

FaceTime IM Director

Planning and Implementation Guide

Release 1.1



FACE TIME
COMMUNICATIONS

Trademark Notices

Copyright 2001–2003, FaceTime® Communications, Inc. All rights reserved.

Not for use or distribution without the express permission of FaceTime Communications. FaceTime, the FaceTime logo, IM Director, and IM Director Administrator are trademarks of FaceTime Communications, Inc. in the United States and other countries. All other names mentioned in this document may be trademarks of their respective owners.

Information subject to change at any time.

Software License Notice

The software described in this publication is furnished under license and may only be used or copied in accordance with the terms of such license. The license agreement with FaceTime Communications specifies the permitted and prohibited uses of the product. Any unauthorized duplication or use of FaceTime software in whole or in part, or in any other storage and retrieval system, is prohibited.

This document is not for use or distribution without the express permission of FaceTime Communications. This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or converted to any electronic or machine-readable form without the prior written consent of FaceTime Communications, 1159 Triton Drive, Foster City, CA 94404 USA.

Contents

Preface	5
Audience	5
Organization	5
Related Documentation	5
Chapter 1. Planning	7
Estimating the Size of the Database	7
Connection Types	9
Proxy Model	9
SOCKS Proxy	10
DNS Routing	11
Standard Enterprise IM Connectors	12
Message Buffering	12
Logging Modes	13
Distributed Environments	13
Yahoo! Messenger Enterprise Edition Connector	13
Network Configuration Scenarios	14
Standard Configuration with No Corporate Proxy Server	15
Standard Configuration with Corporate Proxy Server	15
Failover Configuration	16
High-Availability Configuration	17
Distributed IM Director Servers Connected to Replicated Regional Databases	18
Chapter 2. Installation	19
Before You Begin	19
Upgrading from IM Director 1.0.x	21
Installing IM Director 1.1.	23
Installing Enterprise IM Connectors	27
IBM Lotus Sametime Connector Installation	28
Microsoft Exchange 2000 Connector Installation	31
Yahoo! Messenger Enterprise Edition Installation	33
Handling Installation Problems	33
IM Director Does Not Start	33

Unable to Connect to the Database	34
Chapter 3. Deployment	35
Deployment Overview	35
Creating Rules on Firewalls and Corporate Proxy Servers	36
Configuring IM Clients for SOCKS Proxy Connection	36
Manual Configuration	37
AOL Instant Messenger (AIM)	37
Yahoo! Messenger	38
MSN Messenger	39
Trillian	40
Automatic Configuration	42
Creating Registration Entry and Batch Files	42
Adding the Logon Script to Your Domain Controller	44
Configuring Your DNS Server for DNS Routing	47
Testing DNS Routing	51
Configuring Windows 2000 for Large User Sites	52
Deploying IM Director Administrator	53
Glossary	55
Index	57

Preface

This document provides information for planning your deployment of FaceTime® IM Director™. It also provides instructions for installing IM Director and deploying it throughout your enterprise.

Audience

This guide is intended for system administrators and other personnel responsible for planning for, installing, and deploying IM Director.

Organization

This guide contains three chapters:

- [Chapter 1, “Planning”](#) shows you how to estimate the size of the IM Director database, describes ways IM clients can connect to IM Director, and provides several configuration scenarios.
- [Chapter 2, “Installation”](#) describes how to install or upgrade IM Director and how to install and configure connectors on enterprise IM servers. It also provides troubleshooting information for handling installation problems.
- [Chapter 3, “Deployment”](#) describes how to deploy IM Director throughout your enterprise.

A glossary and an index are included at the end of the guide.

Related Documentation

The *IM Director Administration and Reports Guide* contains information about configuring IM Director and using the IM Director Administrator™ Web-based administration tool. This document is available in PDF format.

Chapter 1

Planning

This chapter contains the following sections:

- “Estimating the Size of the Database” on page 7
- “Connection Types” on page 9
- “Network Configuration Scenarios” on page 14

Estimating the Size of the Database

This section contains information you can use as a guideline to determine the amount of IM Director database storage you need. This process can be complex because it involves variables such as:

- Message length and frequency
- Whether HTML tags are used in disclaimer messages
- Whether employees use special text formatting, emoticons, and so on in their instant messages
- The length of time your enterprise is required to archive conversations
- Whether your database software uses data compression

As a general rule, you can assume that each user requires 0.5 MB of database space each month.

Alternatively, you can use the following formula to estimate the amount of database storage that is required to store one day’s worth of IM conversations. To estimate the monthly storage requirement, multiply the result by 30.

$$\frac{\text{BytesUser} * \text{AvgNumber} * \text{Seats} * (1 - \text{Compression})}{\text{BytesMB}}$$

The parameters used in the preceding formula are described in the following table.

Note: A conversation consists of one or more messages.

Parameter	Description
AvgDur	The average duration of an IM conversation (in seconds).
AvgNumber	The average number of IM conversations each employee has in a day.
BytesConv	The number of bytes in each conversation: $60 * \text{AvgDur} * \text{MsgRate} * \text{MsgLength} + 150$ This formula accounts for overhead such as special text formatting.
BytesMB	The number of bytes per megabyte (MB): 1,048,576
BytesUser	The number of bytes used by each user each day: $\text{BytesConv} * \text{AvgNumber}$
Compression	The compression ratio your database software uses. Assume 5%.
MsgLength	The average number of characters in a message.
MsgRate	The average number of messages that are sent each second during an IM conversation. Assume 0.1 (one message round trip every 10 seconds).
Seats	The number of employees in the enterprise whose conversations are being audited.

Connection Types

There are two models by which IM networks connect to IM Director.

Proxy model. IM Director acts as a proxy server between the IM clients and the IM networks. This means IM clients connect to the IM Director server instead of directly to the IM networks. The proxy model is supported on the AIM, Yahoo! Messenger, and MSN Messenger networks.

Enterprise IM connector model. Communication between enterprise IM clients and IM Director is achieved through a FaceTime Connector or another component installed on an enterprise IM server. The enterprise IM connector model is supported on the IBM Lotus Sametime, Microsoft Exchange, and Yahoo! Messenger Enterprise Edition networks.

Proxy Model

In the proxy model, IM Director is deployed as a proxy server that sits between IM clients and the proxy-supported IM networks. You can force IM clients to connect to IM Director as a proxy server using two methods:

SOCKS proxy. IM clients are configured to point to IM Director as a SOCKS proxy server.

DNS routing. Your DNS server is configured to redirect messages from IM clients to IM Director. The default IM client settings are used and no additional client configuration is necessary.

FaceTime recommends the SOCKS proxy method because in conjunction with enforcing rules at the firewall, this method ensures that all IM traffic passes through IM Director and can be logged. By contrast, with the DNS routing method, there is some exposure for IM clients to connect to the IM networks directly and circumvent IM Director.

Problems with the DNS routing method include:

- The MSN Messenger client caches the IP address used in the last successful connection. If possible, it uses that IP address to make the next connection instead of using the default host name configured for redirection on the DNS server (for example, *messenger.msn.com*).
- All DNS servers in the enterprise must be configured for DNS routing. If a single DNS server is not configured properly, a direct connection is possible.
- If a DNS server that is outside the control of your enterprise is able to resolve the domain name for the IM client, a direct connection is possible.

For example, an employee uses Virtual Private Networking (VPN) to access the corporate network remotely. If the DNS server for the

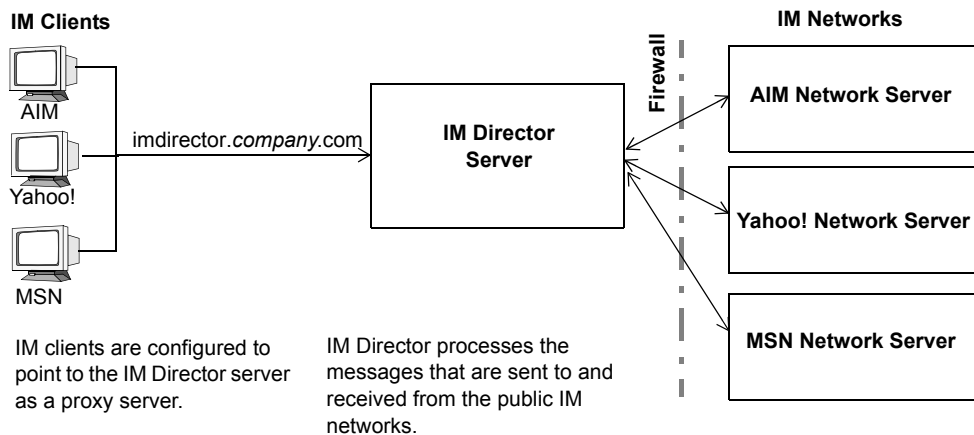
employee's Internet Service Provider (ISP) responds to a connection request from the employee's IM client before the corporate DNS server responds to it, a direct connection is possible.

- In the AIM client, an employee could bypass DNS routing by simply specifying the IP address of the AIM network server instead of **login.oscar.aol.com**.

The following sections describe the two proxy model connection types in more detail.

SOCKS Proxy

When IM Director is deployed as a SOCKS proxy, IM clients must be configured to explicitly point to IM Director as a proxy server instead of connecting directly to the IM networks. The IM client configuration can be done manually or automatically using a script. For more information, see [“Configuring IM Clients for SOCKS Proxy Connection” on page 36](#).



It is highly recommended that you create rules on the firewall to provide additional protection against IM clients connecting directly to the public IM networks. These rules prevent employees who reconfigure their IM clients to *not* point to IM Director from being able to connect to the public IM networks.

For more information and a list of domain names and IP addresses that should be blocked, see [“Creating Rules on Firewalls and Corporate Proxy Servers” on page 36](#).

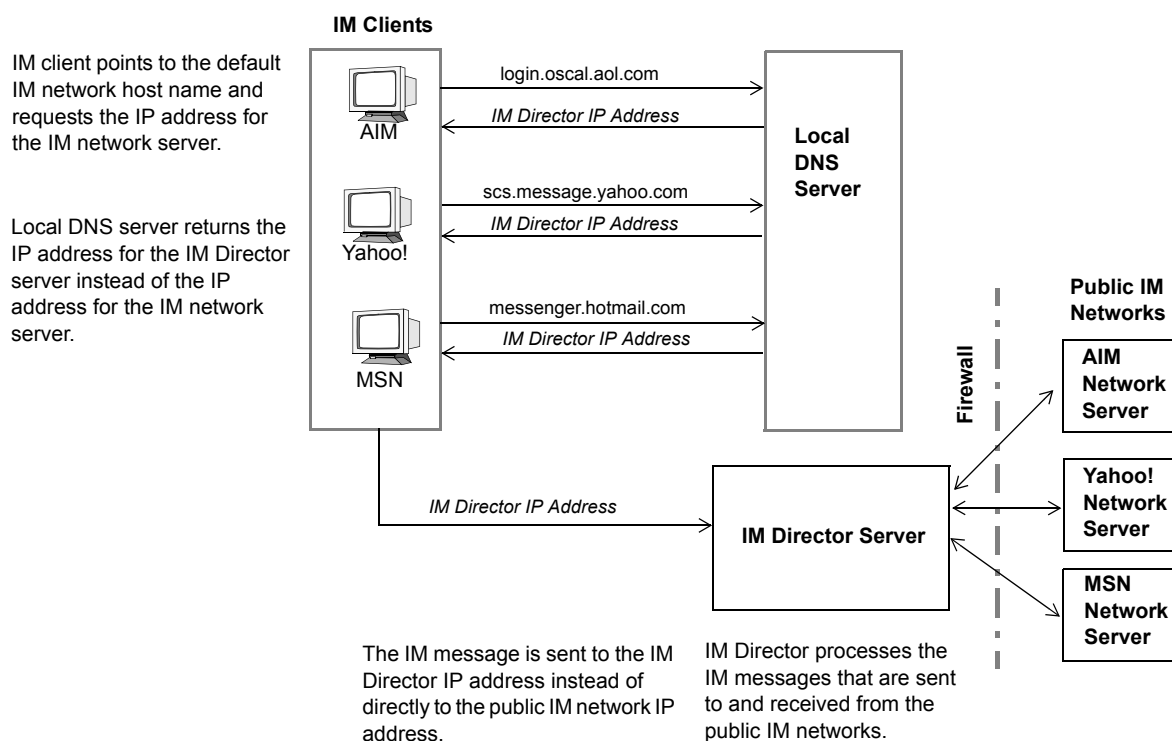
DNS Routing

DNS routing requires changes to your DNS server, but IM clients use their default settings and require no additional configuration.

By default, IM clients point to the host name of the default IM network server. Your local DNS server translates host names to IP addresses so messages can be routed to their destinations.

You must configure the DNS server to translate the host name of the IM network server to the IP address of the IM Director server, *not* to the IP address of the IM network server. This forces messages that would normally be sent directly to the IM networks to be redirected to the IM Director server. For information about configuring your DNS server, see [“Configuring Your DNS Server for DNS Routing” on page 47](#).

Rules must be created on the firewall to block direct connections from IM clients to the public IM networks. For a list of domain names and IP addresses that should be blocked, see [“Creating Rules on Firewalls and Corporate Proxy Servers” on page 36](#).



Note: The server on which IM Director is installed must use a valid DNS server, not the DNS server used by the IM clients.

Standard Enterprise IM Connectors

This section describes how the enterprise IM connector model can be used to integrate IM Director with standard enterprise IM networks.

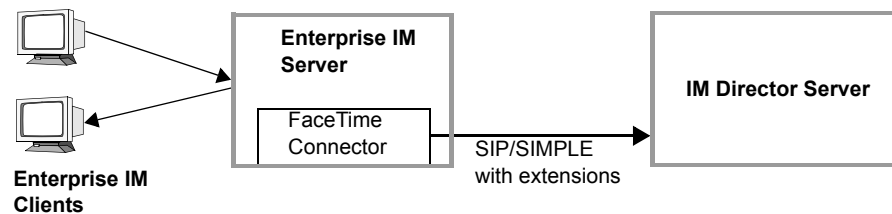
Note: For instructions on installing and configuring the connectors, see [“Installing Enterprise IM Connectors”](#) on page 27.

The integration process involves installing one of the following FaceTime Connectors on your enterprise IM server:

- IBM Lotus Sametime Connector
- Microsoft Exchange 2000 Connector

The connector obtains events and related data from the enterprise server, and interprets and translates them for IM Director. The connector communicates with IM Director using SIP/SIMPLE protocol with FaceTime extensions.

The following diagram illustrates the components that make up the integration.



Note: IM Director and enterprise IM services must be installed on separate servers.

Message Buffering

The connectors use Microsoft Message Queuing (MSMQ), which buffers messages exchanged among enterprise IM users. The use of a queue provides enhanced enterprise connector scalability and the ability to recover messages when the connection to IM Director is lost or the process in which the connector is running is stopped. When the messages stored in the queue are delivered to IM Director, they are recorded with their real timestamps.

Connectors can use *express mode* or *recoverable mode* to store messages in the MSMQ queue.

- In express mode, MSMQ stores the messages in a memory-mapped file, but the messages are not flushed to disk. The messages in the queue can normally be recovered if the connection to IM Director is lost or if the process in which the connector is running is stopped. However, in the event of a catastrophic failure (such as the MSMQ service stopping or the enterprise IM server restarting), all messages are lost. Express mode is recommended and is used by default.

- In recoverable mode, MSMQ stores the messages in a memory-mapped file, but flushes the changed file segments to disk. This means that messages in the queue can be recovered even in the event of a catastrophic failure (such as the MSMQ service stopping or the enterprise IM server restarting). While recoverable mode offers higher reliability, it adversely affects performance.

MSMQ must be installed on the enterprise IM server before the connector is installed, and the account in which the connector is running must have full permission to create and view queues. If you do not want to use MSMQ, you must disable it.

Note: MSMQ functions as described regardless of whether the connector runs in the strict or relaxed logging mode.

Logging Modes

Connectors can run in strict logging mode, in which users cannot send or receive messages when the connection to IM Director is lost, or in relaxed logging mode, in which users can continue to send and receive messages when the connection to IM Director is lost.

For instructions on setting the logging mode, see [“Installing Enterprise IM Connectors”](#) starting on [page 27](#).

Distributed Environments

In distributed environments with multiple enterprise servers:

- The Microsoft Exchange 2000 Connector must be installed on each Exchange 2000 IM home server.
- The Sametime Connector must be installed on each Sametime server.

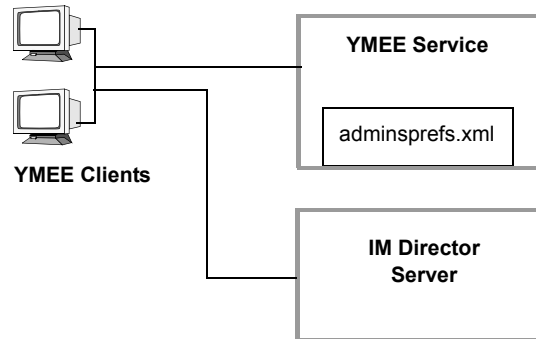
Yahoo! Messenger Enterprise Edition Connector

Yahoo! Messenger Enterprise Edition (YMEE) clients send messages directly to IM Director to be centrally archived and managed. The integration process for YMEE involves specifying configuration parameters in the `centralarchive` element of the `adminprefs.xml` file. This file is part of the YMEE Service, which is a series of servlets installed on a corporate server.

The configuration parameters include the domain name and port number of the IM Director server, and whether strict logging should be enforced. When YMEE users sign on, their YMEE clients request the latest version of the `adminprefs.xml` file from the YMEE Service.

Note: The enforcement of strict logging is required.

The following diagram illustrates the components that make up the integration.



For instructions on installing the YMEE Service and configuring the `adminsprefs.xml` file, see [“Yahoo! Messenger Enterprise Edition Installation” on page 33](#) and the *Yahoo! Messenger Enterprise Edition Installation and Administration Guide*.

Network Configuration Scenarios

This section provides high-level descriptions of the following IM Director configurations.

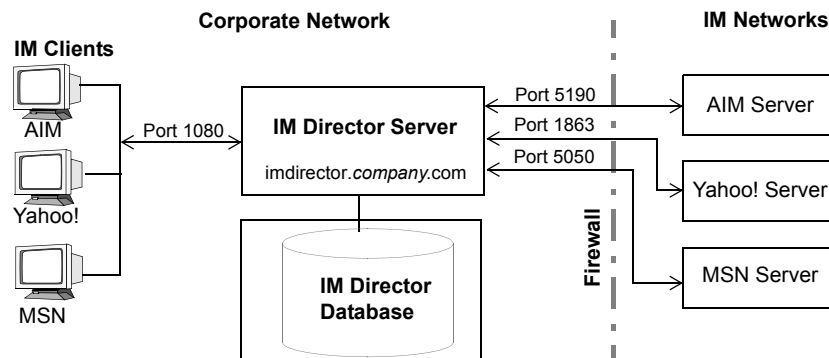
- [“Standard Configuration with No Corporate Proxy Server” on page 15](#)
- [“Standard Configuration with Corporate Proxy Server” on page 15](#)
- [“Failover Configuration” on page 16](#)
- [“High-Availability Configuration” on page 17](#)
- [“Distributed IM Director Servers Connected to Replicated Regional Databases” on page 18](#)

Note: This section is intended to be an overview. It provides guidelines but not step-by-step implementation instructions. Configurations may vary widely based on the third-party software you use and your corporate network environment. The FaceTime Professional Services organization provides fee-based implementation services to help meet your requirements for application and database redundancy, failover, and high availability. Your FaceTime account executive can assist you with the purchase of these services.

Standard Configuration with No Corporate Proxy Server

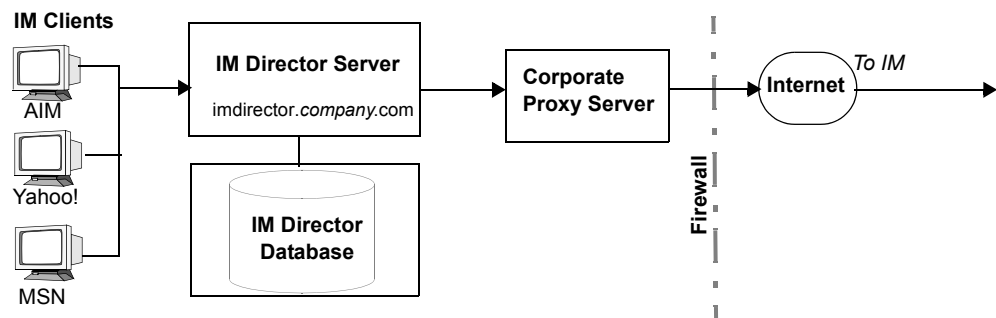
In the standard configuration with no corporate proxy server, IM clients are configured to connect to IM Director as a SOCKS proxy server. No corporate proxy server is used, so IM Director connects directly to the public IM networks through the firewall.

Note: All connections from the IM Director server are established outbound through the firewall. No inbound firewall access is required.



Standard Configuration with Corporate Proxy Server

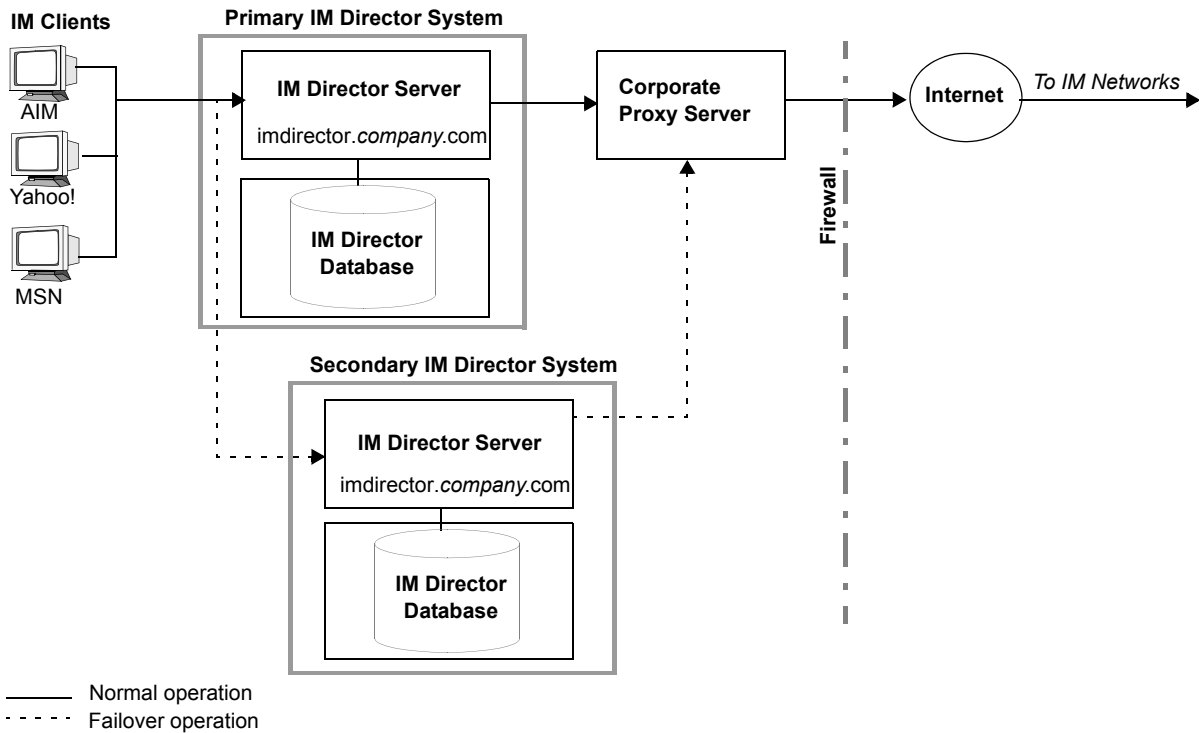
In the standard configuration with a corporate proxy server, IM clients are configured to connect to IM Director as a SOCKS proxy server. A SOCKS or HTTPS corporate proxy server sits between IM Director and the firewall. The corporate proxy server goes through the firewall to establish outbound connections to the IM networks on behalf of IM Director.



Failover Configuration

The failover configuration includes two independent IM Director systems that are managed by server cluster software for redundancy. This configuration offers maximum uptime with no requirement for database synchronization.

In normal operation, the primary system is active, and the secondary system is passive. If the cluster server software detects failure in the primary system, all users are briefly disconnected from the IM networks while the secondary system becomes active. New connections and automatic attempts by IM clients to reconnect are handled by the secondary system.



High-Availability Configuration

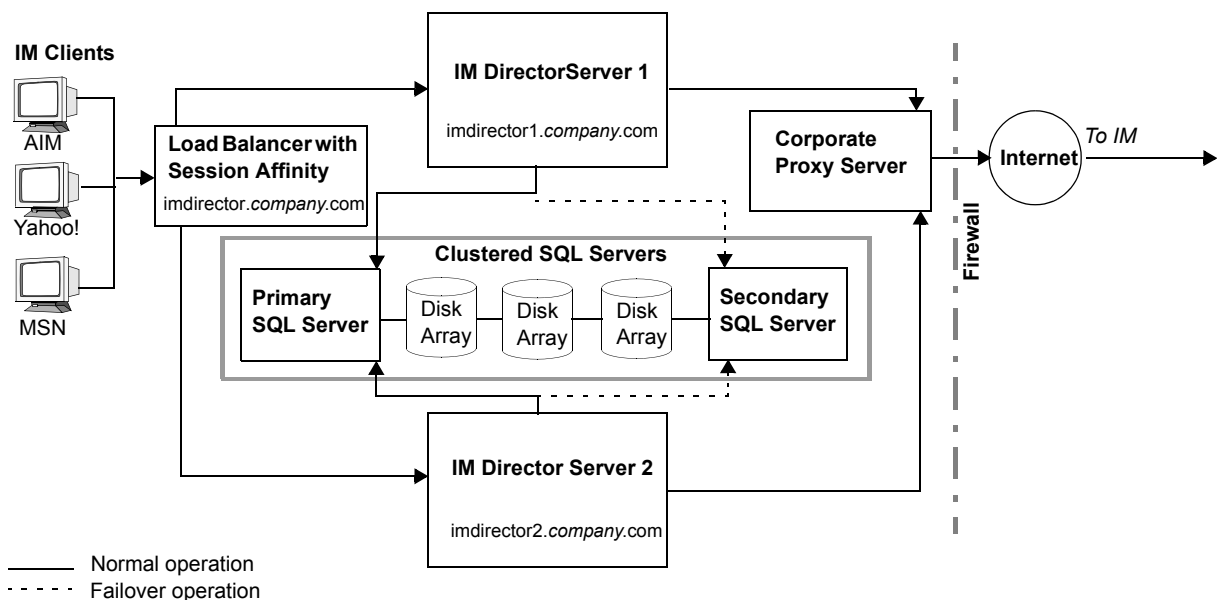
Note: The high availability configuration is required in configurations that include multiple IM Director servers deployed with the SOCKS proxy server connection type. When using the DNS routing connection type, session affinity is not required on load balancers, and DNS round-robin can be used instead of load balancers.

The high availability configuration provides redundancy and scalability because it includes the following components:

- Clustered SQL servers that provide redundancy if a database failure occurs
- Disk arrays that prevent data loss resulting from disk failure, offer higher data processing speed and volume, and ensure that data is synchronized
- Load balancer with session affinity that provides scalability by distributing traffic to multiple IM Director servers based on their availability

Additional IM Director servers and databases can be added to make this configuration even more scalable.

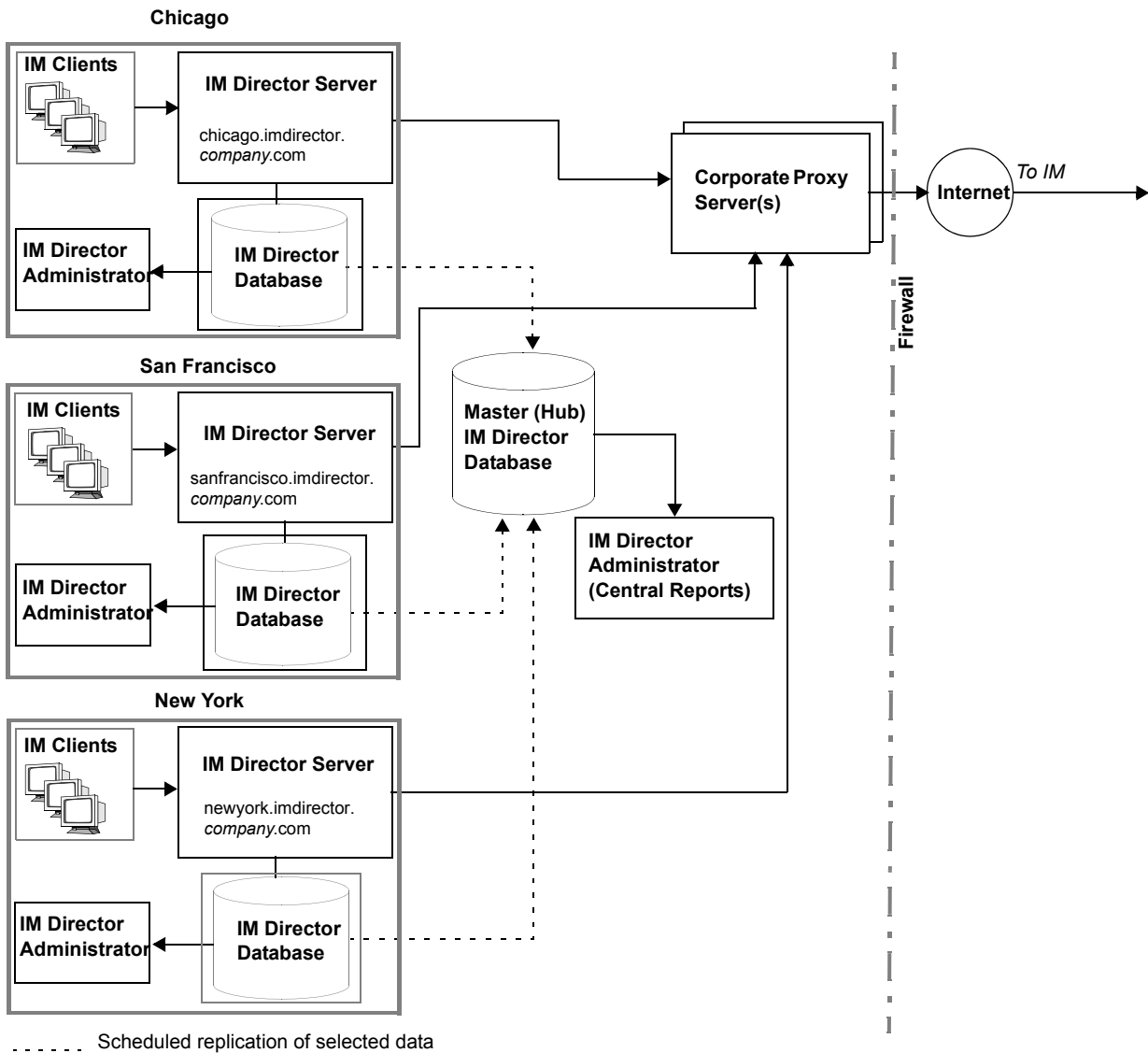
Note: In a load balancing scenario, all IM Director servers must be able to communicate with each other to enable functionality such as local routing.



Distributed IM Director Servers Connected to Replicated Regional Databases

This configuration includes IM Director servers that are located in different cities and that use local databases. On a scheduled basis, selected data from the local databases is copied, or *replicated*, to a master database so the local and master databases can remain synchronized. Replication can be achieved using inherent database replication methods, the log shipping method, or third party replication products.

You use regional IM Director Administrators to perform employee and server administration and view regional reports. You can use a centralized IM Director Administrator to view global reports that include replicated data.



Chapter 2

Installation

This chapter contains the following sections:

- “Before You Begin” on page 19
- “Upgrading from IM Director 1.0.x” on page 21
- “Installing IM Director 1.1” on page 23
- “Installing Enterprise IM Connectors” on page 27
- “Handling Installation Problems” on page 33

Before You Begin

Check that your system meets the minimum hardware, software, and database requirements listed below before installing and using IM Director.

Hardware Requirements	Notes
Minimum <i>IM Director Server</i> <ul style="list-style-type: none">■ Pentium III 800 MHz CPU or higher■ 512 MB of RAM■ 10 GB of available hard disk space	<p>It is recommended that you install IM Director and its database on separate servers.</p> <p>You must install IM Director and enterprise IM services (for example, Microsoft Exchange 2000) on separate servers.</p>

<p><i>Enterprise IM Server</i></p> <ul style="list-style-type: none"> ■ 10 GB of hard disk space beyond what is needed for normal system use 	<p>The additional space is required for connectors that use Microsoft Message Queuing (MSMQ). MSMQ buffers messages exchanged among enterprise IM users. This provides enhanced scalability and the ability to recover messages when the connection to IM Director is lost or when the process in which the enterprise IM connector is running is stopped.</p> <p>The amount of space that is needed varies depending on the number of messages that are sent and the length of the downtime.</p>
<p>Recommended</p> <p><i>IM Director Server:</i></p> <ul style="list-style-type: none"> ■ Pentium 4 2 GHz CPU or higher ■ 1 GB of RAM ■ 10 GB of available hard disk space 	<p>These requirements are recommended for high-end deployments.</p>
<p><i>Database Server:</i></p> <ul style="list-style-type: none"> ■ Pentium 4 2 GHz CPU or higher ■ 1 GB of RAM ■ 40 GB or higher of available hard disk space with SCSI drives 	<p>See “Estimating the Size of the Database” on page 7 for information about estimating the amount of disk space you need depending on the size of your deployment.</p>
Software Requirements	
<p><i>IM Director Server</i></p> <ul style="list-style-type: none"> ■ Microsoft Windows 2000 Server ■ Microsoft SQL Server 2000 Standard Edition ■ Microsoft Internet Explorer 5.5 or later 	<p>All software must have the latest service packs and patches.</p>
<p><i>Enterprise IM Server</i></p> <p>Microsoft Message Queuing (MSMQ)</p>	
<p><i>Corporate Directory</i></p> <ul style="list-style-type: none"> ■ Microsoft Active Directory for Windows 2000 ■ Sun ONE Directory Server 5.1 ■ Lotus Domino Directory 5.0.11 	

Database Requirements	
See “Estimating the Size of the Database” on page 7 for information about estimating the size of the database.	<p>The database must be configured to use SQL Server authentication mode. For more information, see step 3 on page 23.</p> <p>The information listed in the Microsoft SQL Server Parameters row of the table on page 25 must be available.</p>

Upgrading from IM Director 1.0.x

You do not need to remove the existing application before you upgrade to IM Director 1.1.

Note: The amount of time needed to upgrade is proportional to the amount of data in the existing database.

To upgrade to Director 1.1 from IM Director 1.0.x:

1. Back up the existing database.

CAUTION: Backing up the existing database is critical because it allows you to restore your data if the upgrade fails.

2. If your database is being replicated, you must remove the replication before upgrading to IM Director 1.1. Remove the replication in the following order:
 - a. Delete the subscriptions.
 - b. Delete the publications.
 - c. Disable publishing. To do so, run the following script in MS Query Analyzer:


```
EXEC sp_removedbreplication 'yourdatabasename'
```

where *yourdatabasename* is the name of the database for which replication is being removed.

Note: Please refer to Microsoft SQL Server documentation for detailed instructions.
3. Download the IM Director 1.1 setup .exe file from the URL that you obtained from a FaceTime representative or from a FaceTime-authorized Web site. This is a self-extracting file that contains the IM Director distribution.
4. Close all application programs that are currently running.
5. Restart the IM Director server.

6. Double-click the .exe file you downloaded.
7. A message prompts you to confirm that you want to upgrade to IM Director 1.1. Click **Upgrade** and then follow the instructions on your screen.

Note: You can use your existing license key if you do not require support for additional networks or users.

8. When the upgrade is finished, the Setup Complete screen appears. Click **View Readme** to read important information about the IM Director release, and then click **Finish**.
9. The IM Director Administrator Login page appears. Enter a valid user name and password.



IM Director Administrator Login

Username:

Password:

© Copyright 2001-2003, FaceTime Communications, Inc. All rights reserved.

Note: If are unable to log in to IM Director Administrator because you forgot the default sysadmin password, you can reset it as described in the *IM Director Administration and Reports Guide*.

10. Verify that IM Director has started as a Windows service.
 - a. Click the **Start** button on the Windows taskbar, select **Settings**, and then click **Control Panel**.
 - b. In the **Control Panel** window, double-click the **Administrative Tools** icon and then double-click **Services**.
 - c. If the status of the IMDirector service is not **Started**, right-click **IMDirector** and then click **Start**.

Installing IM Director 1.1

To install IM Director:

1. Create an empty database and make sure the database parameters listed in the Microsoft SQL Server 2000 Parameters row of the table in step 8 are available for use later in the installation.
2. *(Optional)* For custom database installations, it is recommended that you populate the database before installing IM Director. (If you do not use this option, the database is automatically populated during the IM Director installation.)

To populate the database before installing IM Director, perform the following steps:

- a. Download the DBInitialization.zip file from the same location from which you obtained the setup .exe file.
- b. Open the .zip file and extract one of the following scripts:
 - IM Director 1.x-SQL-xxx.sql if you want the database to support single-byte characters.
 - IM Director 1.x-SQL-UNICODE-xxx.sql if you want the database to support Unicode characters.

Single-byte is an 8-bit ASCII character set that supports Latin-based languages. Unicode is a 16-bit character set that supports most languages but uses twice as much space in the database.

Note: Using Unicode characters could adversely affect performance. It is recommended that you use Unicode only if employees in your company use non-Latin based languages in their IM clients.

- c. Run the script in MS Query Analyzer to populate the database.
3. Make sure that SQL Server authentication is specified as an authentication mode for connecting to the database.
 - a. In the left pane of the SQL Server Enterprise Manager window, right-click the icon for the database server. Click **Properties** and then click the **Security** tab.
 - b. Select **Authentication**→**SQL Server and Windows**.
 - c. Restart SQL Server.

4. Download the IM Director setup .exe file from the URL that you obtained from a FaceTime representative or from a FaceTime-authorized Web site. This is a self-extracting file that contains the IM Director distribution.
5. Close all application programs that are currently running.
6. Restart the server on which IM Director is being installed.
7. Double-click the .exe file you downloaded.
8. Complete the FaceTime IM Director Setup Wizard as described in the following table.

On this screen	Do this
Welcome	<p>Click Next.</p> <p>If the setup wizard detects that IM Director 1.1 is already installed, a dialog box appears that provides the two options described below.</p> <p>To reinstall IM Director 1.1 over the existing IM Director 1.1:</p> <ol style="list-style-type: none"> 1. Select Reinstall IM Director and then click OK. 2. On the wizard screen, click Finish to complete the reinstallation. <p>To remove and then reinstall the existing IM Director 1.1:</p> <ol style="list-style-type: none"> 1. Select Remove IM Director and then click OK. 2. Click OK in the confirmation dialog box that appears. 3. In the next screen, click Finish to complete the removal process. 4. Double-click the setup .exe file again to restart the setup wizard. 5. Click Next in the Welcome screen that appears.
User Information	<ol style="list-style-type: none"> 1. If necessary, modify the User Name and Company Name. 2. Enter the License Key you were provided, and then click Next. <p>Note: The license key is case-sensitive.</p>
Destination Folder	Click Next to accept the default installation file folder or Browse to select another folder.
Program Folder	Click Next to accept the default program file folder. To specify a different folder, enter or select the folder name.
Choose Character Code	<p>Select Single Byte if you want the database to support single-byte characters, or Unicode if you want the database to support Unicode characters.</p> <p>Single byte is an 8-bit ASCII character set that supports Latin-based languages. Unicode is a 16-bit character set that supports most languages but uses twice as much space in the database.</p> <p>Note: Using Unicode characters could adversely affect performance. It is recommended that you select Unicode only if employees in your company use non-Latin based languages in their IM clients.</p>

On this screen	Do this
Microsoft SQL Server 2000 Parameters	<p>1. Specify the following information:</p> <p>Host Name—Enter the fully-qualified domain name of the computer on which the database is installed. For example, <i>dbserver.company.com</i>.</p> <p>Database Name—Enter the name of the database. Do not include spaces in the name.</p> <p>Instance Name (Optional)—If you are running more than one instance of the database on the same server, enter the name of the instance you want IM Director to use.</p> <p>User Name—Enter a user name with privileges to create, modify, and delete tables; insert, read, modify, and delete data; and create, modify, execute, and delete stored procedures. (CAUTION: If the database was created manually prior to installation, the same user name used to create the database must be specified here.)</p> <p>Password—Enter the password used to access the database.</p> <p>2. Click Next. The setup wizard tests the database connection. If the test fails, a message appears. Click OK to return to the Microsoft SQL Server 2000 Parameters screen and correct the database settings.</p>
Start Copying Files	Verify the information you specified in the previous screens, and then click Next to continue.
Setup Status	<p>This screen shows the progress of the installation. Click Cancel if you want to end the installation.</p> <p>If the setup wizard detects that the database you specified during installation is already being used, you are prompted whether you want to continue with the installation. Click Yes to continue or No to terminate the installation.</p>
Setup Complete	Select View Readme File to read important information about the IM Director release, and then click Finish .

3. If this is a new installation, the Set System Administrator Password page automatically appears. Enter a password of at least 6 characters. Type the password again to confirm it and then click **Submit**.


Set System Administrator Password

System Administrator Password	
Username:	<input type="text" value="sysadmin"/>
Set Password:	<input type="password"/>
Confirm Password:	<input type="password"/>

Note: This is the password used to log in as the default system administrator. The username and employee ID for the default system administrator is

sysadmin and the last name is **Administrator**. Additional system administrators with other usernames can be added to IM Director later.

4. If this is a reinstallation, the IM Director Administrator Login page appears. Enter a valid user name and password.



IM Director Administrator Login

Username:

Password:

© Copyright 2001-2003, FaceTime Communications, Inc. All rights reserved.

Note: If are unable to log in to IM Director Administrator because you forgot the default sysadmin password, you can reset it as described in the *IM Director Administration and Reports Guide*.

5. Verify that IM Director has started as a Windows service.
 - a. Click the **Start** button on the Windows taskbar, select **Settings**, and then click **Control Panel**.
 - b. In the Control Panel window, double-click the **Administrative Tools** icon and then double-click **Services**.
 - c. If the status of the IMDirector service is not **Started**, right-click **IM Director** and then click **Start**.
6. If you are using IM Director in an enterprise IM environment, install the appropriate enterprise IM connector on the enterprise IM server. For instructions, see [“Installing Enterprise IM Connectors”](#) later in this chapter.

Installing Enterprise IM Connectors

This section describes how to install and configure the components required to integrate IM Director in an enterprise IM network.

- If you are integrating IM Director with the **IBM Lotus Sametime** or **Microsoft Exchange 2000** networks, you need to install additional software (known as a *connector*) after IM Director is installed. This connector must be installed on the enterprise IM server. The connector obtains events from the enterprise IM server and interprets and translates them for IM Director.

The connectors use Microsoft Message Queuing (MSMQ), which buffers messages exchanged among enterprise IM users. This provides enhanced scalability and the ability to recover messages when the connection to IM Director is lost or when the process in which the enterprise IM connector is running is stopped. MSMQ must be installed on the enterprise IM server before the connector is installed, and the account in which the connector is running must have full permission to create and view queues. If you do not want to use MSMQ, you must disable it as described in each installation topic in this section.

Note 1: For more information about MSMQ, see [“Message Buffering” on page 12](#).

Note 2: MSMQ functions as described regardless of whether the connector runs in strict or relaxed logging mode.

- If you are integrating IM Director with the **Yahoo! Messenger Enterprise Edition (YMEE)** network, you need to specify parameters in the `adminprefs.xml` file. This file is part of the YMEE Service, which is a series of servlets installed on a corporate server.

The YMEE clients connect directly to IM Director using parameters specified in the `adminprefs.xml` file.

This section contains the following topics:

- [IBM Lotus Sametime Connector Installation](#)
- [Microsoft Exchange 2000 Connector Installation](#)
- [Yahoo! Messenger Enterprise Edition Installation](#)

Note: For information about the enterprise IM connector model configurations, see [“Standard Enterprise IM Connectors” on page 12](#) and [“Yahoo! Messenger Enterprise Edition Connector” on page 13](#).

IBM Lotus Sametime Connector Installation

Note: The same program is used to install the connector for both the IM Auditor and IM Director products. Therefore, installation wizard screens, file names, and directory paths may refer to the IM Auditor product.

To install the Lotus Sametime Connector:

1. Be sure that Microsoft Message Queuing (MSMQ) is installed on the Sametime server and that the account in which the connector will run has full permission to create and view queues.

Note: If you do not want to use MSMQ, you can disable it as described in step 6.

2. Download the IMA_ST-Connect .exe file from the URL you obtained from a FaceTime representative or from a FaceTime-authorized Web site.

Be sure to download the file to the Sametime server.

3. Double-click the .exe file and follow the instructions on the installation wizard screens.

- The directory specified on the Change Destination Location screen must be the directory in which the Sametime application was installed. If this is not the case, click the **Browse** button and then navigate to the directory in which the Sametime application was installed.

- On the IM Auditor Server Info screen:

Host field—Enter the domain name or IP address of the IM Director server.

Port field—Enter the SIP/SIMPLE port number on the IM Director server that listens for events from the Sametime network. The value in the **Port** field should match the value of the **Listening Port** field on the Enterprise IM Access page of IM Director Administrator.

Note: During the installation, if you receive a message that a file is in use, stop the STChatLog service and click **Retry** on the installation wizard screen. When the installation is complete, restart the STChatLog service.

4. If you are installing the Sametime Connector on a Sametime 3.0 server, perform the following steps:
 - a. Stop the Sametime 3.0 server.
 - b. Using a Lotus Notes client, open the Sametime Configuration database (stconfig.nsf) on the Sametime server.
 - c. In the right pane, double-click the date associated with the CommunityServices document.
 - d. Double-click the CommunityServices document so it can be edited.
 - e. For the **Chat Logging Flag** parameter, select **strict** for strict mode or **relax** for relaxed mode. (With strict mode, employees cannot send or receive messages when the connection to IM Director is lost.)
 - f. For the **Capture Service Type** parameter, enter 0x1000.
 - g. Save and then close the CommunityServices document.
 - h. Restart the Sametime 3.0 server.
5. By default, **ft_queue** is the name of the MSMQ queue that is created for the connector. To change the value, add the following line to the FaceTime section of the sametime.ini file (located in the root Sametime directory):

MSMQ_QUEUE_NAME=newname

where *newname* is the name of the queue.

6. If you do not want to use MSMQ, add the following line to the FaceTime section of the sametime.ini file:

USE_MSMQ=false

7. By default, the connector runs in strict mode, in which no messages can be sent if the connection to IM Director is lost. To have the connector run in relaxed mode, change the value of the **VPCONFIG_SNATCH_SRV_TYPE** entry in the Sametime section of the sametime.ini file to any value other than **0x1000**.

Note: This step only applies to the Sametime 2.5 server. See step 4 for Sametime 3.0 server instructions.

8. In some Sametime configurations, the employee ID takes the form of the distinguished name (DN) for the corporate directory. If the DN includes the unique ID (UID) attribute, and you want to extract the UID

and pass it to IM Director as the employee ID, add the following line to the FaceTime section of the `sametime.ini` file:

EXTRACT_UID=true

An example of the original ID and the extracted ID is shown in the following table.

Sametime ID	IM Director ID
uid=a250,ou=people,dc=company,dc=com	a250

Note: If a UID is not found in the Sametime ID, the full Sametime ID is passed to IM Director.

- To complement load balancing, add the following line to the FaceTime section of the `sametime.ini` file:

DISCONNECT_ON_FAILURE=true

When this option is enabled, the connector disconnects from an IM Director server after sequential failures (such as time-outs or service unavailable responses). It then reconnects to the load balancer so the load balancer can attempt to route the new connection to another IM Director server.

- By default, the connector uses MSMQ in express mode. In express mode, messages can be recovered when the connection to IM Director is lost or when the process in which the connector is running is stopped. For added recovery, configure the connector to use MSMQ in recoverable mode. In recoverable mode, messages can be recovered even in the event of a catastrophic failure (such as the MSMQ service stopping or the enterprise IM server restarting). To configure the connector to use recoverable mode, add the following line to the FaceTime section of the `sametime.ini` file:

MSMQ_RECOVERABLE=true

CAUTION: Using recoverable mode adversely affects performance.

Microsoft Exchange 2000 Connector Installation

Note 1: During the installation, an Internet Server Application Programming Interface (ISAPI) filter is installed on the Exchange 2000 server for Internet Information Services (IIS).

Note 2: The same program is used to install the connector for both the IM Auditor and IM Director products. Therefore, installation wizard screens, file names, and directory paths may refer to the IM Auditor product.

To install the Microsoft Exchange 2000 Connector:

1. Be sure that Microsoft Message Queuing (MSMQ) is installed on the Exchange 2000 server and that the account in which the connector will run has full permission to create and view queues.

Note: If you do not want to use MSMQ, you can disable it as described in step 7.

2. Download the IMA_E2K-Connect .exe file from the URL you obtained from a FaceTime representative or from a FaceTime-authorized Web site.

Be sure to download the file to the Exchange 2000 IM server.

3. Double-click the .exe file and follow the instructions on the installation wizard screens.
4. In the **Host** field of the IM Auditor Server Info screen, enter the domain name or IP address of the IM Director server. In the **Port** field, enter the SIP/SIMPLE port number on the IM Director server that listens for events from the Exchange 2000 network. The value in the **Port** field should match the value of the **Listening Port** field on the Enterprise IM Access page of IM Director Administrator.
5. If this is a distributed environment with multiple Exchange 2000 servers, repeat this procedure for each Exchange 2000 IM home server.
6. By default, **ft_queue** is the name of the MSMQ queue that is created for the connector. To change the name, create a registry key as described in the following steps:
 - a. Select **Run** on the Windows **Start** menu. The **Run** dialog box appears.
 - b. Type **regedit** and then click **OK**.
 - c. Navigate to the following location:

HKEY_LOCAL_MACHINE\SOFTWARE\FaceTime\FaceTimeIMAuditor
E2K\Init

- d. On the **Edit** menu, select **New**, and then click **String Value**.

The new registry key appears in the right pane of the Registry Editor window.

- e. Under **Name**, type **queuename** over the default name.
 - f. Double-click **queuename**. The **Edit String** dialog box appears.
 - g. Type the new name in the **Value data** box.
 - h. Click **OK**.
7. If you do not want to use MSMQ, create a registry key as described in step 6, except under **Name**, type **usemsmq** and in the **Value data** box, type **false**.
 8. By default, the connector runs in strict mode, in which no messages can be sent if the connection to IM Director is lost. To have the connector run in relaxed mode, create a registry key as described in step 6, except under **Name**, type **strict_logging** and in the **Value data** box, type **false**.
 9. By default, Exchange 2000 IDs are in the form of a URL. To change the ID to an email address format (for example, *user@host*), create a registry key as described in step 6, except under **Name**, type **transform_ids**, and in the **Value data** box, type **true**.
 10. To complement load balancing, create a registry key as described in step 6, except under **Name**, type **disc_on_failure**, and in the **Value data** box, type **true**.

When this option is enabled, the connector disconnects from an IM Director server after sequential failures (such as time-outs or service unavailable responses). It then reconnects to the load balancer so the load balancer can attempt to route the new connection to another IM Director server.

11. By default, the connector uses MSMQ in express mode. In express mode, messages can be recovered when the connection to IM Director is lost or when the process in which the connector is running is stopped. For added recovery, configure the connector to use MSMQ in recoverable mode. In recoverable mode, messages can be recovered even in the event of a catastrophic failure (such as the MSMQ service stopping or the enterprise IM server restarting). To configure the connector to use recoverable mode, create a registry key as described in

step 6, except under **Name**, type **msmq_recoverable**, and in the **Value data** box, type **true**.

CAUTION: Using recoverable mode adversely affects performance.

Note: Log files are created in the directory in which the connector is installed.

Yahoo! Messenger Enterprise Edition Installation

The adminprefs.xml file is a configuration file that is installed on the corporate server during the installation of the YMEE Service.

Note: For instructions on installing the YMEE Service and configuring the adminprefs.xml file, see the *Yahoo! Messenger Enterprise Edition Installation and Administration Guide*.

To configure the adminprefs.xml file for IM Director operation:

1. Specify the following parameters in the `centralarchive` element:
 - **netlogfailok**—Set this parameter to **no** to enforce strict logging.
 - **server**—Specify the host name and port of the IM Director server.
2. Specify the following parameter in the `customization` element:
 - **exitonlogout enable**—Set this parameter to **yes** to force clients to completely exit when employees disconnect from them.

Handling Installation Problems

This section describes how to handle problems you may encounter while installing IM Director.

IM Director Does Not Start

Problem IM Director does not start.

Reason The following are probable reasons for the problem.

- The SQL Server service (MSSQLServer) is not running. This service must be running before IM Director services can start.
- The IMDirector service is not running.
- The minimum system requirements have not been met.

Action To correct the problem:

- Check the log files. The following is the default path to this folder:
C:\Program Files\FaceTime\IM Director\logs

- Restart the SQL Server service or the database server. The IM Director services will continuously attempt to connect to the database and start when the SQL server service is running again.
- Check that the IMDirector service is running. For instructions, see the *IM Director Administration and Reports Guide*.
- Check that your system meets the minimum hardware, software, and database requirements. For a list of the requirements, see [“Before You Begin” on page 19](#).

Unable to Connect to the Database

Problem Installation program is unable to connect to the database.

Reason The following are probable reasons for the problem.

- Database settings specified in the installation wizard are not valid.
- Database server is not configured in your DNS server.
- The database is not configured to accept both Windows and SQL server authentication modes.

Action To correct the problem:

- Verify that the settings specified in the Microsoft SQL Server 2000 Parameters screen of the installation wizard are valid.
- Make sure the database server is configured in your DNS server and you can ping the database server using its domain name.
- Make sure that SQL Server authentication is specified as an authentication mode for connecting to the database. For instructions, see [page 23](#).

Chapter 3

Deployment

This chapter includes the following sections:

- “Deployment Overview” on page 35
- “Creating Rules on Firewalls and Corporate Proxy Servers” on page 36
- “Configuring IM Clients for SOCKS Proxy Connection” on page 36
- “Configuring Your DNS Server for DNS Routing” on page 47
- “Configuring Windows 2000 for Large User Sites” on page 52
- “Deploying IM Director Administrator” on page 53

Deployment Overview

Before you install and configure IM Director, perform the following tasks.

1. Set up your firewall and corporate proxy server to allow direct connections between IM Director and the IM networks and block direct connections between IM clients and the IM networks. For detailed information, see [“Creating Rules on Firewalls and Corporate Proxy Servers” on page 36](#).
2. Configure the server on which you will install IM Director with a static IP address.
3. Make the server on which you will install IM Director accessible to the IM client computers over the network.
4. If you are using the proxy model, do one of the following:
 - Configure IM clients to point to IM Director as a proxy server. For instructions, see [“Configuring IM Clients for SOCKS Proxy Connection” on page 36](#).

- Configure your DNS server to redirect IM client messages to the IM Director server. For instructions, see [“Configuring Your DNS Server for DNS Routing”](#) on page 47.

Note: For an overview of the proxy model and how it differs from the enterprise IM connector model, see [“Connection Types”](#) on page 9.

Creating Rules on Firewalls and Corporate Proxy Servers

Public IM network destinations are the domain names or IP addresses and ports that public IM networks use to listen for IM messages. To implement IM Director in your network and control direct access to the public IM networks, create rules on your firewall and corporate proxy server (if used) to do the following:

- Allow direct connections between IM Director and public IM network destinations.
- Block direct connections between IM clients and public IM network destinations.

The list of public IM destinations change frequently. The most current list of destinations is provided in the *Controlling Access to IM* document, available from FaceTime Customer Support.

Configuring IM Clients for SOCKS Proxy Connection

When you deploy IM Director as a SOCKS proxy server, IM clients are configured to connect to IM Director as a proxy server instead of connecting directly to the IM networks.

This deployment involves the following steps:

- Configuring IM clients to point to IM Director as a proxy server. This section describes how to do this configuration.
- Blocking destinations at the firewall that IM clients could use to connect directly to the public IM networks. For a list of the destinations to block, please contact FaceTime Customer Support.

Note: If the *DNS Client* Windows service is disabled on employees' computers, it is recommended that AIM and MSN Messenger clients use SOCKS5 protocol and that Yahoo! Messenger clients use SOCKS4 protocol to connect to IM Director.

Manual Configuration

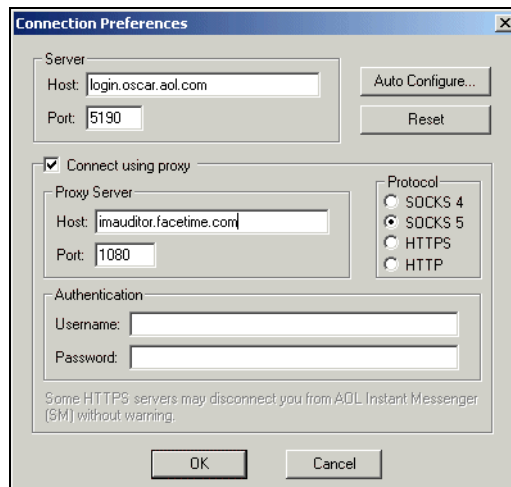
This section describes how to manually configure the public IM clients to connect to IM Director as a proxy server.

Note: The settings shown in this section may vary depending on the IM client version.

AOL Instant Messenger (AIM)

To configure proxy settings in the AIM client:

1. In the AIM client, click the **My AIM** menu.
2. Select **Edit Options** and then click **Edit Preferences**.
3. Under **Category**, click **Sign On/Off**, and then click the **Connection** button. The **Connection Preferences** dialog box appears.



4. Under **Server**, use the default values of **login.oscar.aol.com** in the **Host** field and **5190** in the **Port** field.

Note: If you are using an HTTPS corporate proxy server between IM Director and the AIM network, in the NetworkConnectors table, the value of **loginPort** field needs to be changed to **443**. This change needs to be made in the AIM SOCKS4/5 and AIM DNS Redirect rows.

5. Under **Protocol**, select either **SOCKS4** or **SOCKS5**.

Note: It is recommended that you select **SOCKS5** if you are using a corporate proxy server that uses the HTTPS protocol.

6. Select the **Connect Using Proxy** check box.
7. In the **Host** field under **Proxy Server**, enter the domain name or IP address of the server on which IM Director is installed. Depending on

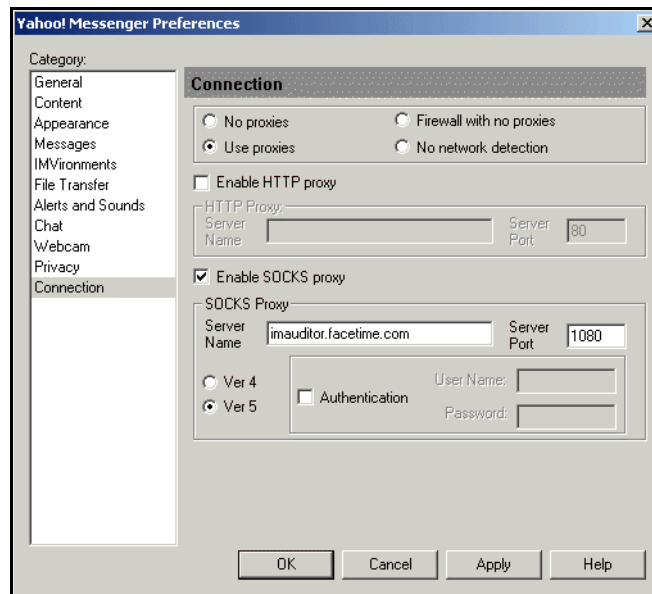
your environment, you might need to enter the IP address instead of the domain name.

8. In the **Port** field under **Proxy Server**, enter the port number used to connect the AIM client to the IM Director server. This is the port number that was specified in the **SOCKS Proxy Connection/Listening Port** field on the Public IM Access page of IM Director.
9. If you are using SOCKS5 authentication, enter the user name and password under **Authentication**.
10. Click **OK**.

Yahoo! Messenger

To configure proxy settings in the Yahoo! Messenger client:

1. In the Yahoo! Messenger client, click the **Login** menu.
2. Click **Preferences**. The Yahoo! Messenger Preferences window appears.



3. Click **Connection** in the **Category** list on the left side of the window.
4. Click **Use proxies**.
5. Select **Enable SOCKS proxy**.
6. In the **Server Name** field under **SOCKS Proxy**, enter the domain name or IP address of the server on which IM Director is installed.

Depending on your environment, you might need to enter the IP address instead of the domain name.

7. In the **Port** field under **SOCKS Proxy**, enter the port number used to connect the Yahoo! Messenger client to the IM Director server. This is the port number that was specified in the **SOCKS Proxy Connection/Listening Port** field on the Public IM Access page of IM Director Administrator.
8. Select **Ver 4** if you are using SOCKS version 4. Select **Ver 5** if you are using SOCKS version 5.

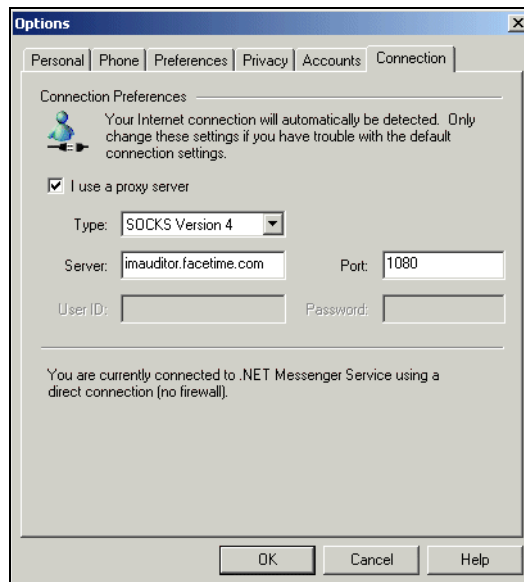
Note: It is recommended that you use SOCKS version 5 if you are using a corporate proxy server that uses the HTTPS protocol.

9. If you are using SOCKS5 authentication, select the **Authentication** check box and then enter the user name and password.
10. Click **OK**.

MSN Messenger

To configure proxy settings in the MSN Messenger client:

1. In the MSN Messenger client, click the **Tools** menu and then click **Options**. The Options dialog box appears.



2. Click the **Connections** tab.
3. Select the **I use a proxy server** check box.

- In the **Type** scroll-down list box, select either **SOCKS Version 4** or **SOCKS Version 5**.

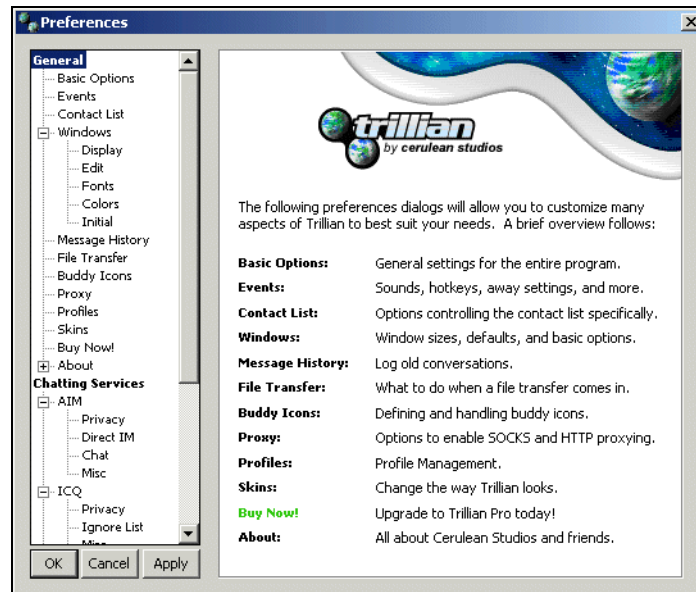
Note: It is recommended that you select **SOCKS Version 5** if you are using a corporate proxy server that uses the HTTPS protocol.

- In the **Server** field, enter the domain name or IP address of the server on which IM Director is installed. Depending on your environment, you might need to enter the IP address instead of the domain name.
- In the **Port** field, enter the port number used to connect the MSN Messenger client to the IM Director server. This is the port number that was specified in the **SOCKS Proxy Connection/Listening Port** field on the Public IM Access page of IM Director Administrator.
- If you are using SOCKS5 authentication, enter the **User ID** and **Password**.
- Click **OK**.

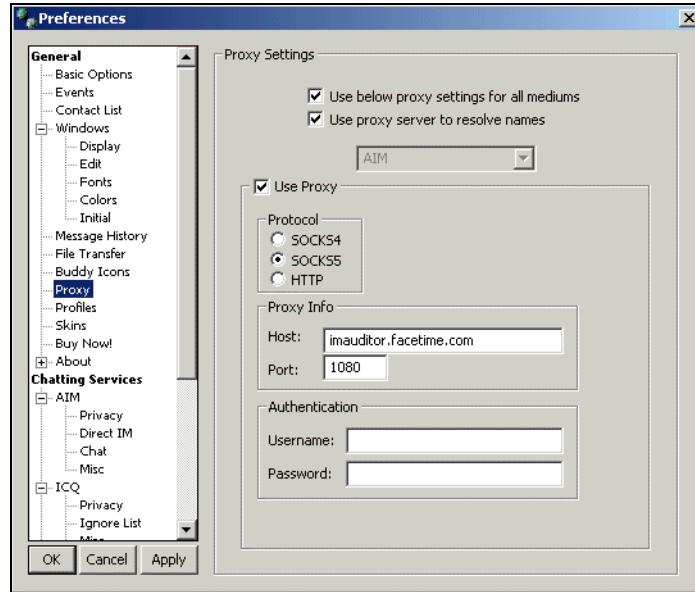
Trillian

To configure proxy settings in the Trillian client:

- From the main menu, click **Preferences**. The Preferences window appears.



- Click **Proxy** under **General** in the left pane of the window. The screen shown in the following illustration appears.



3. Select the **Use Proxy** check box.
4. Under **Protocol**, select either **SOCKS4** or **SOCKS5**.

Note: It is recommended that you select **SOCKS Version 5** if you are using a corporate proxy server that uses the HTTPS protocol.

5. In the **Host** field under **Proxy Info**, enter the domain name or IP address of the server on which IM Director is installed. Depending on your environment, you might need to enter the IP address instead of the domain name.
6. In the **Port** field under **Proxy Info**, enter the port number used to connect the Trillian client to the IM Director server. This is the port number that was specified in the **SOCKS Proxy Connection/Listening Port** fields on the Public IM Access page of IM Director Administrator.
7. If you are using SOCKS5 authentication, enter the user name and password under **Authentication**.
8. Click **OK**.

Automatic Configuration

This section describes how to automatically configure the AIM, Yahoo! and MSN Messenger IM clients to connect to IM Director as a proxy server. This is an advanced option and should be performed by system administrators only.

To automatically configure proxy settings, perform the following steps:

1. Create registration entry (.reg) and batch (.bat) files as described in this section.
2. Add a logon script to your domain controller. The way you do this depends on your operating system and network environment. This section provides an example of how to do this using the Active Directory service in a Windows 2000 domain.

The batch file is run when an employee logs in to Windows. It configures the registry on the employee's computer with the values specified in the registration entry files.

Note: Changing registry settings incorrectly can cause serious problems that could require the operating system to be reinstalled. This procedure should be performed by system administrators only.

Creating Registration Entry and Batch Files

Using a text editor, create the following files:

- A registration entry file for each public IM client and each SOCKS version that employees use to connect to IM Director.

For example, if employees use AIM and Yahoo! Messenger clients and can connect to IM Director using the SOCKS4 or SOCKS5 protocol, you need to create four registration entry files: one for AIM/SOCKS4, one for AIM/SOCKS5, one for Yahoo! Messenger/SOCKS4, and one for Yahoo! Messenger/SOCKS5.

- A batch file that includes a line for each registration entry file you created.

The following table contains a list of the files you might need to create and the text they should contain.

Note: Replace "IM DIRECTOR SERVER HERE" with the name of the server on which IM Director is installed. The name of the server must be enclosed in quotation marks.

File Name/Description	File Content
aim.socks4.reg Registration entry file for AOL Instant Messenger (AIM) clients using SOCKS4 protocol to connect to IM Director.	[HKEY_CURRENT_USER\Software\America Online\AOL Instant Messenger (TM)\CurrentVersion\Proxy] "Enabled"=dword:00000001 "Protocol"="SOCKS4" "Host"="IM DIRECTOR SERVER NAME HERE" "Port"=dword:00000438 "Username"="" "Password"="" "Resolve"=dword:00000000
aim.socks5.reg Registration entry file for AOL Instant Messenger (AIM) clients using SOCKS5 protocol to connect to IM Director.	[HKEY_CURRENT_USER\Software\America Online\AOL Instant Messenger (TM)\CurrentVersion\Proxy] "Enabled"=dword:00000001 "Protocol"="SOCKS5" "Host"="IM DIRECTOR SERVER NAME HERE" "Port"=dword:00000438 "Username"="" "Password"="" "Resolve"=dword:00000000
yahoo.socks4.reg Registration entry file for Yahoo! Messenger clients using SOCKS4 protocol to connect to IM Director.	[HKEY_CURRENT_USER\Software\Yahoo\Pager] "Connection State"=dword:00000002 "Socks Port"=dword:00000438 "Socks Version"=dword:00000004 "SOCKS Enabled"=dword:00000001 "Socks Server"="IM DIRECTOR SERVER NAME HERE"
yahoo.socks5.reg Registration entry file for Yahoo! Messenger clients using SOCKS5 protocol to connect to IM Director.	[HKEY_CURRENT_USER\Software\Yahoo\Pager] "Connection State"=dword:00000002 "Socks Port"=dword:00000438 "Socks Version"=dword:00000005 "SOCKS Enabled"=dword:00000001 "Socks Server"="IM DIRECTOR SERVER NAME HERE"
msn5.socks4.reg Registration Entry file for Microsoft Messenger 5.0 clients using SOCKS4 protocol to connect to IM Director.	[HKEY_CURRENT_USER\Software\Microsoft\MessengerService] "ProxyState"=hex:ff,ff,ff,ff "ProxyType"=hex:01,00,00,00 "SOCKS4Server"="IM DIRECTOR SERVER NAME HERE" "SOCKS4Port"=hex:38,04,00,00
msn5.socks5.reg Registration entry file for Microsoft Messenger 5.0 clients using SOCKS5 protocol to connect to IM Director.	[HKEY_CURRENT_USER\Software\Microsoft\MessengerService] "ProxyState"=hex:ff,ff,ff,ff "ProxyType"=hex:02,00,00,00 "SOCKS5Server"="IM DIRECTOR SERVER NAME HERE" "SOCKS5Port"=hex:38,04,00,00

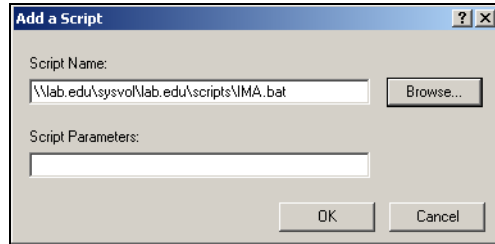
File Name/Description	File Content
msn6.socks4.reg Registration Entry file for Microsoft Messenger 6.0 clients using SOCKS4 protocol to connect to IM Director.	<pre>[HKEY_CURRENT_USER\Software\Microsoft\MSNMessenger] "ProxyState"=hex:ff,ff,ff,ff "ProxyType"=hex:01,00,00,00 "SOCKS4Server"="IM DIRECTOR SERVER NAME HERE" "SOCKS4Port"=hex:38,04,00,00</pre>
msn6.socks5.reg Registration entry file for Microsoft Messenger 6.0 clients using SOCKS5 protocol to connect to IM Director.	<pre>[HKEY_CURRENT_USER\Software\Microsoft\MSNMessenger] "ProxyState"=hex:ff,ff,ff,ff "ProxyType"=hex:02,00,00,00 "SOCKS5Server"="IM DIRECTOR SERVER NAME HERE" "SOCKS5Port"=hex:38,04,00,00</pre>
IMD.bat Batch file used to run the registration entry files.	<pre>regedit /s aim.socks4.reg regedit /s aim.socks5.reg regedit /s msn5.socks4.reg regedit /s msn5.socks5.reg regedit /s msn6.socks4.reg regedit /s msn6.socks5.reg regedit /s yahoo.socks4.reg regedit /s yahoo.socks5.reg</pre> <p>Note: There should be one line in the batch file for each registration entry file you created.</p>

Adding the Logon Script to Your Domain Controller

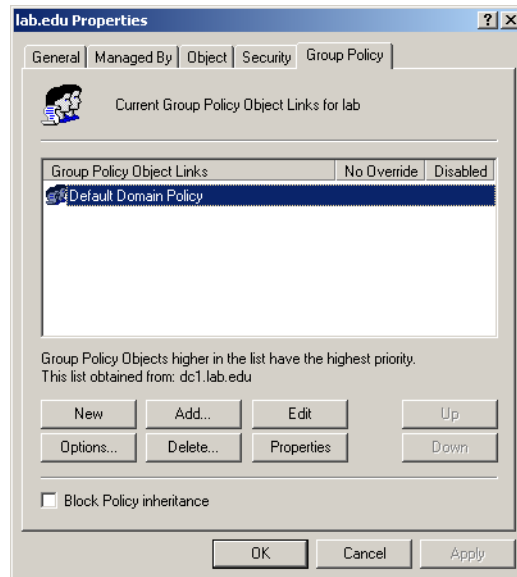
This section describes how to add a logon script to your domain controller in an Active Directory service in the Windows 2000 domain. The procedure you follow may differ depending on your operating system and network environment.

To add the logon script to your domain controller:

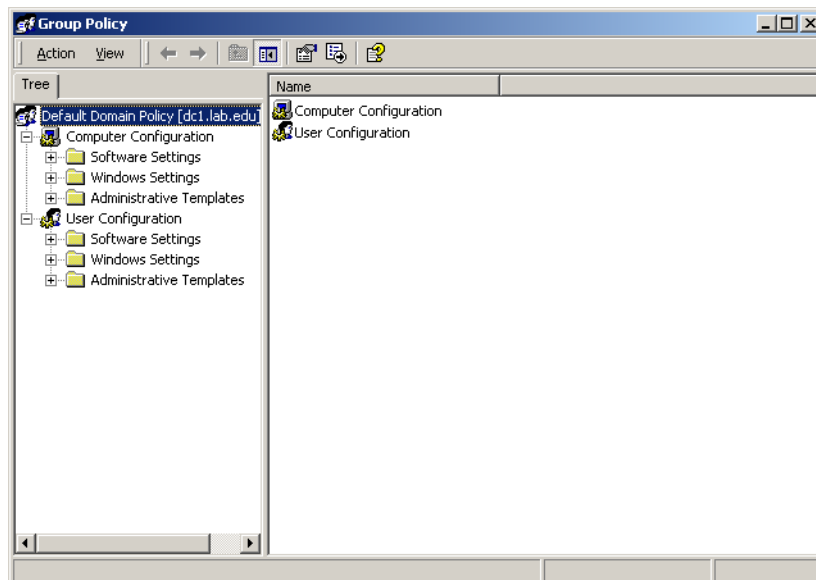
1. Place the IMD.bat file and the .reg files you created in the NETLOGON shared directory. This directory is usually on the domain controller (the NT server that handles NT services for security).
2. On the Windows **Start** menu, select **Start**→**Programs**→**Administrative Tools**→**Active Directory Users and Computers**. The Active Directory Users and Computers window appears.




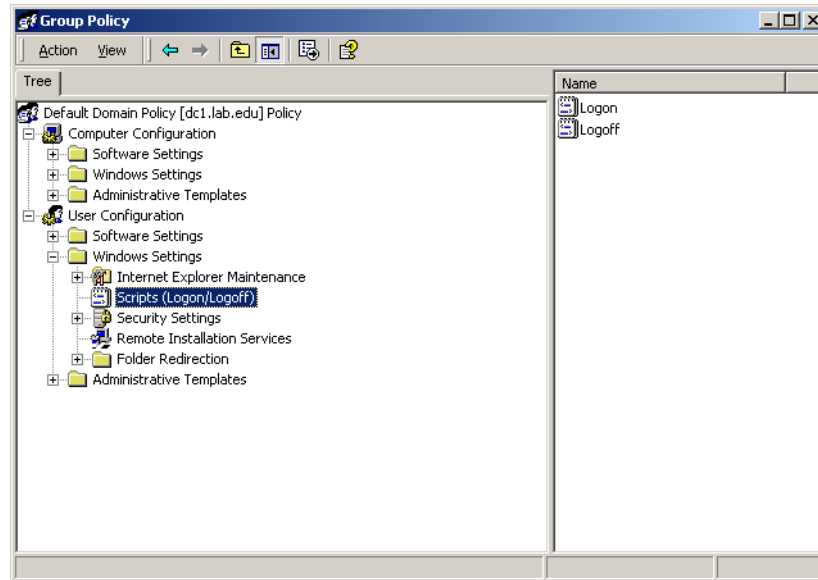
3. Right-click your root domain and then click **Properties**. The group **Properties** dialog box appears.



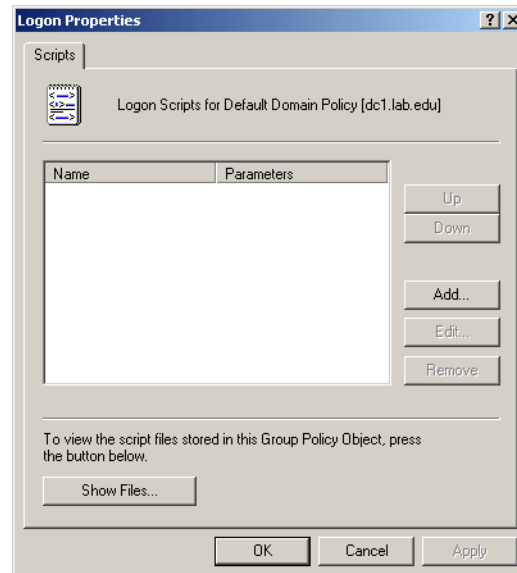
4. Click the **Group Policy** tab. The group policy appears.



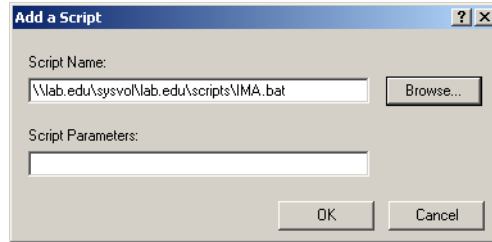
5. Under **User Configuration**, click  to expand the **Windows Settings**.



6. Under **Windows Settings**, click **Scripts (Logon/Logoff)**, and in the pane to the right, double-click **Logon**.



7. In the **Logon Properties** dialog box, click **Add**. Navigate to where you placed the IMD.bat file, select it, and then click **Open**. The file appears in the **Add a Script** dialog box.



8. Click **OK** to close the **Add a Script** dialog box.
9. Click **OK** to close the **Logon Properties** dialog box.

Configuring Your DNS Server for DNS Routing

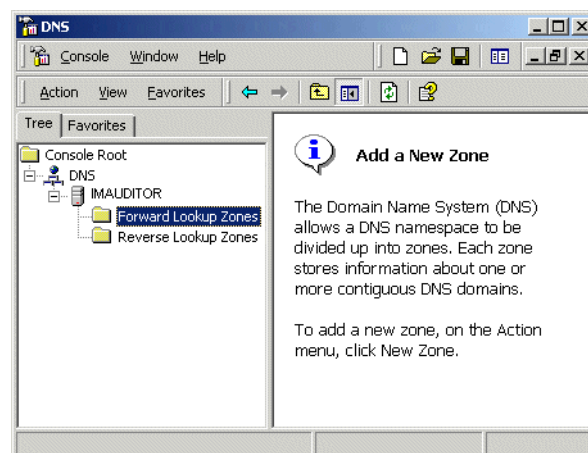
DNS routing is one way to prevent employees from directly connecting to IM networks for which IM Director is a proxy. It involves the following steps:

- Blocking destinations at the firewall that IM clients could use to connect directly to the IM network server. For a list of the destinations to block, please contact FaceTime Customer Support.
- Configuring your DNS server to resolve the default domain names for the IM network server to the IP address for the IM Director server. This section describes how to do this configuration.

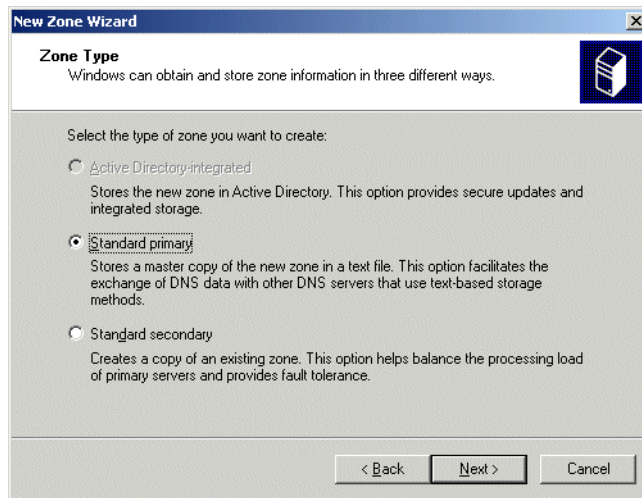
CAUTION: Be sure that the server on which you install IM Director points to a valid DNS server, not to the one you are configuring in this section. Otherwise, an infinite loop results in which no messages are routed to the IM networks.

To configure your DNS server for DNS routing:

1. On the Windows **Start** menu, select **Start**→**Programs**→**Administrative Tools**→**DNS**. The DNS window appears.

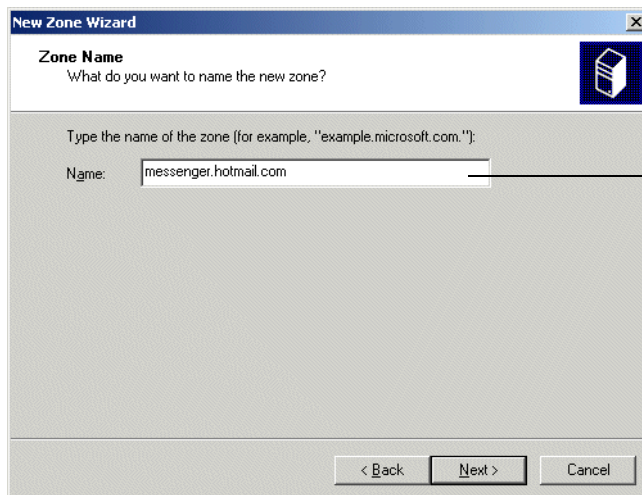


2. Right-click **Forward Lookup Zones**, and then click **New Zone**.
3. Select **Standard primary** and then click **Next**.



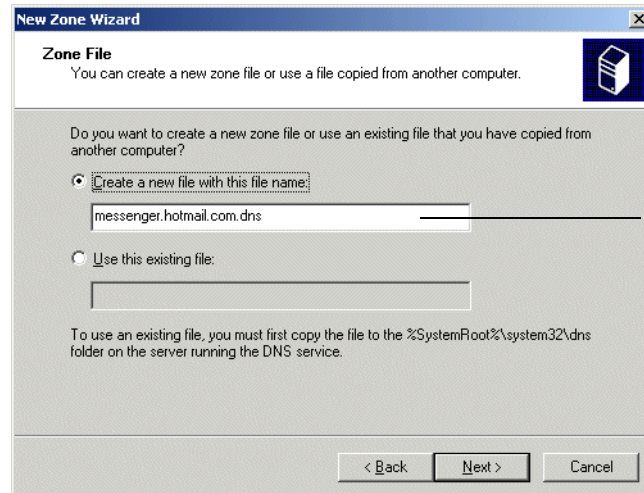
4. Type one of the following domain names in the **Name** box and then click **Next**.

Domain Name	IM Network
login.oscar.aol.com	AOL Instant Messenger (AIM)
scs.msg.yahoo.com	Yahoo! Messenger
messenger.hotmail.com	MSN Messenger

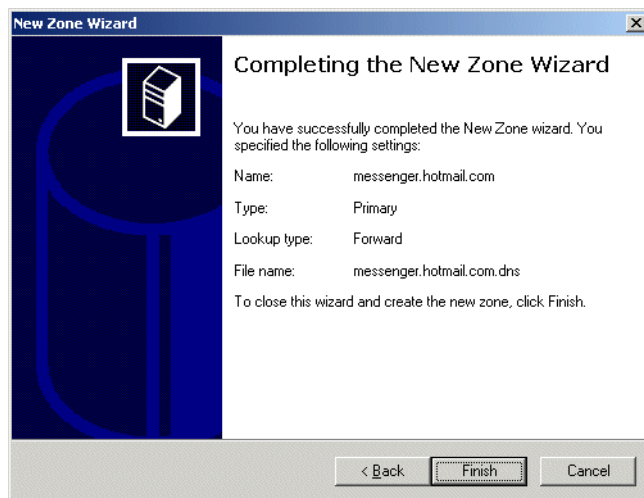


Type the default domain name that clients use to connect to the IM network server.

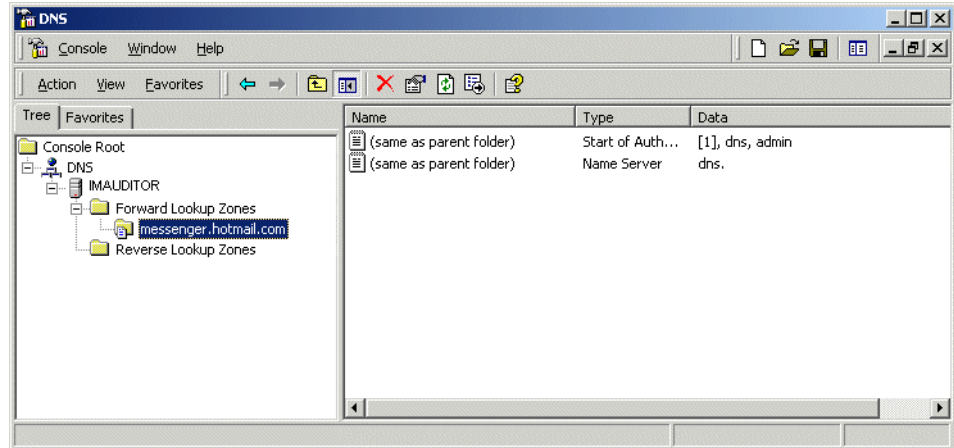
5. The Zone File screen appears with default settings as shown in the following illustration. Click **Next** to accept the settings.



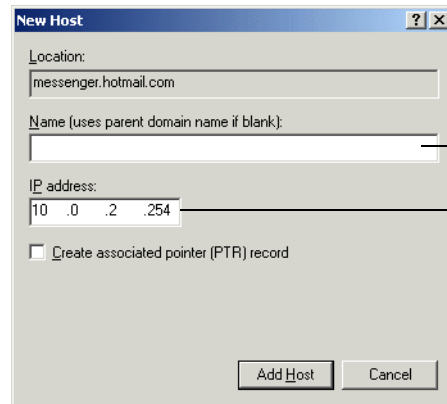
6. Click **Next** to finish creating the zone.
7. Information about the new zone is displayed in the screen that appears. If you need to change the information, click **Back**. If the information is correct, click **Next**.



8. The new zone you created appears in the left pane of the DNS window. Right-click the zone and then click **New Host**.



9. Type the IP address of the IM Director server in the **IP address** box, and then click **Add Host**. If you have more than one IM Director server, repeat steps 8 and 9 for each server.



Leave the **Name** box empty.

Type the IP address of the IM Director server.

10. Repeat steps 2 through 9 for each relevant IM network server.
11. If you have more than one IM Director server and want to use round robin, make sure that it is enabled:
 - a. Right-click the server in the DNS Manager window, and then click **Properties**.
 - b. Click the **Advanced** tab, and make sure **Enable round robin** is selected.

Testing DNS Routing

To test DNS routing:

1. Type one of the following commands at the command prompt and then press ENTER.

On a computer running	Type this command
AIM client	<code>nslookup login.oscar.aol.com</code>
Yahoo! Messenger client	<code>nslookup scs.msg.yahoo.com</code>
MSN Messenger client	<code>nslookup messenger.hotmail.com</code>

The IP address of the IM Director server should be displayed as a result.

2. Repeat this procedure for each IM network server you configured for DNS routing.

Configuring Windows 2000 for Large User Sites

This section describes how you can handle a large number of IM Director users on a single server running Windows 2000.

If you expect to have more than 1000 employees simultaneously signed on to IM networks, create a `MaxUserPort` registry key. This key defines the highest port number that TCP (Transmission Control Protocol) can assign when the system receives a request for an available port.

To determine the value of this registry key, use the following information.

Recommended Value: $(\text{Number of Users} \times 3) + 2000$

Valid Range of Values: 5000—65,534

Default Value: 5000

To create the registry key and change the value:

1. Select **Run** on the Windows **Start** menu. The **Run** dialog box appears.
2. Type **regedit** and then click **OK**.
3. Navigate to the following location:

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

4. On the **Edit** menu, select **New**, and then click **DWORD Value**.

The new registry key appears in the right pane of the Registry Editor window.

5. Under **Name**, type **MaxUserPort** over the default name.
6. Double-click **MaxUserPort**. The **Edit DWORD Value** dialog box appears.
7. Click **Decimal**.
8. In the **Value data** box, type the value you calculated using the Recommended Value formula shown above.
9. Click **OK**.

Deploying IM Director Administrator

Employees can be instructed to log in to IM Director Administrator by typing the URL of the IM Director Administrator Login page in the address bar of their Web browsers:

`http://hostname:8090/imd`

where *hostname* is the name of the server on which IM Director was installed.

Alternatively, during the deployment process, you can do one of the following:

- Create another URL or a link on your company's intranet site. Then create a file (such as an .asp or .htm file) associated with the URL or link that redirects employees' browsers to the URL of the IM Director Administrator Login page.
- Create a shortcut to the URL of the IM Director Administrator Login page and email the shortcut to employees.

Glossary

conversation

A session in which instant messages are exchanged. With AIM and Yahoo! Messenger, a conversation ends after 15 minutes of inactivity (in which no messages are sent or received). The conversation remains active for this period of time even if all participants close their chat windows. With MSN Messenger, a conversation ends after 5 minutes of inactivity or when the participants close their chat windows. In reports, the conversation end time is the time the last message in the conversation was sent. Also known as *interaction*.

corporate proxy

See *proxy server*.

DNS routing

A proxy model connection type in which messages are redirected from a DNS server to IM Director instead of sending them directly to the IM networks. See also *proxy model*. Contrast with *SOCKS proxy*.

enterprise IM connector model

A method by which enterprise IM networks connect to IM Director. In this model, communication between enterprise IM clients and IM Director is achieved through a connector that is installed on an enterprise IM server. The connector obtains events from the enterprise IM server and interprets and translates the events for IM Director. Contrast with *proxy model*.

interaction

See *conversation*.

message

A single segment of an IM conversation.

proxy model

A method by which IM networks connect to IM Director. In this model, IM Director acts as a proxy server between IM clients and the IM networks. This means that IM clients connect to IM Director instead of directly to the IM networks. The proxy model can be deployed using a SOCKS proxy or DNS routing connection type. See also *SOCKS proxy*, *DNS routing*.

proxy server

A server that monitors and captures activity and provides network security. When IM Director is deployed as a proxy server, IM clients are configured to connect to IM Director as a proxy server instead of connecting directly to the IM networks. A corporate proxy server can sit between the IM Director server and the Internet. The corporate proxy server can use SOCKS or HTTPS protocol and includes rules and policies for additional network security.

relaxed logging

In the enterprise IM connector model, a mode of logging in which users can send and receive messages when the connection to IM Director is lost.

SOCKS proxy

A proxy model connection type in which IM clients are configured to point directly to IM Director as a SOCKS proxy server. See also *proxy model*, *proxy server*. Contrast with *DNS routing*.

strict logging

In the enterprise IM connector model, a mode of logging in which users cannot send and receive messages when the connection to IM Director is lost.

Index

C

- cluster server software 16
- clustered SQL servers 17
- configurations 14
 - distributed with replicated regional databases 18
 - failover 16
 - high availability 17
 - standard with corporate proxy server 15
 - standard with no corporate proxy server 15
- connection types 9
- corporate proxy server
 - overview 15
 - rules 36

D

- database
 - estimating size 7
 - instances 25
 - removing replication for upgrades 21
 - replication 18
 - requirements 21
 - settings 25
 - synchronization 18
- DNS round-robin 17
- DNS routing 11
 - configuring DNS server 47
 - network configuration 11
 - testing 51
- DNS server, configuring for DNS routing 47

E

- enterprise IM network connectors 9
 - distributed environments 13
 - IBM Lotus Sametime 12, 28
 - installing 27
 - logging modes 13
 - message buffering 12

- Microsoft Exchange 2000 12, 31
- Yahoo! Messenger Enterprise Edition 13, 33
- Exchange 2000 Connector 31
- express mode 12, 30

F

- failover 16
- firewall rules 36

G

- global reports 18

H

- hardware requirements 19
- high-availability configuration 17

I

- IM clients, configuring for SOCKS proxy 36 to 47
- IM Director
 - deploying 35
 - installing 23
 - reinstalling 24
 - upgrading 21
- IM Director Administrator, deploying 53
- IMDirector service 26
- installing IM Director 23

L

- large user sites 52
- license key 24
- load balancers 17, 30, 32
- log shipping 18
- login page 26

M

MaxUserPort registry key [52](#)
Microsoft Exchange 2000 Connector [31](#)
Microsoft Message Queuing (MSMQ) [27](#)
minimum requirements [19](#)
MSMQ. *See* Microsoft Message Queuing (MSMQ)

N

network configurations [14](#)
 distributed with replicated regional databases
 [18](#)
 DNS routing [11](#)
 enterprise IM network connectors [12](#)
 failover [16](#)
 high availability [17](#)
 proxy model [9](#)
 SOCKS proxy [10](#)
 standard with corporate proxy server [15](#)
 standard with no corporate proxy server [15](#)

P

password
 default system administrator [25](#)
 login page [26](#)
proxy model [9](#)

R

readme file [25](#)
recoverable mode [12](#), [30](#)
redundancy [16](#)
reinstalling IM Director [24](#)
relaxed logging [13](#), [29](#), [32](#)
replication of databases [18](#)

S

Sametime Connector [28](#)
services, IMDirector [26](#)
session affinity [17](#)
single byte characters [24](#)
SOCKS proxy [10](#)
 configuring IM clients [36](#) to [47](#)
 network configuration [10](#)
software requirements [20](#)
SQL Server
 authentication mode [23](#)

 parameters [25](#)
SQL Servers, clustered [17](#)
strict logging [13](#), [29](#), [32](#)
system administrator default password [25](#)
system requirements [19](#)

T

troubleshooting [33](#)

U

Unicode characters [24](#)
upgrading IM Director [21](#)

Y

Yahoo! Messenger Enterprise Edition [13](#), [33](#)