create one mail protocol Site document (IMAP, POP3, or SMTP) for each protocol used by each organization.
- In a hosted environment, Domino IIOP (DIIOP) can use the information in the IIOP Internet site document to define the scope of the Domino Directory used to validate users. With DIIOP, you can use any Java® code running on any server on the network.
- If your configuration has one IP address that is shared by multiple hosted organizations, HTTP, IMAP, LDAP, POP3, and SMTP are the available protocols. For IMAP, LDAP, POP3, and SMTP users, the name provided during authentication must be the user's Internet e-mail address, so that the server knows the organization of which each user is a member. Anonymous access to LDAP is not supported in this configuration.
- To enable SSL for a hosted organization, you must enter the server IP address in the field ″Host names or addresses mapped to this site″ on the Basics tab of the Internet Site document.

Creating an Internet Site document

You can create Internet Site documents for Web, IMAP, POP3, LDAP, SMTP Inbound, and IIOP Internet protocols. You create one document at a time.

To create an Internet Site document:

1. From the Domino Administrator, click Configuration - Web - Internet Sites.
2. Click Add Internet Site, and select the type of Internet Site document to create.

3. Click the Basics tab, and complete these fields:

Field	Action
Descriptive name for this site	(Optional) Enter a name that differentiates this site from all others that you create. This name appears in the Internet Sites view in this format: the type of Internet Site, the descriptive name, and the host name or address. For example: Web Site: MyWebSite (www.acme.com) If you do not enter a name, the default name is the type of Internet Site document with the host name or address appended. For example: POP3 Site: (www.acme.com) **For hosted environments --** The default descriptive name is a combination of the hosted organization name with the type of site document appended. For example, a Domino IIOP site with a hosted organization name of Acme would Acme IIOP Site.
Organization	(Required for all Internet Site documents) Enter the name of the registered organization that hosts the Internet Site document. The name must correspond to the organization's certifier. **Note:** For Web Sites set up in a non-service provider configuration, this name can be any suitable word or phrase.
Use this Web site to handle requests which cannot be mapped to any other Web sites	(Web Site documents only) Choose one: • Yes -- This Web site processes incoming HTTP requests if Domino cannot locate the Web sites that were entered in the ″Host names or addresses mapped to this site″ field. • No (default) -- This Web site does not process incoming HTTP requests for which Domino cannot locate a Web site.
Host names or addresses mapped to this site	(Required for all Internet Site documents) Enter the target host names or IP addresses that trigger a connection's use of this Internet Site document. If the site is set up for SSL, you must specify IP addresses. **For hosted environments --** When creating Domino IIOP Site documents, the first host name IP address that is on this list will be used to advertise DIIOP's service creating diiop_ior.txt. Therefore, it is recommended that each Domino server have its own Internet Site document.
Domino servers that host this site	(Required for all Internet Site documents) Enter the name of one or more Domino servers that host this site. You can use any variation of distinguished name (for example, Server1/Sales/Acme) as well as wildcards (for example, */Acme). The default is (*), which means that all servers in the domain can host this site. If you leave the field blank, the Internet Site will not be loaded on any Domino server.

4. For all Internet Site documents, complete the settings on the Security tab.
5. Some Internet Sites require additional configuration. The table below indicates the Internet Site documents that require additional configuration, and the locations for settings in those documents for enabling additional configuration information unique to those protocols.

Document	Complete
Web Site	• Configuration tab • Domino Web Engine tab
IMAP Site	• Public Folder tab
IIOP Site	• Configuration tab

6. Save and close the document.

Setting up security for Internet Site documents

To set up security for Internet Site documents, you can enable SSL server and client authentication, name-and-password authentication, or anonymous access for Internet and intranet clients.

In order to enable SSL for Internet Sites, you must configure the SSL port on the Server document and set up SSL on the server by obtaining a server certificate and key ring from an Internet certificate authority.

To set up SSL authentication, you must create a server key ring file for each Internet Site document. However, if the Internet site documents are for the same organization, but are created for different protocols, a single server key ring file can be used. Be sure to enter the server key ring file name in the appropriate field on the Security tab of each site document.

If you want to use Certificate Revocation Lists (CRL) for Internet certificate authentication, the server must be using a Domino server-based certification authority for issuing Internet certificates.

To enable SSL for a hosted organization, you must use the server IP address in the field ″Host names or addresses mapped to this site″ on the Basics tab of the Internet Site document.

Note: For Web sites, the common name on the server key ring must match the DNS name to which the IP address in the Web Site document is mapped. The IP address must be stored in the field ″Host name or addresses to map to this site,″ which is located on the Web Site document. If you enable Redirect TCP to SSL in a Web Site document, both the host name and the IP address must be stored in this field.

You should be familiar with SSL authentication, name and password authentication, and anonymous access before completing these steps.

For more information about SSL authentication, see the chapter ″Setting Up SSL on a Domino Server.″

For more information about name-and-password authentication and anonymous access, see the chapter ″Setting Up Name-and-Password Authentication and Anonymous Access on a Domino Server.″

To set up security for Internet Site documents:

Note: In Domino, it is possible to effectively prohibit access to an Internet Site by selecting ″no″ for all authentication options in an Internet Site Document. These options include TCP authentication, SSL authentication, and TCP anonymous access.

1. From the Domino Administrator, click Configuration - Web - Internet Sites.
2. Choose the Internet Site document to modify, and click Edit Document.
3. Click Security, and complete these fields:

Field	Enter
TCP Authentication	

Field	Enter
Anonymous	(Applies to all Internet sites, except IMAP and POP3) Choose one: • Yes -- To allow anonymous access to this site • No -- To prohibit anonymous access
Name & password	Choose one: • Yes -- To require a user to authenticate with the user's name and Internet password to access the site • No -- To not require name and password authentication
Redirect TCP to SSL	(Applies to Web Site only) Choose one: • Yes -- To require clients and servers to use the SSL protocol to access the Web site • No -- To allow clients and servers to use SSL or TCP/IP to access the Web site
SSL Authentication	
Anonymous	(Applies to all Internet sites, except IMAP and POP3) Choose one: • Yes -- To allow users access over the SSL port without authenticating with a name and password • No -- To deny users anonymous access
Name & password	Choose one: • Yes -- To require a user to authenticate with user name and Internet password in order to access this site using SSL • No --To not require a name and password
Client certificate	(Applies to Web Site, IMAP, POP3, and LDAP) Choose one: • Yes -- To require a client certificate for access to this site • No -- To not require a client certificate
SSL Options	
Key file name	Enter the name of the server key ring file.
Protocol version	Choose one: • V2.0 only -- Allows only SSL 2.0 connections. • V3.0 handshake -- Attempts an SSL 3.0 connection. If this fails and the requester detects SSL 2.0, attempts to connect using SSL 2.0. • V3.0 only -- Allows only SSL 3.0 connections. • V3.0 with V2.0 handshake -- Attempts an SSL handshake, which displays relevant error messages. Makes an SSL 3.0 connection if possible. • Negotiated (default) -- Attempts an SSL 3.0 connection. If this fails, attempts to use SSL 2.0. Use this setting unless you are having connection problems caused by incompatible protocol versions.
Accept SSL site certificates	Choose one: • Yes -- To accept the certificate and use SSL , even if the server does not have a certificate in common with the protocol server • No (default) -- To prohibit the acceptance of SSL site certificates for access
Accept expired SSL certificates	Choose one: • Yes -- To allow clients access, even if the client certificate is expired • No -- To prohibit client access using expired SSL certificates

Field	Enter
Check for CRLs	Choose one: • Yes -- To check the certifier's Certificate Revocation List (CRL) for the user certificate you are attempting to validate. If a valid CRL is found and the user certificate is on the list, the user certificate is rejected. • No -- To not use Certificate Revocation Lists
Trust expired CRLs	Choose one: • Yes -- To use expired but otherwise valid Certificate Revocation Lists when attempting to validate user certificates • No -- To reject expired Certificate Revocation Lists
Allow CRL search to fail	Choose one: • Yes -- If the attempt to locate a valid Certificate Revocation List fails, proceed as if ″Check for CRLs″ is set to No. • No -- If a valid Certificate Revocation List for the user certificate is not found, reject the certificate. If ″Trust expired CRLs″ is set to Yes, an expired CRL is valid. If ″Trust expired CRLs″ is set to No, the authentication will fail for every user certificate for which a matching valid CRL is not located.
SSL Security	
SSL ciphers	Click Modify to change the SSL cipher settings for this site document. These settings apply only to SSL v3. SSL v2 ciphers cannot be changed.
Enable SSL V2	Choose Yes to enable SSL v2 for this site document.

4. Save the document.

Enabling Internet Sites on a server

If you enable the use of Internet Sites on a Domino server, the server obtains Internet protocol configuration information from site documents. Comparable configuration settings in the Server document are not used.

If the use of Internet Sites is not enabled, comparable Server document settings are used to obtain protocol configuration information.

You can only use the Internet Sites view for Domino servers. Servers running Domino 5.0x or earlier do not have the option for enabling the Internet Sites view.

Note: Each time you start or restart HTTP, a console message indicates whether the HTTP task is using Internet Sites or the Server document (Web Server Configurations view) to obtain Internet protocol configuration information.

To enable Internet Sites on a server:

1. Open the Server document you want to edit, and click Edit Server.
2. Click the Basics tab.
3. In the Basics section, enable ″Loads Internet configurations from Server/Internet Sites documents.″
4. Save the document.
5. Restart the server.

Note: The HTTP task is backward-compatible with the Web Server Configurations view.

Starting and shutting down the Domino server

Start the Domino server so users can access shared databases and obtain other server services. Do not enter keystrokes or click the mouse while the Domino server is starting or shutting down.

Note: If the server program is running, do not use CTRL+S to stop scrolling the console, because no server services take place until you press a key to continue.

To start the server

Operating system	Action
Windows 2000/2003	Choose Start - Programs - Lotus Applications - Lotus Domino Server.
UNIX	Enter the path for the Domino program directory. For example, if you installed Domino in the /opt directory, enter: /opt/ibm/lotus/bin/server

To shut down the server

Enter either **exit** or **quit** at the console. It may take ten seconds or more for the server to shut down.

Starting Domino as an application or a Windows service

If you have installed Domino as a Windows service, when you start the Domino 7 server, a dialog box appears prompting you to specify whether to start Domino as an application or a Windows service.

1. On the Lotus Domino Server dialog box, choose one:
   - Start Domino as a Windows service -- Starts the Domino server as a Windows service. Domino then runs like any Windows service.
     - If you choose this option without selecting either of the check boxes, the next time you start Domino, this message displays ″Lotus Domino is installed as a Windows service.″ The dialog box does not display again.
     - If you choose this option and you select the ″Always start Domino as a service at system startup,″ Domino always starts as a Windows service and this dialog box no longer appears at start up.

       The ″Don't ask me again″ check box does not apply to the ″Start Domino as a Windows service″ due to the way that Windows services work.
   - Start Domino as a regular application -- Starts the Domino server as any application would be started. This is the traditional method for starting and running the Domino server.
     - If you choose this option without selecting either of the check boxes on the dialog box, the next time Domino starts, you are prompted with this dialog box again.
     - If you choose this option and you select the ″Don't ask me again″ check box, you are not prompted with this dialog box again and Domino always starts as an application.
     - If you choose this option and select the check box ″Always start Domino as a service at system startup″ Domino runs as an application during the current session. The next time you start the server, Domino runs as a Windows service.
2. Optionally, you can also choose neither of the following, one of the following, or both:
   - Always start Domino as a service at system startup -- Select this check box if you want Domino to always start as a Windows service. Once you select this option and click OK, you can not change your selection using this dialog box.
   - Don't ask me again -- Select this check box if you do not want to be prompted again when the Domino server starts. After you select this check box and click OK, you will not be able to reset your selections using this dialog box.
3. Click OK.

When run as a Windows service, Domino runs as any other Windows services runs. Some of the benefits associated with running Domino as a Windows service are listed below.

- If you select ″Automatic″ for starting services, Windows services are started when the system starts.

- Windows services can be controlled via the Windows service manager. The Windows service manager can be used remotely.
- Services continue to run even when you log off the system.

Using instant messaging in the Domino Directory

The Domino Directory is now enabled for instant messaging, meaning that you can conduct an online chat directly from the Domino Directory. The instant messaging Chat feature is available only if you have a Sametime server, and only for Windows versions of IBM Lotus Domino/Notes.

Chats are interactive, real-time text conversations.

From the People document, Group document, and from the Domino Directory itself there is a Chat option in the menu bar. You can perform these instant messaging activities:

- Click Chat and you can choose from the following options:
- Chat with -- Open a chat with the person whose name is currently selected in the open document or directory.
- Add to Instant Contact List -- Add the selected person's name to an instant messaging contact list that you choose.
- Show/Hide Contact List -- Toggles between displaying the names in the contact list and hiding the list.

The Domino Administrator

The Domino Administrator is the administration client for Notes and Domino. You can use the Domino Administrator to perform most administration tasks. You can administer the Domino system using the local Domino Administrator or using the Web Administrator.

Information about the Domino Administrator in this section includes:

- Domino Administrator installation
- Setting up and starting the Domino Administrator
- Selecting a server to administer in the Domino Administrator
- Setting Domino Administrator preferences
- Navigating Domino Administrator
- How administrative tasks are organized on the Domino Administrator tabs

Note: The Domino Administrator client also offers Domino domain monitoring (DDM) which you can use to view the overall status of multiple servers across one or more domains, and then use the information provided by DDM to quickly resolve problems.

For more information about Domino domain monitoring, see the chapter ″Domino Domain Monitoring.″

Installing the Domino Administrator

When you install and set up a Domino server, the Server Setup program does not install the Domino Administrator, which is the administration client. You must run the Domino Administrator client setup to install the Domino Administrator client. There are many ways to set up your Administrator client installation.

Do not install the Domino Administrator on the same system on which you installed the Domino server. Doing so compromises Domino's security and impairs server performance.

For more information on installing the Domino clients, including the Domino Administrator, see the chapter, ″Setting Up and Managing Notes Users.″

Setting up the Domino Administrator

1. Make sure the Domino server is running.
2. Start the Domino Administrator.
3. The first time you start the Domino Administrator, a setup wizard starts. After you answer the questions displayed by the setup wizard, the Domino Administrator client opens automatically.

Starting the Domino Administrator

There are several ways to start Domino Administrator.

1. Make sure the Domino server is running.
2. Do one:
   - From the Windows® control panel, click Start - Programs - Lotus Applications - Lotus Domino Administrator.
   - Click the Domino Administrator icon on the desktop.
   - From the Notes client, click the Domino Administrator bookmark button or choose File - Tools - Server Administration.

Navigating Domino Administrator

The user interface for the Domino Administrator is divided into four panes. Clicking in one pane dynamically updates information in other panes. The following figure shows the user interface for the Domino Administrator.

Server pane

The server pane displays the servers in the domain, grouped in different views. For example, you can view all servers in the domain or view them by clusters or networks. To ″pin″ the server pane open, click the pin icon at the top of the server pane.

Task pane

The tasks pane provides a logical grouping of administration tasks organized by tabs. Each tab includes all the tasks associated with a specific area of administration. For example, to manage the files located on a particular server, select a server and click the Files tab.

Results pane

The appearance of the results pane changes, based on the task you are performing. For example, the results pane may display a list of files, as on the Files tab, or an active display of real-time processes and statistics, as on the Server - Monitoring tab.

Tools pane

The tools pane provides additional functions associated with a selected tab. For example, from the Files tab you can check disk space and perform tasks associated with files.

Window tabs

Use window tabs to switch from one open window to another in the Domino Administrator. Every time you open a database or a document, a new window tab appears beneath the main menu bar.

Domains

You can access the servers in each domain that you administer. Click a domain to open the server pane.

Bookmark bar

The Bookmark bar organizes bookmarks. Each icon on the Bookmark bar (running down the left edge of the Domino Administrator window) opens a bookmark or a list of bookmarks, which can include Web browser bookmarks.

Selecting a server to administer in the Domino Administrator

To administer a server, you select the server from a server list. You can have multiple server lists, each of which is represented by a button. After you select a server, information about that server appears in all the tabs.

Button	Description
Favorites	Lists your ″favorite″ servers -- that is, those you administer most frequently. To add a server to Favorites, choose Administration - Add Server to Favorites, and then specify the name of the server to add.
Domain	Lists all servers in a domain. You can also view servers by hierarchy or by network.

For more information on adding domains, see the topic ″Setting Basics Preferences,″ later in this chapter.

To update a server list

The first time you start the Domino Administrator, the system automatically creates a server list, based on the domains listed in Administration Preferences. If you add new servers to the list, choose Administration - Refresh Server List.

Setting Domino Administration preferences

To customize the Domino Administrator work environment, set any of these administration preferences.

Preference	Description
Basics	• Select domains to administer • Add, edit, or delete domains • Set domain location setting • Select domain directory server • Specify Domino Administrator startup settings • Show Administrator Welcome Page • Refresh Server Bookmarks on Startup
Files	• Customize which columns appear on the Files tab • Change the order in which columns appear • Limit the types of files that the Domino Administrator retrieves
Monitoring	• Configure global settings used to monitor the server • Enable server health statistics and reports
Registration	• Select global settings to use to register users, servers, and certifiers
Statistics	• Select global settings for statistic reporting and charting • Enable statistic alarms while monitoring statistics

Setting Basics preferences

To manage Domino domains, set Basics preferences.

1. From the Domino Administrator, choose File - Preferences - Administration Preferences.

2. In the Basics section, under ″Manage these Domino Domains″ do one:
   - Click New to add a domain, and then continue with Step 3.
   - Click Edit to edit an existing domain, and then continue with Step 3.
   - Click Delete to delete an existing domain
3. Complete these fields:

Field	Action
Domain name	Enter the name of the domain to add, or edit an existing name.
Domino directory servers for this domain	Enter one or more directory servers, separated by commas, or edit the list. For example: Mail-E/East/Acme Mail-W/West/Acme
What location settings do you want to use for this domain?	Choose one: • Do not change location • Change to this location. Specify the location from which you want to manage this domain.

4. Under Domino Administrator Startup Settings, complete these fields:

Field	Action
On startup	Do one: • Choose ″Don’t connect to any server″ • Choose ″Connect to last used server″ • Choose ″Connect to specific server″ and then specify the startup domain and startup server.
Show Administrator Welcome Page	Do one: • Check this box to see the Welcome page each time you start the Domino Administrator. • Uncheck this box if you do not want to see the Welcome page.
Refresh Server Bookmarks on Startup	Do one: • Check this box to update the server’s bookmarks each time you start the Domino Administrator. If you are using Domino and DB2, you check this box because server bookmarks must be up-to-date to allow all of the Domino and DB2 features to work correctly. • Uncheck this box if you do not want to refresh the server’s bookmarks each time you start the Domino Administrator.

5. Click OK, or click Files to continue setting Administration Preferences.

Setting Files preferences

Setting Files preferences, you can customize which columns appear on the Files tab, change the order in which columns display, and limit the types files the Domino Administrator retrieves.

By default, the Files tab displays columns in this order:

- Title
- File Name
- Physical Path

- Files Format
- Size
- Max Size
- Quota
- Warning
- Created
- Last Fixup
- Is Logged
- Template

To set Files preferences

1. From the Domino Administrator, choose File - Preferences - Administration Preferences.
2. Click the Files section.
3. Do one:
   - To add a column, select a column from the Available Columns list and click the right arrow to add it to the ″Use these Columns″ list.
   - To remove a column, select a column from the ″Use these Columns″ list and click the left arrow to remove it from the list.
4. Click the up or down arrows to change the order of the columns in the ″Use these Columns″ list.
5. Check ″Retrieve only (NSF, NTF, BOX) Domino file types (faster)″ to limit the types of files retrieved. Uncheck this box to retrieve all file types.
6. Click OK or click Monitoring to continue setting Administration Preferences.

For more information on setting Files preferences in the Web Administrator, see the topic ″Setting Files Preferences for the Web Administrator″ later in this chapter.

Setting Monitoring preferences

You can use the default Monitoring preferences or customize them.

1. Choose File - Preferences - Administration Preferences.
2. Click Monitoring, and then complete the Global settings for Monitoring:

Field	Action
Do not keep more than <*n*> MB of monitoring data in memory (4 - 99MB)	Enter the maximum amount of virtual memory, in MB, used to store monitoring data. Default is 4.
Not responding status displayed after <*n*> minutes of inactivity	Enter the amount of time after which the ″not responding″ status displays. The default is 10 minutes.
Generate server health statistics and reporting	Select this option to include health statistics in charts and reports. **Note:** You must enable this option to use the Server Health Monitor.

3. In the Location section, complete these fields:

Field	Action
When using this location	Choose the Location document.

Field	Action
Monitor servers	Do one: • Choose ″From this computer″ to monitor servers from the local Domino administration client. • Choose ″From server″ and then click Collection Server. Select the Domino server running the Collector task for the servers being monitored by the location you selected.
Poll server every <*n*> minutes (1-60 minutes)	Enter the server's polling interval, in minutes. • If ″From this computer″ is selected, the default is 1 minute. • If ″From server″ is selected, the default is 5 minutes.
Automatically monitor servers at startup	Select this option to start the Domino Server Monitor when you start the Domino Administrator.

Setting Registration preferences

Within the Domino Administrator, you can set default registration preferences that apply whenever you register new certifiers, servers, and users.

1. From the Domino Administrator, choose File - Preferences - Administration Preferences.
2. Click Registration.
3. Complete any of these fields:

Field	Action
Registration Domain	Select a domain from the list. The registration domain is the domain into which users and servers are registered.
Create Notes IDs for new users	Click to create a Notes ID for each new user during the registration process.
Certifier name list	Choose a certifier ID to use when creating the user name during user registration when a Notes user ID is not being created for the user. This field appears if the check box ″Create a Notes ID for this person″ is not selected. If you are working in a hosted environment and are registering a user to a hosted organization, be sure to register that user with a certifier created for that hosted organization.
Certifier ID	Do one: • Choose ″Certifier ID″ to use the certifier ID and password. Then click Certifier ID, select the certifier ID file, and click OK to select the certifier ID used to register new certifiers, servers, and users. • Choose ″Use CA Process″ to use the Domino server-based certification authority.
Registration Server	Click Registration Server to change the registration server, which is the server that initially stores the Person document until the Domino Directory replicates. Select the server that registers all new users, and then click OK. If you do not explicitly define a registration server, it is, by default: • The local server if it contains a Domino Directory • The server specified in NewUserServer setting in the NOTES.INI file • The administration server
Explicit policy	If you already created explicit policies, select the policy from the list. If you have not created explicit policies, this field displays ″None Available.″
User Setup Profile	Select a profile. The default is none. You can assign either a policy or a user setup profile, but you cannot assign both to the same users.

Field	Action
Mail Options	Click Mail Options to display the Mail Registration Options dialog box. Choose one of the following and complete any required associated fields: • Lotus Notes (default) -- The Internet address is automatically generated. • Other Internet -- The Internet password is set by default during registration. Enter a forwarding e-mail address. • POP -- The Internet address is automatically generated during registration, and the Internet password is set by default during registration. • IMAP -- The Internet address is automatically generated during registration, and the Internet password is set by default during registration. • Other -- Enter a forwarding e-mail address. • None **Note:** If you select Other or Other Internet, you will need to enter a forwarding address for the user during user registration. The forwarding address is the e-mail address to which the user wants their mail sent.
User ID/Password Options	Click User ID/Password Options Settings to open the Person ID File Settings dialog box. Do any of these: • Person ID folder -- Choose a folder or enter a directory path in which to store the ID files generated for this user during registration. • Person password quality -- Set a new password quality for the ID files that are generated for this user during registration. The default for a user ID is 8.
Advanced Options	Click Advanced Options to open the Advanced Person Registration Options dialog box on which you can specify the following: • Whether to keep registered users in the registration queue • Whether to attempt to register users with an error status from a previous registration attempt • Whether to prompt for duplicate files • Whether to search all directories for duplicate names • Other registration settings
Server/Certifier Registration	Click to open the Server Certifier ID File Settings dialog box on which you can define the directories in which to store certifier IDs and server IDs and specify the default password quality setting for each.

4. Click OK.

For more information on explicit policies, see the chapter ″Using Policies.″ For more information on Advanced Options, see Domino Administrator 7 Help.

Setting Statistics preferences

You set statistics preferences to enable statistics reporting and statistics charting. The Statistics section in Administration preferences is also where you specify the polling and reporting time interval used for gathering and reporting statistics.

You also enable statistic alarms for use with statistic event generators. If you create statistics event generators to report alarms, you must enable statistics alarms.

To set statistics preferences

1. From the Domino Administrator, choose File - Preferences - Administration Preferences.
2. Click Statistics.

3. Complete these fields:

Field	Action
Generate statistic reports while monitoring or charting statistics	Do one: • Enable the field and then specify, in minutes, how often to create statistics reports in the Monitoring Results database (STATREP.NSF). Default is 45 minutes. The value must be greater than the monitoring poll interval specified in the Monitoring preferences. • Disable the field if you do not want to create statistics reports or charts.
Check statistic alarms while monitoring or charting statistics	Do one: • Enable the field to report an alarm when a statistic exceeds a threshold. You must enable this field to generate a statistic events. Alarms are reported to the Monitoring Results database (STATREP.NSF). • Disable the field if you do not want to generate alarms.
Chart statistic using same poll interval as monitoring	Do one: • Enable the field to use the poll interval specified in the Monitoring preferences. • Disable the field to set a charting interval that is different than the poll interval. Then specify a time interval in which to chart statistics. The default is 20 seconds.

4. Click OK.

Tools and preferences for debugging in the Domino Administrator

The Domino Administrator client offers several tools and one set of preferences for debugging errors.

From the Domino Administrator, choose Files - Tools and then choose one of these:

- Debug LotusScript -- Enables LotusScript debugging. When a check mark appears to the left of the Debug LotusScript option, LotusScript debugging is enabled. For more information about LotusScript debugging, see the Domino Designer documentation, topic Using the LotusScript Debugger.
- Remote LotusScript Debugger -- Opens the Domino Debugger. The remote debugger allows debugging of LotusScript agents running on remote servers. For more information about remote debugging, see the Domino Designer documentation, topic Using the Remote Debugger.
- Show Java Debug Console -- Opens the Java Debug Console window. For information about the Java Debug Console, see the Domino Designer documentation, topics Writing Java in an agent, Running a Java program, and other related topics.
- Java Debugging Preferences -- Opens the Java Debugging Preferences dialog box. For information, see the topic Enabling Java Debugging.

Enabling Java Debugging

The Domino Administrator supports Java debugging in the following contexts. Each context has its own JVM. Only one user can debug at a time in each context.

- Foreground -- Java code that runs in the Domino Administrator client interactively, for example, an agent triggered from the Actions menu.
- Background -- Java code that runs in the Domino Administrator client under control of the task loader, for example, a locally scheduled agent.

- Web preview -- Java code being previewed in a browser through Domino Designer, for example, an applet on a form.

Java code from a script library runs in the context of the calling code.

To enable and disable Java debugging on the Domino Administrator

Java debugging is disabled by default.

1. From the Domino Administrator, choose Files - Tools - Java Debugging Preferences. The Java Debugging Preferences dialog box appears.
2. Do one or more of these:
   - To enable foreground debugging, click Client Agents/Applets, and then specify a port number to connect the Notes and debugger computers. Deselect to disable.
   - To enable background debugging, click Locally Scheduled Agents, and then specify a port number to connect the Notes and debugger computers. Deselect to disable.
   - To enable Web preview debugging, click HTTP Preview, and then specify a port number to connect the Domino Administrator client and debugger computers. Deselect to disable.

     Note: Specifying a port number may require several attempts before you locate a free port.

If you change the foreground or background preference, the Domino Administrator must be restarted. If you change the Web preview preference, the preview must be restarted.

Domino Administrator tabs

General administration tasks are organized by the tabs described in the following table. Click a tab to display its contents, or use the Administration menu to navigate among the tabs. For example, to move from the Files tab to the Replication tab, choose Administration - Replication.

Tab	Use to administer
People & Groups	People-related Domino Directory items -- such as, Person documents, groups, mail-in databases, and policies
Files	Databases, templates, database links, and all other files in the server's data directory
The Server tabs	Current server activity and tasks. This tab has five sub-tabs: Status, Analysis, Monitoring, Statistics, and Performance.
Messaging	Mail-related information. This tab has two sub-tabs: Mail and Tracking Center.
Replication	Replication schedule, topology, and events
Configuration	All server configuration documents -- such as, the Server, Messaging Settings, Configuration Settings, and Server Connections documents.

People and Groups tab in the Domino Administrator

From the People and Groups tab, you perform these tasks to manage the Domino Directory:

- Register new users and groups
- Manage existing users, groups, mail-in databases, and other resources
- Assign policies to users and groups
- Assign roaming options and Internet settings to users

Files tab in the Domino Administrator

From the Files tab, you perform these tasks to manage database folders and links:

- Access a folder and one or more files inside the folder
- Select the type of files to display -- for example, display only databases or only templates

- Move or copy a database by dragging it onto a Domino server on the bookmark bar
- Manage databases -- for example, compact databases and manage ACLs
- View disk size and free space on the C drive

Server tabs in the Domino Administrator

There are five Server tabs: Status, Analysis, Monitoring, Statistics, and Performance.

Status

From the Status tab, you can:

- See which server tasks are running, stop or restart them, or start new tasks
- See who is connected to the server, including Notes users, browser and e-mail clients
- See which Notes databases are currently in use
- Access the live remote console of the server
- Monitor the schedule of programs, agents, mail routing and replication

Analysis

From the Analysis tab, you can:

- View, search, and analyze the log file (LOG.NSF)
- Access the database catalog on the server
- Access the Monitoring Results database (STATREP.NSF)
- Manage Administration Process requests

Monitoring

From the Monitoring tab, you can:

- Check the status of Domino servers
- Check server availability and sort servers by state or timeline
- View the current status of tasks running on each server and view selected statistics
- Monitor server health status and access server health reports

Statistics

From the Statistics tab, you can see the real-time statistics for the current status of the Domino system.

Performance

From the Performance tab, you can:

- View statistic charts for server performance in real time
- Chart historical server performance over a selected period of time
- Manage server activity trends
- Perform resource load-balancing among servers

Messaging tabs in the Domino Administrator

There are two messaging tabs.

Mail

From the Mail tab, you can:

- Manage the mailboxes on the server
- Check mail
- Manage shared mail
- Monitor the log file for routing-related events
- Run reports on messaging use

Tracking Center

From the Tracking Center tab, you can issue tracking requests to track messages. You must enable the Tracking Center tab in the Web Administrator.

For more information on enabling the Tracking Center for the Web Administration, see the topic ″Message-tracking in the Web Administrator″ later in this chapter.

Replication tab in the Domino Administrator

From the Replication tab, you can:

- View the server replication schedule
- Check the log file for replication events
- View replication topology maps related to the server

Configuration tab in the Domino Administrator

From the Configuration tab, you can configure all server options, settings, and configurations for various subsystem including:

- Security
- Monitoring
- Messaging
- Policies
- Replication
- Directory services
- Off-line services

Domino Administrator tools

Most tabs on the Domino Administrator include a set of tools that change based on the selected tab. For example, the People and Groups tab includes two tools: one for managing people and one for managing groups.

To hide or show the Tools panel, click the triangle. To choose a specific tool, click the triangle to expand or collapse the tools options. Hiding tools on one tab does not hide tools on other tabs.

You can also access tools using:

- Right click -- Select an object that has an associated tool and right click. For example, on the People & Groups tab, right-click a Person document to access the People tools.
- Menus -- For each tab that has tools, the appropriate tools menu appears in the menu bar. For example, when you click the Files tab, the Files menu appears.

The following table describes the tools that are on each tab.

Tab	Tools
People & Groups	• People • Groups
Files	• Disk Space • Folder • Database

Tab	Tools
Server - Status	• Task • User • Ports • Server
Server - Analysis	• Analyze
Messaging	• Messaging
Configuration	• Certification • Registration • Policies • Hosted Org • Server • Miscellaneous

Web Administrator

If you have a browser and want to manage and view settings for a Domino server, you can use the Web Administrator to perform most of the tasks that are available through the Domino Administrator. This section includes the following information about the Domino Web Administrator:

- Setting up the Web Administrator
- Setting up access to the Web Administrator database (WEBADMIN.NSF)
- Giving additional administrators access to the Web Administrator and assigning roles
- Starting the Web Administrator
- Using the Web Administrator

Setting up the Web Administrator

The Web Administrator uses the Web Administrator database (WEBADMIN.NSF). The first time the HTTP task starts on a Web server, Domino automatically creates this database in the Domino data directory. However, you need to make sure that the Web browser and server meet these requirements for the Web Administrator to run.

Web browser requirement

You must use one of these browsers with the Web Administrator:

- Microsoft Explorer 6.0 on Windows 2000 or Windows XP
- Mozilla Browser 1.7.6 on Microsoft Windows XP Professional, Microsoft Windows 2000, IBM AIX, Solaris, Linux REL 3.0 and Novell Linux Desktop 9
- Mozilla Browser on Windows 2000, or on Linux 7.x

For the most current information about supported browsers, see the Release Notes.

Domino server tasks required

You must have the following Domino server tasks running:

- The Administration Process (AdminP) server task must be running on the Web Administrator server.
- The Certificate Authority (CA) process must be running on the Domino 7 server that has the Issued Certificate List database on it to register users or servers.
- The HTTP task must be running on the Web server so that you can use a browser to access it.

To set up the Web Administrator

1. Make sure that the server you want to administer is set up as a Domino Web server and that it is running the HTTP task. The Domino Web server does not have to be a dedicated server, you can use it for other server tasks, such as mail routing and directory services. You can administer only the servers you set up as Domino Web servers.
2. Set up administrator access to the Web Administrator database (WEBADMIN.NSF).

For more information on setting up the Domino Web server, see the chapter ″Setting Up the Domino Web Server.″

Setting up access to the Web Administrator database

Domino automatically sets up default database security when the Web Administrator database (WEBADMIN.NSF) is created for the first time. At that time, all names listed in either the Full Access Administrators or Administrators fields of the Server document are given Manager access with all roles to the Web Administrator database. In addition, the HTTP server task periodically (about every 20 minutes) updates the Web Administrator database ACL with names that have been added to the Server document in either the Full Access Administrators or Administrators fields, but only if the names are not already on the ACL list.

For more information on how the HTTP server task synchronizes names in the Server document with those on the Web Administrator database ACL, see ″Giving additional administrators access to the Web Administrator,″ later in this chapter.

Default database security

The default ACL settings for the Web Administrator database are listed below. You do not need to change these settings if the administrator’s name appears in the Administrators field of the Server document.

Access control list

Default name	**Access level**
User and group names listed in either of these fields on the Server document: • Full Access Administrators • Administrators	Manager with all roles
The name of the server	Manager
-Default-	No access
Anonymous	No access
OtherDomainServers	No access

Authenticating administrators

You can use either an Internet password or an SSL client certificate to access the Web Administrator. The Web Administrator uses either name-and-password or SSL authentication to verify your identity. The method the Web Administrator uses depends on whether you set up the server or the Domino Web Administrator database (WEBADMIN.NSF), or both to require name-and-password or SSL authentication.

To access the Web Administrator database, you must have name-and-password authentication or SSL client authentication set up on the server. Name-and-password authentication is enabled for the HTTP protocol by default.

To use name-and-password authentication, you must have an Internet password in your Person document. To use SSL client authentication, you must have a client certificate, and SSL must be set up on the server.

For more information, see the chapters ″Setting up Name-and-Password and Anonymous Access to Domino Servers,″ ″Setting up Clients for S/MIME and SSL,″ and ″Setting up SSL on a Domino Server.″

Giving additional administrators access to the Web Administrator

You can use the Server document as a convenient way to give additional administrators access to the Web Administrator. To add an administrator to the Web Administrator database (WEBADMIN.NSF) ACL, simply add the name to either the ″Full Access Administrators″ or ″Administrators″ field of the Server document. The HTTP server task routinely synchronizes the names listed in those fields of the Web Server document with those listed on the Web Administration database ACL. Names that are not already listed in the ACL are added with Manager access and all roles. Names that are already listed in the ACL, keep the access granted to them in the ACL. This preserves custom ACL settings, such as limiting the ACL roles of a particular administrator, from being overwritten. It also allows you to restrict administrators from using the Web Administrator, even though they are listed as administrator in the server document. If you delete an administrator’s name from the Server document, the name is also deleted from the Web Administrator database ACL automatically at the next synchronization.

You can also give administrators access to the Web Administrator manually by adding them directly to the Domino Web Administrator database ACL. You can give an administrator full or partial access by restricting the roles assigned. The role assigned to an administrator determines which commands are available to the administrator, and which tabs appear in the Web Administrator client. You cannot restrict roles when you add administrator access to the Web Administrator using the Server document. If you add a name using the server document, you must manually restrict access to the web Administrator through the Domino Web Administrator database ACL. To prevent an administrator from access, assign No access in the ACL.

For more information on Web Administrator roles, see the topic ″Administrator Roles in the Web Administrator″ later in this chapter.

To update access to the Web Administrator database automatically

1. From the Domino Administrator, click the Configuration tab.
2. Select the Server view, and open the Current Server Document for the Web Administration server.
3. Select the Security tab.
4. In one of these fields, enter the name of the administrator to whom you want to give access to the Web Administrator:
   - Full Access Administrators
   - Administrators
5. Click Save & Close

To update the Web Administrator database ACL list manually

You can manually add an administrator to the Web Administrator database ACL list.

1. From the browser using the Web Administrator, click the Files tab.
2. Select the Web Administrator database (WEBADMIN.NSF).
3. From the Tools menu, select Database - Manage ACL.
4. Click Add and add the administrator or group name to the ACL of the Web Administrator database.
5. In the Access field, select Manager.
6. Assign the roles. Assigned roles determine which commands and tabs appear in the Web Administrator.

   Tip: To select more than one role, hold down the Shift or Control key while selecting roles. Selected roles appear highlighted.
7. Do one of the following:

- If the server requires name-and-password authentication, edit each administrator's Person document and enter an Internet password.
- If the server requires SSL client authentication, set up the browser for SSL.

For more information on Managing ACL roles, see the chapter ″Controlling User Access to Domino Databases.″ For more information on SSL authentication, see the chapter ″Setting Up Clients for S/MIME and SSL.

Administrator roles in the Web Administrator

By default, the ACL gives Manager access and all roles to users named in the Administrators and Full Access Administrators fields on the Server document. However, you can restrict a Web administrator's access to parts of the Domino Administrator by limiting the assigned roles. Each role has a corresponding tab and associated commands. When you restrict access, you also restrict which tabs appear in the Web Administrator.

For example, if you assign only the People&Groups role to a Web Administrator, the People & Groups tab is the only tab that appears when that administrator uses the Web Administrator. The following table shows the roles that have been predefined for the Domino Web Administrator.

Role	**Tab**
Files	Files
People&Groups	People & Groups
Replication	Replication
Configuration	Configuration
Mail	Messaging - Mail
MsgTracking	Messaging - Tracking Center
ServerStatus	Server - Status
ServerAnalysis	Server - Analysis
ServerStatistic	Server - Statistic

To restrict a Web administrator's access, use the Manage ACL tool on the Files tab. For more information on managing ACL roles, see the chapter ″Controlling User Access to Domino Databases.″

Starting the Web Administrator

When you start the Web Administrator, it displays the server's administration homepage (information about the server and the administrator using the server). It does not automatically open to a tab, you must choose a tab to begin using the Web Administrator. To return to the server administration homepage at any time, click the top left server icon in the Web Administrator bookmark bar.

To start the Web Administrator

1. Start the HTTP task on the server if it is not already running.
2. From the browser, enter the URL for the Web Administrator database on the server you want to administer. For example, enter:

   ```
   http://yourserver.domain.com/webadmin.nsf
   ```

   Or for SSL, enter:

   ```
   https://yourserver.domain.com/webadmin.nsf
   ```

3. Enter your hierarchical, common name, or short name and your Internet password.
4. Click one of the tabs to being using the Web Administrator.

Using the Web Administrator

The Web Administrator is almost identical to the Domino Administrator with very few exceptions. The user interface looks the same, and most menu options, dialog and information boxes are identical, although the Web Administrator may occasionally display additional information. For example, the Mail tab in the Web Administrator offers additional mail specific statistics -- for example, Mail Routing Schedule, Mail Routing Statistics, and Mail Retrieval Statistics. This information is available in the Domino Administrator; however, it is not displayed the same way.

In addition, there is a new Task tool on the Replication and Mail - Messaging tabs. You can use this tool to issue Tell commands, and to stop, start, and restart replication, router, and messaging tasks.

The Web Administrator includes most of the Domino Administrator functionality. However, the Domino Server Monitor and performance charting are not available in the Web Administrator. And you can restrict further which commands and tabs are available by restricting the roles assigned to an administrator. Information on the availability of specific Web Administrator features and minor changes to how you access a feature are documented throughout the Domino Administrator help documentation.

For the most recent information on using the new Domino Web Administrator, see the Release Notes that shipped with this product or download the Domino Administrator online help from the Lotus Domino Administrator Release 7 download page on the Lotus Developer Domain at http://www.lotus.com/ldd.

Accessing online help

To access online documentation, use the Help button.

Additional buttons

The Domino Web Administrator includes these buttons that appear at to the right of the tabs. These do not appear in the Domino Administrator:

- Sign out -- Use this to log out when you cannot or do not want to close the browser.
- Preferences -- Use this to set Administration preferences.
- Help **--** Use this to access on-line help documents for the Domino Administrator.

The mail bookmark displays in the bookmark area only if you have browsed to your home mail server.

Setting Files preferences for the Web Administrator

You can use the Web Administrator to set Files preferences.

Files preferences

By default, the Files tab in the Domino Administrator displays information about database files in the following order; however, you can customize which columns display in the Web Administrator. The fewer columns you display, the faster the Files panel performs.

- Title
- File Name
- Physical Path
- File Format
- Size
- Space Used
- Max Size
- Quota
- Warning
- Created

- Last Fixup
- Is Logged
- Template Name
- Inherit From
- Type
- Replica ID

To set Files preferences

By default, the Web Administrator displays all columns. You can add or delete columns from the display. Select a column name from the ″Use these Columns″ list and then click Add or Remove.

Registering users and servers with the Web Administrator

To use the Web Administrator to register new Notes users, you must use the Domino server-based certification authority. Any request or task that requires a certifier ID file -- for example, migrate or modify ID -- is not available.

To use the Web Administrator to register users or servers, you must have Registration Authority (RA) access in the server-based certification authority (CA). The server that is running the Web Administrator should also be listed as an RA but that role is not required for the server. If, however, the server is not listed as an RA, the administrator that is an RA must open the Administration Requests database and approve the administration request to register the user. You must assign the RA role in the Domino Administrator, not in the Web Administrator. To assign the RA role, use the Modify Certifier tool on the Configuration panel.

You cannot set registration preferences in the Web Administrator. You must use the registration settings in the CA and in the Registration policy settings document.

In the Web Administrator, you cannot configure a server for SSL during the server registration process.

For more information about modifying certifiers, see the chapter ″Setting up a Domino Server-Based Certification Authority.″ For more information about user registration in the Web Administrator, and about creating and modifying groups, see the chapter ″Setting Up and Managing Notes Users.″ For more information about registering a server, see the chapter ″Installing and Setting Up Domino Servers.″

Managing policies with the Web Administrator

The Policy tools on the Configuration and People & Groups tabs in the Domino Administrator are not available in the Web Administrator. Therefore, from the Web Administrator, you cannot use the Policy Assign tool or the Policy Synopsis tool.

If you create policies before you register users, you can assign them to users and groups during user registration. You can also edit a Notes user's Person document and manually assign an explicit policy by specifying the name of the policy.

Working with policy documents

From the Web Administrator, you can use the Policies view in either the People & Groups or the Configuration tab to add, edit, or delete policy documents. To add or delete policy documents, use the buttons that display in the Results pane. In this view, the names of policy documents are links. To edit one of these documents, click the link for the document you want to edit.

Using the Web Administrator to delete policy documents is not recommended because doing so does not initiate the Administration Process requests required to remove all references to the deleted document from other policy documents.

If you use the Web Administrator to create Setup or Desktop policy settings documents, you cannot add the database links used to set up bookmarks or custom Welcome pages.

For more information about managing policies and policy documents, see the chapter ″Using Policies.″

Using the Web Administrator consoles

The Web Administrator includes two consoles, the Quick Console and the Live Console, which you access from the Server - Status tab. These consoles mirror the server console on the Server Status tab of the Domino Administrator.

Use the Live Console to send commands to a Web server running under a Server Controller. You can send Controller and shell commands, as well as Domino server commands. To use the Live Console, you must install Java Plug-in 1.4 or higher and enable it in your Web browser.

Use the Quick Console to send commands to a Web server that does not run under a Server Controller. Or use it if you are unable to install or use the Java Plug-in in your browser.

For more information on using the console in the Web Administrator to send commands, see the topic ″The Server Controller and the Domino Console,″ later in this chapter and the appendix ″Server Commands.″

Using the Web Administrator with service providers

Service providers may allow administrators at hosted organizations to manage users and groups by allowing remote access through the Web Administrator, with restricted roles. In some cases, the administrator at the service provider site will assume all responsibilities for managing users and groups.

For more information on service providers, see the chapter ″Managing a Hosted Environment.″

Message tracking in the Web Administrator

To use the Web Administrator to trace messages, you must first enable message tracking.

To enable message tracking

1. From the Web Administrator, click the Configuration tab.
2. Open the Messaging view, and select Settings.
3. Click Edit Message Settings.
4. Select the Message Tracking tab.
5. Under Basics, in the Message tracking field, select Enabled. The default is Disabled.
6. Under Access Settings, complete these fields:

Field	Action
Allowed to track messages	Select both of these: • Your name • LocalDomainServers
Allowed to track subjects	Select your name from the list

7. Click Save & Close.

Editing the NOTES.INI file and cleanup script in the Web Administrator

You must be a Full Access Administrator to edit the NOTES.INI file. You must have Administrator access or higher to view the NOTES.INI file, or to edit or view the cleanup script.

For more information on editing the NOTES.INI file, see the appendix ″NOTES.INI File.″

Signing out of the Web Administrator

When you finish using the Web Administrator, close the browser to end the session or click Sign out to end the session and clear your user name and password credentials so that unauthorized users cannot access the browser while the Web Administrator is still running.

The Server Controller and the Domino Console

The Server Controller is a Java® based program that controls a Domino server. Starting the Server Controller starts the Domino server it controls. When a server runs under a Server Controller, you can send operating system commands (shell commands), Controller commands, and Domino server commands to the Server Controller. For example, from a remote console, you can use Controller commands to kill Domino processes on a server that is hung or to start a Domino server that is down.

You can use the Domino Console, a Java-based console, to communicate with a Server Controller. You can run the Domino Console on any platform except Apple Macintosh. Using the Domino Console, you can send commands to multiple servers. The Domino Console doesn't require a Notes ID, only a Domino Internet name and password, so you can connect to servers certified by different certifiers without having multiple Notes IDs or cross-certificates. You can customize output to the Domino Console -- for example, use local event filters to specify the types of events the Console displays. You can also log server output to log files and customize the appearance of the Console.

The Domino Console functions strictly as a server console. Consequently, the Domino Console doesn't include the full set of Domino administration features that are available through the Domino Administrator and the Web Administrator, and you can't use it to open and manage Notes databases.

The files needed to run the Server Controller and to run the Domino Console are provided with Domino and Notes.

You can also use remote consoles in the Domino Administrator and Web Administrator to communicate with a Server Controller.

For information on the available Controller commands and on using the Domino Administrator or Web Administrator to communicate with a Controller, see the appendix "Server Commands."

Starting and stopping the Server Controller

Do the following to start the Server Controller, the Domino server, and the Domino Console:

1. Shut down the Domino server, if it is running.
2. Start the Server Controller using the same command you normally use to start the Domino server but append the argument -jc. For example, if you run a server on Windows XP from the directory c:\lotus\domino using a shortcut icon on the Desktop, use the following target for the shortcut:

   ```
   c:\lotus\domin\nserver.exe -jc
   ```

The Server Controller runs in its own window. You can minimize a Server Controller window, but do not close or kill the window to stop the Server Controller. Instead, use the Controller Quit command from a console to stop a Server Controller and the server it controls.

When you run a Server Controller, you no longer have access to the traditional console at the server. You can communicate only through the Domino Console or a console in the Domino Administrator or Web Administrator.

Optional arguments to use when running the Server Controller

Starting the Server Controller using only the argument -jc starts the Domino Server and the Domino Console along with the Server Controller. There are two optional arguments you can specify to change this default behavior: -c and -s.

Use -c to prevent the Domino Console from running when you start the Server Controller. You might prevent the Console from running on a slow machine or a machine that is low on memory. If you use this argument and the Domino server ID requires a password, the Domino server starts without running its server tasks. To run the server tasks, you must connect to the Server Controller from a console and specify the server password when prompted.

Use -s to prevent the server from running when you start the Server Controller. Use this argument along with -c so that someone who is directly at the server can start only the Server Controller, and then a remote administrator can start the server and specify a required server password remotely from a console.

Example	Result
nserver -jc	Runs the Server Controller, the server, and the Domino Console
nserver -jc -c	Runs the Server Controller and the server
nserver -jc -s	Runs the Server Controller and the Domino Console
nserver -jc -c -s	Runs only the Server Controller

Starting and stopping the Domino Console

You can run the Domino Console from any machine on which a Domino server or the Domino Administrator is installed. To use the Domino Console to communicate with a Domino server, the server must be running under a Server Controller.

To start the Domino Console

1. Make sure that the Domino server or the Domino Administrator is installed on the machine.
2. Run the following command directly from the program directory, or from a directory path that points to the program directory:

   ```
   jconsole
   ```

Note: The Domino Console also starts by default when you start a Server Controller.

For information on using the Domino Console, choose Help - Help Topics from the Domino Console menu.

To stop the Domino Console

1. From the Domino Console, choose File - Exit.
2. If the Console is currently connected to a Server Controller, when you see the prompt ″Exiting the Console by disconnecting all active connections. Do you want to continue?″ do the following:
   a. (Optional) To also stop a Domino server and Domino Server Controller running locally, select the option ″Also, bring down Domino (if running) and quit the local Server Controller - *local server name*.
   b. Click Yes.

Index

Notices

This information was developed for products and services offered in the USA. IBM may not offer the products, services, or features discussed in this document in all countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country/region or send inquiries, in writing, to:

IBM World Trade Asia Corporation Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country/region where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product, and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information that has been exchanged, should contact:

Lotus Software
IBM Software Group
One Rogers Street
Cambridge, MA 02142
USA

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

Trademarks