

Novell Conferencing

1.0.1

May 1, 2008

SERVER INSTALLATION GUIDE

www.novell.com



Novell®

Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2008 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc., has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the [Novell Legal Patents Web page \(http://www.novell.com/company/legal/patents/\)](http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the [Novell Documentation Web page \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see [the Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide	7
1 System Overview	9
1.1 System Components	9
1.2 System Architecture	10
2 Installation Procedures	11
2.1 Supported Platforms	11
2.1.1 Supported Servers	11
2.1.2 Minimum Server Configuration	11
2.1.3 Supported Client Environments	11
2.2 Installation Prerequisites	12
2.2.1 Conferencing Server Requirements	12
2.2.2 Network Requirements	13
2.2.3 Firewall Requirements	13
2.2.4 DNS and Hostname Requirements	13
2.2.5 VoIP Requirements	14
2.2.6 Load Balancer Requirements	14
2.3 Security	15
2.4 Preparing for Installation	15
2.4.1 (Optional) Using ssh()	15
2.4.2 Unpacking the Files	15
2.4.3 Back Up the Directory	16
2.4.4 Installing and Configuring the NMS Boards	16
2.5 Installing the Conferencing Server	17
2.5.1 Running the Installer on SLES:	18
2.5.2 Initial Address Book Configuration (Synchronization)	22
2.6 Installing the Conferencing System Components	22
2.6.1 Initial Installation	23
2.6.2 System Administration E-mail Configuration (Optional)	23
2.6.3 Mailer Configuration (Optional)	23
2.6.4 Database Backup Configuration (Optional)	24
2.6.5 Meeting Archive and Document Sharing Repository Configurations (Optional)	24
2.6.6 Chat Audit Log Configuration (Optional)	25
2.6.7 Event Logging Configuration (Optional)	26
2.6.8 Port Forwarding (Optional)	26
2.6.9 XML Router Security	27
2.6.10 Configuring LDAP Synchronization (Optional)	27
2.6.11 Template Configuration (Optional)	29
2.7 Starting and Stopping the Cluster	29
2.8 Conferencing Administration Console	29
2.8.1 Logging In to the Administration Console	30
2.8.2 Creating Conferencing Communities	30
2.9 Conferencing Client Installation	30
2.9.1 Conferencing Client Components	30
2.9.2 Installing the Conferencing Client	30
2.9.3 Installing the Pidgin Instant Chat Client	31

3	Reconfiguring and Upgrading	33
3.1	Backing Up and Restoring the Database	33
3.1.1	Backing Up the Database	33
3.1.2	Restoring the Database	33
3.2	Reconfiguring Conferencing Hosts	34
3.3	Upgrading the Conferencing Client	34
3.4	Upgrading the Conferencing Servers	34
3.5	Starting and Stopping Conferencing Services	35
3.5.1	Starting and Stopping the Cluster	35
3.5.2	Starting and Stopping Individual Machines	35
4	Modifying Template Files	37
4.1	Modifying the Meeting Invitation Template	37
4.2	Using IF Statements	38
4.3	Modifying the Meeting Summary E-Mail Template	39
4.4	Modifying the New User Greeting E-mail Template	39
A	Configuring ssh() Key Authentication	41
A.1	Generating a Public/Private Key Pair	41
A.2	Configuring the ssh Key Agent	41
A.3	Adding the Public Key to the Root User's Set of Authorized Keys	42
B	Editing the global-config File	43
B.1	Assigning Services to Nodes	43
B.2	Configuring Web Services	45
B.3	Configuring the Mailer	45
B.4	Using Port Forwarding	45
C	Editing the dialing.xml File	47
D	Updating Meeting Invitation Web Pages	49
E	LDAP User Authentication	51
E.1	LDAP User Authentication Input File	51
E.2	Conferencing Field Names	52
E.3	Address Book Configuration (Synchronization)	52
F	Installing the NMS Board	55
F.1	Configuring H.100 Bus Termination	55
F.2	Configuring the DIP Switches	56
F.2.1	S3 DIP Switch	56
F.2.2	S2 DIP Switch	56
F.2.3	S1 DIP Switch	56
F.3	nmsconfig - Board Configuration Utility	57

About This Guide

This guide covers the installation and initial configuration of the Conferencing software. The term “Conferencing” in this guide applies to all versions of Conferencing unless otherwise noted.

This guide provides information about the following:

- ♦ System Overview
- ♦ Installation Procedures
- ♦ Reconfiguring and Upgrading
- ♦ Modifying Template Files
- ♦ Various Appendices

Audience

This guide is intended for Conferencing administrators.

Software and Documentation Version

This guide describes features in Conferencing Version 1.0.1. This is the first version of this guide.

Feedback

We want to hear your comments and suggestions about this guide and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to [www.novell.com](http://www.novell.com/documentation/feedback.html) (<http://www.novell.com/documentation/feedback.html>) and enter your comments there.

Additional Documentation

You may find more information in additional Conferencing documentation:

- ♦ Conferencing Help system
- ♦ *Conferencing Quick Start Guide*
- ♦ *Conferencing User Guide*
- ♦ *Conferencing Operations Guide*

Change History

This table documents changes for recent revisions to this guide:

Guide Revision	Changes
0 (First Version)	

Documentation Updates

For the most recent version of the *Conferencing Server Installation Guide* and other documentation, visit the [Novell Teaming Web site \(http://www.novell.com/documentation/team_plus_conf\)](http://www.novell.com/documentation/team_plus_conf).

Conventions

This guide uses the following conventions:

A greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (® , ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux* or UNIX*, should use forward slashes as required by your software.

System Overview

1

This section provides an overview of the Conferencing architecture and a description of the system components.

This section includes the following topics:

- ♦ [Section 1.1, “System Components,” on page 9](#)
- ♦ [Section 1.2, “System Architecture,” on page 10](#)

1.1 System Components

The Conferencing Server is a highly modular suite of components that you can configure to run on one or more servers. Each component provides a core service to the system through a well-defined XML API. Because all communication occurs over an XML transport, the allocation of components to physical hardware is very flexible.

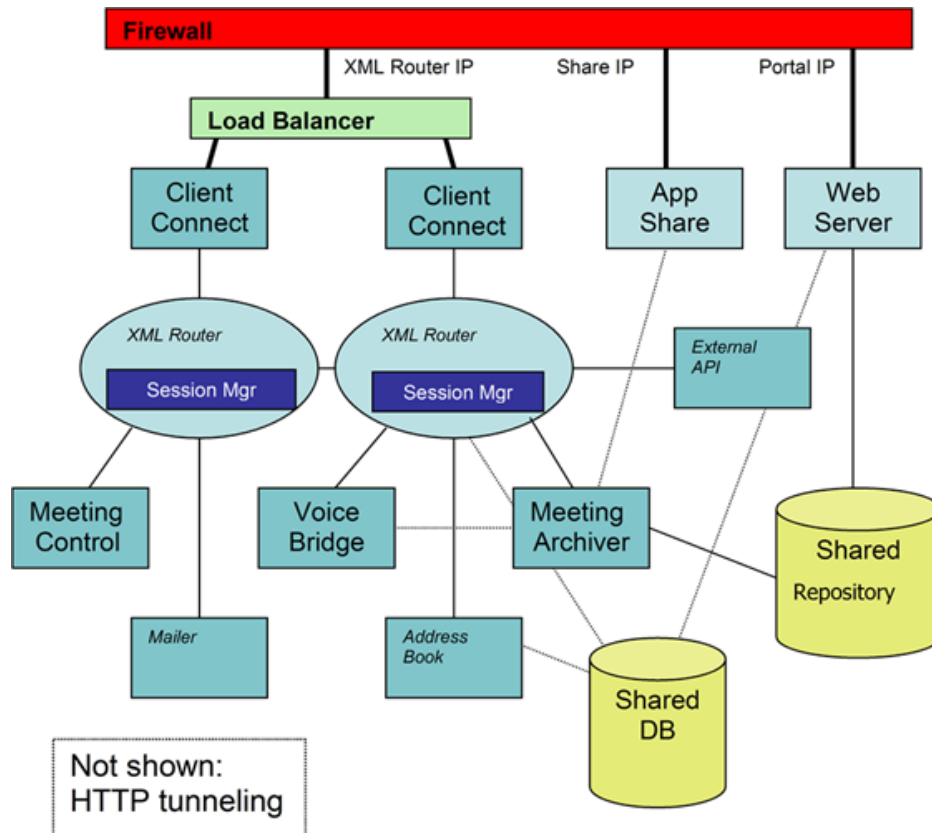
The system components are as follows:

- ♦ XML Router: Routes XML data and API calls among other components.
- ♦ Client Connector: Handles incoming connections from desktop clients and establishes user sessions with the Session Manager component.
- ♦ Session Manager: Tracks connected users and related presence information, and allows users to exchange instant messages.
- ♦ Meeting Controller: Manages in-progress meetings and dispatches meeting events to meeting participants.
- ♦ Notification Server: Sends notification e-mails and IM messages on behalf of the Meeting Controller and Schedule Server components.
- ♦ Address Book: Stores and retrieves community/personal address books and system profile information.
- ♦ Schedule Server: Stores and retrieves meeting schedules, options, and participant information.
- ♦ Voice Bridge: Controls telephony resources, connects calls to conferences, makes outbound calls, and provides telephone access to meeting features.
- ♦ Meeting Archiver Server: Collects audio files, application/desktop shared images, and chat sessions to create meeting archives based on Macromedia* Flash*, which are stored in a Web-accessible repository.
- ♦ App Share Server: Forwards application shared data from the meeting presenter to the meeting participants and manages remote control access to the presenter’s desktop.
- ♦ Invitation Web Service: Joins participants to meetings when they use the invitation URL.
- ♦ External Web Service: Provides a Web service API for external parties as needed for integration with existing service provider systems.

1.2 System Architecture

The following diagram illustrates the architecture of an example Conferencing system. This example displays a multiple server configuration.

Figure 1-1 Conferencing System Architecture



Installation Procedures

2

The following section describes the installation requirements and procedures:

- ♦ [Section 2.1, “Supported Platforms,” on page 11](#)
- ♦ [Section 2.2, “Installation Prerequisites,” on page 12](#)
- ♦ [Section 2.3, “Security,” on page 15](#)
- ♦ [Section 2.4, “Preparing for Installation,” on page 15](#)
- ♦ [Section 2.5, “Installing the Conferencing Server,” on page 17](#)
- ♦ [Section 2.6, “Installing the Conferencing System Components,” on page 22](#)
- ♦ [Section 2.7, “Starting and Stopping the Cluster,” on page 29](#)
- ♦ [Section 2.8, “Conferencing Administration Console,” on page 29](#)
- ♦ [Section 2.9, “Conferencing Client Installation,” on page 30](#)

2.1 Supported Platforms

- ♦ [Section 2.1.1, “Supported Servers,” on page 11](#)
- ♦ [Section 2.1.2, “Minimum Server Configuration,” on page 11](#)
- ♦ [Section 2.1.3, “Supported Client Environments,” on page 11](#)

2.1.1 Supported Servers

Each Conferencing server host must be running SUSE Linux Enterprise Server (SLES) 10 or Linux.

- ♦ SUSE Linux Enterprise Server (SLES) 10, SP1
- ♦ Red Hat Enterprise Server 4

2.1.2 Minimum Server Configuration

- ♦ 1.0 GHz Pentium P4
- ♦ 512 MB RAM
- ♦ 20 GB disk free

NOTE: To use an NMS board you need a chassis with a full length PCI slot.

2.1.3 Supported Client Environments

- ♦ Windows XP, Vista, 2000
- ♦ SUSE Linux Enterprise Desktop (SLED) 10, SP 1
- ♦ openSUSE 10.3

2.2 Installation Prerequisites

The following are requirements for the Conferencing installation unless noted as optional.

- ♦ [Section 2.2.1, “Conferencing Server Requirements,” on page 12](#)
- ♦ [Section 2.2.2, “Network Requirements,” on page 13](#)
- ♦ [Section 2.2.3, “Firewall Requirements,” on page 13](#)
- ♦ [Section 2.2.4, “DNS and Hostname Requirements,” on page 13](#)
- ♦ [Section 2.2.5, “VoIP Requirements,” on page 14](#)
- ♦ [Section 2.2.6, “Load Balancer Requirements,” on page 14](#)

2.2.1 Conferencing Server Requirements

- ♦ **Before running the installer, you need to install the following packages:**

- ♦ neon
- ♦ postgresql
- ♦ postgresql-libs
- ♦ postgresql-server
- ♦ EMACS
- ♦ apache2
- ♦ php5

- ♦ **Installing the neon, postgresql, and postgresql-server packages:** The PostgreSQL database server must be installed on one of the Conferencing hosts. A default Linux installation does not install the PostgreSQL database server. You must choose to install it explicitly. When installing the PostgreSQL software, select the `postgresql` server software. After you have installed the PostgreSQL software, the Conferencing installation initializes the database.

You need to install the `libneon` and `libpq` libraries before running the installer. On SUSE® Linux Enterprise Server (SLES) 10, these libraries are not installed on the system by default. The `libneon` library is inside the `neon` RPM. If you are installing on a 64 bit server, you must use `neon-32bit` and `postgresql-libs-32bit` to complete the install. These are contained in the `postgresql` RPM.

The `neon`, `postgresql`, and `postgresql-server` packages should be available from the original installation media or from the online update. Install dependencies as required.

NOTE: Ensure that you do not have any existing PostgreSQL databases on any of the servers in the Conferencing cluster.

- ♦ **Time synchronization:** All Conferencing hosts must be time-synchronized and the system time zones must all be consistent. To maintain accurate system time, you can configure reliable time servers in *YAST/NetworkServices/NTPConfiguration* or manually with `/etc/ntp.conf` and `/etc/ntp/step-tickers` on SLES (see the `ntpd(1)` man page).
- ♦ **Emacs:** During the installation, you have the opportunity to edit both the new user and invitation templates. You can do this by editing the templates and then importing them, or by using emacs on an install host. If you are going to use emacs on an install host, ensure that emacs has been installed, because it might not be part of the default Linux installation and must be explicitly installed.

- ♦ **License key:** The installation script asks you to provide a license key (`license-key.xml`) for the Conferencing Server. Make sure this file is in the `sitescape-conferencing` directory that contains `install.sh` (the directory files exist after you unpack the compressed tar archive). For more information, see [“Unpacking the Files” on page 15](#).

2.2.2 Network Requirements

You must define at least three static IP addresses that are used by Conferencing clients to connect to Conferencing services. The services that Conferencing clients connect to are the XML router, Web portal and desktop/application share server. The XML router and Web portal each require their own individual IP addresses. The desktop and application share services use the same IP address. If any of the Conferencing clients are outside your firewall, the IP addresses must be externally accessible.

For example:

```
192.168.1.1:80
      :443      --> XML Router
      :1270

192.168.1.2:80      --> Web portal
      :443          (port 443 required if using SSL)

192.168.1.3:80
      :443      --> Desktop and Application Share
      :1270
```

VoIP requires two additional IP addresses. For more information, see [“VoIP Requirements” on page 14](#).

2.2.3 Firewall Requirements

- ♦ **XML router IPs:** IP addresses have ports 1270, 443, and 80 open.
- ♦ **Desktop/Application Sharing IPs:** IP addresses have ports 1270, 443, and 80 open.
- ♦ **Web portal IPs:** You must have port 80 open.

NOTE: Port 443 must be open if you have enabled SSL/TLS. Then, you can choose to block port 80 to disable unencrypted access.

- ♦ **(Optional) DMZ Configuration:** If you run Conferencing services in the DMZ and you are concerned about database security, you can run the database inside the firewall. XML routers and Address Book and Web portal HTTP servers connect to the database through port 5432.

2.2.4 DNS and Hostname Requirements

IMPORTANT: All hostnames currently need to be lowercase.

- ♦ **Three hostnames:** The XML router, desktop/application sharing, and Web portal IP addresses each require a hostname resolvable by Conferencing clients.

A Conferencing server requires three IP addresses and hostnames for proper operation of all services:

1. Typically one address is given a friendly name and used for the XML router service. This is the service to which the Conferencing client initially connects.
 2. The second address has “-share” appended to the base name and is used for the desktop sharing components.
 3. The third address has “-portal” appended to the name and is used for Web services and client download.
- ♦ **Fully qualified domain name:** The Web portal host requires a fully qualified domain name. For example, `www.mycompany.com` or `webportal.conferenceinstall.com`.
 - ♦ **Unique hostnames (multiple machines):** Multiple-machine Conferencing installations require each machine to have a distinct hostname. These hostnames do not need to be resolvable outside the local network.

To Add IP Addresses to a SUSE Enterprise Server:

- 1 Open *YaST Administrator Settings*, select *Network Devices*, and then select *Network Card*.
- 2 Click *Next*, select the desired network interface, then click *Edit*.
- 3 Click *Advanced*, then select *Additional Addresses* from the drop-down list.
- 4 Click *Add*, then specify the IP addresses and netmasks appropriate for your network.
- 5 Click *OK*.

2.2.5 VoIP Requirements

The client connects to a gateway server by using the IAX protocol, and first attempts to use UDP over port 4569. If that fails, it tries a TCP connection on port 443. The VoIP client does not attempt to do HTTP tunneling. The gateway then uses SIP to communicate with the voice bridge itself. The SIP traffic is sent to the voice bridge server itself, and all voice data is streamed via RTP to the NMS board. See [Appendix F, “Installing the NMS Board,” on page 55](#) for instructions on installing the NMS board and associated software to use VoIP with Conferencing.

To configure VoIP, you need to specify two additional IP addresses during server installation. One is for the gateway process and must be exposed to the external network; the second is assigned to the NMS board.

2.2.6 Load Balancer Requirements

Multi-host installations only:

- ♦ A load balancer is only required when either multiple Web portal hosts or multiple XML router hosts are used.
- ♦ Conferencing clients need to maintain an open connection while a user is signed on.
- ♦ Connections to the Web portal should be sticky. For example, if a host is assigned to a Web portal IP address, that host should continue to access the assigned Web portal IP address.

2.3 Security

We recommend that you configure the length of any Conferencing PINs (Invitee PINs and Meeting IDs) to six characters or more for increased security. See the Conferencing online help, *User Guide*, or *Operations Guide* for how to set the length of the Conferencing PINs in your administration Policies.

WARNING: Neither VoIP nor the communication channel between the recording server and the Conferencing server are encrypted.

If you are using LDAP synchronization, we recommend that you enable SSL on your server. The Conferencing Client automatically detects when you have SSL enabled on your server. You also need to get the CA certificate from the LDAP server and copy it into the `sitescape-conferencing` directory. If necessary, rename it to `ldap-ca.cer`.

2.4 Preparing for Installation

IMPORTANT: The following are important pre-installation steps.

- ♦ [Section 2.4.1, “\(Optional\) Using ssh\(\),” on page 15](#)
- ♦ [Section 2.4.2, “Unpacking the Files,” on page 15](#)
- ♦ [Section 2.4.3, “Back Up the Directory,” on page 16](#)
- ♦ [Section 2.4.4, “Installing and Configuring the NMS Boards,” on page 16](#)

2.4.1 (Optional) Using ssh()

For multi-machine installations, we strongly recommend that you configure `ssh()` public/private key authentication between the system administrator on the staging host and the `root` user on the Conferencing hosts. Otherwise, you need to enter the root password for the Conferencing hosts numerous times during the installation. See [Appendix A, “Configuring ssh\(\) Key Authentication,” on page 41](#).

2.4.2 Unpacking the Files

You should have the Conferencing distribution file in a compressed `.tar` archive named `sitescape-conferencing-version.tar.gz` (where *version* is the version of the system you received). Extract the contents of the tar file on an installation-staging host (you can use one of the Conferencing hosts) by using the following command:

```
tar -zxvf sitescape-conferencing-version.tar.gz
```

Unpack the distribution compressed tar archive (`sitescape-conferencing-version.tar.gz`) on a Linux staging machine (you can use one of the cluster nodes). After unpacking, you should see the following files and directories in the `sitescape-conferencing` directory:

```
sitescape-conferencing/uninstall.sh
sitescape-conferencing/check-config.sh
sitescape-conferencing/install.sh
sitescape-conferencing/control-cluster.sh
sitescape-conferencing/conferencing-svr-release_number.tar.gz
```

```
sitescape-conferencing/cluster-prototype/  
sitescape-conferencing/install-cluster.sh  
sitescape-conferencing/ldaputils.sh  
sitescape-conferencing/config-cluster.sh  
sitescape-conferencing/langs.sh  
sitescape-conferencing/nmsconfig  
sitescape-conferencing/utils.sh
```

2.4.3 Back Up the Directory

After configuring the system, back up the `sitescape-conferencing` directory, because it is the location where future upgrades and reconfigurations are performed.

2.4.4 Installing and Configuring the NMS Boards

If you are deploying voice, perform one of these procedures after installing the NMS boards into full-length PCI slots. For more information on installing the physical NMS boards, see “[Installing the NMS Board](#)” on page 55.

To install and configure the NMS boards on the Conferencing server:

- 1 Change directories to the `sitescape-conferencing` directory:
- 2 Download the NMS software to the `sitescape-conferencing` directory from <http://www.novell.com/downloads> (<http://www.novell.com/downloads>) or get them from your support representative.
- 3 Run the following commands, to install the NMS software:

```
# mkdir nms  
# tar -zxvf <NMSTAR> -C nms  
# cd nms  
# ./install
```
- 4 Make sure NMS `ctdaemon` is set to start up on boot and is running:

```
# chkconfig --set nmsctdaemon 345  
# /etc/init.d/nmsctdaemon start
```
- 5 Change directories back to the `sitescape-conferencing` directory:

```
# cd ..
```
- 6 Run `nmsconfig` and enter information for detected boards (refer to the [nmsconfig](#) section for more information on `nmsconfig`):

```
# ./nmsconfig
```

NOTE: The `nmsconfig` utility requests the Bridge IP address. This address is not the NMS CG board IP address, it is the Bridge IP address.

To install and configure the NMS boards on a remote server:

- 1 Download the NMS software from <http://www.novell.com/downloads> (<http://www.novell.com/downloads>) or get them from your support representative.
- 2 Run the following commands, to install the NMS software:

```
# mkdir nms  
# tar -zxvf <NMSTAR> -C nms
```


- ```
cd nms
./install
```
- 3 Make sure NMS ctdaemon is set to start up on boot and is running:

```
chkconfig --set nmsctdaemon 345
/etc/init.d/nmsctdaemon start
```
  - 4 Untar the Conferencing software:

```
tar -zxf sitescape-conferencing-Version.tar.gz
```
  - 5 Change directories to the `sitescape-conferencing` directory:

```
cd sitescape-conferencing
```
  - 6 Run `nmsconfig` and enter information for detected boards (refer to the [nmsconfig](#) section for more information on `nmsconfig`):

```
./nmsconfig
```
  - 7 Copy the `voiceinfo.sh` file to the `sitescape-conferencing` directory on the Conferencing server.

---

**NOTE:** The `nmsconfig` utility requests the Bridge IP address. This address is not the NMS CG board IP address, it is the Bridge IP address.

---

## 2.5 Installing the Conferencing Server

---

**NOTE:** If you plan on using VoIP with Conferencing, you must install and configure the NMS board and associated software before running the main installation. For more information, see [“Installing and Configuring the NMS Boards”](#) on page 16.

---

Perform this procedure after you extract the `sitescape-conferencing-version.tar.gz` Conferencing server distribution file on an installation-staging host.

To install or upgrade the Conferencing System Components:

- 1 Verify that the [Installation Prerequisites](#) are in place and that you have performed all pre-installation steps, see [“Preparing for Installation”](#) on page 15.
- 2 Unpack the files.
- 3 Back up the `sitescape-conferencing` directory (if applicable).
- 4 Open the `sitescape-conferencing` directory.
- 5 Run: `./install.sh`, which prompts you for the configuration information, license key and then installs the software, see [“Running the Installer on SLES:”](#) on page 18:
  - ♦ Initialization of the database server
  - ♦ Installation and configuration of the XML router services
  - ♦ Installation and configuration of the Web portal services
  - ♦ Installation and configuration of the application/desktop sharing
  - ♦ Installation and configuration of e-mail configuration
  - ♦ Installation and configuration of backup, meeting archive, logging and port forwarding
  - ♦ Modification of the template files

During the installation process, you are asked whether you want to modify the associated templates. For more information, see [Chapter 4, “Modifying Template Files,” on page 37](#).

This section contains the following topics:

- ♦ [Section 2.5.1, “Running the Installer on SLES;,” on page 18](#)
- ♦ [Section 2.5.2, “Initial Address Book Configuration \(Synchronization\),” on page 22](#)

## 2.5.1 Running the Installer on SLES:

- 1 Unpack the distribution compressed tar archive (sitescape-conferencing-<version>.tar.gz):  

```
#/ tar -zxvf filename.tar.gz
```
- 2 Copy the license key to the `sitescape-conferencing` directory that contains `install.sh` (the directory files exist after you unpack the compressed tar archive):  

```
cp license_key.xml
```
- 3 Change directories to the `sitescape-conferencing` directory that contains `install.sh`:  

```
cd sitescape-conferencing
```
- 4 (Optional) If you plan on running Active Directory\* LDAP Synchronization, edit the `ldap.xml.in` file in the `cluster-prototype` directory. (For more information, see [Appendix E, “LDAP User Authentication,” on page 51](#)):
  - 4a Open the `ldap.xml.in` file.
  - 4b Comment out the `eDirectory` attributes section and uncomment out the `ActiveDirectory` attributes section.
  - 4c Save the file.
- 5 Run the installer:  

```
./install.sh
```
- 6 When the installer prompts you to accept the license agreement (the default is N), enter Y:  

```
Accept License (Y/N): Y
```
- 7 When the installer prompts you to proceed, enter Y:  

```
Ready to proceed (Y/N): Y
```
- 8 When the installer prompts you to select whether this is a new install or an upgrade (the default is N), enter Y to run a new installation:  

```
New Install or upgrade (Y/N): Y
```
- 9 When the installer prompts you to enter a name for the install (the default is `ourzon`), enter the name you want to use for the install:  

```
Choose a name for Install: <enter_install_name>
```

The name of the installation cannot contain spaces, but can contain any combination of ASCII and alphanumeric characters.
- 10 When the installer prompts you to initialize the database for a new install (the default is Y), you must enter Y here for a new installation or the database service does not start:  

```
Initialize Database for new install (Y/N): Y
```

Ensure that you have installed the PostgreSQL database prior to installation. For more information, see [“Installation Prerequisites” on page 12](#).

---

**IMPORTANT:** If you are upgrading and have an existing database, you can enter `N`. For new installations, always enter `Y`.

---

- 11** Provide a password when the installer prompts you to enter a password for the new administrator account that the installer creates for Conferencing (this should be set for security reasons, because the Administrator account needs to be a controlled environment):

Password for Admin User: `<enter_password>`

---

**IMPORTANT:** The cursor does NOT advance with each keystroke (no asterics are displayed).

---

- 12** The installer prompts you whether to enable SSL/TLS security (the default is `Y`):

Should System enable SSL/TLS security (Y/N): `<enter_value>`

SSL= Secure Socket Layer and TLS= Transport Layer Security. If you enable SSL/TLS security, the user and password information is encrypted on the network and shows up as hashes in the database table. If you select `N`, password information is still hashed in the database, but user and password are in the clear on the wire.

- 13** The installer prompts you to enter the path and name of the certificate for the XML router (the default is `/opt/iic/conf/server.pem`), enter the default certificate:

Insert path and name of certificate for XML router:  
`/opt/iic/conf/server.pem`

---

**IMPORTANT:** You must use the default XML router certificate for the Conferencing server to function correctly.

---

- 14** Use the following path when the installer prompts you to enter the path and name of the certificate for the Web Server:

`/opt/iic/conf/webserv.pem`

---

**IMPORTANT:** You must use the default Web Server certificate for the Conferencing server to function correctly.

---

- 15** When the installer prompts you to identify whether you are installing on a Single-Host or a Multiple-Host installation (the default is `Y`), select `N` if you have multiple servers, and the installer prompts you to enter the additional information for a Multiple-Host installation:

Are you installing on single host (Y/N): `<enter_value>`

- 16** When the installer prompts you to enter the IP address for the XML router, enter the address:

What is IP address for XML router?: `<enter_ip_address>`

The installer attempts to ping hosts and IP addresses to ensure that they are running and reachable. If an intervening firewall is filtering out ICMP messages or the host is intentionally down, it might not appear to be reachable even though the entered value is valid.

- 17** Enter a value when the installer prompts you to enter the hostname of the conferencing server:

What is hostname that conferencing clients will use to connect to XML?: `<enter_value>`

- 18** When the installer prompts you to enter the IP address for the Web portal, enter the address:

What is IP address for Web Portal?: `<enter_ip_address>`

- 19** When the installer prompts you to enter the portal name, enter the name:

What is Web Portal name URL's?: `<enter_portal_name>`

For example, `Renaldo.homedns.org-portal`.

- 20** When the installer prompts you to enter the IP address for the App-Share, enter the address:  
What is IP address for App-Share?: <enter\_ip\_address>
- 21** Enter a value when the installer prompts you to enter the Hostname for the desktop App-Share:  
What is Hostname for desktop app-share: <enter\_hostname>  
For example, renaldo.homedns.org-share.
- 22** Enter a value when the installer prompts you to select whether you are running Conferencing Bridge (the default is N). If you enter Y, the installer prompts you to enter the bridge information:  
Are you running Conferencing Bridge? (Y/N): <enter\_value>
- 23** Enter a value when the installer prompts you to select whether you want to change the system administration e-mail configuration (the default is N). If you enter Y, the installer prompts you to enter the new e-mail address configuration information instead of using default configuration:  
Do you want to change system admin email configuration? (Y/N): <enter\_value>  
For more information on optional configurations you can use, see [Section 2.6.2, “System Administration E-mail Configuration \(Optional\),” on page 23](#).
- 24** The installer prompts you to verify what you have entered up to this point. Enter Y if the information is correct or enter N if you need to make any changes:  
Is this correct (Y/N): <enter\_value>  
The questions from [Step 25](#) through [Step 38](#) all have default values of N.  
If you select Y, the installer prompts you to enter additional values and information to customize your server configuration. You can customize your configuration for information such as how long a file is archived, with a different header look, the way summaries are viewed, security settings. If you use the defaults and decide to customize your server configuration later, you must rerun the installer to change these values.
- 25** Enter a value when the installer prompts you to select whether you want to change the mailer configuration:  
Do you want to change mailer config? (Y/N): <enter\_value>  
For more information on optional configurations you can use, see [Section 2.6.3, “Mailer Configuration \(Optional\),” on page 23](#).
- 26** Enter a value when the installer prompts you to select whether you want to change the database backup configuration:  
Do you want to change DB backup config (Y/N):  
For more information on optional configurations you can use, see [Section 2.6.4, “Database Backup Configuration \(Optional\),” on page 24](#).
- 27** Enter a value when the installer prompts you to select whether you want to change the meeting archive maintenance configuration:  
Do you want to change meeting archive maint? (Y/N): <enter\_value>  
For more information on optional configurations you can use, see [Section 2.6.5, “Meeting Archive and Document Sharing Repository Configurations \(Optional\),” on page 24](#).
- 28** Enter a value when the installer prompts you to select whether you want to change the document share repository maintenance configuration:  
Do you want to change doc share repository maint config? (Y/N): <enter\_value>

For more information on optional configurations you can use, see [Section 2.6.5, “Meeting Archive and Document Sharing Repository Configurations \(Optional\),” on page 24.](#)

- 29** Enter a value when the installer prompts you to select whether you want to change the audit logs:

Do you want to change Audit logs? (Y/N): <enter\_value>

For more information on optional configurations you can use, see [Section 2.6.6, “Chat Audit Log Configuration \(Optional\),” on page 25.](#)

- 30** Enter a value when the installer prompts you to select whether you want to change the logging configuration:

Do you want to change logging config? (Y/N): <enter\_value>

For more information on optional configurations you can use, see [Section 2.6.6, “Chat Audit Log Configuration \(Optional\),” on page 25.](#)

- 31** Enter a value when the installer prompts you to select whether you want to change the real-time call user-reservations logs:

Do you want to change real-time call user-reservations logs? (Y/N): <enter\_value>

For more information on optional configurations you can use, see [Section 2.6.7, “Event Logging Configuration \(Optional\),” on page 26.](#)

- 32** Enter a value when the installer prompts you to select whether you want to change the security configuration:

Do you want to change security configuration? (Y/N): <enter\_value>

For more information on configurations you can use, see [Section 2.6.9, “XML Router Security,” on page 27.](#)

- 33** Enter a value when the installer prompts you to select whether you want to change the LDAP configuration:

Do you want to change LDAP (Y/N): <enter\_value>

For more information on optional configurations you can use, see [Section 2.6.10, “Configuring LDAP Synchronization \(Optional\),” on page 27.](#)

For Active Directory LDAP Synchronization, you need to complete [Step 4 on page 18](#) first.

- 34** Enter a value when the installer prompts you to select whether you want to change the system e-mail header configuration:

Do you want to change system email header config? (Y/N): <enter\_value>

- 35** Enter a value when the installer prompts you to select whether you want to change the e-mail template:

Do you want to change Email template? (Y/N): <enter\_value>

- 36** Enter a value when the installer prompts you to select whether you want to change the meeting invitation template:

Do you want to change Meeting invite template? (Y/N): <enter\_value>

- 37** Enter a value when the installer prompts you to select whether you want to change the summary e-mail template:

Do you want to change Summary email template? Y/N): <enter\_value>

- 38** Enter a value when the installer prompts you to select whether you want to change the meeting archive e-mail template:

```
Do you want to change Meeting archive email template? (Y/N):
<enter_value>
```

**39** When the installer lists all the services running on the local host, press Enter to continue:

```
All services running on local host
```

**40** When the installer lists all the configuration information, press Enter to continue:

```
View Config
```

**41** Enter a value when the installer prompts you to select whether you are satisfied with the configuration (the default is Y). Enter N to change the configuration:

```
Satisfied with config (Y/N): <enter_value>
```

The installation begins and uses whatever values you entered during the installation setup. The installation completes and displays information stating the services that should be running.

After you have completed the installation script, you are presented with a summary of the choices you selected. If you are not satisfied with the configuration setup, you can either modify the configuration or you can exit the installer and run the script again. If you exit the installer, the current configuration is saved, and when you rerun the install script, it is used for the default values during the reconfiguration.

## 2.5.2 Initial Address Book Configuration (Synchronization)

If you are using LDAP synchronization, execute `/opt/iic/bin/ldap-sync.sh` `<portal-server-hname>` to perform the initial synchronization.

---

**NOTE:** After starting the server, wait about 20 seconds before executing this command; if you do not get an XML message in return, you probably did not wait long enough.

---

This script displays an XML message if it fails (the fault message is clearly visible); if it succeeds, the XML data contains a single number that is the number of users actually synchronized. You can run this script manually as needed, or use `cron` to configure it to run periodically. The default setting is for it to run daily.

## 2.6 Installing the Conferencing System Components

The installation script takes you through the following to install and configure a new Conferencing Server instance:

- ♦ [Section 2.6.1, “Initial Installation,” on page 23](#)
- ♦ [Section 2.6.2, “System Administration E-mail Configuration \(Optional\),” on page 23](#)
- ♦ [Section 2.6.3, “Mailer Configuration \(Optional\),” on page 23](#)
- ♦ [Section 2.6.4, “Database Backup Configuration \(Optional\),” on page 24](#)
- ♦ [Section 2.6.5, “Meeting Archive and Document Sharing Repository Configurations \(Optional\),” on page 24](#)
- ♦ [Section 2.6.6, “Chat Audit Log Configuration \(Optional\),” on page 25](#)
- ♦ [Section 2.6.7, “Event Logging Configuration \(Optional\),” on page 26](#)
- ♦ [Section 2.6.8, “Port Forwarding \(Optional\),” on page 26](#)

- ♦ [Section 2.6.9, “XML Router Security,” on page 27](#)
- ♦ [Section 2.6.10, “Configuring LDAP Synchronization \(Optional\),” on page 27](#)
- ♦ [Section 2.6.11, “Template Configuration \(Optional\),” on page 29](#)

## 2.6.1 Initial Installation

- 1 Create and name a new Conferencing installation. See [“Installing the Conferencing Server” on page 17](#).

The name of the installation cannot contain spaces, but can contain any combination of ASCII and alphanumeric characters.

- 2 Initialize the PostgreSQL database.

Ensure that you have created the PostgreSQL database prior to installation. For additional information, see [“Installation Prerequisites” on page 12](#).

- 3 Identify a single-host or a multiple-host installation.

- 4 Provide the IPs and the hostnames for the XML Router, Web Portal and Desktop/App Server.

The installer attempts to ping hosts and IP addresses to ensure that they are running and reachable. If an intervening firewall is filtering out ICMP messages or the host is intentionally down, it might not appear to be reachable even though the entered value is valid.

- 5 (Optional) Install a Conferencing Voice Bridge.

## 2.6.2 System Administration E-mail Configuration (Optional)

During installation you can define a list of system administrator e-mail addresses that are used when an error or event occurs:

- 1 Perform [Step 1](#) through [Step 22](#) in [Section 2.5.1, “Running the Installer on SLES;,” on page 18](#). In [Step 23](#), use the following procedure to configure your list of e-mail addresses.
- 2 Type the system administrator’s e-mail address.
- 3 To configure multiple e-mail addresses, type the first e-mail address (for example `admin@company.com`) and press *Enter*. At the next `EMAIL>>>` prompt, type the second e-mail address and press *Enter*, etc.
- 4 Continue with [Step 24](#) in [Section 2.5.1, “Running the Installer on SLES;,” on page 18](#).

## 2.6.3 Mailer Configuration (Optional)

The mailer is used to notify Conferencing users of events. By default, the mailer uses the SMTP service provided on its host, but you can change the SMTP Server and provide user and password authentication for that server, if required:

- 1 Perform [Step 1](#) through [Step 24](#) in [Section 2.5.1, “Running the Installer on SLES;,” on page 18](#). In [Step 25](#), use the following procedure to configure your mailer.
- 2 Identify the SMTP Server.
- 3 Configure the SMTP Server’s User and Password Authentication.
- 4 Continue with [Step 26](#) in [Section 2.5.1, “Running the Installer on SLES;,” on page 18](#).

## 2.6.4 Database Backup Configuration (Optional)

Daily database backups are stored in the `/var/iic/db-backups` directory.

- 1 Perform [Step 1](#) through [Step 25](#) in [Section 2.5.1, “Running the Installer on SLES;,” on page 18](#). In [Step 26](#), use the following procedure to configure database backups.
- 2 Identify the directory where you want to store the database backups.  
We recommend that you do not store the database backups on the database server. Mount an external file system using NFS to maintain the daily database backup archives.
- 3 Configure the number of days backups are kept.
- 4 Define when backups are performed.
- 5 Continue with [Step 27](#) in [Section 2.5.1, “Running the Installer on SLES;,” on page 18](#).

## 2.6.5 Meeting Archive and Document Sharing Repository Configurations (Optional)

The Meeting and Document Sharing (DocShare) Archive Repositories are both monitored daily at 4:00 a.m. to ensure that they have not reached a size of 2500 MB. When a repository exceeds 2500 MB, archives that have not been accessed within the last 30 days are deleted until the archive repository reaches 2000 MB. If the system cannot delete archives to reach the 2500 MB repository size, a warning e-mail is sent to the system administrator indicating the need for appropriate manual action. To avoid the automatic deletion of archives, the maintenance procedure can be configured to send daily notification when a meeting or document sharing archive repository reaches the specified maximum.

- 1 Perform [Step 1](#) through [Step 26](#) in [Section 2.5.1, “Running the Installer on SLES;,” on page 18](#). In [Step 27](#) and [Step 28](#), use the following procedure to configure your Meeting and Document Sharing (DocShare) Archive Repositories.
- 2 Determine the repository maximum size. Set the repository size in MBs.
- 3 Identify the action to take if the archive repository maximum is exceeded. The two available options are to automatically clean up archives that have not been accessed within the last 30 days, or to send e-mail notification to the systems administrator with no automatic archive deletion.
- 4 Determine what time of day the archive maintenance occurs.
- 5 If automatic maintenance was specified in Step 2, do the following:
  - 5a Determine the minimum target repository size after automatic clean up.
  - 5b Identify the minimum days-since-accessed that an archive can be deleted during the automated clean up procedure. For example, if the minimum days-since-accessed was set to 60 days, the automated clean up procedure does not delete archives that have been accessed within the past 60 days.
  - 5c Determine if the archives should be permanently deleted, or moved into another designated folder, which must be monitored manually by the system administrator.
- 6 Continue with [Step 29](#) in [Section 2.5.1, “Running the Installer on SLES;,” on page 18](#).



## 2.6.6 Chat Audit Log Configuration (Optional)

You can configure chat audit logging at system installation or reconfiguration time using the `install.sh` script.

1 Perform [Step 1](#) through [Step 28](#) in [Section 2.5.1, “Running the Installer on SLES:,”](#) on page 18. In [Step 29](#) and [Step 30](#), use the following procedure to configure your chat audit logging.

2 For [Step 29](#), select where the logs should be stored:

- ♦ The chat audit logs are placed in `/var/iic/chatlog` on the hosts assigned to run the XML router and meeting controllers. Conferencing IM and Conferencing chat room messages are written to the file `/var/iic/chatlog/chat.log`. Meeting chat messages are written to `/var/iic/chatlog/mtgchat.log`.

- ♦ The chat messages contained in `chat.log` are XML stanzas:

```
<message type='<"chat"|"groupchat">' from='<from_jid>'
to='<to_jid>' time='<timestamp>' >
<body> ... </body><x xmlns='jabber:x:event' />
</message>
```

The `from_jid` and `to_jid` tags have the forms:

```
<screenname>@<xmlrouter_hostname>/<resource>
```

Resource is a session identifier in the case where the message type is chat and it identifies the sender screen name in the case of groupchat type messages.

The time stamp has the form `<YYYY><MM><DD>"T"<hh><mm><ss>` and uses GMT time.

- ♦ Each chat message is logged to a line in `mtgchat.log`. The each line contains comma-separated fields. Each field has double quotes at the beginning and end of the field (for example, “field value”).

3 For [Step 30](#), edit the log configuration:

The fields are as follows:

Field	Type	Description
timestamp	String (YYYYMMDDTHH:MM:SS)	The time of the chat message in GMT.
from_jid	String	The participant ID of the sender. A participant ID is assigned to each meeting participant and is sent in meeting invitations.
from_name	String	The display name of the meeting participant who sent the chat message.
delivery	String (one of: ToAll, ToOne, ToHost, ToModerators, ToNonModerators)	This field shows to whom the message was delivered.
to_id	String	This participant ID received the message. This field is empty unless the <i>delivery</i> field value is ToOne.
to_name	String	The display name of the meeting participant who received the chat message. This field is empty unless the <i>delivery</i> field value is ToOne.

Field	Type	Description
message	String	The contents of the chat message.

- 4 Continue with [Step 31](#) in [Section 2.5.1, “Running the Installer on SLES;,”](#) on page 18.

## 2.6.7 Event Logging Configuration (Optional)

Log files are written to `/var/log/iic`, except for the Web portal and external API server logs, which are written to files in `/usr/local/apache2/logs`. Additional information may be found in `/var/log/messages`.

There are three levels for logging. You can modify these logging levels at any time from the Administration Console (see the *Conferencing Operations Guide*):

- ♦ Error: Logs only error conditions.
- ♦ Info: Logs error conditions as well as summary information about all server tasks.
- ♦ Debug: This level logs error conditions, summary information, and detailed debugging information.

---

**NOTE:** We recommend that the Error logging level be the default logging level because of the increased CPU and I/O loads associated with more verbose logging.

---

To set the logging:

- 1 Perform [Step 1](#) through [Step 30](#) in [Section 2.5.1, “Running the Installer on SLES;,”](#) on page 18. In [Step 31](#), use the following procedure to set the event logging:
- 2 Set default logging levels for system components.
- 3 Determine at what size the logs should be rotated.
- 4 Configure the number of rotated logs that should be kept.
- 5 Configure real time, call, user and reservation logging.

You can configure the Conferencing servers to produce real-time event logs for call, user and meeting reservation events. The real-time interface provides the event data records as they occur so that third-party systems (billing systems, cost accounting systems, management reporting systems, directory databases, etc.) can use them. The records are provided to event record consumers via a TCP connection to Conferencing server hosts. Real-time event logs are stored in the `/var/iic/cdr` directory.

You cannot modify real-time event logging from the Administration Console. If you do not install real-time event logging during installation, you need to re-run the installation script when you want to install real-time event logging.

- 6 Continue with [Step 32](#) in [Section 2.5.1, “Running the Installer on SLES;,”](#) on page 18.

## 2.6.8 Port Forwarding (Optional)

The Conferencing client attempts to connect to ports 1270, 443 and 21 when the primary port (either 5222 for the XML router or 2182 for desktop/app-share server) is blocked by a firewall.

Connections to these ports should be forwarded to the primary port. If you are not running a load

balancer that performs this task, you must forward these ports locally on the XML router hosts or the desktop/app-share server hosts.

## 2.6.9 XML Router Security

In order for a Conferencing service (meeting controller, voice bridge, etc.) to connect to the XML router, it must use the correct authentication key. If your XML router allows connections from the Internet, change the Service Connection Key so that unauthorized services cannot access and connect to your router. Additionally, the meeting controller needs to provide a User Session Creation Key. You should change this key so that unauthorized meeting controllers cannot create sessions on behalf of your users.

- ♦ The default value for the Service Connection Key is: `secret`
- ♦ The default value for the User Session Creation Key is: `QAZXSW88`

## 2.6.10 Configuring LDAP Synchronization (Optional)

Synchronization between eDirectory™ or Active Directory\* users and Conferencing users is established when you install Conferencing.

---

**NOTE:** If you plan on running Active Directory LDAP Synchronization, you need to edit the `ldap.xml.in` file in the `cluster-prototype` directory (see [Appendix E, “LDAP User Authentication,” on page 51](#)) before running the installer.

---

- 1 Perform [Step 1](#) through [Step 32](#) in [Section 2.5.1, “Running the Installer on SLES;,” on page 18](#). In [Step 33](#), use the following procedure to configure your list of e-mail addresses.

- 2 Type `y`, then press Enter.

Next, you are prompted:

```
Should the system enable LDAP synchronization? (y/n)
```

- 3 Type `y`, then press Enter.

Next, you are prompted with options:

LDAP servers

```
1: URL=ldap://ldapserver
 bindDN=cn=admin,o=novell
 bindPW=password
 baseDN=ou=users,o=novell
 dc=com
 import filter=(objectClass=User)
 auth filter=(uid=%s)
 (%s represents your users)
 community=2
 (The community automatically created during installation).
```

A - Add

E - Edit

D - Delete

Q - Quit

The line of settings indicates the information that the Conferencing installation program gathers for each LDAP server.

- 4** Type `e` for *Edit* to define your first LDAP server, then press Enter.
- 5** Type `1` for the server number, then press Enter.  
Next, you are prompted:  
Input the URL of the LDAP server:
- 6** Specify the URL in the following format, then press Enter.  
`ldap://hostname`  
Next, you are prompted:  
Input the dn with which to bind to the LDAP server:
- 7** Specify the Admin-equivalent username with full context, then press Enter.  
Next, you are prompted:  
Input the password for the bind dn:
- 8** Type the password for the Admin-equivalent user, then press Enter.  
Next, you are prompted:  
Input the base dn under which to search for users:
- 9** Specify the eDirectory/ActiveDirectory container that defines the search scope, then press Enter.  
Next, you are prompted:  
Input the filter used to select users for import:
- 10** Press Enter to accept the default value.  
Next, you are prompted:  
Input the filter used to select users for import:
- 11** Press Enter to accept the default value.  
Next, you are prompted:  
Input the community into which to place users imported from LDAP:
- 12** Press Enter to accept the default value.  
You return to the original options prompt, which displays the information you have provided for the first LDAP server.
- 13** To add more LDAP servers to the list, type `a` for Add, press Enter, then repeat **Step 5** through **Step 12**, adjusting the information as needed for each LDAP server.
- 14** If you make a mistake and need to remove an LDAP server from the list, type `d` for Delete, press Enter, type the number of the server to delete, then press Enter, type `y` to confirm, then press Enter again.
- 15** When you are finished listing LDAP servers, type `q` for Quit, then press Enter.
- 16** Continue with **Step 34** in **Section 2.5.1, “Running the Installer on SLES:,”** on page 18.  
See **“Address Book Configuration (Synchronization)”** on page 52 for testing the LDAP synchronization.

## 2.6.11 Template Configuration (Optional)

You can modify the e-mail templates that Conferencing uses to communicate with users (see [Chapter 4, “Modifying Template Files,” on page 37](#)).

1. Configure system e-mail headers.
  - ♦ Configure the New User e-mail *From* display name.
  - ♦ Configure the New User e-mail *Subject*.
  - ♦ Configure the Meeting Invitation e-mail *Subject*.
  - ♦ Configure the New Meeting Archive e-mail *From* display name.
  - ♦ Configure the New Meeting Archive e-mail *From* e-mail address.
2. Configure the New User e-mail template.
3. Configure the Meeting Invitation template.
4. Configure the Meeting Summary e-mail template.
5. Configure the New Meeting Archive e-mail template.

## 2.7 Starting and Stopping the Cluster

You can start and stop the Conferencing services for the entire cluster using the `control-cluster.sh` script.

To stop Conferencing Services, enter:

```
./control-cluster.sh --cluster <your-cluster> [--single-host <your-host>] stop
```

To start Conferencing Services, enter:

```
./control-cluster.sh --cluster <your-cluster> [--single-host <your-host>] start
```

Use the `--single-host` argument with the script if there is only one host in your cluster.

## 2.8 Conferencing Administration Console

After you have successfully installed the Conferencing System Components, you can access the Web-based Conferencing Administration Console. Use the Administration Console to monitor the state of the Conferencing components and services, as well as to create Conferencing communities.

The Conferencing Administration Console is available via the following URL:

```
http://<webportalhostname>/imidio/console/
```

---

**NOTE:** If you have SSL enabled, you should specify https in the URL instead of http.

---

- ♦ [Section 2.8.1, “Logging In to the Administration Console,” on page 30](#)
- ♦ [Section 2.8.2, “Creating Conferencing Communities,” on page 30](#)

## 2.8.1 Logging In to the Administration Console

The initial installation creates the screen name *admin* with password *admin*. You can use these values to log in, and change them later (see the *Conferencing Operations Guide* for further information on using the Conferencing Administration Console).

## 2.8.2 Creating Conferencing Communities

See the *Conferencing Operations Guide* for information on adding Conferencing Communities.

# 2.9 Conferencing Client Installation

You need to untar the `pidgin-version-tar.gz` file to the `/var/iic/htdocs` directory on the Web servers after completing the server install to make Pidgin available for download.

The Conferencing client download files are automatically generated during the server install process and placed in the download directories on your Web servers.

The following topics are included in this section:

- ♦ [Section 2.9.1, “Conferencing Client Components,” on page 30](#)
- ♦ [Section 2.9.2, “Installing the Conferencing Client,” on page 30](#)
- ♦ [Section 2.9.3, “Installing the Pidgin Instant Chat Client,” on page 31](#)

## 2.9.1 Conferencing Client Components

To install and administer communities and new users:

- 1 Launch the Administration Console (see the *Conferencing Operations Guide* for more information).
- 2 Create new Communities with the Administration Console.
- 3 Install a Conferencing Client.
- 4 Use the Conferencing Client to create users and perform other administrative tasks.

## 2.9.2 Installing the Conferencing Client

- 1 After installing the Conferencing server, you can download the Conferencing client from the following URLs:
  - ♦ Windows: `http://<conferencing-portal-hostname>/imidio/downloads/conferencing.exe`
  - ♦ Linux: `http://<conferencing-portal-hostname>/imidio/downloads/conferencing.rpm`

You can send these Conferencing client installation URLs to your Conferencing users via e-mail for them to install the Conferencing client on their desktops.

If you have SSL enabled, you should specify https in the URL instead of http.

- 2 Select *Open* or *Run* to invoke the installer after the download completes.

It might take a while for the installation to begin on a Linux desktop.

After you install the client, use the *admin* screen name (password = *admin*) or the screen name of the first user of the first community to sign on.

After you sign on, you can add Conferencing users to the community (see the “Conferencing Operations Guide”).

### 2.9.3 Installing the Pidgin Instant Chat Client

After installing the Conferencing server, you can download the Pidgin client with Conferencing protocol support from the following URLs:

- ♦ Windows: <http://conferencing-portal-hostname/imidio/downloads/pidgin.exe>
- ♦ Linux: <http://conferencing-portal-hostname/imidio/downloads/pidgin.rpm>

---

**NOTE:** The SLED version is packaged in several RPMs. Install the RPMs listed under the heading that matches your system in the order listed. If you already have Pidgin installed, you can skip libpurple and pidgin.

---

- 1** Download the `pidgin.exe` (Windows) or `pidgin.rpm` (Linux) executable file to your desktop. The URLs for downloading these files should be in your invitation e-mail.
- 2** In Linux and Windows, double-click the *pidgin* (`.rpm` or `.exe`) installer (placed on the desktop during download), or select *Open* or *Run* to invoke the installer. It might take a while for the installation to begin on the Linux desktop.
- 3** In the *Installer Language* dialog that appears, select your language from the drop-down list. The installer wizard walks you through the installation process. The defaults should be fine for your install, though you might want to select the *Shortcut > Desktop* option.
- 4** Click *Finish* to complete the installation process. The integrated Pidgin instant chat client is now installed and ready for use.

See the Conferencing online help or the *Conferencing User Guide* for information on using the integrated Pidgin client with Conferencing.





# Reconfiguring and Upgrading

# 3

The following sections discuss both reconfiguration and upgrading the Conferencing servers and clients:

- ♦ [Section 3.1, “Backing Up and Restoring the Database,” on page 33](#)
- ♦ [Section 3.2, “Reconfiguring Conferencing Hosts,” on page 34](#)
- ♦ [Section 3.3, “Upgrading the Conferencing Client,” on page 34](#)
- ♦ [Section 3.4, “Upgrading the Conferencing Servers,” on page 34](#)
- ♦ [Section 3.5, “Starting and Stopping Conferencing Services,” on page 35](#)

## 3.1 Backing Up and Restoring the Database

Before doing any reconfiguration or upgrade of the Conferencing software, we recommend that you perform a backup of your existing database.

- ♦ [Section 3.1.1, “Backing Up the Database,” on page 33](#)
- ♦ [Section 3.1.2, “Restoring the Database,” on page 33](#)

### 3.1.1 Backing Up the Database

The system automatically backs up the database on a daily basis. The backups can be found in `/var/iic/db-backups` on the `db-host` (as defined in `/opt/iic/conf/global-config`). Each backup is a `tar(1)` archive compressed using the `bzip2(1)` utility. The current daily backup is called `db.tar.bz2`.

You can also back up the database at any arbitrary time using the `pg_dump(1)` utility. The state of the database in the backup is that of all committed transactions at the time `pg_dump(1)` is run. Any updates done after the backup is started are ignored.

The following command line shows how to dump the contents of the database to a `tar(1)` archive named `db.tar`:

```
pg_dump -b -F t -f db.tar <db_name>
bzip2 db.tar
```

You can either execute `pg_dump` on the `db_host` machine or set up the PostgreSQL environment variables according to the database configuration in `/opt/iic/conf/global-config`.

### 3.1.2 Restoring the Database

Restoring an archived database is done by using the `pg_restore` command. To restore a backup in a `bzip2` compressed tar file, the following command line can be used:

```
bunzip2 db.tar.bz2
pg_restore -d <db_name> db.tar
```

You can either execute `pg_restore(1)` on the `db_host` machine or set up the PostgreSQL environment variables according to the database configuration in `/opt/iic/conf/global-config`.

## 3.2 Reconfiguring Conferencing Hosts

Follow these steps to rerun the installation and change the configuration of the Conferencing hosts:

- 1 Make a backup copy of the `sitescape-conferencing` directory:  

```
cp -r sitescape-conferencing sitescape-conferencing.bk
```
- 2 Open the `sitescape-conferencing` directory.
- 3 Run `./install.sh`

The installation script prompts you for the configuration information. The prior configuration is used as the default values for the new configuration.

You are also asked whether you want to initialize the system database. You must initialize a database once before it can be used by the system. However, initializing a database that is already in use by the system results in all of the data being lost. Only initialize a database once on a database host.

## 3.3 Upgrading the Conferencing Client

- 1 Make a backup copy of the `sitescape-conferencing` directory:  

```
cp -r sitescape-conferencing sitescape-conferencing.bk
```
- 2 Open the `sitescape-conferencing` directory.
- 3 Copy the new `installers.tar.gz` archive into your installation directory
- 4 Run `./install.sh`

Conferencing users are automatically upgraded the next time they log on.

## 3.4 Upgrading the Conferencing Servers

- 1 Make a backup copy of the `sitescape-conferencing` directory:  

```
cp -r sitescape-conferencing sitescape-conferencing.bk
```
- 2 Extract the new distribution file using:  

```
tar zxvf sitescape-conferencing-<version>.tar.gz.
```
- 3 Open the `sitescape-conferencing` directory.
- 4 Copy the prior configuration directory to the current location:  

```
cp -r ../sitescape-conferencing.bk/myzon
```
- 5 Run `./install.sh`

The installation script prompts you for the configuration information. The prior configuration is used as the default values for the upgrade.

---

**WARNING:** When asked whether you want to initialize the system database, answer `no` unless you want to delete all of your data.

---

## 3.5 Starting and Stopping Conferencing Services

- ♦ [Section 3.5.1, “Starting and Stopping the Cluster,” on page 35](#)
- ♦ [Section 3.5.2, “Starting and Stopping Individual Machines,” on page 35](#)

### 3.5.1 Starting and Stopping the Cluster

You can start or stop Conferencing services for the entire cluster by using the `control-cluster.sh` script.

To stop Conferencing Services, enter:

```
./control-cluster.sh --cluster <your-cluster> [--single-host <your-host>] stop
```

To start Conferencing Services, enter:

```
./control-cluster.sh --cluster <your-cluster> [--single-host <your-host>] start
```

Use the `--single-host` argument with the script if there is only one host in your cluster.

### 3.5.2 Starting and Stopping Individual Machines

To start or stop services on only one of the machines on the cluster, use the following script:  
`/opt/iic/conf/control-services.sh`.

To stop Conferencing Services with `control-services.sh`, enter:

```
/opt/iic/conf/control-services.sh stop
```

To start Conferencing Services with `control-services.sh`, enter:

```
/opt/iic/conf/control-services.sh start
```



# Modifying Template Files

# 4

The `install.sh` installation script prompts you to indicate whether you want to modify various e-mail body templates. The following sections describe the available e-mail body templates and how to modify them:

- ♦ [Section 4.1, “Modifying the Meeting Invitation Template,” on page 37](#)
- ♦ [Section 4.2, “Using IF Statements,” on page 38](#)
- ♦ [Section 4.3, “Modifying the Meeting Summary E-Mail Template,” on page 39](#)
- ♦ [Section 4.4, “Modifying the New User Greeting E-mail Template,” on page 39](#)

During the installation, you have the opportunity to edit both the new user and invitation templates. You can do this by editing the templates and then importing them, or by using emacs on an install host.

## 4.1 Modifying the Meeting Invitation Template

The meeting invitation template has two roles. The first role is to fill the body of the meeting invitation e-mail sent to meeting participants. The second role is to create the content of an IM invitation sent to meeting participants. In order to fulfill these two roles, the template is divided into sections. The purpose of each section is to specify whether the text produced in a section should be included in an e-mail body, IM content or both. The syntax for a section is as follows:

```
#SECTION selector
.
.
.
#SECTION END
```

The *selector* variable represents one of the following values:

**Table 4-1** *Selector Variable Values*

Value	Description
EMAIL_IM	The text produced in this section is present in both e-mail and IM meeting invitations.
EMAIL_ONLY	The text produced in this section is present only in e-mail meeting invitations.
IM_ONLY	The text produced in this section is present only in IM meeting invitations.

The basic operation in the section is to echo (that is output) text. For example:

```
echo Click here to enter the meeting <MEETINGURL><NEWLINE>
echo Pin:
echo <INVITEE-PIN><NEWLINE>
```

There are several things to notice about these lines. One is that the output from an echo is appended to the result of the prior echoes. If you want a line break at a particular point, you must explicitly provide the line break by using the `<NEWLINE>` tag. Also, an echo line might contain tags that are replaced with values particular to the meeting to which the participant is invited. You can use the following tags:

**Table 4-2** *Meeting Value Tags*

Tag	Description
<code>&lt;TITLE&gt;</code>	This tag is replaced with the title of the meeting.
<code>&lt;HOST&gt;</code>	This tag is replaced with the host of the meeting.
<code>&lt;TIME&gt;</code>	This tag is replaced with the scheduled start time of the meeting.
<code>&lt;DESCRIPTION&gt;</code>	This tag is replaced with the description of the meeting.
<code>&lt;MESSAGE&gt;</code>	This tag is replaced with the invitation message (if any) that the host provided when creating the meeting.
<code>&lt;INVITEE-NAME&gt;</code>	This tag is replaced with the name of the participant.
<code>&lt;INVITEE-PHONE&gt;</code>	This tag is replaced with the phone number of the participant.
<code>&lt;INVITEE-PIN&gt;</code>	This tag is replaced with the Pin of the participant.
<code>&lt;MEETING-URL&gt;</code>	This tag is replaced with URL to click for the participant to join the meeting.
<code>&lt;ANONYMOUS-URL&gt;</code>	This tag is replaced with URL to click for an anonymous meeting participant to join the meeting.
<code>&lt;MEETING-PHONE&gt;</code>	This tag is replaced with the title of the meeting.
<code>&lt;ANONYMOUS-PIN&gt;</code>	This tag is replaced with the Pin for an anonymous invited participant.
<code>&lt;PASSWORD&gt;</code>	This tag is replaced with the meeting password for the meeting.

## 4.2 Using IF Statements

In addition to the `echo` command, conditional text can be generated. The way to specify conditional text is using an `%IF` statement. The `%IF` statement is as follows:

```
%IF variable-expression
.
.
%IF END
```

The *variable-expression* variable is either a Boolean variable, or if it is prefixed with an exclamation point, the negation of the variable. If the *variable-expression* is true, the contents of the `%IF` are executed. If false, they are not. There is no `ELSE` clause.

The following variables are available for use:

**Table 4-3** *Variable-Expression Variables*

Variable	Description
CALL_IN	True when the meeting has a voice conference associated with it and the participant has no phone number.
CALL_OUT	True when the meeting has a voice conference associated with it and the participant has a phone number.
DESCRIPTION	True when a non-empty description exists for the meeting.
MESSAGE	True when a non-empty invitation message exists for the meeting.
PASSWORD	True when a non-empty password exists for the meeting.
PRIVATE	True when the meeting is a private meeting.

## 4.3 Modifying the Meeting Summary E-Mail Template

The meeting summary e-mail body template contains text with embedded tags that are replaced with values particular to the meeting that ended. The non-tag text is left as is in the e-mail body.

The following table lists the available tags:

**Table 4-4** *Meeting Summary Embedded Tags*

Tag	Description
<MeetingID>	This tag is replaced with the meeting ID of the meeting that ended.
<StartDateTime>	This tag is replaced with the start time and date of the meeting that ended.
<Duration>	This tag is replaced with duration of the meeting that ended.
<VoiceRecording>	This tag is replaced with YES or NO depending on if there is a voice recording associated with the meeting that ended.
<DataRecording>	This tag is replaced with YES or NO depending if there is a recording of the app/desktop sharing sessions associated with the meeting that ended.
<MeetingParticipants>	This tag is replaced with a list of the participants and some of their contact information for the meeting that ended.

## 4.4 Modifying the New User Greeting E-mail Template

When new users are added to the system, they receive an e-mail notification informing them that they are now a user of the system and providing them with information on using Conferencing. You can tailor the body of this e-mail by modifying the following file:  
`sitescape-conferencing/<cluster>/new-user-template.default.`

When the system creates the body of new user e-mail, it replaces a number of tags with information particular to the new user. Any remaining text that is not a tag is left as is.

The following table lists the available tags:

**Table 4-5** *New User E-Mail Tags*

Tag	Description
<IICNAME>	This tag is replaced with the user's full name.
<IICUSERNAME>	This tag is replaced with the user's screen name.
<IICPASSWORD>	This tag is replaced with the user's initial password.
<IICDIALIN>	This tag is replaced with the voice bridge phone number.
<IICPERSONALPIN>	This tag is replaced with the user's Instant Meeting PIN.
<IICMEETINGID>	This tag is replaced with the user's Instant Meeting ID.
<IICPRODNAME>	This tag is replaced with the name of the product entered by the installer during server installation.
<ZONLANG>	This tag is replaced with the locale entered by the installer during server installation.
<IICPORTAL>	This tag is replaced with the URL of the server – e.g. iic.homedns.org.



# Configuring ssh() Key Authentication

# A

The installation script uses `ssh()` and `scp()` to copy files to and execute scripts on the Conferencing hosts. In order to avoid typing the `root` password for the Conferencing hosts numerous times during the install, you can configure private/public key authentication for `ssh(1)`. If private/public key authentication is in place, rather than prompting for the `root` password, `ssh()/scp()` gets an authentication token generated by using the private key. It authenticates the token on the Conferencing host by using the `root` user's list of authorized public keys.

**Use the following procedures to configure public/private key authentication:**

- ♦ [Section A.1, “Generating a Public/Private Key Pair,” on page 41](#)
- ♦ [Section A.2, “Configuring the ssh Key Agent,” on page 41](#)
- ♦ [Section A.3, “Adding the Public Key to the Root User’s Set of Authorized Keys,” on page 42](#)

## A.1 Generating a Public/Private Key Pair

To generate a key pair, use the `ssh-keygen(1)` command.

Here is a sample interaction with `ssh-keygen`:

```
-bash-2.05b$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/admin/.ssh/id_rsa):
Enter passphrase (empty for no passphrase): *****
Enter same passphrase again: *****
Your identification has been saved in /home/admin/.ssh/id_rsa.
Your public key has been saved in /home/admin/.ssh/id_rsa.pub.
The key fingerprint is:
8c:ff:d4:50:65:46:9f:6b:59:34:43:3a:5f:e7:5a:54 admin@staging.my.com
```

At this point, there are two new files in the home directory: `~/.ssh/id_rsa` and `~/.ssh/id_rsa.pub`. The first file is the private key (in binary form) and the second is the public key (in text form).

## A.2 Configuring the ssh Key Agent

In order to use the newly generated private key, you must start the ssh key agent, `ssh-agent`, and add the key to the set of keys held by the agent. In order to have the keys available whenever you log on, edit the `~/.bash_profile` file. The following shell script snippet should be inserted at the end of the file:

```
if [-z "$SSH_AUTH_SOCK"]; then
 eval $(ssh-agent)
 ssh-add
fi
```

After saving `~/.bash_profile`, log off and log back in to the staging host. You are prompted for the private key passphrase entered when the key pair was generated. After you successfully enter the passphrase, the private key is available for generating authentication tokens.

## A.3 Adding the Public Key to the Root User's Set of Authorized Keys

The final step is to add the public key (`~/.ssh/id_rsa.pub` on the staging host) to the set of authorized keys for the `root` user on the Conferencing host.

Enter the following commands to add the key:

```
$ scp ~/.ssh/id_rsa.pub root@zonhost:/tmp
$ ssh root@zonhost
The authenticity of host 'zonhost (W.X.Y.Z)' can't be established.
RSA key fingerprint is
df:c7:21:77:ec:53:89:77:4f:32:4d:a8:7a:a2:c2:7c.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'jabber,10.0.1.3' (RSA) to the list of
known hosts.
root@zonhost's password: *****
cat /tmp/id_rsa.pub >> .ssh/authorized_keys
chmod 700 .ssh
chmod 600 .ssh/authorized_keys
```

Repeat the above process for all the Conferencing hosts.

# Editing the global-config File

# B

The `./install.sh` installation script takes care of updating the `global-config` file. If you want to edit the file directly, use the information in this section.

The overall system configuration is in the `global-config` file. The following procedures are required to configure a Conferencing server system.

- ♦ [Section B.1, “Assigning Services to Nodes,” on page 43](#)
- ♦ [Section B.2, “Configuring Web Services,” on page 45](#)
- ♦ [Section B.3, “Configuring the Mailer,” on page 45](#)
- ♦ [Section B.4, “Using Port Forwarding,” on page 45](#)

---

**IMPORTANT:** All hostnames currently need to be lowercase.

---

## B.1 Assigning Services to Nodes

The following steps are necessary to configure the services that run on the cluster nodes.

### 1 Configure the database server for each node:

**1a** Change the `db_host` variable assignment to specify the database host.

**1b** For new installations, do not change `db_name`, `db_user` and `db_pswd`.

**1c** Define the host access to the database.

The servers that run the address book, XML routers, and Web portals must have access to the database. You can specify access to the database host using a set of IP addresses and netmasks. An IP address/netmask pair specifies a range of IP addresses that are allowed to connect to the database. For instance, `10.1.1.1/255.255.255.0` allows IP addresses `10.1.1.*` to connect to the database. The IP addresses are specified in `db_ip_addr` and the netmasks in `db_netmask`. Both are arrays, so the above example would be:

```
db_ip_addr=(10.1.1.1)
db_netmask=(255.255.255.0)
```

### 2 Configure XML router services:

**2a** Set `external_hname` to the hostname used by Conferencing clients to connect to XML router services.

**2b** Set the `lcl_xmlrouter` and `lcl_xmlrouter_ip` arrays to specify the cluster hosts and IP addresses for the XML router services. More than two XML routers are not currently supported.

### 3 Configure services connected to the XML router:

**3a** Configure the meeting controller service and the backup meeting controller service if necessary. Specify the cluster hosts to run each and the XML router listen ports. The hosts are specified in the `controller_host` array and the listen ports in the `controller_port` array.

- 3b** Configure the `addressbk` service. Specify the cluster host and XML router listen ports by setting the `addressbk_host` array and the `addressbk_port` array. Currently, only one `addressbk` is supported.
- 3c** Configure the `mailer` service. Specify the cluster host and XML router listen ports by setting the `mailer_host` array and the `mailer_port` array. Currently, only one `mailer` is supported.
- 3d** Configure the voice bridges. Multiple voice bridges can be configured for scaling purposes (see [Appendix C, “Editing the dialing.xml File,” on page 47](#)):
  - 3d1** Specify the cluster hosts and XML router listen ports by setting the `voice_host` array and the `voice_port` array.
  - 3d2** Specify the voice provider for the voice bridges using the `voice_provider` variable. If no voice support has been purchased, use the value `stub`. If an NMS voice bridge has been purchased, use the value `nms`.
  - 3d3** Specify the phone numbers allocated to each bridge by using the `voice_phones` array. You can assign multiple phone numbers to a single voice bridge by separating the phone numbers with commas. Note that if spaces appear in phone numbers, the phone numbers must be quoted. Also, if the `stub` voice provider is in use, a dummy voice bridge number must be specified (such as “999-555-1234”).
- 3e** Configure the meeting archiver services. You can configure multiple meeting archivers for scaling purposes:
  - 3e1** Specify the assigned cluster hosts and XML router listen ports by setting the `mtgarchiver_host` array and the `mtgarchiver_port` array.
  - 3e2** If the meeting archiver hosts are separated from a voice bridge host by a NAT router, use the `mtgarchiver_voice_host` array to specify the voice bridge hosts from the meeting archivers’ perspective. If no NAT router is involved, the meeting archivers attempt to connect to the voice bridges using the hostnames found in `voice_host`.
- 3f** Configure the external API service by specifying the cluster host and XML router listen ports to set the `extapi_host` and `extapi_port` arrays. You can use multiple external API hosts.
- 4** Configure the app/desktop sharing servers:
  - 4a** Configure the `share_host` array to specify which hosts run as app/desktop sharing servers.  
  
You can run multiple app/desktop servers on a single host by specifying a host multiple times. For instance if `share_host` was assigned the value `kanga kanga roo`, the host named `kanga` would run two servers and `roo` would run one. Also, be aware that you would need to define two distinct IP addresses on `kanga`, because both servers use port 80 for tunneling through firewalls.
  - 4b** Configure the port to use for each share server using the `share_port` array.  
  
This port can remain as 2182, because the IP addresses must be distinct for each share server. Port 2182 does not conflict with any default Linux service.

## B.2 Configuring Web Services

You can implement the Web portal for the system across multiple hosts. When you use multiple Web services, the meeting archive repository must reside in a file system accessible to all HTTP daemons. For instance, it can reside on a NAS box or via an NFS exported file system on one of the cluster hosts. In any event, the shared file system must be accessible via `/usr/local/apache2/htdocs/repository/mtgarchive` on all the machines hosting the HTTP daemon. Also, you are responsible for configuring a load balancer for HTTP requests to these machines.

When configuring the external API HTTP daemons, administrative functions are performed via HTTP on the external API hosts. For added security, these hosts can be placed behind a firewall. However, the hosts assigned to run the Web portal must be able to connect to the external API hosts via port 8000 in order for the admin console to function properly.

### 1 Configure Web portal hosts:

- 1a** Modify the `portal_hname_local` array to specify all the cluster hosts for Web service.
- 1b** Ensure that `/usr/local/apache2/htdocs/repository/mtgarchive` is the same shared file system for all cluster hosts in `portal_hname_local`.
- 1c** Modify the `portal_ip` array to include the IP addresses that the HTTP daemon should listen on for connections.
- 1d** Modify the `portal_hname` variable to define the hostname used in URLs to the Web portal.

### 2 Configure external API hosts:

- 2a** Modify the `extapi_hname_local` array to specify all the cluster hosts for the external API service.
- 2b** Modify the `extapi_portal_ip` array to specify the IP addresses on which an external API HTTP daemon listens.
- 2c** Modify the `extapi_portal_hname` to specify the hostname in URLs to the external API.

## B.3 Configuring the Mailer

By default, the system is configured to assume that the cluster node assigned to the mailer is able to perform mail delivery. If that is not the case for some reason, you can configure the mailer to use an external SMTP host for mail delivery. You can use the variables `smtp_host`, `smtp_user`, and `smtp_pswd` in `global-config` for this purpose.

## B.4 Using Port Forwarding

By default, each cluster host running either an XML router or app/desktop sharing servers forwards ports 1270 and 443 to the respective service ports. If you have an installation that is running a load balancer that provides port forwarding, set the `global-config` variable `iptables_port_forwarding` to `no` and configure your load balancer accordingly.



# Editing the dialing.xml File

# C

This section applies only to those clusters that are running a voice bridge.

The role of the `dialing.xml` file is to specify the rules whereby a given phone number is transformed into the set of digits dialed by the voice server. For example, default area codes that must be appended to all 7-digit phone numbers. Most of the file consists of a collection of attributes and their values. The following table lists the attributes and their roles:

**Table C-1** *Dialing.xml Attributes*

Attribute	Description
areaCode	This attribute is a default area code to use when none is present in a phone number.
tollPrefix	This attribute is the prefix to dial in order to place a long-distance call. In the US, it is a 1.
i18nPrefix	This attribute is the prefix to use when placing international calls. In the US, 011.
country	A short description of the country the bridge is located in (such as US).
countrycode	This is the international country code of the voice bridge. This code is used to decide whether a number requires that an international call be placed. For the US, the value is 1.
dialingMode	The attribute can be one of the following values: <ul style="list-style-type: none"><li>♦ normal: Do not dial an area code except for long distance calls.</li><li>♦ dialAreaCodeAlways: The phone numbers always have an area code. The area code of the bridge can be used to supply missing area codes.</li><li>♦ DialAreaCodeOnLD: Only dial an area code for long distance numbers (see areaCodes/exchanges lists below).</li></ul>

The remaining components of the file are two lists: area codes and exchanges. The role of these lists is to determine whether a specified phone number requires a long-distance call by specifying a default condition (either local or long-distance) for area codes or exchanges. The list itself is a set of exceptions to the default. For instance, to specify that all area codes are long-distance except for 978, the following can be used:

```
<areaCodes default="ld">
 <local>978</local>
</areaCodes>
```

Similarly with exchanges, you could, for example, specify that most exchanges are long-distance, but 865 is local:

```
<exchanges default="ld">
 <local>865</local>
</exchanges>
```





# Updating Meeting Invitation Web Pages

# D

The image that appears at the top of meeting invitation Web pages can be found in `/usr/local/apache2/imidio/images/instant.jpg`. On the Web portal hosts, you can replace that file with another logo. However, this file is not preserved during updates or reconfigurations and must be restored after the upgrade or reconfiguration is complete.

If the dimensions of the new logo are different from the default, you might need to adjust the `<img>` element in `/usr/local/apache2/htdocs/imidio/invite/frame_header.php`.

You can modify the body of the meeting invitation Web pages by updating `/usr/local/apache2/htdocs/imidio/invite/*.html`

---

**NOTE:** These files are not saved after upgrades or reconfigurations.

---



# LDAP User Authentication



The password for `admin` always comes from the Conferencing internal database so that an administrator is able to log on even if directory servers are not available. Because the password must be passed over the network in plain text, we recommend deployment through SSL.

Once you synchronize Conferencing using LDAP, you cannot use the `useradmin` account to manage users rights, unless you have a matching user in your LDAP directory. Only the `admin` account continues to work with its original password.

---

**NOTE:** You can use the `admin` account to sign on to and manage any community using this form of screen name:

`admin@community name`

For example, to sign on to the default user community, use:

`admin@Users`

You can then configure users synced from the LDAP directory to be community administrators. You can also adjust system policies, etc. for that community. The preferred method for changing fields synced from LDAP is to change them on the LDAP server. If you change fields locally, those changes might get overwritten during the next LDAP sync.

---

**IMPORTANT:** You must be in the `/opt/iic/bin/` directory whenever you run the `ldap-sync.sh` command.

---

- ♦ [Section E.1, “LDAP User Authentication Input File,” on page 51](#)
- ♦ [Section E.2, “Conferencing Field Names,” on page 52](#)
- ♦ [Section E.3, “Address Book Configuration \(Synchronization\),” on page 52](#)

## E.1 LDAP User Authentication Input File

You can modify the `sitescape-conferencing/cluster-prototype/ldap.xml.in` input file to use Active Directory\* synchronization instead of eDirectory\* synchronization, and to map additional LDAP attributes to Conferencing contact fields.

To use Active Directory synchronization, you need to comment out the eDirectory section in the file and uncomment out the Active Directory section. See the examples below:

### eDirectory Section

```
<!-- configuration for eDirectory and generic LDAP server -->
<attributes>
 <attribute>
 ...
 </attribute>
</attributes>
```

Move the closing XML comment tag (`-->`) after the `...generic LDAP server` comment so that it follows the `</attributes>` tag under the eDirectory section:

```

<!-- configuration for eDirectory and generic LDAP server
<attributes>
 <attribute>
 ...
 </attribute>
</attributes>
-->

```

### ActiveDirectory Section

```

<!-- configuration for ActiveDirectory
<attributes>
 <attribute>
 ...
 </attribute>
</attributes>
-->

```

Move the closing XML comment tag (`-->`) after the `</attributes>` tag so that it follows the configuration for ActiveDirectory comment:

```

<!-- configuration for ActiveDirectory -->
<attributes>
 <attribute>
 ...
 </attribute>
</attributes>

```

## E.2 Conferencing Field Names

Use the following names to configure the mapping of LDAP attributes to Conferencing contact fields:

“screenname” - “title” - “firstname” - “middlename” - “lastname” - “suffix” - “company” - “jobtitle” - “address1” - “address2” - “state” - “country” - “postalcode” - “aimname” - “email” - “email2” - “email3” - “busphone” - “homephone” - “mobilephone” - “otherphone” - “extension” - “msnscreen” - “yahooscreen” - “aimscreen” - “user1” - “user2” - “defphone”

---

**NOTE:** For eDirectory, the `uid` attribute is mapped to the Conferencing `screenname` by default. If you want to use the `cn` LDAP attribute instead of the `uid` attribute, you can change this mapping to map the `cn` attribute to the Conferencing `screenname`.

---

## E.3 Address Book Configuration (Synchronization)

Make sure you are in the `/opt/iic/bin/` directory, then execute `ldap-sync.sh portal-server-hname` to perform the initial synchronization.

---

**NOTE:** After starting the server, wait about 20 seconds before executing this command. If you do not get an XML message back, you probably did not wait long enough.

---

This script displays an XML message if it fails (the fault message is clearly visible):

```
./ldap-sync.sh 151.155.136.84
curl: (7) couldn't connect to host
```

In this example, the right server was used with the wrong address. Check the global-config file:

```
portal_ip=(151.155.136.85)
portal_local_hname=(localhost)
```

If it succeeds, the XML data contains a single number that is the number of users actually synchronized:

```
./ldap-sync.sh 151.155.136.85
<methodResponse>
<params>
<param><value><array><data>
<value><i4>6</i4></value>
</data></array></value></param>
</params>
</methodResponse>
```

You can run this script manually as needed, or use `cron` to configure it to run periodically. The default setting is for it to run daily.



# Installing the NMS Board

# F

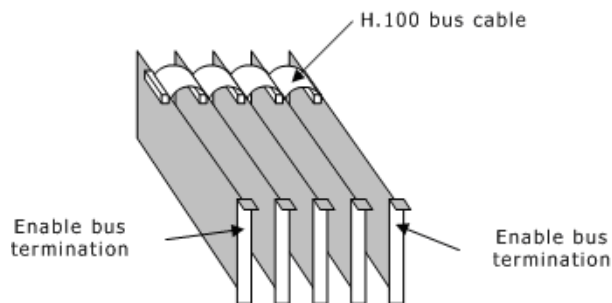
**WARNING:** The CG 6565 and CG 6060 board is shipped in a protective anti-static container. Leave the board in its container until you are ready to install it. Handle the board carefully and hold it only by its edges and avoid touching its circuitry. NMS recommends that you wear an anti-static wrist strap connected to a good earth ground whenever you handle the board.

- 1 Ensure that your computer meets the systems requirement below:
  - ♦ A chassis with an available PCI bus slot with 5.0 V and 3.3 V of supplied power.
  - ♦ 32 bit SUSE Linux 10 SP1 kernel version 2.6.16.46-0.12
- 2 Power down the chassis and disconnect it from the power source.
- 3 Remove the cover and set it aside.
- 4 If you are installing more than one board, configure the two boards that are at the ends for H.100 bus termination. This is also a good time to configure the board(s) for PCI mode or PCI-X mode. This depends on the PCI slots in your chassis. Detailed instructions for both [H.100 termination](#) and [PCI, PCI-X mode configurations](#) are provided.
- 5 Arrange the CG board(s) in adjacent PCI bus slots. Make sure each board's PCI bus connector is seated securely in a slot.
- 6 Secure the end bracket on the board(s) to the chassis.
- 7 If you have multiple CG boards, connect the H.100 bus cable to each of the CG boards.
- 8 Replace the cover and connect the computer to its power source.
- 9 Skip this step if your conference bridge only supports IP clients. If you have installed CG6565/64, now is the time to connect the mini RJ21 cable to the back of the CG6565/64 and the other end to the SEP panel to gain access to the 8 T1 or E1 trunks.

## F.1 Configuring H.100 Bus Termination

H.100 boards are connected to one another with an H.100 bus cable. The two boards located at either end of the H.100 bus must have bus termination enabled, as shown in the following illustration. Bus termination is controlled by a DIP switch as explained below.

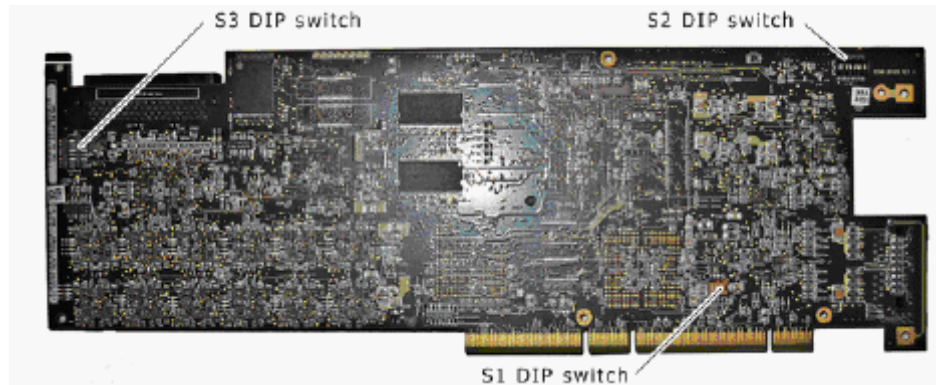
**Figure F-1** H.100 Bus Termination



## F.2 Configuring the DIP Switches

The CG 6565 DIP switches are located on the board, as shown in the following illustration:

**Figure F-2** CG 6565 DIP Switches



### F.2.1 S3 DIP Switch

The S3 DIP switch controls the H.100 bus termination. By default, all S3 switches are set to OFF (H.100 bus termination disabled). Setting all S3 switches to ON enables H.100 bus termination. Set all S3 switches to ON only for the boards that are on the ends of the H.100 bus.

---

**NOTE:** The switches in the S3 DIP switch must be set to either all ON or all OFF.

---

### F.2.2 S2 DIP Switch

Switch 5 in the S2 DIP switch allows you to control if the board LEDs can be off or on. (This is known as the dark office feature.) By default, switch 5 is set to OFF (all LEDs can be on). Setting switch 5 to ON turns off all LEDs on the board unless there is an error.

### F.2.3 S1 DIP Switch

The S1 DIP switch sets the mode of the board. By default, the switches set the board to the PCI mode.

---

Mode	Settings
PCI	Switch 1 is set to ON.
	Switch 2 is set to OFF.
	Switch 3 is set to ON for 33 MHz or to OFF for 66 MHz.
	Switch 4 is set to ON.

---



Mode	Settings
PCI-X	Switch 1 is set to OFF. Switch 2 is set to ON for 66 MHz or to OFF for 100-133 MHz. Switch 3 is set to OFF. Switch 4 is set to ON.

## F.3 nmsconfig - Board Configuration Utility

nmsconfig is a board configuration utility that detects the CG boards in the chassis and asks you a series of questions to configure the boards properly.

Fill out this worksheet below before running the install script.

### nmsconfig Worksheet

Print out one worksheet for each board you install in the chassis.

Board IP address: \_\_\_\_\_

Board Subnet mask: \_\_\_\_\_

Board Gateway address: \_\_\_\_\_

Circle the number that best describes the conference bridge:

1. The bridge will only support IP clients
2. The bridge will support both IP and PSTN clients

If 1 is circled above the worksheet is done for this board otherwise continue to fill out the rest of the worksheet.

Circle the type of trunks that will be used on the board:

1. T1
2. E1

Circle the type of signaling that will be used:

1. CAS (Channel Associated Signaling, i.e. wink start, ground start etc.)
2. ISDN

If you circled T1 and CAS for the last two questions go to the T1 CAS section.

If you circled T1 and ISDN then go to the T1 ISDN section of the worksheet.

If you circled E1 and CAS then go to the E1 CAS section of the worksheet.

If you circled E1 and ISDN then go to the E1 ISDN section of the worksheet.

## **T1 CAS Section**

Circle the trunk frame type:

1. D4 (Superframe Formatting)
2. ESF (Extended Superframe Formatting)

Circle the trunk line code:

1. B8ZS (Binary 8-Zero code Suppression)
2. AMI (Alternate Mark Inversion)
3. AMI with jammed bit 7 zero code suppression
4. AMI with jammed bit 7 zero code suppression Bell Ver.
5. AMI with zero data byte replaced with 1001 1000
6. AMI with jammed bit 8 zero code suppression

Circle the trunk protocol:

1. Wink start protocol
2. Ground start protocol
3. Loop Start protocol
4. Feature group D protocol
5. Off-premises station protocol
6. Multi-frequency R2 protocol
7. European Digital CAS protocol
8. Australian P2 protocol
9. NEC PBX protocol

The worksheet is done for this board.

## **T1 ISDN Section**

Circle the trunk frame type:

1. D4 (Superframe Formatting)
2. ESF (Extended Superframe Formatting)

Circle the trunk line code:

1. Binary 8-zero code suppression (B8ZS)
2. Alternate mark inversion (AMI)
3. AMI with jammed bit 7 zero code suppression
4. AMI with jammed bit 7 zero code suppression Bell Ver.
5. AMI with zero data byte replaced with 1001 1000
6. AMI with jammed bit 8 zero code suppression

The worksheet is done for this board.

## **E1 CAS Section**

Circle the trunk line code:

1. HDB3 (High Density Bipolar 3 code)
2. AMI (Alternate Mark Inversion)

Circle the trunk impedance:

1. G.703 - standard 75 ohm cables
2. G.703 - standard 120 ohm cables

Circle the trunk protocol:

1. Wink start protocol
2. Ground start protocol
3. Loop Start protocol
4. Feature group D protocol
5. Off-premises station protocol
6. Multi-frequency R2 protocol
7. European Digital CAS protocol
8. Australian P2 protocol
9. NEC PBX protocol

The worksheet is done for this board.

## **E1 ISDN Section**

Circle the trunk line code:

1. HDB3 (High Density Bipolar 3 code)
2. AMI (Alternate Mark Inversion)

Circle the trunk impedance:

1. G.703-standard 75 ohm cables
2. G.703-standard 120 ohm cables

The worksheet is now done for this board.