Notes.net

Notes News Iris Today

Configuring
Sametime servers
in your
Domino Environment

by
Michael
Dempsey

Level: Advanced
Works with: Domino 4.6
Updated: 05/01/2000

This article focuses on the steps to integrate one or more Sametime servers in a Domino environment. It describes the different server installation configurations that are available, and explains in detail the Sametime server configuration used at Lotus and Iris as an example of a deployment that spans different Domino domains to unify several organizations into a single Sametime community.

The information in this article applies to Sametime 1.5, which is the current release at the time this article was published. Note that this article is not a complete installation guide; for that, see the **Sametime 1.5 Installation Guide** and the **Sametime 1.5 Administrator's Guide**.

Sametime in brief
A Sametime server is a real-time collaborative solution comprised of three major sets of services:

- Domino services provide directory, storage, and web server support

- Community services provide online awareness, place-based awareness, private and public instant messaging, and text chat

- Meeting services provide scheduled meetings, instant meetings, application sharing, and whiteboard presentation

Domino provides the foundation for the synchronous collaboration services in Sametime 1.5. Domino is bundled and automatically installed as part of Sametime 1.5, or Domino can be installed separately and then the Sametime 1.5 synchronous collaboration services can be added to a pre-configured Domino server.

Scenario 1: Install a standalone Sametime server
Installing a standalone server is the simplest, quickest way to get a Sametime server installed and running for tests, pilots, or new communities that are established by using self-registration. During configuration, choose "Set up as a server in a Sametime community," as shown in the setup dialog box below:

To complete the configuration of the server, only a few more pieces of information are required -- community name, server name, and administrator information.
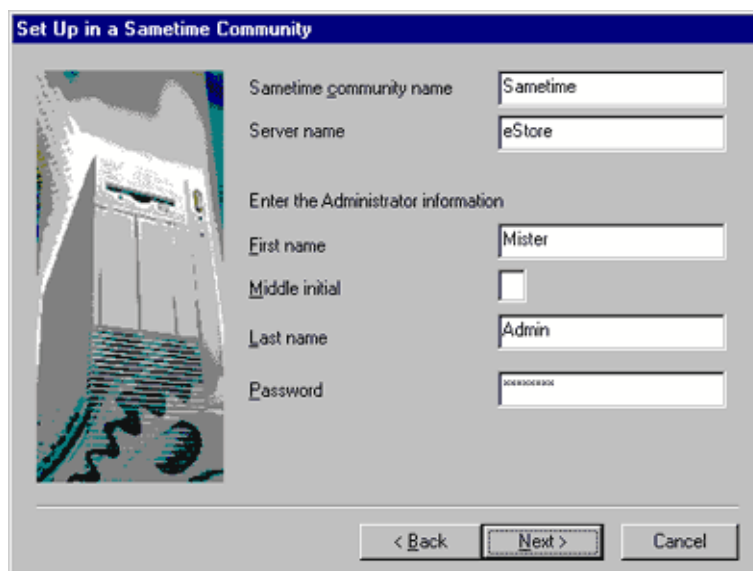
The Domino services of Sametime use the community name as the Domino domain name. In this example, the Domino server name is eStore/Sametime and the DNS name for TCP/IP use is estore.sametime.com.

A certifier ID, server ID, and administrator ID are generated automatically. A Domino Directory (or address book) is created and the administrator is registered in the directory. The Sametime server is configured as a set of NT services that start automatically when the machine is booted. This includes the use of Domino as an NT service, which appears under the service name "Sametime Server."

Once the server is configured and running, the user community is created. This is done by registering users through the use of Sametime Web Administration, importing users into the directory from an external source, or using self-registration. Self-registration is a common technique used for this

environment. Here are specific recommendations to secure your server when using self-registration.

Securing your server for self-registration
1. Remove any ID files from the Domino Directory. Be sure to remove the administrator ID file, which is stored in the person document by default when the server is configured.

2. Set the Domino Directory Access Control List (ACL) to "No Access" for anonymous and default users. This prevents anyone who has not authenticated from accessing the directory.

    The default setting is Reader when the server is configured, which is often acceptable for internal, private sites in order to allow users to read and browse the directory.

3. Check the signature of the agents used in the self-registration database (STREG.NSF). These agents process self-registration requests, such as change password requests, and are responsible for creating entries in the directory as well as modifying these entries. The default signature on the agents is "Sametime Development/Lotus Notes Companion Products."

4. Check that the signature used for the agents in the self-registration database has the proper ACL settings for the Domino Directory. The proper ACL settings are:

    - Access: Author

    - Roles: [Group Creator], [Group Modifier], [User Creator], [User Modifier]

> **Sametime Development/Lotus Notes Companion Products Signature**
> The signature "Sametime Development/Lotus Notes Companion Products" is set with the proper ACL settings for the Domino Directory by default when a standalone Sametime server is configured. Administrators can also sign the self-registration database (STREG.NSF) with another signer, usually the administrator signature or server signature, and give that signer the ACL settings described in step 4 above.
>
> The signature is not automatically added to the ACL list in the Domino Directory when the Sametime server is installed in an existing Domino environment or on a pre-configured Domino server (see these scenarios below). This is because the Domino Directory already exists in these scenarios and the installation of the Sametime server cannot and should not automatically change the security of the directory as part of the installation. Therefore, the administrator is responsible to add any new ACL settings that are required.

Scenario 2: Install a Sametime server as a new server in a Domino domain

Use this scenario when you already have a Domino domain with a directory of users and you have a server machine on which Domino is not already installed.

Before proceeding with this scenario, consider the following information concerning Domino Directory design versions, security, and directory size.

Domino Directory design considerations
Sametime 1.5 uses the Domino Directory design template (PUBNAMES.NTF) that is included with Domino 4.6.5. This design is also compatible with the design included with Domino 5.0.2.

In short, the Domino Directory design of Sametime 1.5 = Domino 4.6.5 = Domino 5.0.2.

This means you can easily integrate a Sametime 1.5 server into a Domino domain that is using a directory design from Domino 4.6.5 or later or Domino 5.0.2 or later.

Note: Because the existing Domino domain already has a directory, the self-registration capability for Sametime is turned off by default.

During installation, the primary directory is pulled from the Domino server to the new Sametime server. The directory is then refreshed with the design (PUBNAMES.NTF) that is delivered with Sametime. This is a time-consuming process for large directories. Installing Sametime on top of a Domino server (described in the next section) is a way to avoid this time-consuming phase of the installation.

Security considerations
Sametime uses agents that require access to the directory for some functions such as creating an online meeting. This means that the signature of the agent must also have rights to access the primary directory. The minimum access required is "Reader." If the default access for the directory is "No Access," then an ACL setting for the signature of the Sametime agents must be added to the primary directory. The default signature for the Sametime product is "Sametime Development/Lotus Notes Companion Products." Some organizations choose to use an administrator's signature or server signature to re-sign databases. Your chosen signature must be added to the ACL of the primary directory with at least "Reader" access. This signature also must be allowed to "run unrestricted Lotuscript/Java agents" on the Sametime server as these agents run on behalf of Sametime users with the rights of the signature. The specific steps needed to configure the Server document for the Sametime server prior to installation are described below.

Another important security issue to review before setting up your Sametime server is workstation security, or the Execution Control List (ECL). Similar to the agents discussed above, the databases and templates delivered with Sametime also have the Sametime Development/Lotus Notes Companion Products signature. The signature determines when Notes client users are warned about unapproved or insecure actions that can occur on their workstations.

Prior to release 5.0.3 of Notes/Domino, Notes client users will receive ECL warnings when they access Sametime databases. To prevent confusing workstation security warnings, review your organization's policies for managing workstation security and ECL lists. Two fundamental approaches are suggested to manage this issue effectively:

1. Update the default administration ECL to include "Sametime Development/Lotus Notes Companion Products" as an approved signature for workstation security.

2. Sign Sametime databases and templates with an administrative signature for the organization that already is an approved signature for workstation security.

With Notes/Domino release 5.0.3 and later, the signature "Sametime Development/Lotus Notes Companion Products" has workstation access rights by default, so these ECL alerts will not appear.

Directory size considerations
Directory Assistance can be used to integrate multiple directories into the

Sametime community. A recently detected scalability limitation means that some large directories (on the order of 10,000 or more users) are not loaded properly when the Sametime 1.5 server is started. The solution is in development now with testing and delivery to follow. A workaround is to replicate the directories that fail to the Sametime server or servers in the community or to use cascaded directories.

Preparing the Domino domain and installing the Sametime server
After considering Domino Directory design versions, security, and directory size, you are ready to prepare the existing Domino domain and install the Sametime server.

1. Register the new Sametime server in your existing Domino domain. This step generates the server ID file and Server document.

    Note: The Sametime server ID file must not use a password. This is because the Sametime services, including the Domino service, are configured to run automatically as background NT services, and the Domino password prompt cannot be handled. The plan is to change this for the next release of Sametime so that the Domino console is run in the foreground by default for this configuration.
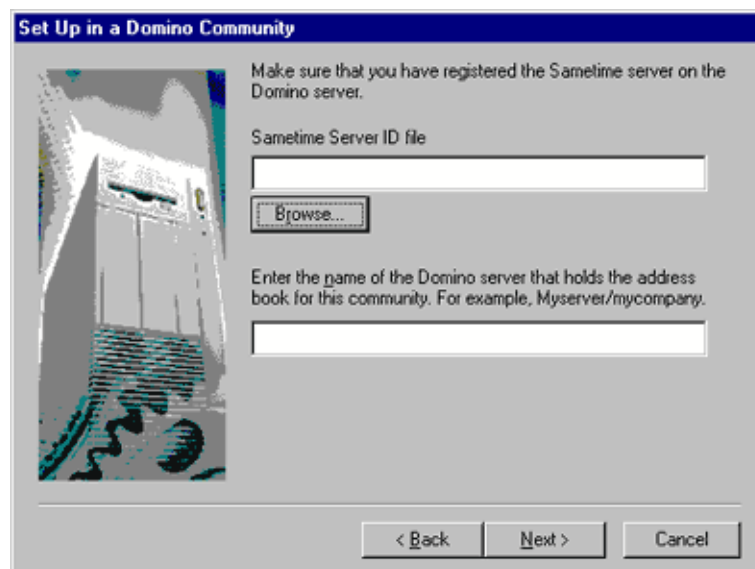
2. Detach the server ID file so that it is available on a diskette or networked drive for the Sametime installation and setup.

3. Set the following fields in the Server document for the new Sametime server:

Tab	Field	Setting
Basics	Is this a Sametime server?	Yes
Security	Run unrestricted Lotuscript/Java agents	Sametime Development/Lotus Notes Companion Products*
*and any other administrators or administrator groups authorized to sign agents		

After you prepare the Domino domain, you can run the Sametime server setup program. Choose to set up the server in an existing Domino domain, as shown below:
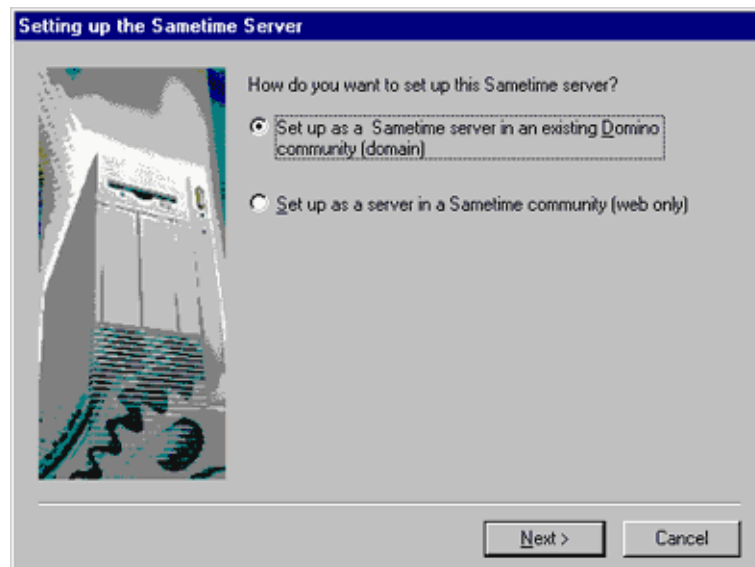
Supply the server ID file and specify the name of the Domino server that contains the primary directory for the domain. The directory must be a replica that contains the Server document for the new Sametime server. This may be a special directory server or administration server, for example. The primary directory will be pulled to the Sametime server in the same way that this is done for any secondary Domino server that is added to a domain.

Set Up in a Domino Community

Make sure that you have registered the Sametime server on the Domino server.

Sametime Server ID file

[   ]

[Browse...]

Enter the name of the Domino server that holds the address book for this community. For example, Myserver/mycompany.

[   ]

[< Back] [Next >] [Cancel]

The configuration is then completed automatically and the Sametime server is ready to use.

Scenario 3: Install Sametime onto an existing Domino server

Use this scenario when you already have a Domino domain with a directory of users and you have an existing Domino server.

Your Domino server must be release 4.6.5, 4.6.6, or 4.6.7 because Sametime 1.5 uses the same directory design included with 4.6.5.or later. Sametime 1.5 does not install on an R5 server -- this capability will be included in the next release of Sametime.

Considerations

The considerations for this configuration are essentially the same as the considerations for installing a Sametime server as a new server in an existing Domino domain, as described in Scenario 2 above. The principle differences are:

- The Sametime installation automatically detects if a Domino 4.6.x server is already installed on the same machine. In this case, only the additional files that comprise the Sametime services are installed and the Domino server installation is not altered. The configuration steps to set up the Domino services are skipped by the Sametime installation.

- The directory design is not automatically refreshed. If a version of Domino earlier than 4.6.5 is used, then the directory design refresh for the Sametime server must be done manually.

- The Sametime add-in task named "staddin" is added to the ServerTasks setting in NOTES.INI. This task launches the Sametime NT services when the Domino server is started and shuts down the Sametime NT

services when the Domino server is stopped.

This scenario is an effective approach to use for environments where Domino is already widely deployed. This approach splits the configuration of the Sametime server into two distinct phases:

1. First, configure the core Domino server capabilities that Sametime depends on.
2. Then, focus on the specific installation and configuration of the Sametime capabilities.

This is the configuration model that is used to deploy new Sametime servers at Lotus. The next section provides more details on the Sametime infrastructure at Lotus and illustrates how Sametime is used in a large organization that is composed of multiple Domino domains and geographically dispersed workgroups.

Case study: Sametime servers at Lotus

This section describes the overall deployment of Sametime at Lotus and its affiliates. Here is a diagram showing the worldwide deployment of Sametime servers:
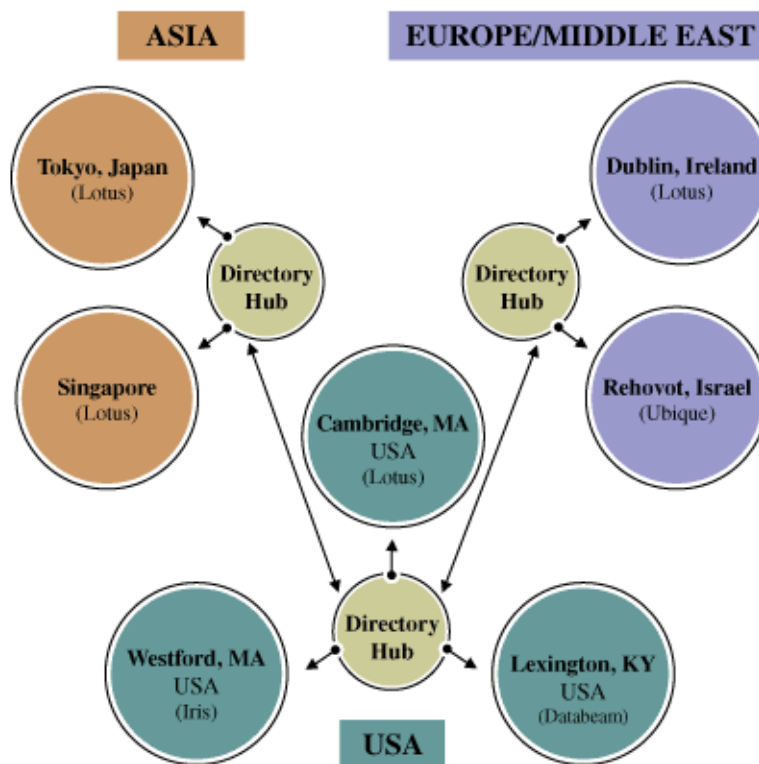
Directory Hubs represent Domino servers that store and replicate the address books for multiple Domino domains, such as Lotus, Iris, and Ubique. The different cities represent one or more Sametime servers in each location

The Sametime deployment at Lotus is expanding on a regular basis as new sites are added and as the number of regular Sametime users continues to increase.

There are four major Domino domains used within Lotus and its affiliated

companies. These domains are:

- Lotus -- This is the primary corporate domain. The Databeam, SoftSwitch, and Edge Research subsidiaries are all part of this domain.

- LotusInt -- This domain is used to manage servers at non-U.S. sites.

- Iris -- This domain is used to manage servers at Iris Associates.

- Ubique -- This domain is used to manage servers at Ubique, Ltd.

While each domain has its own administrators and administration policies, there is much more in common than different.

The set up of a new Sametime server for any domain follows these general steps:

1. Register and install a new Domino server in a domain.
2. Install Sametime 1.5 on the new Domino server to create a full Sametime server.
3. Configure the security for the Sametime server.
4. Configure the support for the "Who Is Online" feature included with Notes mail in releases 5.0.2 and later.
5. Assign users to the new server.
6. Announce and roll-out.

Register and install a new Domino server in the domain
The first set of tasks is to configure a Domino server on which Sametime will be installed.

1. A new Domino server is registered in one of the four domains. This is done from an administration server in the domain.

2. In the Server document for the new server, the field "Is this a Sametime server?" is set to Yes.

3. Also in the Server document the field "Run unrestricted Lotuscript/Java agents" is set with the following values:

   - Sametime Development/Lotus Notes Companion Products (for agents signed by Sametime)

   - The name of the server (for agents that are signed by the server ID)

   - The name of the administrators group for the domain (for agents signed by an administrator of the domain)

4. The Server document field "Directory assistance database name" is set to the file name for the Sametime master address book in each domain, for example, STMAB.NSF.

   As discussed in Scenario 2 above, there is a scalability limitation that affects the use of large directories. To work around this limitation, the Sametime master address book is structured to look for local replicas first and then look for replicas on a directory server. Directories that fail are replicated locally to each Sametime server. This solution allows a smooth transition when a production solution for this problem is deployed.

5. Some servers are configured to use cascaded directories. On these servers, the following settings are made in the NOTES.INI file:

   - NAMES is configured to list the directories for the community. There are four directories for the four domains at Lotus.

   - NOMABFORWEBNAMES is set to 1 to allow web authentication when directory assistance is not used.

6. Domino is then installed on the new server. 4.6.6a is the current version installed for new Sametime servers, while 5.0.2b is used for preliminary

testing of the next version of Sametime for an R5 server.

7. The R5.0.2 directory design is used throughout the Lotus and LotusInt domains. New directory designs and Domino releases are tested in the Iris domain prior to broader deployment throughout Lotus.

This approach makes it easier to upgrade the Domino services and Sametime services separately. A small number of servers are installed as full Sametime servers (such as in Scenario 1 above) so that interoperability and upgrade scenarios are also exercised in the production deployment. These servers run Sametime 1.5, which includes Domino 4.6.3a services.

Install Sametime 1.5 on the new Domino server to create a full Sametime server
Once the Domino infrastructure is in place for the new Sametime server, the Sametime 1.5 software is installed on the newly configued Domino server.

Any necessary updates are then installed. New update downloads are posted on the **Lotus Support** web site with more detailed information about each update. The following updates are installed for all new servers:

- **Directory Service fix** to correct a problem with using multiple directories containing multiple groups of the same name.

- **Meeting Center template** to fix two problems: 1) Web browser hangs when specifying names for the "Restrict to attendees" field of a new online meeting and 2) Dates display incorrectly on the "Unlisted meetings" page.

The Sametime server is operational at this stage. The next set of tasks is to make specific configuration settings for the Lotus community.

Configure security and interoperability
Once the Sametime server is installed, the security settings for using the server are checked. This determines which users can access the server and what capabilities they can use. It also determines how one Sametime server will interoperate with other Sametime servers in the community.

First, the authentication system is reviewed. The system allows users to authenticate with Sametime by verifying their authentication with Domino. Two databases comprise the authentication system for Sametime: Secrets (STAUTHS.NSF) and Tokens (STAUTHT.NSF).

Secrets
One server in the community is designated as the secret generator. For Lotus, this server is based in Cambridge, MA. The SecretGenerator agent is enabled in the Secrets database for this server. This causes a new secret to be created each day. Three days worth of secrets are stored in the database to accommodate authentication across time zones. This Secrets database is then replicated to the other Sametime servers in the community so that authentication is consistent throughout the entire community of Sametime servers.

Tokens
The Tokens database uses a secret in combination with user-specific data to produce an authentication token, which is used to verify that a given Domino user is the same person he or she claims to be when using Sametime. Each Sametime server has its own Tokens database; this database is not replicated between servers. Token documents are created and destroyed as needed to authenticate Sametime users. These documents are transient and exist for very short periods of time. In addition to these transient documents, the Tokens database contains 3 additional documents:

- SametimeServer -- The DNS name of the Sametime server

- SametimeIPAddress -- The DNS name of the Sametime server or the IP address of the Sametime server, if different from the DNS name

- SametimeHTTPPort -- The HTTP port used by Sametime (80 by default)

These documents support connectivity to the Sametime server for Sametime applications that are deployed on a Domino server.

Next, the ACL for the Sametime Online Meeting Center database (STCONF.NSF) is set to "No Access" for anonymous users. This ensures that all online meetings are created and attended only by authenticated users.

The ACL for the Sametime Web Admin database (STADMIN.NSF) is modified to include the domain administrator group. The Sametime administrative roles are also selected. This ensures that the appropriate IT managers and administrators have administrative access to manage the Sametime server.

Finally, Connection documents are created to support the distribution of online meetings to multiple Sametime servers. This is commonly referred to as "invited servers." An online meeting created on one Sametime server can optionally be propagated to additional Sametime servers so that people in different locations can access local Sametime servers to attend the online meeting or so that load balancing for online meetings can be achieved within a location.

The following graphic shows parts of the Basics tab of a Connection document that allows a Sametime server in Cambridge to propagate an online meeting to another Sametime server in Dublin. The topology to support online meetings evolves and is adjusted over time as we learn more about usage patterns and server and network resource usage.

Configure "Who is Online" for Notes mail
The "Who is Online" feature, introduced in Notes release 5.0.2, allows users to see who among those listed in the From, To, and CC fields of the mail

document is using Sametime. The people online are shown in a small
window so that an immediate conversation can be initiated, for example:
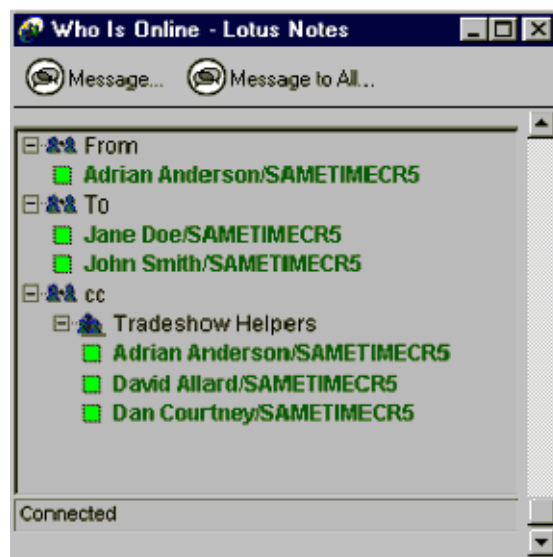
This can streamline the path to solving a problem, planning a meeting, or
clarifying a question. It is also useful for reducing long e-mail threads.

Note: This capability is implemented using an applet that is deployed on the
Sametime server. This applet can also be added to other types of databases
besides mail.

To configure this capability once the Sametime server is installed:

1. Install the template STDOMINO.NTF and the Java applet files vpapi.jar
   and mailapplet.jar on the Sametime server.
2. Create the STDOMINO.NSF database on the Sametime server. This
   database is accessed when a user clicks the Who is Online button in the
   action bar of a mail document.

Assign users to the new server
The final step before announcing and activating the server for use is to
assign specific users to use the new server. This is done by specifying the
new server in the "Sametime server" field of the users' person documents.

This step is not required in order to use the Sametime Connect client, but
when it is specified, it directs the login of Sametime Connect users to the
specified server. This technique is used to support load balancing.

For use of Sametime applications, the Sametime server field is used by
Sametime components in the applications to determine which Sametime
server to use for the person using the application. There are two important
concepts to manage a user's presence and support awareness of online
users:

● A user's presence is registered with only one Sametime server at a time.
  That is, a person can only log in to a single server to use Sametime
  Connect or any Sametime application. The Sametime server field in the
  person document determines the server used for that person's presence.

● A user's presence can originate from only one client machine at a time.
  This is determined by the IP address of the machine the user is using. If
  a Sametime application is used on one machine and the user begins use
  of a Sametime application on a second machine, then the Sametime

application used on the first machine is disconnected. The user's presence is changed to originate from the second machine.

Announce and roll-out
Now the Sametime server is ready for use. Typically an e-mail announcement is sent with instructions that describe the availability of the new server, how to get and install the required Sametime Connect client, and the details of any changes that users must make to use the new server. Support information is provided so that problems can be reported and assigned accurately and efficiently. Individual sites such as Iris post new server updates to a common discussion database that serves to announce items of interest and importance to the entire site. The exact type of announcement varies according to the scope and magnitude of the roll-out.

Lessons
Sametime has become indispensable to a large number of individuals, groups, and locations throughout Lotus. This is dramatically evident for those people who must coordinate and communicate with others at remote sites or within a single office complex but not situated close by.

Sametime is more slowly adopted in small co-located teams who primarily work with each other on a daily basis. Although this scenario is true for some project teams, most projects require significant interaction and coordination with a wide variety of disciplines both within a project team and across project teams.

The blending of asychronous collaboration tools such as e-mail and discussion databases combined with synchronous collaboration tools such as instant messaging, chat, application sharing, and online meetings provides a powerful and compelling combination. This is a focus of new solutions that are being built to meet the desires and demands of both internal users at Lotus as well as the broad and growing range of Sametime customers.

ABOUT MICHAEL
Michael Dempsey is development manager for the Sametime team at Iris in Westford, Massachusetts. The Iris team works closely with the development teams at Databeam in Lexington, KY and Ubique in Rehovot, Israel, using Lotus Sametime to produce Lotus Sametime.