**Lotus** software

**IBM**

# Redbooks Paper

Mario Gereci
William Tworek

# Integrating IBM Lotus Workplace with IBM Lotus Instant Messaging and Web conferencing (Sametime)

This IBM® Redpaper covers the technology and techniques for integrating instant messaging and awareness between a IBM Lotus® Workplace™ environment and a IBM Lotus Instant Messaging and Web Conferencing (Sametime®) environment. Such integration efforts are needed because each of these environments uses a different infrastructure to support its presence and instant messaging functionality. For example, the Lotus Instant Messaging and Web Conferencing server uses an infrastructure based on the proprietary IBM Lotus Virtual Places (VP) protocol while the Lotus Workplace server uses an infrastructure based on the open standard Session Initiation Protocol (SIP).

To support the seamless integration of these two environments and technologies, IBM has developed and released the Lotus Instant Messaging (LIM) Gateway. This software-based gateway is basically an intermediary, or translator, between the two separate IBM instant messaging environments. This Redpaper provides an understanding of this gateway technology, including a review of usage scenarios, installation guidelines, and troubleshooting techniques.

**ibm.com**/redbooks    **1**

**Note:** It is assumed that any readers of this Redpaper will already have a certain level of knowledge and familiarity with the Lotus Instant Messaging and Web Conferencing (and Lotus Workplace) products and technologies. Readers not yet familiar with these core technologies should reference the following Redbooks/Redpapers for information about these core products prior to continuing with this Redpaper:

*IBM Lotus Workplace Team Collaboration 2.0.1*

http://www.redbooks.ibm.com/Redbooks.nsf/RedbookAbstracts/redp3929.html

*Lotus Domino 6.5.1 and Extended Products Integration Guide*

http://www.redbooks.ibm.com/Redbooks.nsf/RedbookAbstracts/sg246357.html

**Note:** For the remainder of this Redpaper, the IBM Lotus Instant Messaging and Web Conferencing (Sametime) product is abbreviated as LIMWC and the IBM Lotus Workplace product is abbreviated as LWP.

# Introduction to the LIM Gateway

As described in the introduction of this Redpaper, the Lotus Instant Messaging (LIM) Gateway is a software-based gateway that supports a seamless integration between the two IBM Lotus instant messaging technologies. It basically acts as a "proxy," passing messages and awareness between the two separate environments without the knowledge of the end user that two separate environments are actually involved.

Figure 1 on page 4 highlights the seamless integration provided by this gateway technology. It shows a LIMWC (for example Sametime) and a LWP user chatting, both using the native interfaces of their specific product, and both unaware that the other user is not using the same product. In this particular example, a user named Marco Foellmer is using the Sametime Java™ Connect client and is connecting to a Lotus Instant Messaging server, while a user name Mario Gereci is using the Web browser based interface to the Lotus Workplace server.
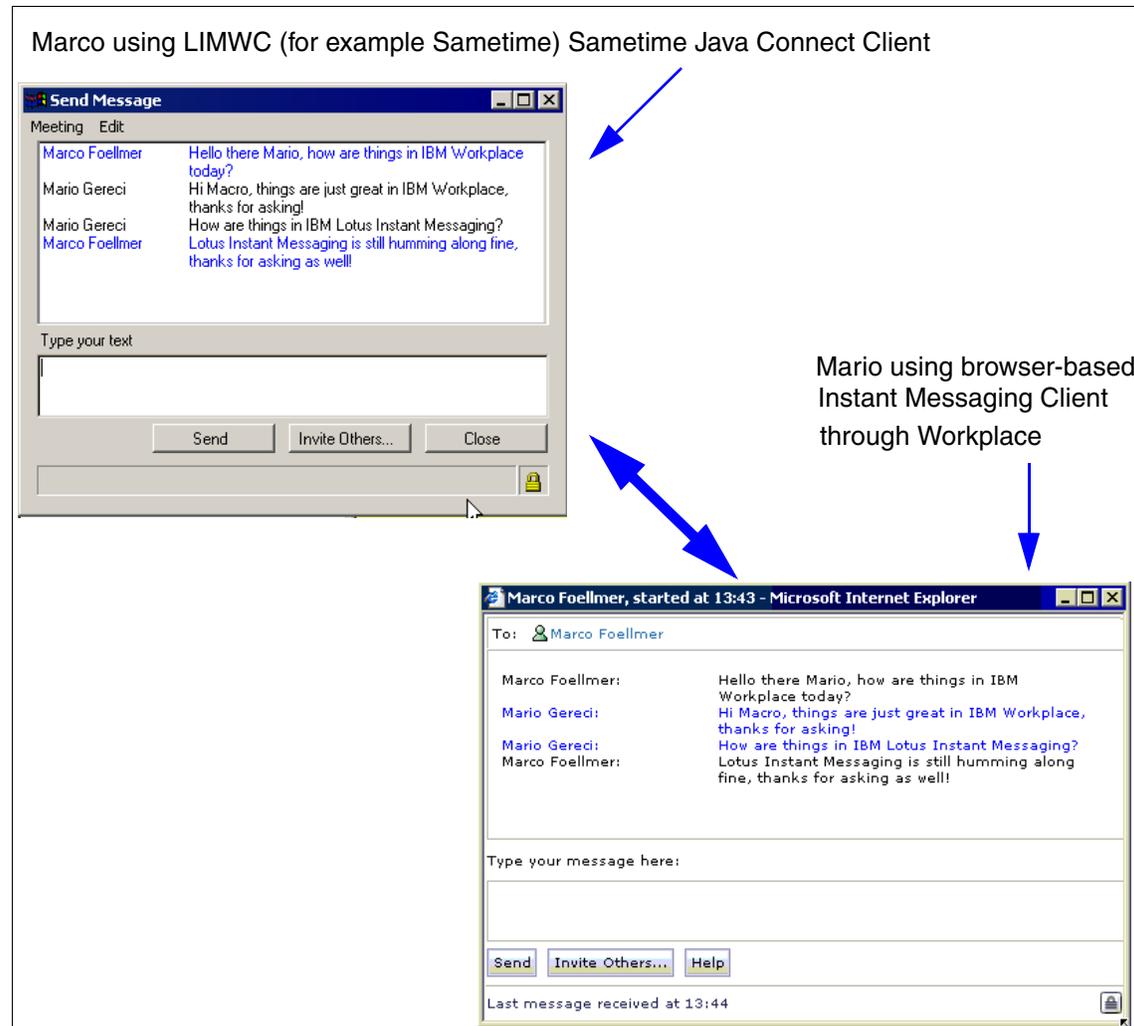
Marco using LIMWC (for example Sametime) Sametime Java Connect Client

Mario using browser-based Instant Messaging Client through Workplace



*Figure 1   LIMWC and LWP users seamlessly chatting*

This seamless integration can be demonstrated further in terms of the integration of basic presence awareness, as shown in Figure 2 on page 5. This figure shows the same users' buddylists within the native product interfaces, highlighting the fact that the presence awareness of other users *looks the same to both users*. In this example, the user Markus Adolph is a Lotus Workplace user who has currently set a "Do not disturb" status, and this awareness status shows correctly in both the LIMWC and LWP environments/technologies, even though Markus is a LWP-only user.
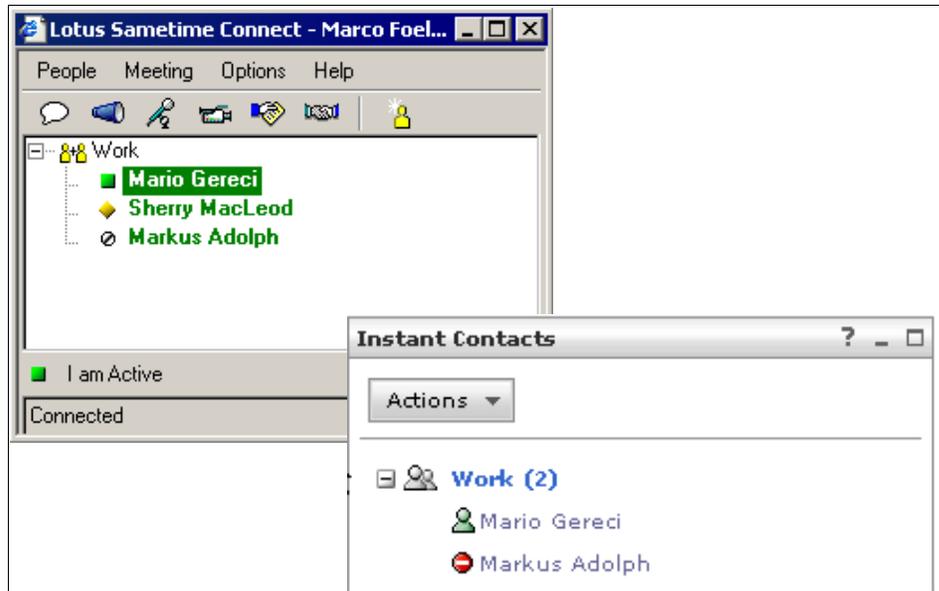
*Figure 2   LIMWC and LWP users with seamless presence awareness*

## LIM functionality

While the LIM Gateway provides a seamless experience for end users, it is important to clarify the functionality that is supported by this gateway in such a seamless fashion.

In general, users who communicate with the other environment through the LIM Gateway can use regular instant messaging and presence client features to engage in the activities listed below:

► One-to-one chat

A user in one environment can engage a single user from the other environment in a one-on-one chat session.

► Add an individual user or a public group to a buddy list

Users can add an individual user or group of users to buddy lists, regardless of which environment the user primarily works in.

► Change presence status (I am active, I am away, Do not disturb)

When a user changes his presence status on a client connected to a server in one environment, this change is also reflected in the buddy lists of clients connected to a server in the other environment.

► Alert me when

A user in the LIMWC environment can use an "Alert me when" client feature to receive alerts when a user in the LWP environment comes online. Note that LWP clients do not have an "Alert me when" feature at this time.

► Auto away

Users in both environments can use client features that change a user's status to Away after a specified period of keyboard and mouse inactivity on the user's local computer. When the user's status changes, the gateway detects the change and communicates the new status to the other environment.

Any client functionality not included in the list above is not supported by the LIM Gateway. Specific features which are *not* supported by the LIM Gateway are as follow.

► Nway chats

Chats between more than one user are not supported by the LIM Gateway. If a user in one of the two instant messaging environments uses the *Invite others* button to invite multiple users to an nway chat, any users within the other proxied environment will not receive the invitation.

► Buddylists

If a user operates clients in both the LIMWC environment and the LWP environment, the buddy list changes a user makes in one environment are not reflected in the other environment. Users must manage buddy lists independently in the two environments. This is due to the fact that Buddy lists are stored on the respective servers and are maintained independently in each environment. The LIM Gateway does not synchronize these lists between the environments.

► Instant meetings

A user in one environment cannot start an instant whiteboard or application sharing meeting with a user in the other environment. The LIM Gateway does not support the integration of meeting capabilities.

► AOL instant messaging

The Sametime Connect 3.1 "client" provides support for external AOL user communities at a client level. Since this is purely a client feature in LIMWC, the external AOL community support does not extend to the LWP environment through the LIM Gateway.

# How the LIM Gateway works

Now that we have explained the end user experience to use the LIM Gateway, it is important to define how the LIM Gateway works behind the scenes.

At a high level, once it is installed and configured, the LIM Gateway performs four basic functions to enable instant messaging and presence communications between the LIMWC environment and the LWP environment:

1. Monitoring client logins to one environment and logging users into the other environment

2. Monitoring the client logouts in one environment and logging users out of the other environment

3. Detecting changes in a user's presence status and reflecting those changes via the "proxied" user logged into the other environment

4. Handling instant messages that are sent between users in the two environments

However, the difficulties are always in the details, so one must examine specifics of how the LIM Gateway interacts with both LIMWC and LWP users and environments to truly understand its operations.

## How the LIM Gateway works with LIMWC users

To enable LIMWC users to communicate with LWP users, the LIM Gateway logs LIMWC users into the LWP environment and transmits presence status information and instant messages from those users into the LWP environment.

To optimize performance and scalability, the LIM Gateway does not automatically log every online LIMWC user into the LWP server. The LIM Gateway logs an LIMWC user into the LWP server only if an LWP user has "subscribed on" the LIMWC user.

An LWP user "subscribes on" an LIMWC user in either of these scenarios:

1. The LWP user adds the LIMWC user to a buddy list in an LWP instant messaging client.

2. An LIMWC user initiates a chat session by sending an instant message to an LWP user. In this scenario, the chat window that opens on the LWP user's computer programmatically subscribes on the LIMWC user. The chat window subscribes on the LIMWC user even if no LWP users have added the LIMWC user to a buddy list.

The following steps summarize the operations that occur to log LIMWC users into the LWP environment:

1. When the LIM Gateway starts, it connects to servers in both the LIMWC and LWP environments (Figure 3 on page 8, No.1).

2. An LWP server sends the LIM Gateway lists of all LIMWC users and groups that are subscribed on by all LWP users (Figure 3 on page 8, No.2).

3. The LIM Gateway then sends SIP register requests to an LWP server to register the subscribed on LIMWC users into the LWP environment (Figure 3 on page 8, No.3).

After registering an LIMWC user into the LWP environment, the LIM Gateway performs the following activities *on behalf* of the LIMWC user:

► Detects the LIMWC user's presence status (for example, "I am active" or "I am away") on the LIMWC server and communicates the user's presence status to the LWP environment. If an LIMWC user changes presence status, the LIM Gateway detects this status change on the LIMWC server and transmits this change to the LWP server. The LWP server notifies the interested LWP users of this status change (Figure 3 on page 8, No.4+5).

► Handles instant messages sent from the LIMWC user to an LWP user. When an LIMWC user sends an instant message to an LWP user, the message is sent from the LIMWC client to the LIM Gateway and transmitted from the LIM Gateway to the LWP server. The LWP server transmits the message to the LWP user.

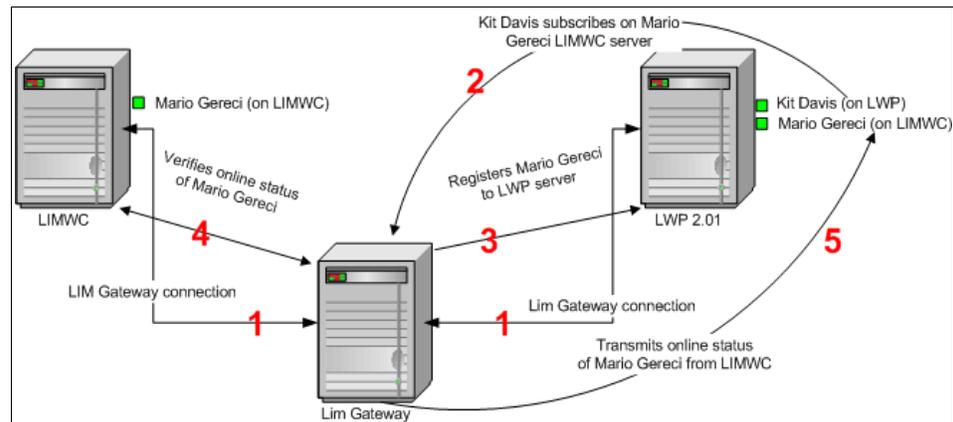► Detects the user logouts on the LIMWC server and logs the users out of the LWP environment.



*Figure 3   How the LIM Gateway works with LIMWC users*

## How the LIM Gateway works with LWP users

To enable LWP users to communicate with LIMWC users, the LIM Gateway logs the LWP users into the LIMWC environment. After logging LWP users into the

LIMWC environment, the LIM Gateway transmits presence status information and instant messages from those users into the LIMWC environment.

It is important to note that because the LIMWC server has a larger user-handling capacity than the LWP server's current capabilities, the LIM Gateway logs *all* online LWP instant messaging and presence users into the LIMWC server.

The steps below summarize the operations that occur to log LWP users into the LIMWC environment:

1. When the LIM Gateway starts, it connects to servers in both the LIMWC and LWP environments (Figure 4 on page 10, No.1).

2. The LWP server notifies the LIM Gateway each time an LWP user logs in. (Figure 4 on page 10, No.2)

3. The LIM Gateway logs the LWP user into the LIMWC server (Figure 4 on page 10, No.3 ).

After logging an LWP user into the LIMWC environment, the LIM Gateway performs the following activities on behalf of the LWP user:

1. Detects the LWP user's presence status and communicates the user's presence status to the LIMWC environment. If an LWP user changes presence status, the LIM Gateway detects this status change on the LWP server and transmits this change to the LIMWC server. The LIMWC server notifies the interested users of this change (Figure 4 on page 10 No.4 and 5 ).

2. Handles instant messages sent from an LWP user to a user in the LIMWC environment. These messages are sent from the LWP user to the LIM Gateway and transmitted from the LIM Gateway to an LIMWC server. The LIMWC server transmits the message to the LIMWC user.

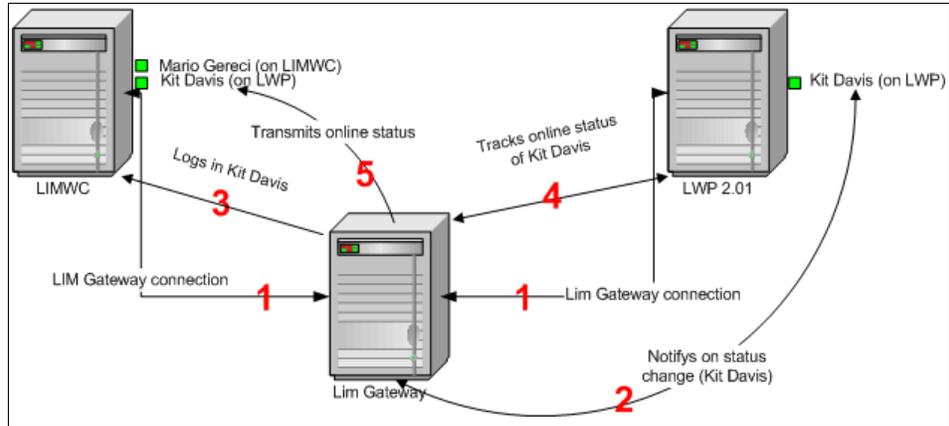3. Detects the user logouts on the LWP server and logs the users out of the LIMWC environment.

*Figure 4   How the LIM Gateway works with LWP users*

## LIM usage scenarios

At this point, we have explained what the LIM Gateway is, how it interacts with the end user, and how it interacts with LIMWC and LWP environments. To complete the picture, it is important to discuss the various scenarios in which the LIM Gateway might be used.

There are two main ways in which the LIM Gateway can be utilized:

► Integration of separate LIMWC and LWP environments

This scenario involves separate Lotus Instant Messaging and Web Conferencing, and Lotus Workplace environments, where there are no immediate plans for the sunset of one environment or the other. This scenario may be applicable toward two divisions within a company that have each made a different technology decision, or may even be applicable for two companies in the process of merging. The important consideration in this scenario would be to ensure that adequate directory integration exists between the two environments to allow the LIM Gateway to function properly. This directory integration concern is highlighted in "Directory considerations" on page 17.

► Migration of a LIMWC environment to LWP

The more typical usage of the LIM Gateway will involve the migration of an existing LIMWC environment to a newer LWP environment. In this scenario, the LIM Gateway is deployed only for the time that both environments exist. The LIM Gateway allows users in both environments to continue to use instant messaging without any knowledge of the migration. Once all LIMWC users have been migrated onto the newer LWP platform, the LIMWC environment can be sunset, and the LIM Gateway can be turned off.

Additionally, it is important to highlight the fact that the LIM Gateway is simply a rather small software component and thus does not necessarily require dedicated hardware in either of the above scenarios. While all diagrams up until this point have shown the LIM Gateway installed on a separate piece of hardware, there are no limitations keeping the LIM Gateway from being installed on the LIMWC or LWP servers, or any other server in your environment, such as a WebSphere® Portal server. As long as adequate capacity is available, and the server meets the requirements defined in "LIM system requirements" on page 14, there are no software conflicts in running the LIM Gateway alongside other software components.

## LIM Gateway versus the LIMWC SIP Connector

One item of common confusion regarding the LIM Gateway is its comparison to the *SIP Connector* available as part of Lotus Instant Messaging and Web Conferencing. This SIP capability that is part of the LIMWC environment is intended to allow users in one LIMWC community to communicate with users in a different LIMWC community using SIP.

To support these external communities, an administrator installs an LIMWC feature called the SIP Connector in each LIMWC community. When SIP Connectors are used to connect two different LIMWC communities, users in one LIMWC community can use SIP to share presence and instant messaging capabilities with users in another LIMWC community.

Since the SIP Connector is used to connect multiple LIMWC communities, and the LIM Gateway is intended to connect LIMWC and LWP communities, confusion can obviously occur. However, the key difference between the SIP Connector capabilities and the LIM Gateway capabilities discussed in this Redpaper can be highlighted via two key aspects of the SIP Connector:

1. The SIP Connector is intended to allow integration between two different LIMWC communities; the SIP Connector capabilities *cannot* be utilized to integrate with an LWP environment. A typical use of the SIP Connector can be seen in Figure 5, which depicts IBM's own usage of the LIMWC SIP Connector capabilities to integrate with external IBM Business Partner and client LIMWC environments.
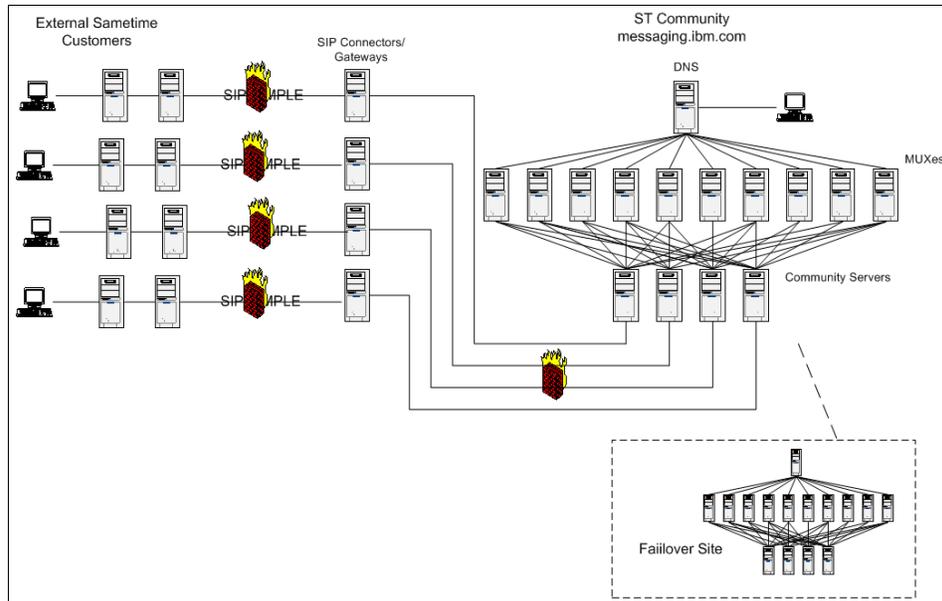
*Figure 5   An example usage of the LIMWC SIP Connector capabilities at IBM*

2.  The SIP Connector does not provide for a seamless integration from the end
    user's perspective as is provided by the LIM Gateway. Rather than logging
    users from one community into the other community in a "proxy" fashion like
    the LIM Gateway, the SIP Connector simply provides the users with the ability
    to request information or communication with an external user. The end user
    leveraging SIP Connector integration must know that they wish to
    communicate with a user in an external community, and specifically request
    this. This specific request to chat with an external community is shown in
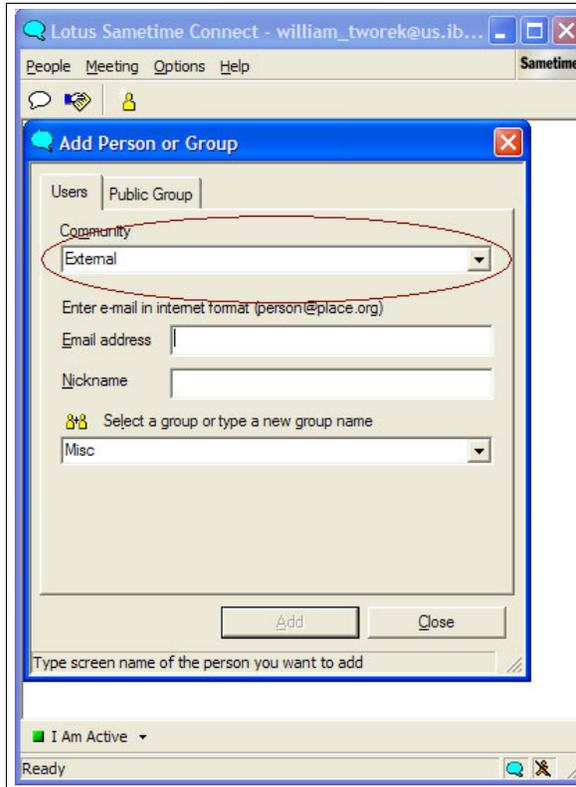    Figure 6.

*Figure 6   LIMWC client requesting an external community via the SIP Connector*

The interface in Figure 6 should be compared to the interface shown in Figure 1 on page 4, which showcases the seamless integration provided by the LIM Gateway.

Table 1 provides a summary of the differences between the LIM Gateway and SIP Connector.

*Table 1   Comparing the SIP Connector and LIM Gateway*

|  | **LIMWC SIP Connector** | **LIM Gateway** |
|---|---|---|
| Can be used to integrate two or more LIMWC communities | Yes | No |
| Can be used to integrate a LIMWC community to a LWP community | No | Yes |

| | LIMWC SIP Connector | LIM Gateway |
|---|---|---|
| Integration provided is seamless to the end user | No | Yes |
| Proxies user logins from one community to another | No | Yes |

More information about the LIWMC SIP Connector can be found in the IBM Redpaper *Connecting Communities Using the Lotus Instant Messaging SIP Gateway*, available at:

http://www.redbooks.ibm.com/abstracts/redp3834.htm

## LIM system requirements

As described previously, a LIM Gateway can be installed on a dedicated machine, or can be installed and run on one of the existing LIMWC or LWP machines in your environment. Of course, if you are installing the LIM Gateway on the same computer as an LWP server, an LIMWC (Sametime) server, or an IBM Lotus Portal server, the computer should exceed the minimum LIM requirements to the extent necessary to accommodate both the functionality of the LIM Gateway and the functionality of the other server application.

### Microsoft® Windows® server installation requirements

Minimum hardware:

► CPU: Pentium® II 400 MHz
► Memory: 512MB (minimum), 1 GB (recommended)

Operating system:

► Windows 2000 Server/Advanced Server
► Windows 2003

### IBM AIX® installation requirements

Minimum hardware:

► Server: An IBM pSeries® server based on PowerPC® (RISC) technology
► Memory: 512MB (minimum), 1 GB (recommended)

Operating system:

► IBM AIX 5.1 with patch level 4 (5100-04)
► IBM AIX 5.2 with patch level 2 (5200-02)

**Note:** The LIM Gateway also requires the IBM JVM 1.3.1 on both Windows and Linux®. However, this JVM is installed by the LIM Gateway installation.

### Supported LIMWC environments

For the LIM Gateway to interoperate with a Lotus Instant Messaging and Web Conferencing environment, the server side of the LIMWC environment must meet the following version and operating system requirements:

► Sametime 3.1 (or higher) servers that operate on Windows, AIX, Solaris, and OS/400® platforms. If your Sametime servers are Sametime 3.0 (or earlier), you must upgrade your servers to use them with the LIM Gateway.

> **Note:** The platforms listed above include all platforms supported by the LIMWC (Sametime) server at the publication date of this Redpaper. If the LIMWC server is built on an additional platform in the future, check with an IBM representative to determine if the LIM Gateway operates with the server on the additional platform.

► IBM WebSphere Portal 5.0 (or higher) servers. If your LIMWC environment includes IBM WebSphere Portal servers, the portal servers must be version 5.0 or higher. Only portlet presence and instant messaging clients that operate with portal server version 5.0 or higher can be used with the LIM Gateway.

► Lotus Domino® 6.5 (or higher) servers. If your LIMWC environment includes Lotus Domino servers, they must be version 6.5 or higher. Only Lotus Notes® clients that operate with version 6.5 or higher can be used with the LIM Gateway.

Additionally, any LIMWC clients used when the LIM Gateway is deployed must also meet a defined set of requirements, or any users utilizing non-support clients will not be able to take advantage of the LIM Gateway's capabilities.

In general, all instant messaging and awareness clients that operate with the server versions listed above are supported, including:

► Sametime Connect (both the Windows and browser versions).

► Any client developed with a Sametime Links toolkit that is created for use with Sametime 3.1 or higher servers. These clients include:

  – Any portlet provided in the Collaboration Center of a Portal 5.0 (or higher) server that supports instant messaging and presence, such as a Lotus Team Workplaces portlet or a buddy list portlet.

  – Any portlet (5.0 or higher) developed by IBM Lotus that operates with a Lotus Domino and LIMWC server to combine Domino functionality and LIMWC presence and instant messaging functionality, such as the Web Access (iNotes™) portlet.

- Sametime links (or "live names") embedded into a Lotus Notes 6.5.x client to integrate instant messaging and awareness with the Notes client.

- Any other presence and instant messaging client built with any IBM Lotus developer toolkit created for use with Sametime 3.1 or higher servers.

### Supported LWP environments

For the LIM Gateway to interoperate with a Lotus Workplace environment, the server side of the LWP environment must be at release 2.0.1 (or higher), with servers that operate on the Windows, AIX, or Linux operating system.

> **Note:** The platforms listed above include all supported platforms for the LWP server as of the publication date of this Redpaper. If the LWP server is built on an additional platform in the future, check with an IBM representative to determine if the LIM Gateway operates with the server on the additional platform.

Additionally, all instant messaging and presence clients that operate with an LWP 2.0 (or higher) server are supported. No modifications to these presence and instant messaging clients are required to operate with the LIM Gateway. These clients include:

► Any portlet provided with an LWP 2.0 (or higher) server that supports instant messaging and presence.

► Workplace Client Technology™ (WCT) clients (for example, the Lotus Workplace rich client for Messaging and Documents).

► Any other instant messaging and presence client built with any IBM Lotus developer toolkit created for use with the LWP 2.0 (or higher) server.

> **Note:** If users in your LWP environment use third-party SIP clients to access an LWP server, the third-party SIP client users may be unable to respond to chat messages initiated by users from the LIMWC environment, depending on how the third-party SIP clients are programmed. The SIP clients developed by IBM Lotus for use with the LWP server avoid this problem because these clients are designed to programmatically subscribe on users who initiate chat sessions with them.

# LIM Gateway deployment considerations

To discuss the various areas that need careful consideration when deploying a LIM Gateway environment, we must start with a basic or typical deployment, as shown in Figure 7.

This figure depicts a basic LIM Gateway deployment with several characteristics:

► The LIMWC and LWP environments share a common authentication and name directory.

► The LIM Gateway has been installed on its own dedicated hardware or logical partition.

► The LIMWC environment is leveraged for embedded awareness within both a WebSphere Portal environment and a Lotus Domino environment.
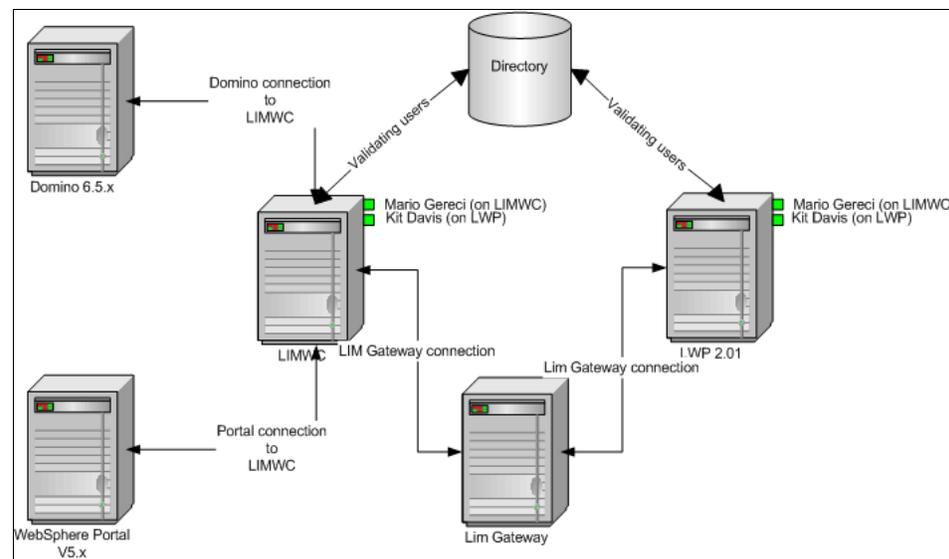


*Figure 7   A typical architecture for installation of a LIM Gateway*

It is when going beyond this typical architecture that various deployment options must be analyzed and carefully considered. The remained of this section will discuss these key items to be considered in a LIM Gateway deployment.

## Directory considerations

In general, one can use the LIM Gateway with any type of directory that is supported by an LIMWC or LWP environment. The LIM Gateway interacts

directly with the LIMWC servers and LWP servers in the two environments, but does not access the directories used in those environments on its own.

Based on this, the type of directory used in each environment is irrelevant to the LIM Gateway. If the directory is supported by that environment, and the environment functions appropriately with that directory, the LIM Gateway will also function correctly when working with the environment.

For example, the LIM Gateway will operate successfully with any of these directory configurations (assuming that the directories used are supported in each environment):

► An LIMWC environment that operates with a native Domino directory and an LWP environment that operates with an LDAP directory.

► An LIMWC environment that operates with an LDAP directory and an LWP environment that operates with a different LDAP directory. (For example, one environment operates with a Domino LDAP directory while the other environment operates with an IBM LDAP directory.)

► An LIMWC environment and an LWP environment that operate with the same LDAP directory.

► If an environment uses multiple directories, and the environment functions appropriately with the multiple directory configuration, the LIM Gateway will also function correctly when working with the environment.

Although the type of directory used in an environment is irrelevant to the LIM Gateway, there are specific requirements regarding the person entries and Internet e-mail addresses that appear in the directories if two separate directories are used in the LIMWC and LWP environments.

► A single user must have a person entry in both the directory used in the LIMWC environment and the directory used in the LWP environment. These duplicate directory entries are mandatory regardless of whether the user accesses the clients from only one environment or both environments.

   For example, the user John Smith must be entered in both the LIMWC and LWP directories to enable the LIM Gateway to represent him in both environments. If John Smith uses only LWP clients, he still must have a directory entry in the LIMWC directory to communicate with the LIMWC users. Similarly, if John Smith uses only LIMWC clients, he must have a directory entry in the LWP directory to communicate with the LWP users.

► The Internet e-mail address for each user must be identical in both directories. For example, if John Smith has an the Internet e-mail address of John_Smith@acme.com in the LIMWC directory, he must have this same Internet e-mail address specified in the LWP directory.

If necessary, the administrator must manually edit the directory entries or use script files to ensure that each user has an identical Internet e-mail address in each directory.

The fact that user names and e-mail address must exist in both directories when two directories are utilized leads to the possibility that a directory synchronization tool may be needed to integrate the two directories in this manner.

Additionally, groups must also be considered when two directories are utilized. As with user names in the directory, to enable a user to add a group from one environment to a client that operates in the other environment, the administrator must ensure that the group exists in the directory used in the other environment as well.

This group aspect again speaks to the importance of a good directory synchronization strategy, should multiple directories be involved in your LIM Gateway deployment. Obviously, the ideal solution would be to have a single directory as depicted in Figure 7. However, this will not always be feasible in a real world environment.

# Security considerations

There are several security issues that must be understood with the LIM Gateway. These involve the security of the gateway's communications with both the LWP and LIMWC environments, as well as the ports and protocols used by the gateway.

## LIM Gateway security in the LWP environment

The LIM Gateway connects to every LWP server in an LWP environment. When establishing these connections, the LIM Gateway must transmit a name (Internet e-mail address) and password to each LWP server so that each LWP server can authenticate the connection from the LIM Gateway.

To support this, an administrator must create a unique LDAP directory entry for each LWP server in the environment to be used for login from the LIM Gateway. For example, if there are three LWP servers in the environment, you must create three unique LDAP directory entries. Each of these LDAP directory entries must include a different user name, Internet e-mail address, and password.

**Note:** All of the configuration settings for the LIM Gateway are set within a text file known as the IMAProxy.poperties file. This includes the parameters defining the ID and passwords used for the LIM Gateway to log in to LWP servers. Thus, access to this properties file must be carefully controlled to ensure that these IDs and passwords are kept confidential.

Additionally, all data transmitted between the LIM Gateway and the LWP servers is encrypted with Transport Layer Security (TLS). To enable this encryption, the administrator specifies TLS as the connection protocol for LIM Gateway connections to the LWP server when configuring the LIM Gateway.

### LIM Gateway connections with the LIMWC environment

Connections from the LIM Gateway to the LIMWC server are authenticated using the IP address of the LIM Gateway in the normal LIMWC "trusted server" model. The administrator must allow the LIM Gateway as a "trusted server" on the LIMWC configuration.

To log LWP users into the LIMWC server, the LIM Gateway uses the standard "light log-in" functionality provided for LIMWC Web-based clients in the LIMWC server developer toolkits.

Finally, all data transmitted between the LIM Gateway and the LIMWC servers is encrypted using RC 2 with a 128-bit key for symmetric encryption. No configurations are required by the administrator to encrypt this data.

### Ports used for LWP connections

If a firewall exists between the LIM Gateway and the LWP servers, the following ports must be open through the firewall to enable the LIM Gateway to communicate with the LWP servers.

► Port 5061 (using TLS): the LIM Gateway communicates with the SLSP component of an LWP server on this port by default.

► Port 1516 (using TCP): the LIM Gateway communicates with the Presence server component of an LWP server on this port by default.

► Any available port on the LIM Gateway computer (using TLS): a port must be available to transmit instant messages between the LIM Gateway and the LWP environment.

   When an LWP user sends an instant message to an LIMWC user, the instant message must be transmitted on a connection from the LWP server to the LIM Gateway. The administrator selects the port used for this connection when configuring the LIM Gateway. The administrator can select a specific port for this purpose or configure the LIM Gateway to dynamically select any available port on the LIM Gateway computer.

### Ports used for LIMWC connections

If a firewall exists between the LIM Gateway and the LIMWC servers, TCP port 1516 must be open through the firewall to enable the LIM Gateway to communicate with the LIMWC servers.

All communications between the LIM Gateway and the LIMWC environment occur using port 1516.

# Scalability considerations

As the size of a LIMWC and/or LWP environment grows, additional LIM Gateways will be needed to support the volume. To understand the number of LIM Gateways to utilize, it is important to understand the specific communications happening with each connection. The number of LIM Gateways must thus be considered from both an LWP and an LIMWC perspective.

## LIM scalability regarding LWP connections

Due to the architecture of the instant messaging environment within Lotus Workplace, there are two areas of communication between the LIM Gateway and an LWP environment:

► Stateless SIP Proxy (SLSP)

The administrator configures the LIM Gateway to establish a connection with the Stateless SIP Proxy (SLSP) component on one LWP server in the environment. Over this connection, the LIM Gateway sends the SIP methods that register LIMWC users into the LWP environment.

► Presence Server

The administrator also configures the LIM Gateway to establish a connection to the Presence server component on each LWP server in the environment. Over these connections, the LIM Gateway receives the following information about user activity on each of the LWP servers in the environment:

– LWP user logins and logouts occurring on each LWP server

– LWP user presence status changes occurring on each LWP server

– LIMWC users that are subscribed on by the LWP users connected to each LWP server

With an understanding of these connections, one could scale LIM Gateways interaction with LPW via scenarios featuring one, two, three or more gateways.

### *Single LIM Gateway scenario*

If you deploy one LIM Gateway into an environment that includes a single LWP server, the LIM Gateway must establish two connections to the LWP server: one connection to the SLSP component of the LWP server and one connection to the Presence server component of the LWP server.
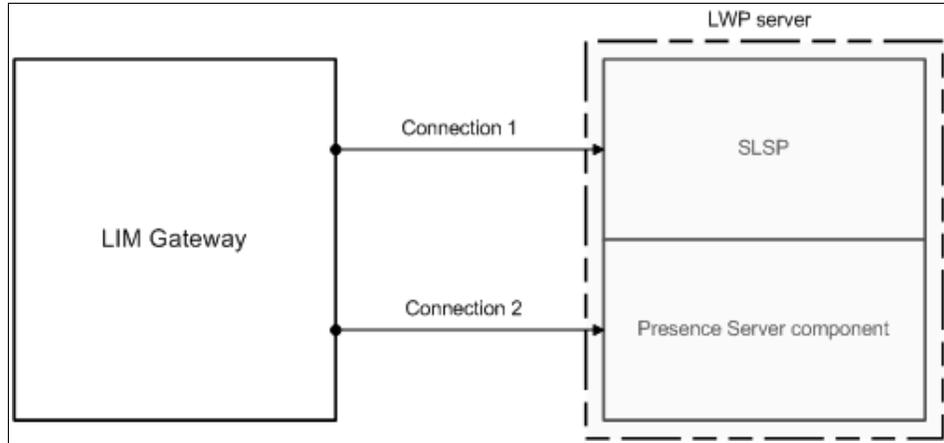
*Figure 8   Single LIM Gateway connects to single LWP server*

If you deploy one LIM Gateway into an environment that includes multiple LWP servers, you can configure the connections in the following way:

► LIM Gateway 1 connects to the SLSP component on LWP server 1.

► LIM Gateway 1 connects to the Presence server components on all LWP servers in the environment, including the Presence server component of LWP server 1.
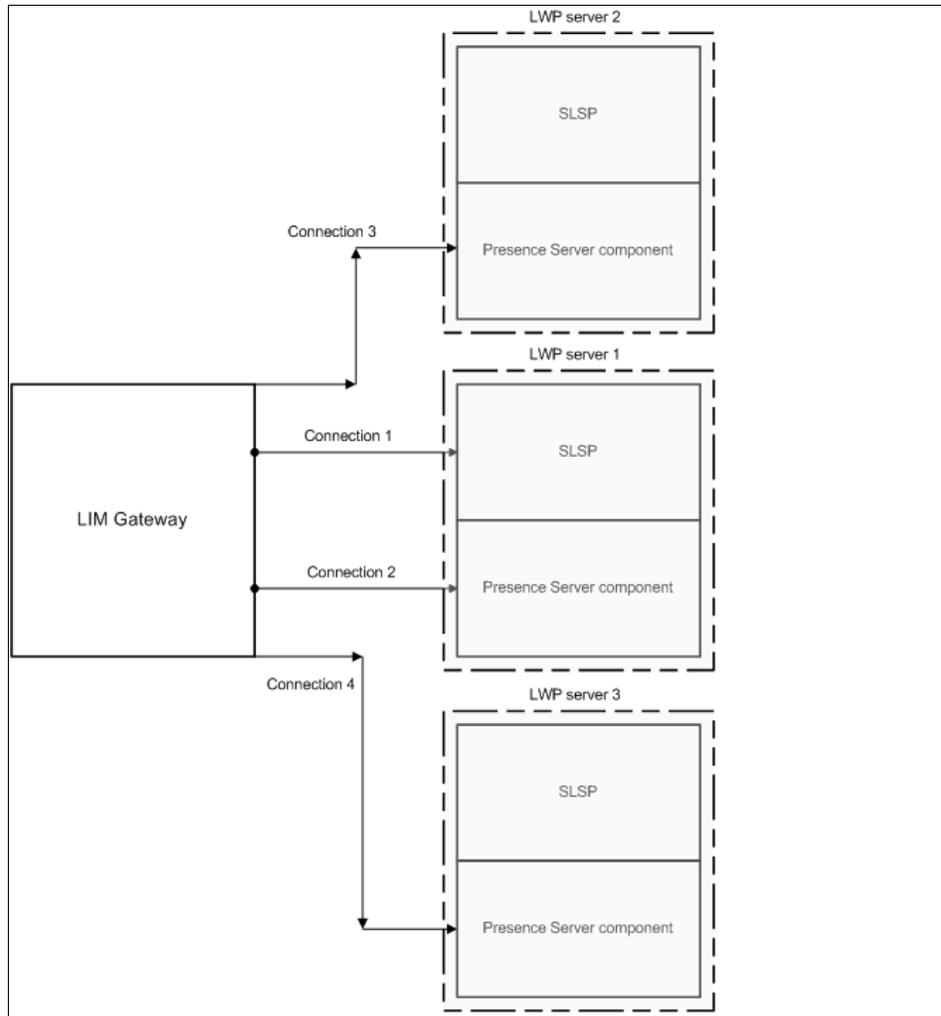
*Figure 9   Single LIM Gateway connects to multiple LWP servers*

### Two LIM Gateways scenario

If you deploy two LIM Gateways to support three LWP servers, you can configure the connections in the following way:

► LIM Gateway 1 can connect to both the SLSP component and the Presence server component on LWP server 1.

► LIM Gateway 2 can connect to the SLSP component on LWP server 2.

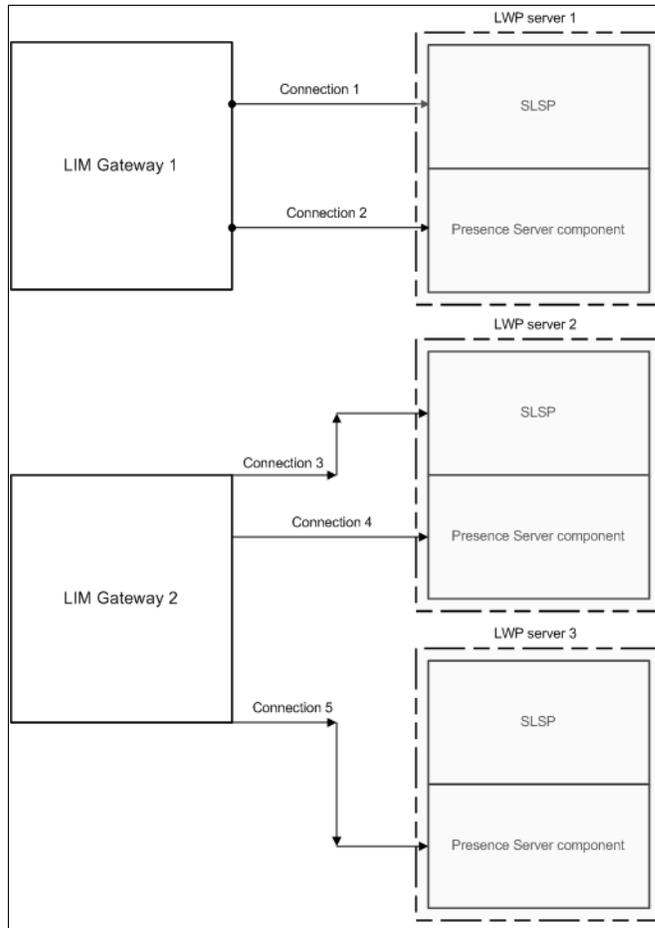► LIM Gateway 2 can connect to the Presence server components on both LWP server 2 and LWP server 3.

*Figure 10   Two LIM Gateways connecting to three LWP servers*

### Three LIM Gateways scenario

If you deploy three LIM Gateways to support three LWP servers, you can configure each LIM Gateway to establish its connections with a different LWP server. Configuring the connections in the following way provides the most efficient performance:

► LIM Gateway 1 can connect to both the SLSP component and the Presence server component on LWP server 1.

► LIM Gateway 2 can connect to both the SLSP component and the Presence server component on LWP server 2.

► LIM Gateway 3 can connect to both the SLSP component and the Presence server component on LWP server 3.
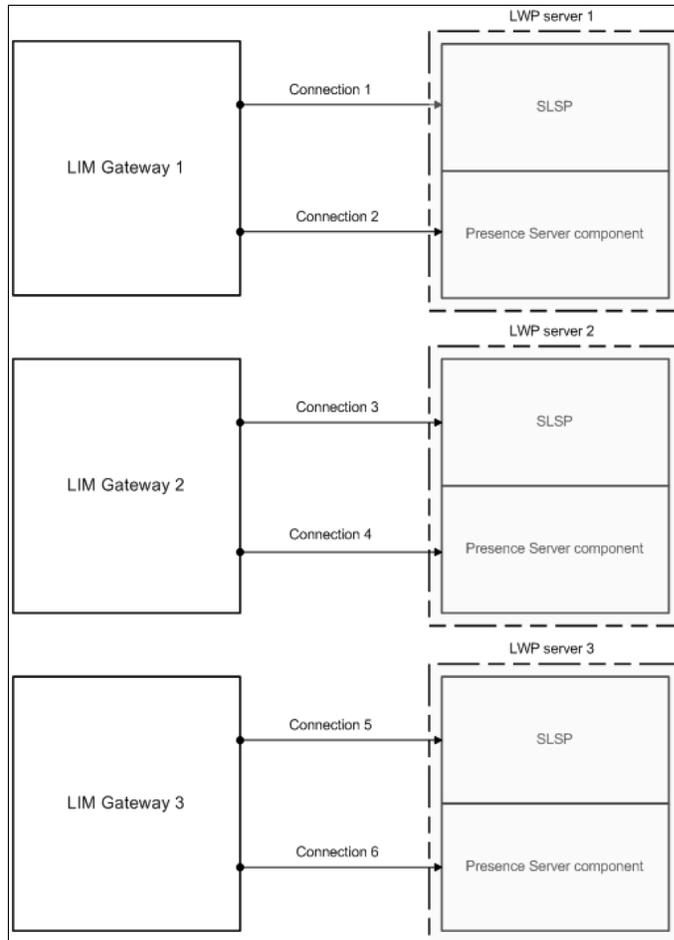
*Figure 11   Example for connecting three LIM Gateways with three LWP servers*

## LIM scalability regarding LIWC connections

Scaling a LIM Gateway to support the connections to an LIMWC environment is a bit different than from the LWP side of things, due to the "single events channel" of the LIMWC architecture. Basically, when multiple LIMWC servers operate together as a community, all LIMWC community events are handled on a single channel. This single events channel is available on all LIMWC servers in the community through intraserver connections between the LIMWC servers. This design enables the LIM Gateway to connect to a single LIMWC server in the community and communicate with all LIMWC servers in the community.

Thus, if only one LIM Gateway service is deployed, it does not matter which specific LIMWC server it is configured to communicate with, because all LIMWC

community servers will participate on the single events channel that is part of the community. This is depicted in Figure 12.
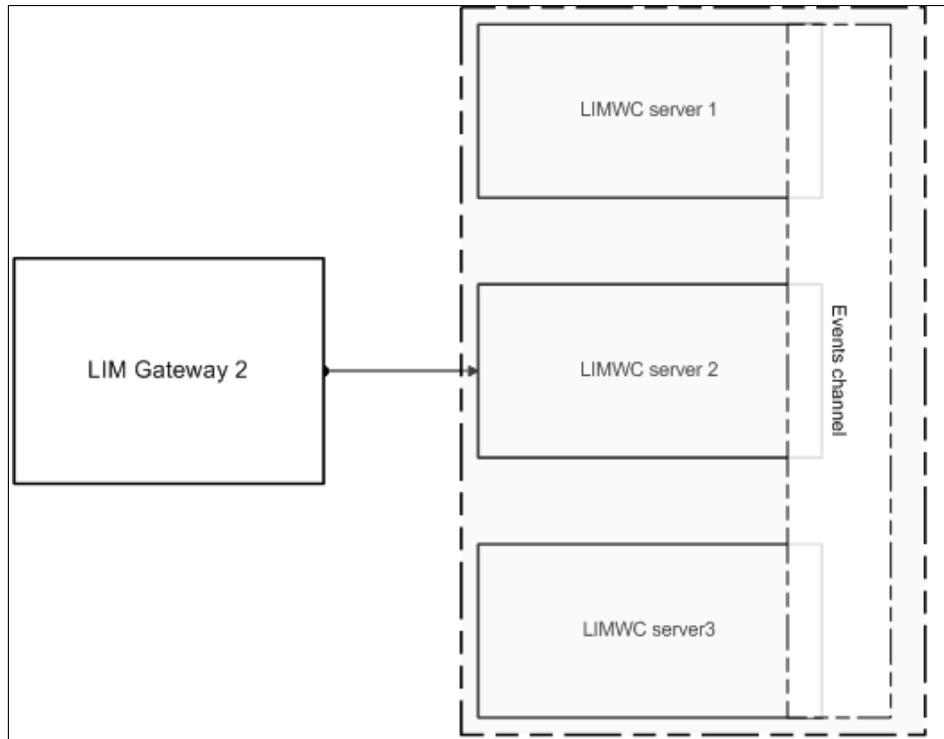


*Figure 12   Single LIM Gateway connects to a group of LIMWC servers*

If multiple LIM Gateways are deployed, each LIM Gateway can connect to the same LIMWC server in the LIMWC community, or each LIM Gateway can connect to a different LIMWC server (as shown in Figure 13). However, there are no real performance advantages to having multiple LIM Gateways connect to multiple LIMWC servers, other than a certain level of failover and redundancy.
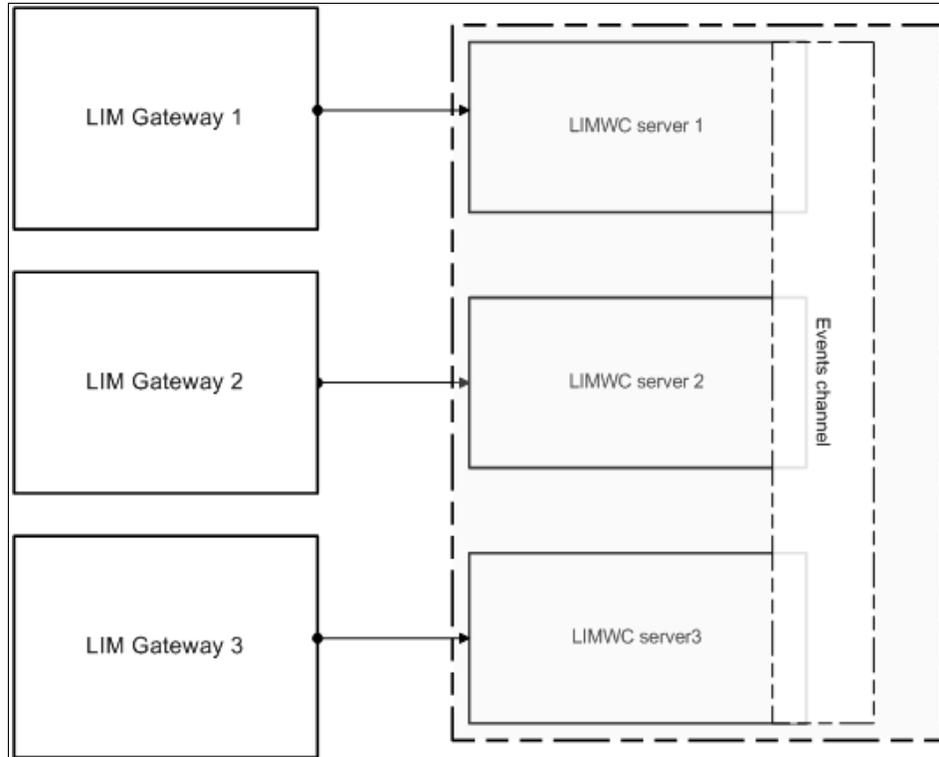
*Figure 13   Example to connect multiple LWP servers to multiple LIMWC servers*

## Miscellaneous deployment considerations

We have covered the key areas of directory, security, and scalability associated with a LIM Gateway deployment. However, there are a few other items than any administrator should be aware of with any LIM deployment.

### *Mixed OS installations are not an issue*

After you have installed the LIM Gateway on an AIX or Windows operating system, the LIM Gateway can communicate with servers running on these platforms:

▶ Sametime 3.1 (or higher) servers running on Windows, AIX, Solaris, or OS/400

▶ LWP 2.0.1 (or higher) servers running on Windows, AIX, or Linux

For example, an LIM Gateway running on a Windows computer can communicate with an iSeries™ (OS/400) Sametime 3.1 server and a Linux LWP 2.0.1 server.

### Impact on LWP and LIMWC capacity should be considered

It is important that any administrator remember the "proxy" operations of the LIM Gateway in terms of the increased load that will be placed on LIMWC and LWP environments when they are connected together with a LIM Gateway. For example, if the LWP environment is scaled for 1 000 users, and the LIMWC is also scaled for 1 000 users, each environment may have 2 000 users logged in once a LIM Gateway is implemented! This is because the LIM Gateway will end up performing "proxied" logins on behalf of each user in one environment into the other environment.

Thus, careful analysis should be made of the available capacity in both LIMWC and LWP environments, and of the impact of an increased user load, prior to implementing the LIM Gateway.

### Server failover

The LIM Gateway performs failover functions if it loses communication with either an LIMWC server or an LWP server.

► If the LIM Gateway loses communication with an LIMWC server, the gateway logs all users of that LIMWC server off of the LWP server(s) to which the LIM Gateway is connected.

► Similarly, if the LIM Gateway loses communication with an LWP server, the gateway logs all users of that LWP server off of the LIMWC server(s) to which the LIM Gateway is connected.

When the LIM Gateway loses communication to either an LIMWC server or an LWP server, the LIM Gateway automatically attempts to reconnect to the server at 60 second intervals.

### Avoiding unnecessary logins of LIMWC users to LWP

As discussed in "How the LIM Gateway works with LIMWC users" on page 7, the LIM Gateway logs an LIMWC user into the LWP server only if the LIMWC user is subscribed on by an LWP user. However, in certain cases, this characteristic of the LIM Gateway can still result in unnecessary logins of LIMWC users to the LWP server.

For example, if an LWP user subscribes on a public group that includes all members of the LIMWC server community, the LIM Gateway may log all members of the LIMWC server community into the LWP server. For example, if a user subscribes on a public group that contains 150 people, but is only interested in chatting with 15 of these group members, this user can create up to 135 unnecessary logins to the LWP server. This scenario may result in an unnecessary drain on the system resources of the LWP server.

Administrators should work to avoid situations where LWP users subscribe on large public groups when the users are only interested in chatting with a few members within the group. Furthermore, administrators may want to caution LWP users against adding large groups to the buddy lists or suggest breaking larger groups into smaller groups, as necessary, to prevent this unnecessary drain on the system resources of the LWP server.

### Reverse proxy and firewall considerations of the LIM Gateway

The LIM Gateway must establish connections with both LWP servers and LIMWC servers.

You cannot use a reverse proxy server with the LIM Gateway. The LIM Gateway cannot connect to an LWP server or an LIMWC server through a reverse proxy server.

# LIM Gateway installation guidelines

This section provides procedures and guidelines for installing and configuring the LIM Gateway on Microsoft Windows. These procedures can be used regardless of whether the LIM Gateway is being installed on a dedicated Windows computer or on the same Windows computer as another server service.

> **Note:** Instructions for installing on AIX are included within the product documentation. However, configuration steps documented in this section would be the same for any operating system.

## High-level installation and configuration steps

1. Install the LIM Gateway code.
2. Configure Lotus Instant Messaging and Web Conferencing to accept LIM Gateway connections.
3. Configure Lotus Workplace to accept LIM Gateway connections.
4. Configure the LIM Gateway via the IMAProxy.properties file.

## Installing the LIM Gateway code

1. Verify that the computer that will host the LIM Gateway meets the Windows system requirements specified in "LIM system requirements" on page 14.
2. Log in to the Windows operating system as a user with Administrator rights.

3. Download the Windows version of the Lotus Instant Messaging Gateway package from the IBM Developerworks site:

   http://www-136.ibm.com/developerworks/lotus/products/instantmessaging/

4. Extract the contents of the LIM package to the root (C:\) of the Windows computer.

   Extracting the contents of this package to the root (C:\) automatically creates a C:\IMGateway directory on the Windows computer. The LIM Gateway files are placed in the C:\IMGateway directory.

   **Important:** The C:\IMGateway directory is used by default for running the LIM Gateway. Running it from another location without performing any customization will create errors.

   To change the installation directory, you must open the install.bat file with a text editor and change the installation directory parameter in this file. Make this change before running the install.bat file.

   *Example 1   Default install.bat file*

   ```
   set IMAWORKDIR=c:\IMGateway
   set JVMPATH=%IMAWORKDIR%\jre\bin\classic\jvm.dll
   JavaLauncher -i service=IMGateway jvmdll=%JVMPATH%
   class=com/ibm/wkplc/ProxyMain -Djava.class.path=.;imaproxy.jar;config
   -Djava.ext.dirs=lib;%IMAWORKDIR%\jre\lib\ext wrkdir=%IMAWORKDIR%
   ```

   If the installation is supposed to be made to a different directory, the parameter set IMAWORKDIR has to be changed.

5. Run the install.bat file provided in the C:\IMGateway directory to install the LIM Gateway as a Windows service. For example, enter this command from the server command prompt:

   C:\IMGateway>install.bat

   This batch file executes a Java process, which in turn creates a Windows service called IMGateway, as shown in Figure 14.
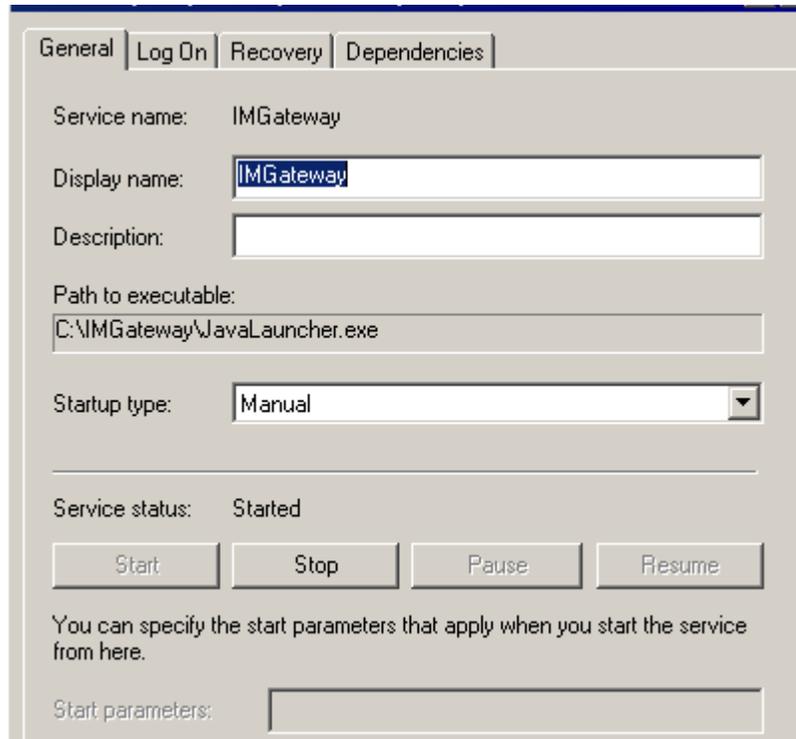
*Figure 14   IMGateway Windows Service*

> **Note:** After this step, the LIM Gateway can be launched by running the
> IMGateway windows service, or can be manually started from a command line
> by executing the **IMGatewayLaunch.exe** command, which can be found within
> the C:\IMGateway directory.

## Configuring LIMWC to accept LIM Gateway connections

To enable an LIMWC server to operate with the LIM Gateway, you must specify
the IP address of the LIM Gateway as an IP address that is allowed to establish
connections with the LIMWC server, and you must confirm the proper LDAP
configuration of your LIMWC server.

### *Trusting the LIM Gateway in LIMWC*

To perform this configuration, enter the IP address of the LIM Gateway into the
CommunityTrustedIps field of the CommunityConnectivity document in the
Configuration database (stconfig.nsf) on the LIMWC server.

1. Use a Lotus Notes client to open the Configuration database (stconfig.nsf) on the LIMWC server.
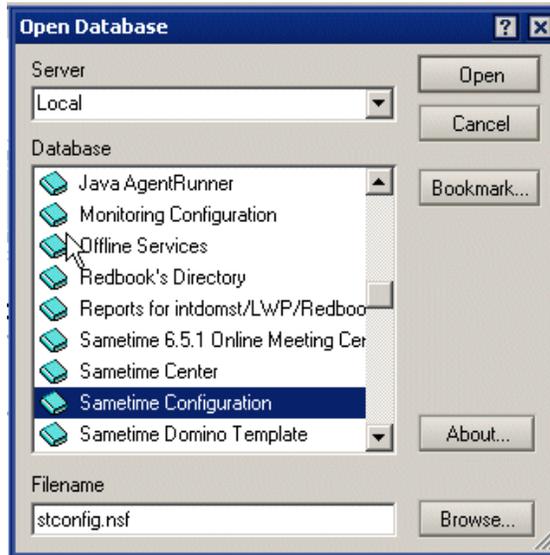


*Figure 15   Opening the stconfig.nsf*

2. Open the CommunityConnectivity document in the stconfig.nsf database by double-clicking the date associated with the document.
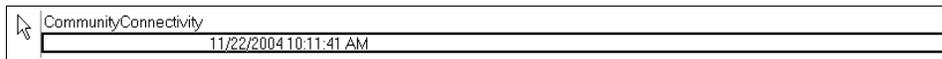


*Figure 16   Select the CommunityConnectivity document from the view All- By Form and Date*

If the CommunityConnectivity document does not exist in the stconfig.nsf database, you must create it. To create the CommunityConnectivity document, choose **Create** → **CommunityConnectivity** from the menu bar in the stconfig.nsf database.

*Figure 17   Optional: creating the CommunityConnectivity document*
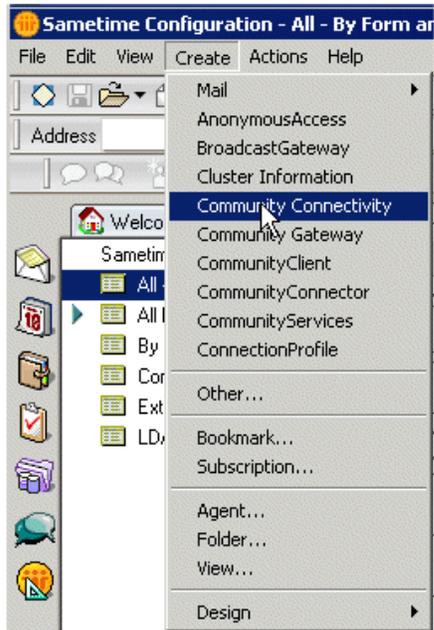
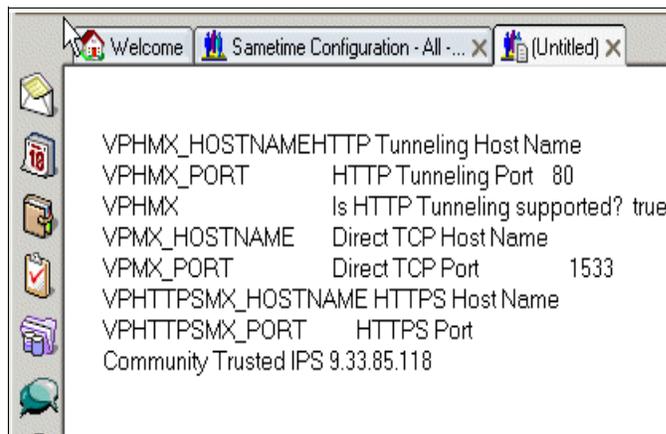3. In the CommunityTrustedIps field, enter the IP address(es) of the LIM Gateway.



*Figure 18   CommunityConnectivity document*

4. Save and close the CommunityConnectivity document.
5. Restart the LIMWC server; it is now ready for the LIM Gateway.

### Verifying proper LIMWC LDAP configuration

While an existing LIMWC server will obviously be configured properly to authenticate to your directory, if the directory used is an LDAP directory, then the LIMWC must be configured to also recognize the correct e-mail address LDAP attribute of all users. This is needed because the LIM Gateway utilizes the e-mail address as the "unique ID" for each user, and thus must resolve the e-mail address of a LIMWC user to be able to proxy log them into the LWP environment.

Verification of the LDAP configuration of your LIMWC server is performed within the Sametime Administration Web interface (stconfig.nsf).

1. Open the Sametime Administration page in your Web browser:

   `http://yoursametimeservername/stconfig.nsf`

2. Go to the LDAP Directory's Basics section.

3. Verify that the LDAP attribute name listed for the e-mail address is the correct LDAP attribute name from your LDAP server, as shown in Figure 19.
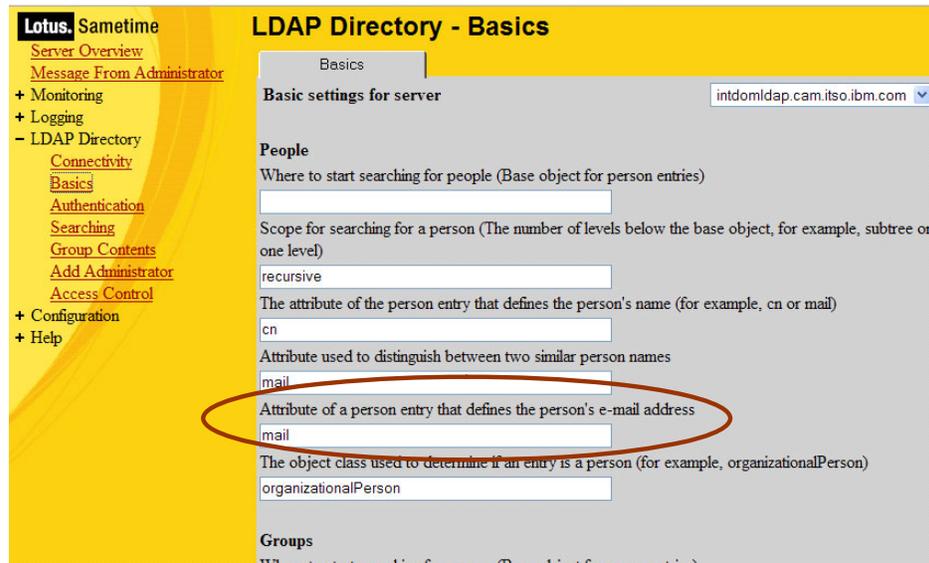


*Figure 19   Sametime LDAP E-mail attribute verification for LIM Gateway*

## Configuring Lotus Workplace to accept LIM Gateway connections

To configure an LWP server to operate with the LIM Gateway, you must perform two procedures:

1. Replace the presenceimservices.jar file on the LWP server with the presenceimservices.jar file provided with the LIM Gateway package. This step is required for the 2.01 release of the Lotus Workplace products only. It may not be needed for future releases.

2. Specify the IP address of the LIM Gateway as an IP address that is allowed to establish connections to the SIP Presence server component of the LWP server.

You must replace the presenceimservices.jar file that currently exists on the LWP server with the presenceimservices.jar file provided with the LIM Gateway package.

1. Make a back-up copy of the presenceimservices.jar file located in the following directory on the LWP server.

   `c:\WebSphere\WorkplaceServer\ps_extdir`

   Store this copy in a safe location. You can use this file to restore the LWP server to its original configuration if necessary.

2. Copy the presenceimservices.jar file provided by the LIM Gateway installation over the presenceimservices.jar file on the LWP server.

   The presenceimservices.jar provided with the LIM Gateway is located in the following directory on the LIM Gateway computer:

   `c:\IMGateway\lib`

3. Repeat this procedure on every LWP computer in the LWP environment.

Next, use the WebSphere Administrator's Console on an LWP server to specify the IP address of the LIM Gateway as "trusted." If multiple LWP servers operate in a WebSphere cell, you must repeat this procedure on each LWP server in the cell.

To add the IP address of the LIM Gateway to the list of IP addresses that are allowed to establish connections to the SIP Presence server component of the LWP server, follow these steps:

1. Open the WebSphere Administrator's Console on the LWP server.

   `http://yourfullqualifiedhostname:9091/admin`

2. Select **Servers** → **Application Servers** → **Portal Server** → **Custom Properties**.

3. Set the lwpSIPBypassTrustedIps field to `True`.

4. In the lwpSIPTrustedIps field, enter the IP address of the computer on which the LIM Gateway is installed.

5. Restart the LWP server. It is now ready for the LIM Gateway.

# Configuring the LIM Gateway (IMAProxy.properties)

To complete the LIM Gateway installation, you must configure settings in the IMAProxy.properties file to enable the gateway to function correctly with your LWP and LIMWC environments.

The IMAProxy.properties file is located in the following directory of the server on which the LIM Gateway is installed:

`<root>\IMGateway\config (Windows)`

The IMAProxy.properties file includes configuration settings that enable it to connect to and communicate with servers in both the LWP environment and the LIMWC environment. These configurations include SIP-related parameters needed to establish connections with LWP servers as well as the addresses of servers in both environments.

As noted in "Directory considerations" on page 17, the LIM Gateway also presents a different name (Internet e-mail address) and password to each LWP server in an environment to authenticate when connecting to the LWP servers. The administrator must also enter these valid user IDs and passwords when configuring the IMAProxy.properties file.

To configure the IMAProxy.properties file, open it with a text editor and enter the settings appropriate for your environment. To assist you with the configuration of the IMAProxy.properties file, a description of every setting in this file is provided in Table 2.

> **Important:** If you have already configured the IMAProxy.properties file, and you want to alter an existing setting, you must alter the setting and then restart the LIM Gateway service for the new setting to take effect.

## IMAProxy.properties file settings descriptions

The IMAProxy.properties file is divided into three sections: Proxy Main Information, LWP Information and ST Information. All of the settings in the IMAProxy.properties file are described in the table below.

*Table 2   IMAProxy.properties settings description*

| IMAProxy.properties settings | Description |
|---|---|
| **PROXY MAIN INFORMATION:** | The PROXY MAIN INFORMATION settings below enable or disable error/trace message reporting and specify the file to which error/trace messages are written. |
| `proxy.traceEnable` | This setting enables or disables error/trace message reporting for troubleshooting purposes. When this setting is enabled, error/trace messages are written to the file specified in the `proxy.traceFileName` setting below. This setting can have a value of either true (enabled) or false (disabled). An example setting is:<br><br>`Proxy.traceEnable=true` |
| `proxy.traceFileName` | This setting specifies the path and file name to which error/trace messages are written. The file specified in this setting is created only when the proxy.traceEnable setting above is set to true (enabled).<br><br>An example setting on a Windows system is:<br><br>`Proxy.traceFileName=c:\temp\IMGateway.txt` |
| **LWP INFORMATION:** | The LWP INFORMATION settings below enable the LIM Gateway to operate with the LWP server environment. |

| IMAProxy.properties settings | Description |
| --- | --- |
| `javax.sip.OUTBOUND_PROXY` | This setting specifies the DNS host name, port, and the connection protocol used to establish a connection to the Stateless SIP Proxy (SLSP) component of one LWP server in the environment. The LIM Gateway registers LIMWC users into the LWP environment over this connection. An example setting is:<br><br>`javax.sip.OUTBOUND_PROXY=lwpserver1.ibm.com:5061/tls`<br><br>**Note:** This setting must specify only one LWP server. If you have deployed multiple LIM Gateways, other LIM Gateways can also connect to this same SLSP component on the same LWP server, if necessary. For more information about configuring multiple server environments, see "Scalability considerations" on page 21. |

| IMAProxy.properties settings | Description |
|---|---|
| `javax.sip.listeningPoint.1` | This setting specifies the SIP listening point associated with the LIM Gateway. This setting should contain the DNS host name of the computer on which the LIM Gateway is installed, the port on which the LIM Gateway listens for SIP connections, and the connection protocol used to establish SIP connections.<br><br>When an LWP user sends an instant message to an LIMWC user, the message is transmitted from the LWP client to the LWP server. The SLSP component of the LWP server then establishes a connection to the LIM Gateway using the address specified in this setting. The SLSP component routes the instant message to the LIM Gateway over the connection established using this address. An example setting is:<br><br>`javax.sip.listeningPoint.1=limproxy.ibm.com:5060/tls`<br><br>Optionally, an administrator can enter 0 (zero) as the port number to enable the LIM Gateway to randomly generate a port number for this purpose. For example:<br><br>`javax.sip.listeningPoint.1=limproxy.ibm.com:0/tls` |
| `com.ibm.ssl.protocol` | This setting must have the value SSL if you want to encrypt the data transmitted between the IMA Gateway and the LWP servers with TLS (TLS is a newer version of SSL). An example value for this setting is:<br><br>`com.ibm.ssl.protocol=SSL` |

| IMAProxy.properties settings | Description |
|---|---|
| `com.ibm.ssl.keystore`<br>`com.ibm.ssl.keyStorePassword`<br>`com.ibm.ssl.truststore`<br>`com.ibm.ssl.trustStorePassword` | These settings specify the key store and the trust store files that support TLS encryption of the data transmitted between the LIM Gateway and the LWP servers, and the passwords required to access these files. Example values for these settings are:<br><br>`com.ibm.ssl.keystore=DummyClientKeyFile.jks`<br>`com.ibm.ssl.keyStorePassword=keyfilepassword`<br>`com.ibm.ssl.truststore=DummyClientTrustFile.jks`<br>`com.ibm.ssl.trustStorePassword=trustfilepassword`<br><br>You can use different key store and trust store files to support the TLS encryption. To use different key store and trust store files, copy the key store and trust store files into the LIM Gateway installation directory and use the settings above to specify the file names and passwords appropriate for these new files. For more information, see "Optional additional setup" on page 45. |

| IMAProxy.properties settings | Description |
|---|---|
| `proxy.lwp.presenceservername.#`<br>`proxy.lwp.proxyname.#`<br>`proxy.lwp.password.#` | These three settings enable the LIM Gateway to establish a connection to the Presence server component of one LWP server and to present that LWP server with authentication credentials when establishing this connection.<br><br>An example configuration for these three settings appears below:<br><br>`proxy.lwp.presenceservername.1=lwpserver1.ibm.com:1516/tcp`<br>`proxy.lwp.proxyname.1=lwpserver1@ibm.com`<br>`proxy.lwp.password.1=password1`<br><br>The `proxy.lwp.presenceservername.#` setting should specify the host name of the LWP server, the port on which the Presence server component of an LWP server listens for connections, and the connection protocol used to establish the connection.<br><br>The LIM Gateway uses this information to establish a connection with the Presence server for the purpose of receiving needed information about LWP user activities (that is, logins/logouts, presence status changes, and subscription information).<br><br>The `proxy.lwp.proxyname.#` setting and the `proxy.lwp.password.#` setting specify the name (Internet e-mail address) and password the LIM Gateway uses to authenticate when connecting to the Presence server component of an LWP server. |

| IMAProxy.properties settings | Description |
|---|---|
| `proxy.lwp.presenceservername.#`<br>`proxy.lwp.proxyname.#`<br>`proxy.lwp.password.#`<br>`(continued)` | These three settings are always specified together to provide the LIM Gateway with the connection information and authentication credentials required to establish a connection to the Presence server component of a single LWP server. In a multiple LWP server environment, you must repeat this group of three settings for each LWP server to which you want this LIM Gateway to connect. For example, if you want one LIM Gateway to connect to two LWP servers, you must have entries like these in the IMAProxy.propertie*s* file:<br><br>`proxy.lwp.presenceservername.1=lwpserver`<br>`1.ibm.com:1516/tcp`<br>`proxy.lwp.proxyname.1=firstlwpserver@ibm`<br>`.com`<br>`proxy.lwp.password.1=firstserverpassword`<br>`proxy.lwp.presenceservername.2=lwpserver`<br>`2.ibm.com:1516/tcp`<br>`proxy.lwp.proxyname.2=secondlwpserver@ib`<br>`m.com`<br>`proxy.lwp.password..2=secondserverpasswo`<br>`rd`<br><br>**Note:** When listing multiple servers in the IMAProxy.properties file, always increment the numeric identifier of the server by one so that the servers are listed sequentially. Do not skip numbers. For example, if you have two servers, do not specify the first server as `proxy.lwp.presenceservername.1` and the second server as `proxy.lwp.presenceservername.3.` The second server must be listed as |

| IMAProxy.properties settings | Description |
|---|---|
| `proxy.lwp.presenceservername.#`<br>`proxy.lwp.proxyname.#`<br>`proxy.lwp.password.#`<br>`(continued)` | proxylwp.presenceservername.2. The LIM Gateway will not function correctly if the servers are not numbered sequentially.<br>As discussed earlier, you can deploy multiple LIM Gateways to support multiple LWP servers. The examples below illustrate how to configure these settings in an environment that includes multiple LIM Gateways.<br>This example assumes you have deployed two LIM Gateways to support three LWP servers. In this example, one of the LIM Gateways must connect to the Presence server component of one LWP server and the other LIM Gateway must connect to the Presence server components of the remaining two LWP servers.<br>In the IMAProxy.properties file on LIM Gateway 1, the settings should be configured as illustrated below:<br>`proxy.lwp.presenceservername.1=lwpserver1.ibm.com:1516/tcp`<br>`proxy.lwp.proxyname.1=firstlwpserver@ibm.com`<br>`proxy.lwp.password.1=firstserverpassword`<br><br>In the IMAProxy.properties file on LIM Gateway 2, the settings should be configured as illustrated below:<br>`proxy.lwp.presenceservername.1=lwpserver2.ibm.com:1516/tcp`<br>`proxy.lwp.proxyname.1=secondlwpserver@ibm.com`<br>`proxy.lwp.password.1=secondserverpassword`<br>`proxy.lwp.presenceservername.2=lwpserver3.ibm.com:1516/tcp`<br>`proxy.lwp.proxyname.2=thirdlwpserver@ibm.com`<br>`proxy.lwp.password..2=thirdserverpassword` |
| **ST INFORMATION:** | The ST INFORMATION setting below enables the LIM Gateway to operate with the LIMWC server environment. |

| IMAProxy.properties settings | Description |
|---|---|
| `proxy.sametime.hostname` | This setting specifies the DNS name of an LIMWC server. The LIM Gateway establishes a connection to this LIMWC server to communicate with all LIMWC servers in the LIMWC community.<br><br>An example setting is:<br><br>`proxy.sametime.hostname=sametimeserver.ibm.com`<br><br>If you have deployed multiple LIM Gateways, each LIM Gateway can connect to the same LIMWC server in the environment, or each LIM Gateway can connect to a different LIMWC server. |

As a further guideline to readers in configuring their own IMAproxy.properties file, Example 2 provides a sample IMAProxy.properties file that was successfully used for all of our testing in the Redbook test lab environment.

*Example 2   Sample IMAProxy.properties file*

```
########################
# PROXY MAIN INFORMATION
########################
proxy.traceEnable = true
proxy.traceFileName = IMAProxy.txt

#####################
# LWP INFORMATION
#####################

# SLSP address of LWP primary server
javax.sip.OUTBOUND_PROXY = intlwpst.cam.itso.ibm.com:5061/tls

# listening point of the proxy
javax.sip.listeningPoint.1 = intlwpst.cam.itso.ibm.com:5060/tls

# SSL properties to be used by sip stack
com.ibm.ssl.protocol=
com.ibm.ssl.keyStore=DummyClientKeyFile.jks
com.ibm.ssl.keyStorePassword=WebAS
com.ibm.ssl.trustStore=DummyClientTrustFile.jks
com.ibm.ssl.trustStorePassword=WebAS

# LWP presence server to connect
```

```
proxy.lwp.presenceservername.1 =intlwpst.cam.itso.ibm.com:1516/tcp
proxy.lwp.proxyname.1 = lwpstserver1@redbook.com
proxy.lwp.proxypassword.1 = lwpstserver1

#####################
# ST INFORMATION
#####################
proxy.sametime.hostname = intdomst.cam.itso.ibm.com
```

After all of the appropriate settings have been defined, the LIM Gateway service must then be stopped and started. If everything is working properly, seamless awareness should now exist between the two environments. If awareness is not functioning, then the reader should proceed to "LIM Gateway troubleshooting guidelines" on page 46.

## Optional additional setup

One optional procedure that can be performed is to change the default key store file and trust store file that support TLS encryption of the connections between the LIM Gateway and the LWP servers.

To support TLS encryption of the connections between the LIM Gateway and the LWP server, the LIM Gateway installation places a DummyClientKeyFile.jks and a DummyClientTrustFile.jks file in the C:\IMGateway directory. These are the same jks files that IBM provides by default with all WebSphere servers.

If you want to use different jks files as the key stores that support TLS connections, follow the instructions below:

1. Copy the new key store jks file and new trust store jks file that you want to use into the C:\IMGateway directory or the <root>/IMGateway directory.

2. Open the IMAProxy.properties file with a text editor and alter the following settings so that they specify the new key store file name and new trust store file name, and the passwords required to access the new files.

   – `com.ibm.ssl.keystore`=<enter the new key store file name>

   – `com.ibm.ssl.keyStorePassword`=<enter the password for the key store file>

   – `com.ibm.ssl.truststore`=<enter the new trust store file name>

   – `com.ibm.ssl.trustStorePassword`=<enter the password for the trust store file>

3. Save and close the IMAProxy.properties file.

4. Restart the LIM Gateway.

# LIM Gateway troubleshooting guidelines

Even the most skilled installer and administrator will undoubtedly run into occasions where they need to troubleshoot an issue with the LIM Gateway. Fortunately, the LIM Gateway provides a rather thorough logging capability that allows you to resolve most issues. This section describes how to enable the logging, where to look for log files, and how to interpret the logs files once they are found.

## Turning on error/trace message logs

To enable error/trace message reporting, the administrator configures these two parameters in the IMAProxy.properties file on the LIM Gateway computer:

► `proxy.trace.Enable=true`

► `proxy.traceFileName`=<file path and file name>

The `proxy.traceFileName` value is at your discretion. For example, if you enter `c:\temp\IMGateway.txt`, the trace messages are written to the IMGateway.txt file in the c:\temp directory on the LIM Gateway computer.

### Instructions to enable error/trace message reporting

1. Open a text editor on the computer on which the LIM Gateway is installed.

2. Open the IMAProxy.properties file at the following location:

   `c:\IMGateway\config`

3. In the IMAProxy.properties file, populate the `proxy.traceEnable` and `proxy.traceFileName` parameters as shown below:
   - `proxy.traceEnable=true`
   - `proxy.traceFileName=c:\temp\IMGateway.txt`

4. Close and save the IMAProxy.properties file.

5. Restart the LIM Gateway.

## Interpreting the log files

The IMGateway.txt log files can seem overwhelming at initial glance. However, once you understand the key processes involved in LIM conversations, the log files can be quickly understood.

The key LIM processes, and log entries, that any administrator should understand can be broken up into those processes that monitor the LIMWC side of the conversation, and those that monitor the LWP side of the conversation:

### Key log entries related to LIM-LIMWC communications

The key process involved in LIMWC communications is called the *STUsersSideMgr*. As communications occur with the LIMWC servers, the following types of messages will be seen in the trace file.

- ► If the LIM Gateway logs out from LIMWC server, the message `>> LoginSAMgr::Loggedout reason: ...` will appear in the trace file.

- ► If the LIM Gateway logs into the LIMWC server, the message `LoggedIn to ST server =...` will appear in the trace file.

- ► When a user from LWP logs in, and thus the LIM Gateway needs to proxy that login to LIMWC, the message `STUsersAgent::doLogin: userName =` will appear in the trace file.

- ► As part of a proxied login, the LIM Gateway will need to first resolve the LWP user on the LIMWC side. When this name resolution takes places, then messages regarding a "Resolver" process will appear in the trace file, such as `Resolver::setFQNuserId: eMailAdd=tworek@us.ibm.com userFQNid = {CN=William Tworek,O=IBM,}`. As you can see, the eMailAdd is empty.

- ► When a user from the LWP logs out, and thus the LIM Gateway needs to log out the proxied user in LIMWC, the message `STUserObject::doLogout: for =` will appear in the trace file.

- ► When a new message from a user on the LWP side to a user on the LIMWC side is received by the LIM Gateway, the message `STUserObject::continueMessage: from =...  to = ...` will appear in the trace file.

- ► When a user from the LWP side changes his status, and thus the LIM Gateway must proxy this status change, the message `STUserObject::changeStatusOfUser -> user =` will appear in the trace file.

### Key log entries related to LIM-LWP communications

The key process involved in LIMWC communications is called the *LWPSideMonitoring*. As communications occur with the LIMWC servers, the following types of messages will be seen in the trace file.

- ► When a user from the LIMWC side logs in, the LIM Gateway will attempt to proxy this login to the LWP side, and the message `LWPUserAgent::doLogin: new request received initiator name = ..` will appear in the trace file.

- ► If no LWP user has yet to "subscribe" to the LIMWC user, then this LIMWC user does not yet need to be logged into LWP, and will instead be added to a

"waiting table," and the message `LWPUserAgent::doLogin: add to waiting table initiator name = ...` will appear in the trace file.

► When a user from LIMWC side logs out, the LIM Gateway will log out the proxied user from the LW side (or remove them from the "waiting table"), and the message `LWPUserAgent::doLogout: new request received initiator name =` will appear in the trace file.

► When a user from the LIMWC side changes his status, the LIM Gateway will proxy this status change to the LWP side, and the message `LWPUserAgent::changeStatus: new request received initiator name =` will appear in the trace file.

► When a message from a user on the LIMWC side is sent to a user on the LWP side, the message `LWPUserAgent::doMessage: new request received from =... to = ...` will appear in the trace file.

► If the LIM Gateway failed to connect to the LWP side server, a message stating `LWPConnection::reCreateConnection to ...` will appear in the trace file as the LIM Gateway attempts to retry the connection.

# Example troubleshooting

To further aid in troubleshooting efforts, a few examples can be shown of common issues that the redbook team experienced within their test lab. These examples are in no way comprehensive, but rather are simplistic illustrations of the types of issues that one might see in a real world environment.

### SSL not configured properly

When initially setting up our LIM Gateway environment, we experienced issues regarding the ability to negotiate an SSL connection to the LWP servers. The initial symptom was that users were unable to communicate through the LIM Gateway. However, we were able to isolate the issue to an SSL error as follows:

1. We examined the trace file and found that all LIM Gateway services appeared to happily initialize until the "SIPStackMgr":

```
SipStackMgr::init....
com.ibm.workplace.jain.protocol.ip.sip.SipStackImpl.SipStackImpl: trying to
load sip stack
```

2. Immediately in the trace files after this init statement, multiple Java stack traces and error messages appeared as follows:

```
java.security.NoSuchAlgorithmException: No such algorithm:
....

java.lang.IllegalStateException: No such algorithm at
com.ibm.workplace.sip.stack.transaction.transport.connections.tls.SIPConnec
tionFactoryImpl.initSSL
```

```
....
com.ibm.workplace.sip.stack.transaction.transport.SIPConnectionsModel.initL
isteningPoints: could not instansiate Listenning connection!
```

3. The fact that the errors were related to the SIP pointed to an issue with the LWP connection, since SIP is used to talk to LWP, while the VPBuddy protocol is used to talk to LIMWC. The Java exceptions related to SSL algorithm negotiations pointed towards the SSL handshake as the breakdown in this communication.

4. We then examined our IMAProxy.properties file, and found the issue. We made a typo in defining the SLSP server.

```
# SLSP addres of LWP primary server
javax.sip.OUTBOUND_PROXY = intlwpst.cam.itso.ibm.com:5061/tcp
```

We had inadvertently replaced the /tls at the end of the SLSP server with a /tcp. While TLS is a valid SSL protocol, TCP is an underlying transport, and therefore not valid.

5. After changing the properties file to properly refer to the tls protocol, and restarting the LIM Gateway, the connection to LWP succeeded.

### LIM Gateway not trusted

Once we had the conversations working properly to the LWP side of the equation, we then had an issue communicating with the LIMWC server side. The symptom in this case was, again, that the LIM Gateway was not providing any of the expected integration. We once again looked into the trace files to examine the situation.

1. First, we noticed that the connection the LWP side was now succeeding.

```
SipStackMgr::init m_lp.host 9.33.85.103 m_lp.port = 5060 m_lp.transport =
tcp transport = tls
SipStackMgr::initialized - transport = tls
```

2. Thus, we next turned our attention to verifying the LIMWC side connection. We then noticed the following error in the trace files associated with the LIMWC side of things:

```
Try login to ST server = intdomst.cam.itso.ibm.com
m_name = Java Co-Existence Proxym_prevCommunity = nullm_prevLoginId =
nullm_prevAgreedKey = nullm_quickTokenEncrypted = nullm_quickTokenCacheTime
= 0
IPs from Dns:
IP (0)intdomst.cam.itso.ibm.com/9.33.85.102
Trying to connect to: intdomst.cam.itso.ibm.com/9.33.85.102
VPKernel(0)onLogout: reason = 80000207
```

3. While we did not have immediate access to the error code 80000207, we knew that our LIMWC server was up and running, and could see traffic flowing

between the LIM Gateway and LIMWC server via a quick network trace. Therefore, we double-checked that the LIM Gateway was indeed a trusted server to LIMWC, and found that we had a typo in the IP address that we defined as trusted as described in "Trusting the LIM Gateway in LIMWC" on page 31.

4. After correcting the typo and restarting both the LIMWC and LIM Gateway servers, the connection to the LIMWC servers succeeded.

```
IPs from Dns:
IP (0)intdomst.cam.itso.ibm.com/9.33.85.102
Trying to connect to: intdomst.cam.itso.ibm.com/9.33.85.102
Receiver: run started
ConnectionFactory: Connection initialized:
VPKernel(0): Loging in as Java Co-Existence Proxy
VpKernel: Attempting server login
VPKernel(0)onLogin: UserInstance =
{com.lotus.sametime.core.types.STUserInstance@95f28d00 name =  id = {{,}}
desc = loginId
= {16 09215566,}}
PKernel(0)onSetPrivacyMode: privacyMode = 1
VPKernel(0)onSetPrivacyList: privacyList = Excluding { }
VPKernel(0)onSetStatus: type = 20, time = 0, description =
LoggedIn to ST server = intdomst.cam.itso.ibm.com
```

### *Unable to resolve e-mail address for Sametime users*

Another issue we experienced was the LIM Gateway working in one direction only. LIMWC users could see awareness of LWP users, and even send LWP users an instant message. However, LWP users always saw LIMWC users as offline, and could not reply to any messages received.

In this case, we had to dig a little more deeply into the trace files to understand the issue. We were logging in to the LIMWC environment with the user name Jane Doe, so we started looking for information and events in the log associated with this user. We identified the following basic sequence of events with each login, or status change, from Jane Doe:

```
STusersSideMgr::onUserLoggedIn ->  user = CN=Jane Doe,OU=LWP,O=Redbook,C=BU
server  = 0
...
STUserAgent::onUserStatusChanged -> need to find eMail for user {CN=Jane
Doe,OU=LWP,O=Redbook,C=BU,}
...
Resolver::findUserEmail: user name = CN=Jane Doe,OU=LWP,O=Redbook,C=BU
initiator name
...
Resolver::setFQNuserId: eMailAdd =  userFQNid = {CN=Jane
Doe,OU=LWP,O=Redbook,C=BU,}
```

This specific log entry is a little harder to interpret, since no specific error is listed. However, after some analysis, we noticed that the Resolver was attempting to find Jane's e-mail address, but the result returned was blank. No e-mail address was returned.

We quickly realized that we had forgotten the key step of ensuring that the LDAP attribute for user e-mail was clearly defined to the Sametime server. After going back and updating the Sametime server's LDAP settings as described in "Verifying proper LIMWC LDAP configuration" on page 34, everything worked as expected. The resolver was able to locate an e-mail address for Jane, and all instant messages and status changes properly flowed through the environment.

```
Resolver::setFQNuserId: eMailAdd = jane.doe@redbooks.com userFQNid = {CN=Jane
Doe,OU=LWP,O=Redbook,C=BU,}
```

# Summary

In this Redpaper, we introduced the Lotus Instant Messaging Gateway and its ability to seamlessly integrate a Lotus Instant Messaging and Web Conferencing, and Lotus Workplace environment. We discussed various deployment considerations, installation and configuration aspects, and provided troubleshooting hints and tips. This paper should help any reader to better understand the role of the LIM Gateway, and assist in getting it deployed and working within any environment.

For details about the latest Lotus Instant Messaging products and capabilities, visit:

http://www-306.ibm.com/software/lotus/collaboration/

To download the Lotus technical whitepaper for the Lotus Instant Messaging Gateway, visit:

http://www-10.lotus.com/ldd/notesua.nsf/find/sametime

For other IBM Redbooks™ that cover Lotus Instant Messaging and Workplace technologies, please visit:

http://publib-b.boulder.ibm.com/redbooks.nsf/portals/Lotus

# The team that wrote this Redpaper

This Redpaper was produced by a team of specialists from around the world working at the International Technical Support Organization, Cambridge Massachusetts.

**William Tworek** is a Senior IT Architect within the Office of the IBM CIO, responsible for key the strategy, conceptual architecture, and program management of various pieces of IBM's internal application hosting environment and On Demand Operating Environment. He has previously authored many IBM Redbooks/Redpapers as a member of the IBM International Technical Support Organization. Prior to CIO and ITSO activities in IBM, he was an architect in the consulting industry working for Andersen Consulting/Accenture, followed by IBM Software Services for Lotus. His areas of expertise include collaborative technologies and business portals, system integration, and systems infrastructure design.

**Mario Gereci** is a Consultant with ebf-EDV Beratung Foellmer GmbH in Cologne, Germany (http://www.ebf.de). He has over six years of experience working with Lotus Software, focusing primarily in administration and managing projects within the banking and advertising sectors. He has extensive Lotus and WebSphere installation, deployment, and application development skills. He is a Certified Lotus Professional (CLP) for administration and PCLP for application development in R5 and ND6. Additionally, Mario has certifications in Tivoli® and DB2®. Recently Mario has made IBM Workplace his primary focus. Mario was an author for the IBM Redbook, *Lotus Workplace 1.1 Products Deployment Guide*, SG24-7087.

# Additional contributors

Thanks to the following people for their contributions to this project:

Roger Eames, Program Director, Lotus Collaboration Infrastructure & Lotus Sametime Development
IBM, Westforfd, MA

Uri Segev, Manager, SIP Infrastructure Development team
IBM Haifa Labs, Israel

Orit Yaron-Duzy
IBM Haifa Labs, Israel

Anat Fradin
IBM Haifa Labs, Israel

# Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other 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.*

**The following paragraph does not apply to the United Kingdom or any other country 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.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:
This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

This document created or updated on June 30, 2005.
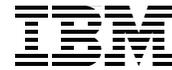
Send us your comments in one of the following ways:
- ► Use the online **Contact us** review redbook form found at:
  **ibm.com**/redbooks
- ► Send your comments in an email to:
  redbook@us.ibm.com
- ► Mail your comments to:
  IBM Corporation, International Technical Support Organization
  Dept. HYJ  Mail Station P099, 2455 South Road
  Poughkeepsie, New York 12601-5400 U.S.A.

# Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

| | | |
|---|---|---|
| @server | Domino | Redbooks |
| @server | DB2 | Sametime |
| Redbooks (logo) | IBM | Tivoli |
| ibm.com® | Lotus Notes | WebSphere |
| iNotes | Lotus | Workplace |
| iSeries | Notes | Workplace Client Technology |
| pSeries | OS/400 | Workplace Team Collaboration™ |
| AIX | PowerPC | |

The following terms are trademarks of other companies:

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, Windows NT®, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel®, Intel logo, Intel Inside®, Intel Inside logo, Intel Centrino™, Intel Centrino logo, Celeron®, Intel Xeon™, Intel SpeedStep®, Itanium®, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

UNIX® is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.