Novell Conferencing

1.0.1

www.novell.com

OPERATIONS GUIDE

May 1, 2008

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/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

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/) 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).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (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 The Administration Console 11

2.1 Starting the Administration Console . . . 11
2.2 Using the Administration Console . . . 11
2.2.1 Component Status Page . . . 12

3 Conferencing Communities 13

3.1 Managing Communities . . . 13
3.2 Adding Communities . . . 14
3.3 Viewing Communities . . . 15
3.3.1 To Show All Communities . . . 15
3.3.2 To Find a Community by Name . . . 15
3.4 Removing Communities . . . 17
3.5 Updating Communities . . . 17

4 Adding Users and Policies 19

4.1 Creating Policies . . . 19
4.2 Creating a New User . . . 23
4.3 Change the Policy for a User . . . 24
4.4 Reset the Password for a User . . . 25

5 Obtaining Server Status 27

5.1 Viewing Components . . . 27
5.2 Viewing Active Meetings . . . 28
5.3 Determining Voice Port Status . . . 30
5.4 Conferencing System Component Logging . . . 30
5.5 Assessing System Load . . . 31

6 Auditing System Events 33

6.1 Real-Time Event Logs . . . 33
6.1.1 Determining Whether Real-Time Events Are Enabled . . . 33
6.1.2 Determining Hosts and Ports . . . 34
6.1.3 Call Record Host and Port . . . 34
6.1.4 User Record Host and Port . . . 34
6.1.5 Reservation Record Host and Port . . . 34
6.1.6 Connecting to Real-Time Event Logs . . . 34
6.2 User Record Format . . . 34
6.3 Call Data Records . . . 36

6.4 Reservation Data Records . . . 38
6.4.1 Reservation Data Record (RDR) Interface . . . 39
6.5 Chat Audit Log Configuration . . . 39

7 Conferencing Administration 41

7.1 Starting and Stopping Conferencing Services . . . 41
7.1.1 Starting and Stopping the Cluster . . . 41
7.1.2 Starting and Stopping Individual Machines . . . 41
7.2 Backing Up the Database . . . 42
7.3 Restoring the Database . . . 42

A LDAP User Authentication 43

A.1 LDAP User Authentication Input File . . . 43
A.2 Conferencing Field Names . . . 44
A.3 Address Book Configuration (Synchronization) . . . 44

B Troubleshooting Strategies 47

B.1 Verifying That Everything is Running . . . 47
B.2 Enabling Debug Logging . . . 47
B.3 Using the Service Watchdog . . . 48
B.4 Error Codes . . . 48
B.5 Advanced Checks . . . 50
B.6 Conferencing Client . . . 50
B.7 Voice Bridge . . . 51
B.8 Meeting Archiver . . . 51

About This Guide

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

This guide provides information about the following:

- Conferencing Communities
- Adding Users
- Obtaining Server Status
- Auditing System Events
- Conferencing Administration
- Troubleshooting Strategies
- LDAP User Authentication

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) 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 Server Installation 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 Operations Guide* and other documentation, visit the Novell Teaming Web site (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 provides a description of the system components.

- 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.

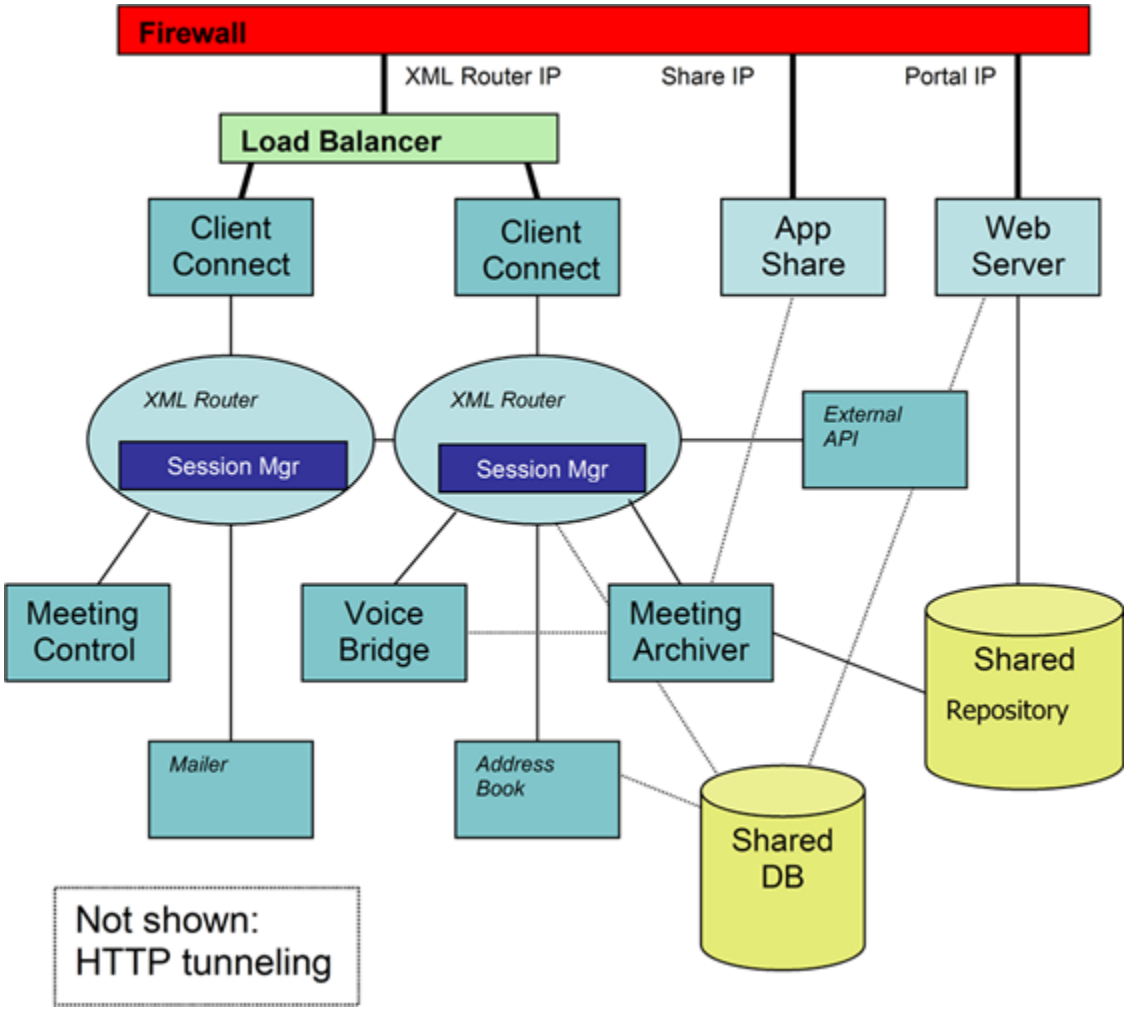
The system components are as follows:

- 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 and 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, application/desktop shared images, and chat sessions to create meeting archives based on Macromedia* Flash* and 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 based on invitation URL.
- External Web Service: Provides Web service APIs 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*



The Administration Console 2

This section describes the Conferencing Administration Console, including logging into the console and a description of the available tools.

- Section 2.1, “Starting the Administration Console,” on page 11
- Section 2.2, “Using the Administration Console,” on page 11

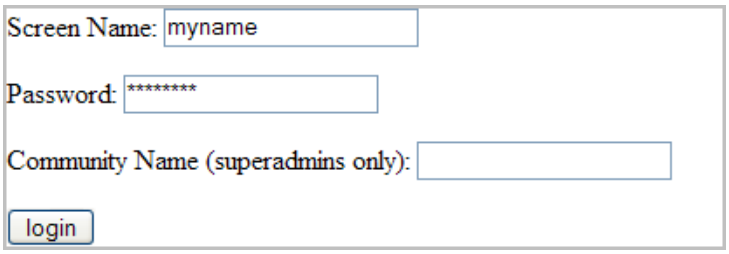
2.1 Starting the Administration Console

Conferencing provides an Administration Console based on a Web browser, to assess the status of clusters and manage system communities. The URL for the Administration Console depends on the setting of the `global-config` variable `<portal-hname>` defined at system installation time. The Administration Console can be accessed by using the following URL:

`http://portal_hname/imidio/console/`

After you access this page, you need to log in. When the software is installed, a default Super Administrator account is created with the screen name `admin` and password `admin`. A Super Administrator has the authority to manage all communities, while Community Administrators only have administrative authority within their specific community or communities. However, a Super Administrator can be restricted to a single community by entering a community name when logging in.

Figure 2-1 *Administration Console Login*



2.2 Using the Administration Console

Use the Administration Console to monitor the Conferencing server environment. Use the Administration Console tabs to perform the following functions:

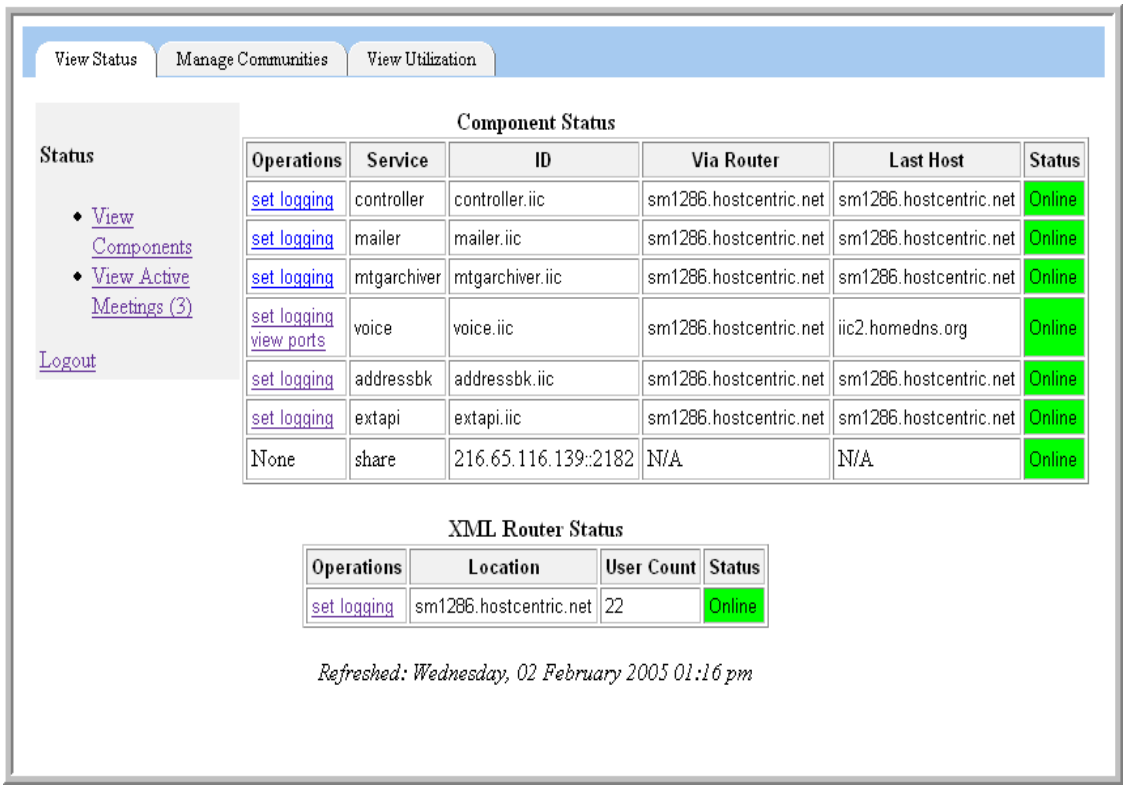
- Work with Conferencing user communities
- Obtain server and component status
- Determine the system load

For each function, an operations menu is available in a shaded box on the left of the page. You can exit the Administration Console at any time by clicking *Logout*.

2.2.1 Component Status Page

After you log on, you are on the main page of the Administration Console > Component Status Summary Page, which is a page similar to the following:

Figure 2-2 *Component Status Summary Page*



From this page, you can use the tabs to determine system status, manage communities or view system load. For each function, an operations menu is available in a shaded box on the left of the page. You can exit the Administration Console at any time by clicking *Logout*.

Conferencing Communities 3

A community is a group of users, usually within the same company or within a specific division within an organization. After you install and configure the Conferencing software, you need to set up communities and administrators for those communities. Community-member contacts are displayed in the Community Address Book in the Conferencing Client. When the Conferencing software is installed, a default System Community is created. This community provides the Super Administrator login and password information.

This section includes the following topics:

- Section 3.1, “Managing Communities,” on page 13
- Section 3.2, “Adding Communities,” on page 14
- Section 3.3, “Viewing Communities,” on page 15
- Section 3.4, “Removing Communities,” on page 17
- Section 3.5, “Updating Communities,” on page 17

3.1 Managing Communities

You can manage Conferencing communities with the Conferencing Administration Console. The *Manage Communities* tab provides tools for creating, deleting and modifying communities:

Figure 3-1 *Manage Communities Tab*

Use the *Manage Communities* tabs to perform the following functions:

- Display all communities
- Search for specific communities
- Add a new community
- Remove an existing community
- Modify an existing community

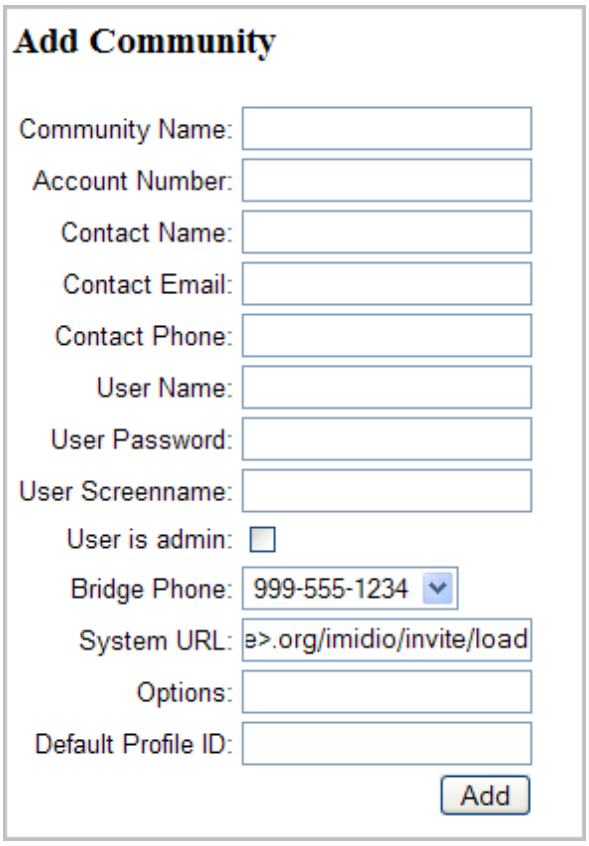
3.2 Adding Communities

A default System Community is created when you install the software. This System Community contains the Super Administrator username and password.

NOTE: A second community is automatically created to accomodate LDAP synchronization.

To Add a Community:

1. From the *Manage Communities* tab, click *Add* to display the *Add Community* form.



2. In the *Community Name* field, type a community name.

   The name of the community should be descriptive, and should only contain ASCII characters.

3. (Optional) In the *Account Number* field, type an account number.

   You can create an optional account number that you use for billing/cost center purposes. The *Account Number* field is alphanumeric.

4. In the *Contact Name* field, type the name of the individual who is the primary contact for this community.

5. In the *Contact Email* field, type the e-mail address of the primary contact.

6. In the *Contact Phone* field, type the phone number for the primary contact.

7. In the *User Name* field, type the name of the community administrator for the community (the user who creates the other users in the community via the Conferencing Client console). Enter the full name of the community administrator (for example, Bob Smith).

8 In the *User Password* field, type a password for the community administrator.

9 In the *User Screenname* field, type a screen name for the community administrator.

This is the screen name that other Conferencing users see for the community administrator when they access their Conferencing clients.

10 Select the *User is Admin* option to indicate that the user is a community administrator. Do not select this option if the first user in this community should not have administrative access.

11 Select the phone number of the voice bridge for this community from the *Bridge Phone* drop-down list.

12 In the *System URL* field, type the assigned system URL for community meeting invitations.

- The *Options* field is currently reserved and should be left blank.
- The *Default Profile ID* is also a reserved field and should be left blank.

13 After you have entered the new community data, click *Add* to create the community.

By default, when communities are defined, they are enabled. An enabled community is available for users to log into.

3.3 Viewing Communities

To view existing communities use the *Manage Communities* tab, then select the *Show All* or select the *Find* tool.

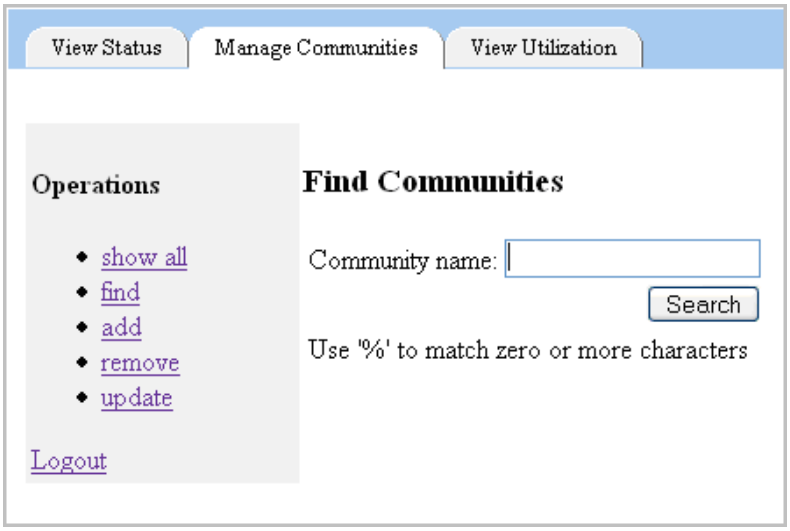
3.3.1 To Show All Communities

Use the *Show All* link to display all of the communities on the system. If more communities exist in the system than can be displayed on a page, use the *Previous* and *Next* buttons to scan the list of communities.

3.3.2 To Find a Community by Name

Use the *Find* link to display an entry field for the community name and a *Search* button:

Figure 3-2 *Community Search*



You can enter the entire community name, or use the % wildcard character to find a community. When a community that matches your search parameter is found, the *Find Communities* table displays the matching communities.

For example:

Figure 3-3 *Find Communities Table*

The *Find Communities* table contains the following values for each community returned in the search:

Operations Tools that allow you to update, remove or enable/disable a community. The users of a disabled community cannot log into the system.

Community ID: – The ID of the community that has been assigned by the database.

Community Name: The community name.

Account Number: The account number for the community, which can be used for billing/cost center purposes.

Contact Name: The primary contact for the community.

Contact Email: The e-mail address of the primary contact.

Contact Phone: The phone number of the primary contact.

User Name: The full name of the initial user of the community. Generally, the initial user is the community administrator.

User Password: The password for the initial user of the community.

Bridge Phone: The phone number for the voice bridge assigned to the community.

System URL: The URL that is used for community meeting invitation.

Account Type: The account type for the initial user. The account type can be either normal or admin.

Account Status: Indicates whether the community is enabled or disabled. A disabled community is not accessible by any of the community members.

3.4 Removing Communities

To delete existing communities, use the *Manage Communities* tab. You can do either of the following:

- Use *Remove*:
  1. Click *Remove* in the left column of the page to see a list of community names.
  2. Select the community you want to delete.
  3. Click *Delete*.
- Use *Show All* or *Find*:

  In either case, each community in the table contains a *Remove* link that removes that community.
  1. Select *Show All* or *Find* to search by community name. The *Community Results* table appears.
  2. In the row containing the community you want to delete, click *Remove*.

3.5 Updating Communities

To update or modify existing communities, use the *Manage Communities* tab. You can do either of the following:

- Click *Update* in the left column of the page to display a list of community names. Select the community to update and click *Edit*.
- Use *Show All* or *Find* to search by community name. In either case, each community in the community results table contains an *Update* link that updates that community.

Adding Users and Policies

4

After you establish your communities, you can add users to the system. Use the Conferencing client to accomplish this task.

This section includes the following topics:

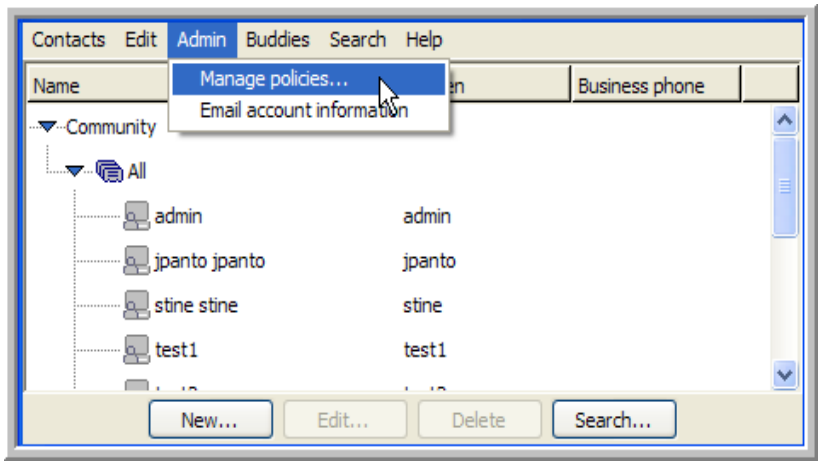
- Section 4.1, “Creating Policies,” on page 19
- Section 4.2, “Creating a New User,” on page 23
- Section 4.3, “Change the Policy for a User,” on page 24
- Section 4.4, “Reset the Password for a User,” on page 25

4.1 Creating Policies

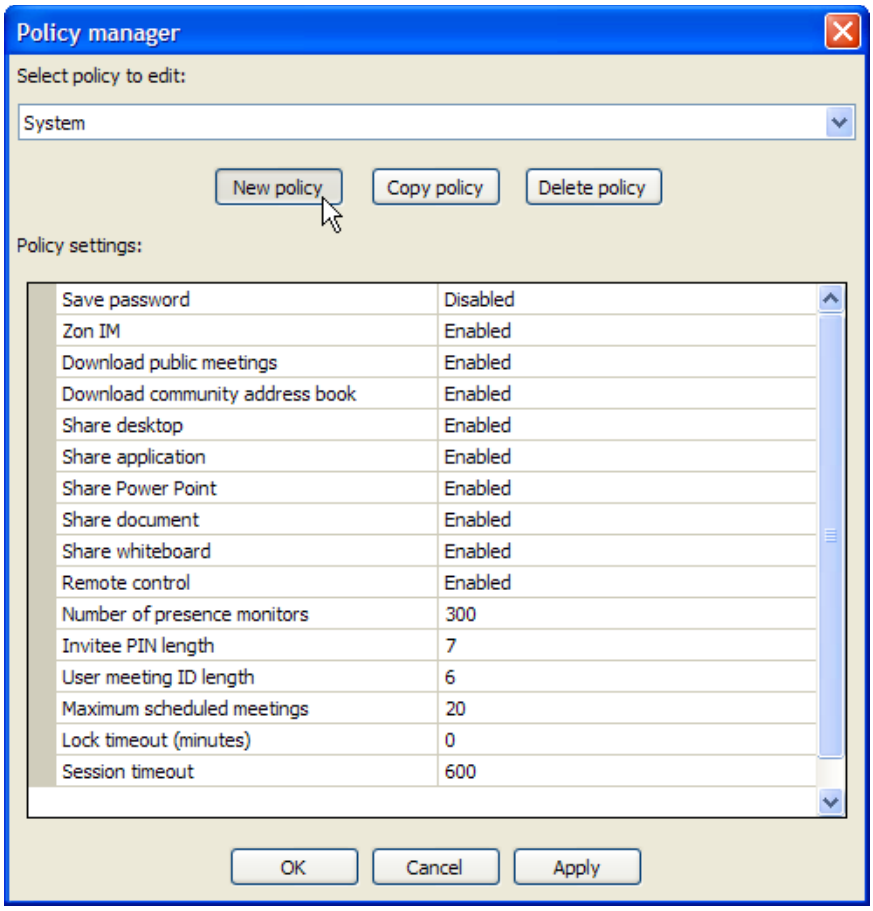
A policy is a set of privileges that governs the availability and limitations of certain features for a given user. Each user has a policy. Typically, an Administrator creates a small number of policies (appropriate for different levels of users) and assigns a policy to each user.

To create a new policy:

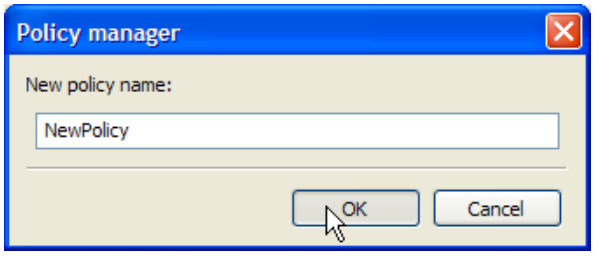
1 From the Conferencing client’s *Manage Contacts* window, select the *Admin* > *Manage Policies* menu item.



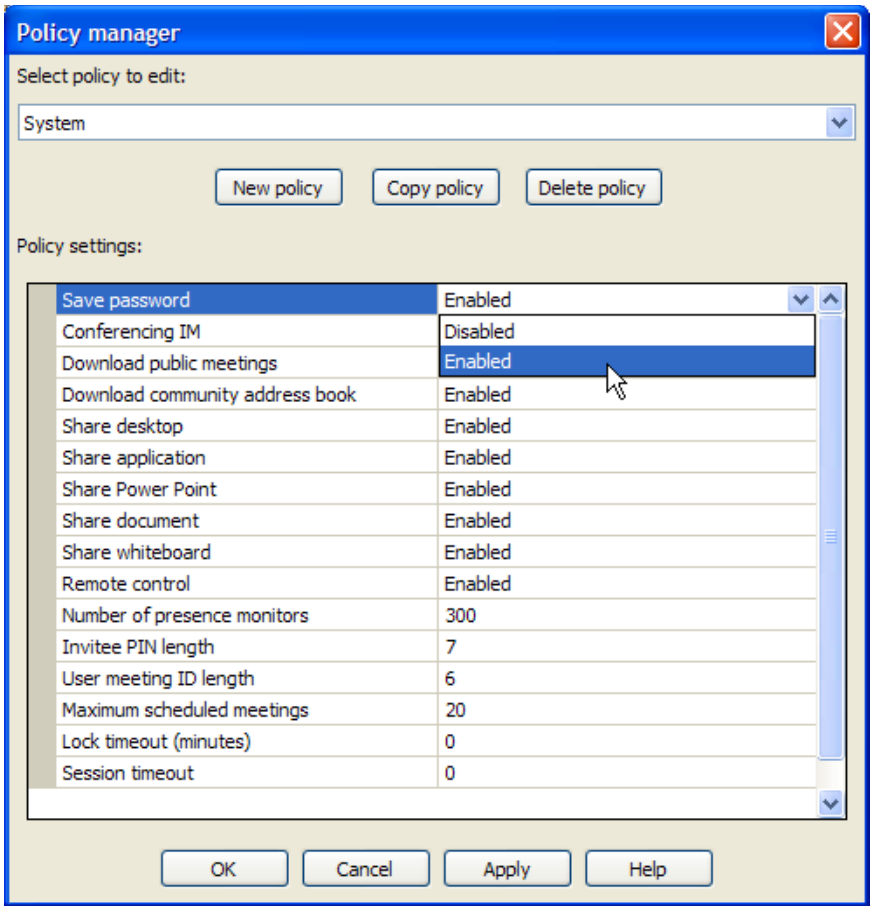
2 In the *Policy Manager* window, click the *New Policy* button.



3 In the *Policy Manager* dialog that appears, type a name for your new policy and click *OK*.



4 In the *Policy Manager* window, click on the right column of the policy setting you want to change.



5 After you adjust all of the policy settings, click *OK*.

If you are creating a policy that is very similar to an existing policy, select the existing policy, click *Copy Policy*, provide a name for the new policy, and edit the settings.

When creating a new policy, you have the ability to configure the following policy settings:

Table 4-1 *Policy Manager Settings*

This Setting...	Means...
Save Password	Allows the user to use the *Save Password* and *Auto Sign On* features (if enabled) or requires that the user log in for every use of the client (if disabled). When this feature is enabled, the user is provided with a *Save Password* option in the *Sign On* window. If this option is selected, Conferencing then stores the user's password locally in encrypted form. The next time the user accesses the client, Conferencing uses the locally stored password to perform an automatic login.
Conferencing IM	Allows or disallows Conferencing instant messaging and chat. This setting does not affect chat within the context of a meeting.

This Setting...	Means...
Download Public Meetings	Allows or disallows the display of public meetings in the *Meetings* window. This setting is useful for large organizations. For more information, read the section immediately after this table.
Download Community Address Book	Allows or disallow the download of the *Community Address Book*. This setting is useful for large organizations. For more information, read the section immediately after this table.
Share Desktop	Allows or disallows the ability to share one's desktop during a meeting.
Share Application	Allows or disallows the ability to share an application during a meeting.
Share PowerPoint	Allows or disallows the ability to share a PowerPoint* presentation during a meeting.
Share Document	Allows or disallows the ability to share a document during a meeting.
Share Whiteboard	Allows or disallows the ability to share the whiteboard during a meeting.
Remote Control	Allows or disallows the ability for meeting attendees to be given control of the presenter's desktop or application.
Number of Presence Monitors	Indicates the total allowable number of personal buddies.
Invitee PIN Length	The number of digits in a meeting PIN.
User Meeting ID Length	The number of digits in a meeting ID.
Max Scheduled Meetings	Indicates the maximum number of meetings the user is allowed to schedule.
Lock Timeout (minutes)	The number of minutes of inactivity before the user is required to unlock the client by entering a password.
Session Timeout (minutes)	The number of minutes of inactivity before the client is required to sign on again.

The *Download Public Meetings* and *Download Community Address Book* policy settings are particularly useful for very large organizations. By disabling these settings, you enhance the performance of the client by not requiring it to download very large amounts of contact and public-meeting information that is most likely irrelevant for any one user.

Despite the utility of these settings, disabling them requires the user to search for contacts and public meetings that might be of interest to her or him. For example, if you disable the display of the *Community Address Book* for a user, the user has to use the *Search* feature to add a contact to the buddy list.

See the Conferencing online Help or *Conferencing User Guide* for detailed information on searching.

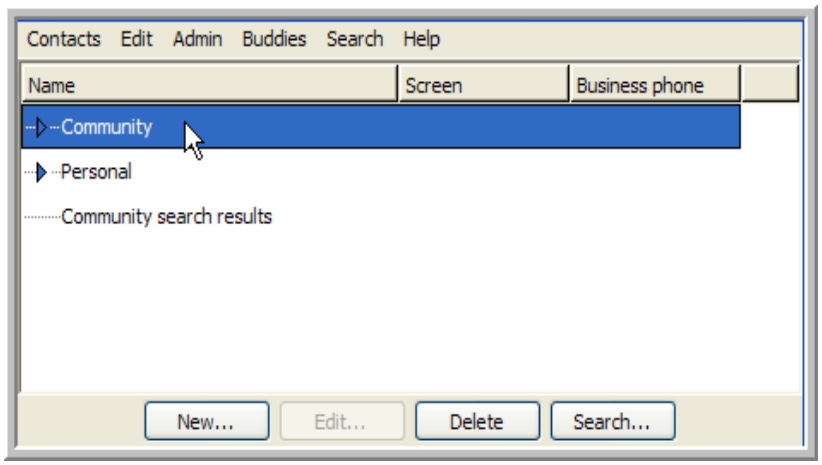
In summary, if you decide to disable the display of either the Community Address Book or public meetings, be sure that your users have the information or training they need to use search to locate contacts and public meetings of interest.

4.2 Creating a New User

After you establish a small number of policies that you want to apply to various groups of people in your organization, you can create user accounts.

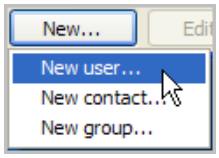
To create a user account:

1. From the Manage Contacts and Users window, select the Community Address Book.



   If the Download Community Address Book feature is disabled, you can skip this step, and the remaining steps still create a new user properly. However, this step is very important when creating a contact or a new group.

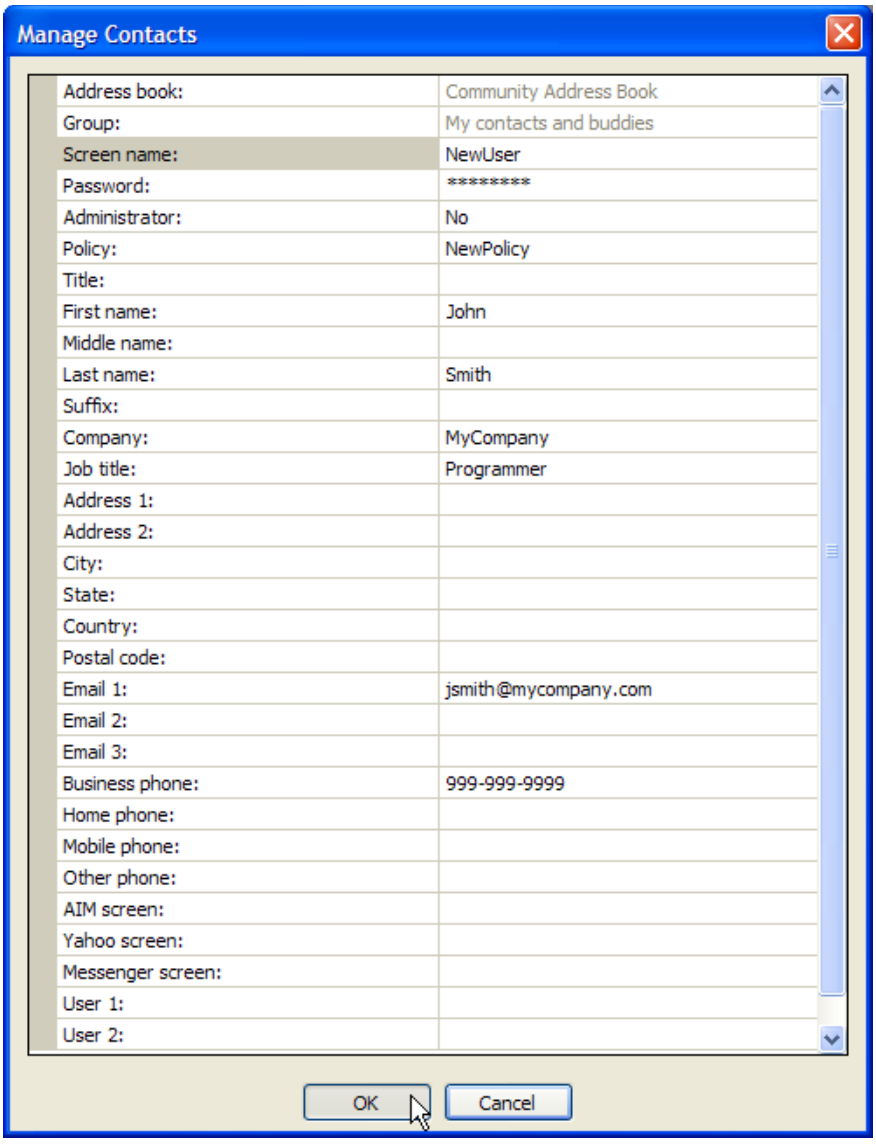
2. Click *New* in the lower left corner of the window, and select the *New User* menu item.



3. In the *New User* window, click items in the right column of the table to provide values for the new user's contact information.

4. Provide values for at least the required contact-list items.

   To make the account reasonably usable, we recommend that you also provide first name, last name, and at least one e-mail address (so that the new user can receive the *New User* e-mail message). See the Conferencing online Help or *Conferencing User Guide* for detailed information on these fields.

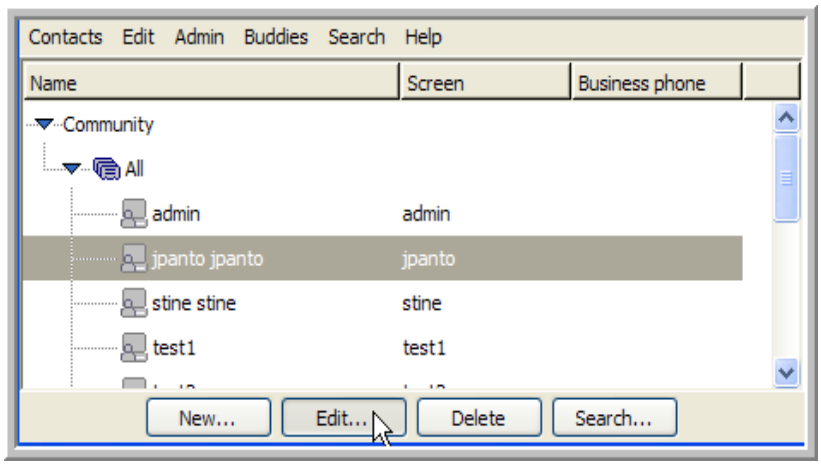


5 Click *OK*.

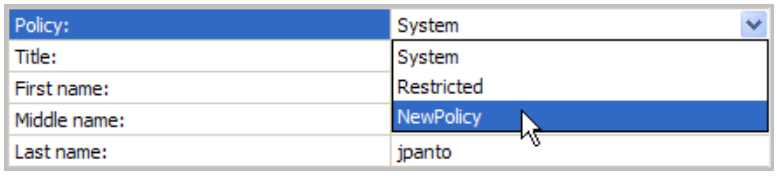
Conferencing creates the new user and a contact listing for that user.

4.3 Change the Policy for a User

1 In the *Manage Contacts and Users* window, select the user and click *Edit*.



2 Select the currently applied policy from the *Policy* drop-down list.

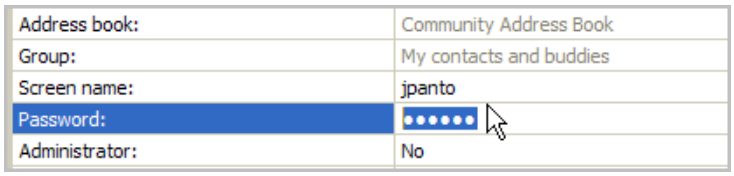


3 Click *OK*.

4.4 Reset the Password for a User

1 In the *Manage Contacts and Users* window, select the user and click *Edit*.

2 In the *Password* field, type the new password.



3 Click *OK*.

Obtaining Server Status

5

The *View Status* tab of the Administration Console provides a summary of the server components for any services that are directly connected to an XML router or for the XML routers themselves.

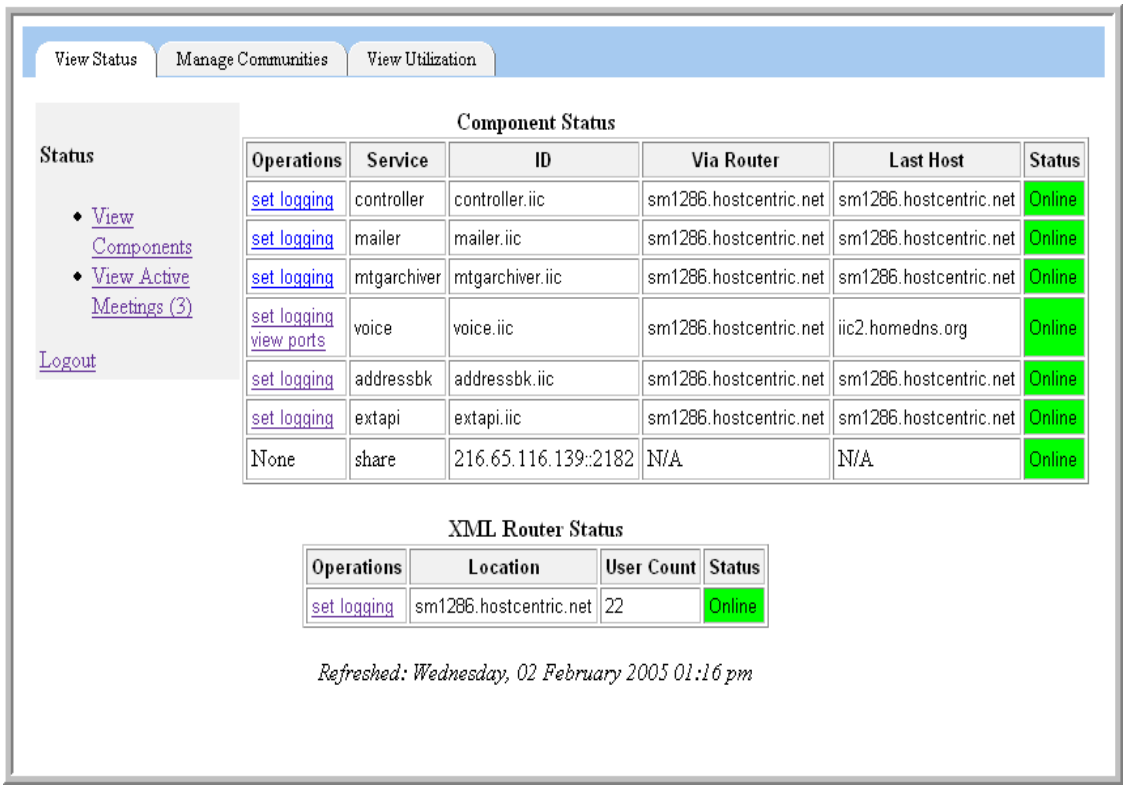
This section includes the following topics:

- Section 5.1, “Viewing Components,” on page 27
- Section 5.2, “Viewing Active Meetings,” on page 28
- Section 5.3, “Determining Voice Port Status,” on page 30
- Section 5.4, “Conferencing System Component Logging,” on page 30
- Section 5.5, “Assessing System Load,” on page 31

5.1 Viewing Components

When you select the *View Status* tab, the main page is the *Component Status* page. You can determine the status of components connected to the XML router by looking at the *Component Status* table. The status of the XML Routers is displayed in the *XML Router Status* table. In both tables, the *Status* column shows whether the component is connected to the XML Routers.

Figure 5-1 *Components Status Table*



The *Component Status* table has a number of columns for different attributes for each of the rows. The following table describes each column:

Table 5-1 *Components Table Attributes*

Column	Description
Operations	These tools allow you to set the logging level for the XML router; for voice bridges, they allow you to view the status of the voice ports on that bridge.
Service	This column identifies the service associated with each row.
ID	This column identifies the ID of the service associated with each row. The ID is useful, for instance, for analyzing system log output.
Via Router	This column identifies the XML Routers to which each service is connected (if any).
Last Host	This column identifies the last host on which the service was known to be running.
Status	Either Online or Offline. This identifies whether the service is online or not.

The *XML Router Status* table has a number of columns for different attributes for each of the rows. The following table describes each column:

Table 5-2 *XML Router Status Table Attributes*

Column	Description
Operations	The links under this column allow you to set the logging level for components; for voice bridges, they allow you to view the status of the voice ports on that bridge.
Location	This column identifies the on which host the router is running.
User Count	This column identifies the current number of Conferencing users logged on to each XML Router
Status	Either Online or Offline. This identifies whether the service is running or not.

5.2 Viewing Active Meetings

Select *View Active Meeting*.

The View Active Meeting table appears. This table contains a list of active meetings with the following information:

Table 5-3 *View Active Meeting Table Attributes*

Column	Description
Mtg ID	The Meeting ID of the active meeting.
Host ID	The User ID of the host. This value is placed in CDR records and is useful for analyzing log output.
Type	This value shows whether the active meeting is an instant or scheduled meeting.

Column	Description
Privacy	The privacy setting that is in effect for the active meeting. It can be private, public or unlisted.
Title	The title of the active meeting.
Description	The description of the active meeting.
Duration (mins)	The current duration of the active meeting.
Time	The start time of the active meeting.
Options	The meeting options in effect for the active meeting. (See Table 5-4 for a description of the meeting options.)
Num Invited	The number of participants invited to the active meeting.
Num Connected	The number of participants connected via Conferencing clients to the active meeting.
Appshare Server	The app/desktop server associated with the active meeting.
Num Appshare Sessions	The number of app/desktop sharing clients connected to the active meeting.
Voice Server	The voice bridge associated with the active meeting. This is also a link to get the voice port status for that bridge.
Num Calls	The number of phone calls connected to the voice conference for the active meeting.

The following meeting option values can be found in the *Options* column:

Table 5-4 *Meeting Options*

Column	Description
Screen callers	This option specifies that caller names are recorded and played when callers enter the meeting.
Lecture	This option specifies that all non-host/non-moderators are muted by default when they join the conference. This is useful for large meetings.
No new participants	This option specifies that new participants are denied entry into the meeting.
Has password	This option means that there is a password associated with the active meeting.
Continue without moderator	Normally, a meeting ends when the last moderator leaves the meeting. This option allows a meeting to continue even though no moderator is present.
Expirationless invitations	The option means that participants are given invitations that do not expire. Normally, participant PINs expire.
Invitations valid before start	This option means that invited participant's PINs are valid before the host or moderator starts the meeting.
Recording meeting	This option means that the meeting is currently being recorded.

Column	Description
No join/leave announcements	This option means that when a participant joins or leaves a voice conference, no tone or announcement is played. This is useful for large meetings were the playing of tones would be distracting.

5.3 Determining Voice Port Status

Click the *Voice* link for an active meeting. The table that appears provides the following information:

Table 5-5 *Voice Link Attributes*

Column	Description
Operation	The only operation currently available for voice ports is to reset them. A reset operation drops any connected call and then stops and restarts line services.
ID	This value identifies the board, trunk, and channel for the port. The formula used to create an ID is: `board << 9 | trunk << 7 | channel` Board, trunk, and channel are integers beginning with 0.
State	This value is either no call or is connected according to whether an active call is present on the port.
Meeting ID	The Meeting ID of the meeting to which the port is associated.
Participant ID	The Participant ID of the caller.
Screen name	The screen name of the caller.
Name	The full name of the caller.
Last Event Time	The time of the last telephony event. The format is YYYYMMDDHHmmSS.
Last Event Name	The name of the last telephony event.

5.4 Conferencing System Component Logging

You can adjust the logging level of Conferencing components by using the Administration Console. The initial page contains Set Logging tools for the system components. After you have selected a component, you can modify the logging level for that component.

There are three levels for logging:

- **Error:** The default logging level. It only logs error conditions. This option creates smaller files.
- **Info:** Logs error conditions and also provides summary information on server tasks.
- **Debug:** Logs error conditions, summary information, and detailed debugging information.

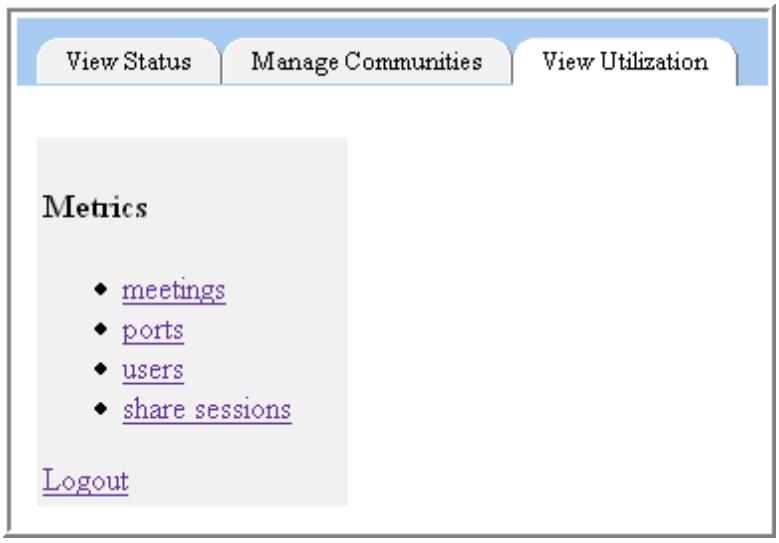
IMPORTANT: Keep the default logging level at *Error* to minimize CPU and I/O loads.

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

5.5 Assessing System Load

The *View Utilization* tab is used to obtain metrics on server capacity. When you access the *View Utilization* tab, the following page displays.

Figure 5-2 *View Utilization Tab*



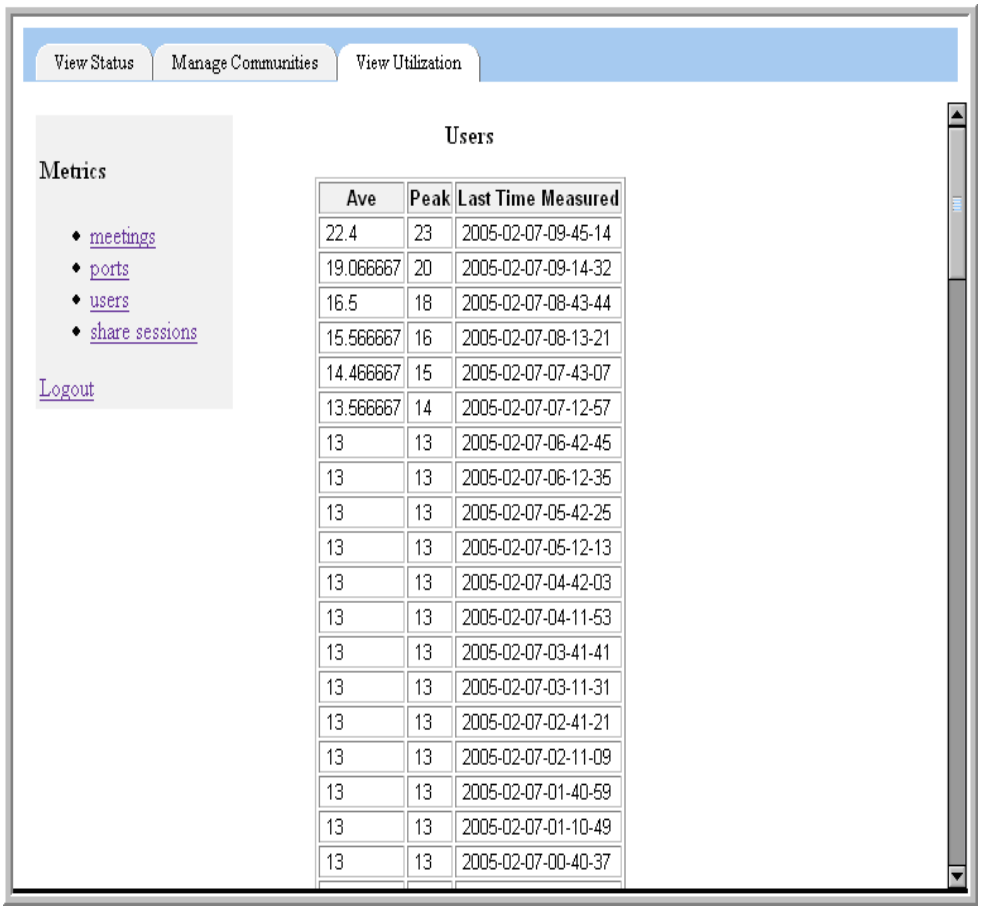
Use this page to view a number of different system load metrics (measuring system load over time). The load parameters the system monitors are:

Table 5-6 *System Load Metrics*

Parameter	Description
Meetings	The number of currently active meetings.
Ports	The number of voice ports with a connected call.
Users	The number of users connected to the system via Conferencing clients.
Share sessions	The number of active app/desktop sharing sessions.

The average and peak values for the load parameter are gathered by sampling the above parameters once a second over a half hour interval. For example, the following is a sample of the *Users* table:

Figure 5-3 *System Load Metrics Users Table*



Ave	Peak	Last Time Measured
22.4	23	2005-02-07-09-45-14
19.066667	20	2005-02-07-09-14-32
16.5	18	2005-02-07-08-43-44
15.566667	16	2005-02-07-08-13-21
14.466667	15	2005-02-07-07-43-07
13.566667	14	2005-02-07-07-12-57
13	13	2005-02-07-06-42-45
13	13	2005-02-07-06-12-35
13	13	2005-02-07-05-42-25
13	13	2005-02-07-05-12-13
13	13	2005-02-07-04-42-03
13	13	2005-02-07-04-11-53
13	13	2005-02-07-03-41-41
13	13	2005-02-07-03-11-31
13	13	2005-02-07-02-41-21
13	13	2005-02-07-02-11-09
13	13	2005-02-07-01-40-59
13	13	2005-02-07-01-10-49
13	13	2005-02-07-00-40-37

The last time-measured values are in the following format:

`<year>-<month>-<day>-<hour>-<min>-<sec>`

These values also show the end of the sampling interval of the load parameter (in this case the number of users connected via Conferencing clients).

Auditing System Events

6

Conferencing provides the ability to monitor user and call record events, and to create files that can be exported or imported between other applications, such as a user database or a time tracking application.

The system writes event logs in the `/var/iic/cdr` directory on the meeting controller hosts (call events) and the address book host (user and reservation event). If you have a multiple-machine configuration, you can determine these hosts by using the Administration Console.

Every day at 6 a.m. GMT (1 a.m. EST), the event logs are rotated. The active event log file is renamed to include a time stamp of when the rotation was performed. If this file is not imported and deleted within 120 days, it is automatically removed.

This section includes the following topics:

- Section 6.1, “Real-Time Event Logs,” on page 33
- Section 6.2, “User Record Format,” on page 34
- Section 6.3, “Call Data Records,” on page 36
- Section 6.4, “Reservation Data Records,” on page 38
- Section 6.5, “Chat Audit Log Configuration,” on page 39

6.1 Real-Time Event Logs

You can configure the Conferencing servers, either at installation time or later, to produce real-time event logs for call, user and meeting reservation events. The real-time interface provides the event data records as they are occur so that third-party systems can use them (for example, a billing system or cost accounting system, management reporting systems or user directory database). The records are delivered via a TCP connection to Conferencing server hosts.

- Section 6.1.1, “Determining Whether Real-Time Events Are Enabled,” on page 33
- Section 6.1.2, “Determining Hosts and Ports,” on page 34
- Section 6.1.3, “Call Record Host and Port,” on page 34
- Section 6.1.4, “User Record Host and Port,” on page 34
- Section 6.1.5, “Reservation Record Host and Port,” on page 34
- Section 6.1.6, “Connecting to Real-Time Event Logs,” on page 34

6.1.1 Determining Whether Real-Time Events Are Enabled

If the value of the `enable_rt_logs` file is set to `yes`, the system delivers the records to consumers connecting to Conferencing hosts. If it is set to `no`, the system does not provide the real-time interface. If real-time records are required but not enabled, rerun the installer script to change the setting.

6.1.2 Determining Hosts and Ports

You can find the hosts and ports providing the real-time event records by examining the global configuration found in `/opt/iic/conf/global-config` directory on any Conferencing host.

6.1.3 Call Record Host and Port

The connected call record hosts are specified by the `controller_host` array in the `global-config` file. The port to use for the connection is specified by the `rt_call_port` variable.

6.1.4 User Record Host and Port

The connected user record host is specified by the `addressbk_host` array in the `global-config` file. The port to use for the connection is specified by the `rt_user_port` variable.

6.1.5 Reservation Record Host and Port

The connected user record host is specified by the `addressbk_host` array in the `global-config` file. The port to use for the connection is specified by the `rt_rsrv_port` variable.

6.1.6 Connecting to Real-Time Event Logs

When a consumer of real-time events connects to one of the event logs described above, the system sends the contents of the event log for the current day. Future events are sent to the consumer as they occur for the duration of the time that the consumer remains connected to the event log host. Each night, the event logs are rotated. After the logs have been rotated, the prior day's events are no longer available to the real-time event log consumer. If needed, you can obtain them from the time-stamped event log files (`call+<timestamp>.elg, user+<timestamp>.elg` and `rsrv+<timestamp>.elg`) in the `/var/iic/cdr` directory on the same host used for the real-time event log connection. The time stamp on the files refers to the time that the log rotation happened.

6.2 User Record Format

You can synchronize your databases whenever you add, update, or delete users. The User Record format provides a standard comma-delimited text file that allows you to import or export a user list to other enterprise databases.

The user records are stored in `/var/iic/cdr/user.elg` on the host specified in `addressbk_host` in the `global-config` file for the cluster. The file is rotated daily to `/var/iic/cdr/user+<timestamp>.log`. You might want to place `/var/iic/cdr` on a network file system to facilitate the retrieval of user records. Otherwise, you can retrieve the call data records by using tools such as `ssh/scp`.

Importing user record data is handled through the `addressbk.update_contact` API call, which is described in the External API document. The database service outputs the data in the following table when users are added, updated, or deleted. The following table describes each of the records, their type, and the maximum length allowed:

Table 6-1 *User Record Fields*

Record	Type	Maximum Length
Record ID	String: <hostname>-<10-digit sequence number>	11 + <max host name length>
Community ID	4-byte non-negative integer	10
User ID	4-byte non-negative integer	10
Event	Integer:	1
	1 = Added	
	2 = Updated	
	3 = Deleted	
Title	String	32
First Name	String	256
Middle Name	String	256
Last Name	String	256
Suffix	String	32
Company	String	256
Job Title	String	256
Address 1	String	256
Address 2	String	256
State	String	256
Country	String	256
Postal Code	String	32
IIC Screen Name	String	256
Email 1	String	256
Email 2	String	256
Email 3	String	256
Business Phone	String	32
Home Phone	String	32
Mobile Phone	String	32
Other Phone	String	32
Extension	String	32
AIM Screen Name	String	128
Yahoo Screen Name	String	128
MSN Screen Name	String	128

Record	Type	Maximum Length
User 1	String	128
User 2	String	128
Default Phone	Integer:	1
	0 - None	
	1 - Business	
	2 - Home	
	3 - Mobile	
	4 - Other	
Default Email	Integer:	1
	0 - None	
	1 - Email 1	
	2 - Email 2	
	3 - Email 3	
Type	Integer:	1
	0 - Registered User	
	1 - Admin	
Modified Time	String: <YYYY>-<MM>-<DD>-<HH>-<mm>-<SS>	19

NOTE: Updated user records have zeros for *Default Phone* and *Default Email* fields. Deleted records have only the following content fields: *Record ID*, *User ID*, *Event* and *Modified Time* (that is, *Deleted Time*).

6.3 Call Data Records

Call data record files are created and stored by Conferencing and allow you to track information about each event. The comma-delimited text file records each event, including meeting times and duration, call connection times, and which clients joined the meetings. This information is useful when determining billing.

The call data records are stored in `/var/iic/cdr/calls.elg` on the host specified in `controller_host` in the `global-config` file for the cluster. The file is rotated daily to `/var/iic/cdr/calls+<timestamp>.log`. After the call data record of one of the rotated files is exported, you can delete it. You might want to place `/var/iic/cdr` on a network file system to ease exporting call data records. Otherwise, you can fetch the call data records using tools such as `ssh/scp`.

The database service outputs the following information:

Table 6-2 *Database Service Output*

Record	Type	Maximum Length
Record ID	String: <hostname>-<10-digit sequence number>	11 + <max host name length>
Time	String: <YYYY>-<MM>-<DD>-<HH>-<mm>-<SS>	19
Duration	Integer	10
Event	Integer	2
	1 = meeting started	
	2 = meeting ended	
	3 = inbound call started	
	4 = outbound call started	
	5 = call connected	
	6 = call ended	
	7 = IIC client joined meeting	
	8 = IIC client left meeting	
	9 = App share started	
	10 = App share ended	
	11 = App share viewer connected	
	12 = App share viewer disconnected	
	13 = Meeting recording started	
	14 = Meeting recording stopped	
Event Info	String:	297 + <max host name length>
	DNIS (inbound call)	
	Dialed number (outbound call)	
	User name (IIC client)	
Community ID	4-byte non-negative integer	10
Meeting ID	8-byte non-negative integer	19
Meeting Start (in seconds)	4-byte non-negative integer	10
Host ID	4-byte non-negative integer	10
Participant ID	8-byte non-negative integer	19

6.4 Reservation Data Records

Reservation Data Records (RDR) are data records that are formatted as lines of quoted comma-separated values. The values are as follows:

Table 6-3 *Reservation Data Record Values*

Record	Type	Maximum Length
Record ID (Assigned in ascending order)	String: <hostname>-<10-digit sequence number>	11 + <max host name length>
Meeting ID	8-byte non-negative integer	19
Meeting Start (in seconds)	4-byte non-negative integer	10
Meeting End (in seconds)	4-byte non-negative integer	10
Community ID	4-byte non-negative integer	10
Host ID	4-byte non-negative integer	10
Meeting Options		
Participant ID	8-byte non-negative integer	19
Participant PIN	8-byte non-negative integer	19
Operation	Integer	2
	1 = Add Meeting Reservation[1]	
	2 = Update Meeting Reservation[1]	
	3 = Remove Meeting Reservation[1]	
	4 = Add Participant[2]	
	5 = Remove Participant[2]	
	6 = Remove All Participants[3]	
Event Info	String:	297 + <max host name length>
	DNIS (inbound call)	
	Dialed number (outbound call)	
	User name (IIC client)	

1. When this Operation value is selected, the *Participant ID* and *Participant PIN* fields display no data.
2. When this Operation value is selected, the *Community ID*, *Host ID*, *Meeting Start*, *Meeting End*, and *Meeting Options* fields display no data.
3. When this Operation value is selected, only the *Record ID* and *Meeting ID* fields display data.

6.4.1 Reservation Data Record (RDR) Interface

The Reservation Data Records are available to any consumers connected via TCP to an RDR port. RDRs are also written to files so that consumers can initialize and not lose billing data.

For RDRs written to a file, after a configurable interval of time, the file is closed and renamed to include a time stamp (such as `/var/iic/cdr/rsrv-2005-01-28-08-27.log`). Then a new RDR file is created.

When a real-time RDR consumer connects to the RDR port, all current RDR records are sent to the RDR consumer. Current RDR records are stored in `/var/iic/cdr/rsrv.elg` file until the log rotation time. A real-time RDR consumer can get the current information by retrieving all of the available rotated RDR files in the `/var/iic/cdr` directory.

6.5 Chat Audit Log Configuration

Chat audit logging can be configured at system installation or reconfiguration time using the `install.sh` script.

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 is quoted with double quotes at the beginning and end of the field (for example, "`field value`").

The fields are as follows:

Table 6-4 *Chat Audit Log Fields*

Record	Type	Description
timestamp	String (YYYMMDDTHH:MM:SS)	The time of the chat message in GMT.
from_id	String	The participant ID of the sender. The participant ID is assigned to each meeting participant and is sent in meeting invitations.

Record	Type	Description
from_name	String	The displayed 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 is empty unless `delivery` is `ToOne`.
to_name	String	The display name of the meeting participant who received the chat message. This is empty unless `delivery` is `ToOne`.
message	String	The contents of the chat message.

Conferencing Administration 7

Use the following commands to administer Conferencing. Run these commands on the Conferencing servers by using the command line interface (not the Conferencing Administration Console).

This section includes the following topics:

- Section 7.1, “Starting and Stopping Conferencing Services,” on page 41
- Section 7.2, “Backing Up the Database,” on page 42
- Section 7.3, “Restoring the Database,” on page 42

7.1 Starting and Stopping Conferencing Services

The following topics cover how you start and stop Conferencing clusters and individual machines.

- Section 7.1.1, “Starting and Stopping the Cluster,” on page 41
- Section 7.1.2, “Starting and Stopping Individual Machines,” on page 41

7.1.1 Starting and Stopping the Cluster

Conferencing services for the entire cluster can be started and stopped by using the `control-cluster.sh` script described in the *Conferencing Installation Guide*.

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
```

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

7.1.2 Starting and Stopping Individual Machines

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

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
```

7.2 Backing Up the Database

The system automatically backs up the database on a daily basis. The backups are 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 bzip21 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 reflects 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 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`.

7.3 Restoring the Database

Restoring an archived database is done by using the `pg_restore` command. To restore a backup from a `bzip2` compressed tar file, use the following command:

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

You can 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`.

LDAP User Authentication

A

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 A.1, “LDAP User Authentication Input File,” on page 43
- Section A.2, “Conferencing Field Names,” on page 44
- Section A.3, “Address Book Configuration (Synchronization),” on page 44

A.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>
```

A.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`.

A.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.

Troubleshooting Strategies

B

This section presents several troubleshooting strategies in the following topics:

- Section B.1, “Verifying That Everything is Running,” on page 47
- Section B.2, “Enabling Debug Logging,” on page 47
- Section B.3, “Using the Service Watchdog,” on page 48
- Section B.4, “Error Codes,” on page 48
- Section B.5, “Advanced Checks,” on page 50
- Section B.6, “Conferencing Client,” on page 50
- Section B.7, “Voice Bridge,” on page 51
- Section B.8, “Meeting Archiver,” on page 51

B.1 Verifying That Everything is Running

Run the following command to verify that all services indicate that they are running:

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

Run the following command to verify that two `jabberd` services are running:

```
ps -fA | grep jabberd
```

There should be processes listening on the following ports:

```
netstat -nl | grep 5222
netstat -nl | grep 2182
```

There should be processes listening on the following port on each IP:

```
netstat -l | grep http
```

B.2 Enabling Debug Logging

- For most services:

  Edit `/opt/iic/conf/config.xml` and change `debug level` from `error` to `debug`.

- For jabberd:

  Edit `/opt/iic/jabberd/jabber.xml` and search for `elogger`. Under this element, find the `debug` attribute and set to `1`.

- Restart services by using `/opt/iic/conf/control-services.sh stop` and `/opt/iic/conf/control-services.sh start`.

- Logs are in `/var/log/iic`, except for the client connector (`jadc2s`) which uses `syslog`.

- You can also enable logging from the console, but that setting only lasts until the server is restarted and must be enabled service-by-service.

- Logs are rotated according to the size and number specified in `config.xml`. In some cases these numbers must be made larger to capture enough tracing.
- Apache logs are in `/usr/local/apache2/logs`.

B.3 Using the Service Watchdog

Most system services are run by the service watchdog application `nanny`, which monitors the service process and restarts it automatically if it fails for any reason.

If an administrator e-mail is configured when the system is installed, an e-mail is sent when any Conferencing services fail and need to be restarted. `Nanny` also outputs to `syslog` (i.e. `/var/log/messages`) when a service status changes.

B.4 Error Codes

The following error codes can appear in server or client logs:

```
// Common error codes
Failed                = -1000,
InvalidPIN            = -1001,
InvalidSessionID      = -1002,
InvalidMeetingID      = -1003,
InvalidSubmeetingID   = -1004,
InvalidUserID         = -1005,
InvalidParticipantID  = -1006,
InvalidServiceID      = -1007,
DuplicateID           = -1008,
InvalidParameter      = -1009,
ParameterParseError   = -1010,
DuplicateUserName     = -1011,
PINAllocationError    = -1012,
NoClientConnection    = -1013,
PINExpired            = -1014,
PINNotValidYet        = -1015,

// Error codes from controller
InvalidAddress        = -2000,
NotAuthorized         = -2001,
NotMember             = -2002,
InsufficientResources = -2003,
NotLoaded             = -2004,
AlreadyConnected      = -2005,
NotConnected          = -2006,
NotActive             = -2007,
NoPhoneNumber         = -2008,
InAnotherMeeting      = -2009,
MeetingExists         = -2010,
```

```
InvalidPassword       = -2011,
Disconnected          = -2012,
NotWhileLecture       = -2013,
MeetingLocked         = -2014,
PhoneNumberNotFound   = -2015,
MeetingStartTimeout   = -2016,
NoPort                = -2017,
MtgArchiverTimeout    = -2018,
MeetParamNotFound     = -2019,

// Error codes from voice service
InvalidCallID             = -3000,
NotConferenced            = -3001,
MissingPIN                = -3002,
NoAvailResource           = -3003,

// Error codes from address book/schedule
DBAccessError             = -4000,
AddressBookError          = -4001,
DuplicateContact          = -4002,
ProfileSystemDeleteError  = -4003,
ProfileInUseError         = -4004,
UnknownGroup              = -4005,
CommunitySystemDeleteError = -4006,
CommunityNotFound         = -4007,
CommunityStatusNotFound   = -4008,
CommunityDisabled         = -4009,
CommunityNameNotUnique    = -4010,
DirectoryNotFound         = -4011,
ProfileNotFound           = -4012,
DuplicateUsername         = -4013,
MaxMeetingsExceeded       = -4014,
ProfileNameNotUnique      = -4015,
InstantMeetingNotFound    = -4016,
UserNotFound              = -4017,
MaxPresenceExceeded       = -4018,
InvalidScreenName         = -4019,
InvalidScreenPassword     = -4020,
CommunityOwnerDeleteError = -4021,

// Error from app share
NoShareSession            = -5000,
ShareFailed               = -5001,
```

B.5 Advanced Checks

To reveal jabber start-up errors that happened before normal logging was enabled, use the following command (usually, only a database problem stops it at this point):

```
/etc/rc.d/iicjabberd stop
cd /opt/iic/jabberd
jabberd/jabberd -H /opt/iic/jabberd -D
```

B.6 Conferencing Client

The following symptoms and possible causes are visible to the user of the Conferencing client.

Symptom: The client displays the error `Unable to connect to server.`

Possible Cause:

- The hostname of the XML Router does not resolve properly on the client machine.

  Check `\Documents and Settings\<user-name>\Application Data\meeting\zon.log` (Win32) or `~/.meeting/zon.log` (Linux) in the system drive of the client machine for lines containing the text `Unable to resolve hostname`.

- The client concentrator, jadc2s, is not running.
  1. Verify that the jadc2s process is running on all XML Router hosts.
  2. Verify that port 5222 is in LISTEN state.
  3. Look in `/var/log/iic/jadc2s.log` for more information.
- The XML Router, jabberd, is not running.
  1. Verify that the jabberd processes are running on all XML Router hosts.
  2. Verify that a system component port is in LISTEN state.
  3. Look in `/var/log/iic/xmlrouter_error.log` for more information.
- The meeting controller is not running or not connected
  1. Check `\Documents and Settings\<user-name>\Application Data\meeting\zon.log (Win32) or ~/.meeting/zon.log (Linux)` in the system drive of the client machine for lines containing the text `err=-995, msg=Internal Timeout, code=-1000, id=rpc_controllerauth`.
  2. If Step A is true, check the meeting controller log files for more information and check the network connectivity between the meeting controller host and the XML Router host.
- The address book is not running or not connected
  1. Check `\Documents and Settings\<user-name>\Application Data\meeting\zon.log` (Win32) or `~/.meeting/zon.log` (Linux) in the system drive of the client machine for lines containing the text “err=-995, msg=Internal Timeout, code=-1000, id=rpc_versionck”.
  2. If Step A is true, check that the address book daemon is running. If it is, check the address book log files in `/var/log/iic` for more information and check the network connectivity between the address book host and the XML Router host.

Symptom: The client displays `Contact data fetch failed` in the Edit User dialog box status line.

Possible Cause:

The address book is not running or is not connected:

1. Check `\Documents and Settings\<user-name>\Application Data\meeting\zon.log` (Win32) or `~/.meeting/zon.log` (Linux) in the system drive of the client machine for lines containing the text `err=-995, msg=Internal Timeout, code=-1000, id=rpc_getdata23`.
2. If you find this text, check that the address book daemon is running. If it is, check the address book log files for more information and check the network connectivity between the address book host and the XML Router host.

B.7 Voice Bridge

Symptom: The voice bridge prompts `Unable to join the meeting` even though the meeting is available and both the password and the PIN are correct.

Possible Cause:

The meeting controller is not responding to requests from the voice bridge.

1. Check the network connectivity between the voice bridge and the XML router for excessive packet loss.
2. If there is no excessive packet loss, check the meeting controller log.

B.8 Meeting Archiver

Symptom: If meeting archiver fails to process the meeting, the system administer receives e-mail notification.

Possible Cause:

1. The archiver might be out of disk space. Free up disk space by removing old files.
2. The archiver failed to retrieve raw recording data.

Solution:

Run the following command to restart the meeting archiver:

```
/etc/init.d/iicmtgarchiver stop
/etc/init.d/iicmtgarchiver start
```

The meeting archiver processes the failed meeting recordings.

Symptom: The meeting Flash movie does not contain all of the necessary components; for example, there is no voice recording with the movie.

Possible Cause:

1. The raw data for each meeting is stored for seven days after the end of the meeting before it is deleted. If you move the meeting instance from `/var/mtgspool/done` to `var/mtgspool/active` within the seven day window, the meeting instance is formatted with a meeting ID followed by the meeting start time. For example, 555555-2007-02-22-12-16-16.

2. After the file for the meeting instance has been renamed, run the following command to restart the meeting archiver:

```
/etc/init.d/iicmtgarchiver stop
/etc/init.d/iicmtgarchiver start
```