



ICEcore™

Discover Cool Collaboration

Operations Guide →

ICEcore Conference Version 1.0



September, 2007

www.icecore.com

Legal Notices

SiteScape, 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, SiteScape, 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, SiteScape, 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, SiteScape, Inc., reserves the right to make changes to any and all parts of SiteScape 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.

SiteScape, Inc., has intellectual property rights relating to technology embodied in the product that is described in this document.

SiteScape, Inc.
12 Clock Tower Place, Suite 210
Maynard, MA 021754
U.S.A.
www.SiteScape.com

Third-Party Materials

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

Contents

About This Guide	v
1 System Overview	7
1.1 System Components	7
1.2 Cluster Architecture	8
2 The Administration Console	9
2.1 Starting the Administration Console	9
2.2 Using the Administration Console	9
2.2.1 Component Status Page	10
3 ICEcore Conference Communities	11
3.1 Managing Communities	11
3.2 Adding Communities	12
3.2.1 To Add a Community:	12
3.3 Viewing Communities	13
3.3.1 To Show All Communities	13
3.3.2 To Find a Community by Name	13
3.4 Removing Communities	15
3.5 Updating Communities	15
4 Adding Users and Policies	17
4.1 Creating Policies	17
4.2 Creating a New User	21
4.3 Change the Policy for a User	23
4.4 Reset the Password for a User	23
5 Obtaining Server Status	25
5.1 Viewing Components	25
5.2 Viewing Active Meetings	26
5.3 Determining Voice Port Status	28
5.4 ICEcore Conference System Component Logging	28
5.5 Assessing System Load	29
6 Auditing System Events	31
6.1 Real-Time Event Logs	31
6.1.1 Determining Whether Real-time Events are Enabled	31
6.1.2 Determining Hosts and Ports	31
6.1.3 Call Record Host(s) and Port	31
6.1.4 User record host(s) and port	32
6.1.5 Reservation record host(s) and port	32
6.1.6 Connecting to real-time event logs	32
6.2 User Record Format	32

6.3	Call Data Records	34
6.4	Reservation Data Records	36
6.4.1	Reservation Data Record (RDR) Interface	37
6.5	Chat Audit Log Configuration	37
7	ICEcore Conference Administration	39
7.1	Starting and Stopping ICEcore Conference Services	39
7.1.1	Starting and Stopping the Cluster	39
7.1.2	Starting and Stopping Individual Machines	40
7.2	Backing Up the Database	40
7.3	Restoring the Database	40
A	LDAP User Authentication	41
B	Troubleshooting Strategies	43
B.1	Verify That Everything is Running	43
B.2	Enable Debug Logging	43
B.3	Service watchdog	44
B.4	Error codes	44
B.5	More advanced checks	45
B.6	ICEcore Conference Client	46
B.7	Voice Bridge	47
B.8	Meeting Archiver	47

About This Guide

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

Audience

This guide is intended for administrators.

Additional Documentation

You may find more information in additional ICEcore Conference documentation:

- ♦ ICEcore Conference Help system
- ♦ ICEcore Conference Quick Start Guide
- ♦ ICEcore Conference User Guide
- ♦ ICEcore Conference Server Installation Guide

Contents of this Manual

This manual provides information about the following:

- ♦ System Overview
- ♦ The Administration Console
- ♦ ICEcore Conference Communities
- ♦ Adding Users
- ♦ Obtaining Server Status
- ♦ Auditing System Events
- ♦ ICEcore Conference Administration
- ♦ Troubleshooting Strategies
- ♦ LDAP User Authentication

Document Conventions

This manual 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 SiteScape 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.

What you see	What it means
Click the <i>Add toolbar</i> item.	References to toolbar items, links, menu items, and buttons are presented in <i>italic</i> font.
Click the <i>Getting Started</i> link.	
Click the <i>Add Document</i> menu item.	
Click <i>Close</i> .	
Type <code>status</code> , then press Enter.	Text that you must type and file names are presented in <code>Courier</code> font.
Open the <code>ManagerGuide.pdf</code> file.	

System Overview

1

This chapter provides an overview of the ICEcore Conference architecture and provides a description of the system components.

This chapter includes the following sections:

- ♦ [Section 1.1, “System Components,” on page 7](#)
- ♦ [Section 1.2, “Cluster Architecture,” on page 8](#)

1.1 System Components

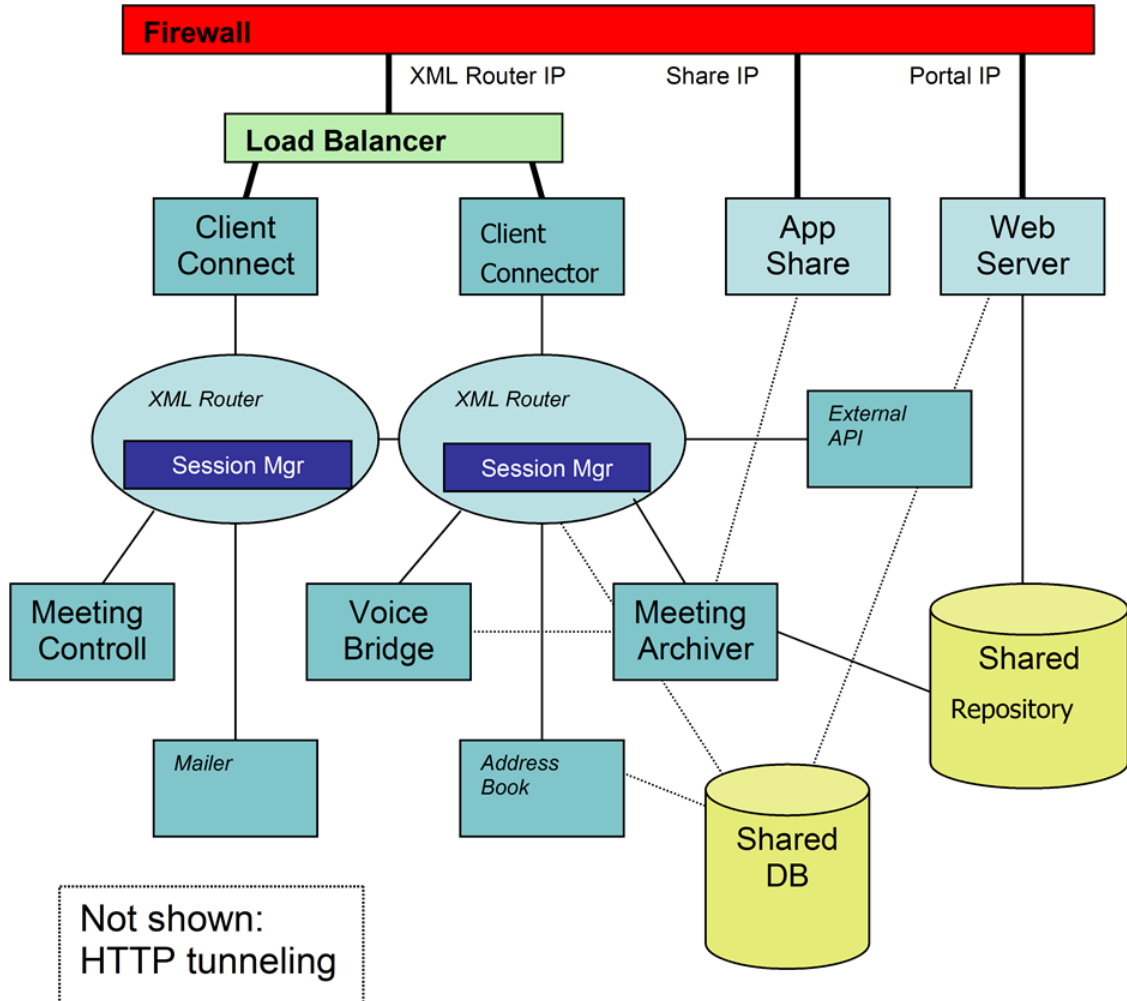
The ICEcore Conference Server is a highly modular suite of components that you can configure to run on one or more servers. Each component provides a core service to the system through a well-defined XML API. Since all communication occurs over an XML transport, the allocation of components to physical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

The system components are as follows:

- ♦ XML Router - Routes XML data and APIs calls between 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 schedule, 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 Macromedia Flash-based meeting archives stored in a web accessible repository.
- ♦ App Share Server - Forwards application shared data from meeting presenter to meeting participants, and manages remote control access to presenter desktop.
- ♦ Invitation Web Service - Joins participants to meetings based on invitation URL.
- ♦ External Web Service - Provides web service API for external parties as needed for integration with existing service provider systems.

1.2 Cluster Architecture

A cluster is a set of components providing services to a community of users. The following diagram illustrates the architecture of an example cluster. This example displays a multiple server configuration.



The Administration Console

2

This chapter describes the ICEcore Conference *Administration Console*, including logging into the console and a description of the available tools.

This chapter includes the following sections:

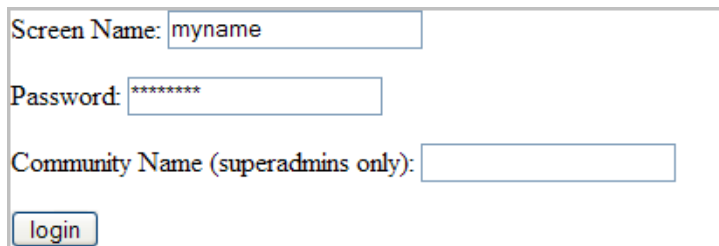
- ♦ [Section 2.1, “Starting the Administration Console,” on page 9](#)
- ♦ [Section 2.2, “Using the Administration Console,” on page 9](#)

2.1 Starting the Administration Console

ICEcore Conference provides a web-browser-based *Administration Console* 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 using the following URL:

`http://<portal-hname>/imidio/console/`

Once 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 versus Community Administrators, who 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.



The screenshot shows a login form with three input fields and a login button. The first field is labeled 'Screen Name:' and contains the text 'myname'. The second field is labeled 'Password:' and contains a series of asterisks '*****'. The third field is labeled 'Community Name (superadmins only):' and is empty. Below the fields is a button labeled 'login'.

2.2 Using the Administration Console

Use the *Administration Console* to monitor the ICEcore Conference server environment. Use the *Administration Console* tabs to perform the following functions:

- ♦ Work with ICEcore Conference 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

Once 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:

Component Status

Operations	Service	ID	Via Router	Last Host	Status
set logging	controller	controller.iic	sm1286.hostcentric.net	sm1286.hostcentric.net	Online
set logging	mailer	mailer.iic	sm1286.hostcentric.net	sm1286.hostcentric.net	Online
set logging	mtgarchiver	mtgarchiver.iic	sm1286.hostcentric.net	sm1286.hostcentric.net	Online
set logging view ports	voice	voice.iic	sm1286.hostcentric.net	iic2.homedns.org	Online
set logging	addressbk	addressbk.iic	sm1286.hostcentric.net	sm1286.hostcentric.net	Online
set logging	extapi	extapi.iic	sm1286.hostcentric.net	sm1286.hostcentric.net	Online
None	share	216.65.116.139::2182	N/A	N/A	Online

XML Router Status

Operations	Location	User Count	Status
set logging	sm1286.hostcentric.net	22	Online

Refreshed: Wednesday, 02 February 2005 01:16 pm

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*.

ICEcore Conference Communities

3

A community is a group of users, usually within the same company or within a specific division within an organization. Once you install and configure the ICEcore Conference software, you need to set up communities and administrators for those communities. Community-member contacts are displayed in the *Community Address Book* in the ICEcore Conference Client.

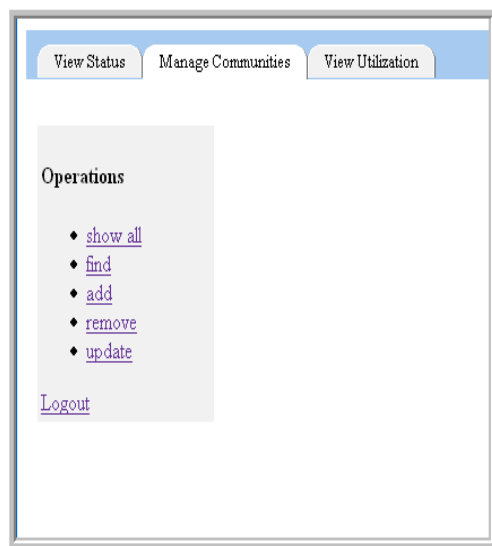
When the ICEcore Conference software is installed, a default *System Community* is created. This community provides the Super Administrator login and password information.

This chapter includes the following sections:

- ♦ [Section 3.1, “Managing Communities,” on page 11](#)
- ♦ [Section 3.2, “Adding Communities,” on page 12](#)
- ♦ [Section 3.3, “Viewing Communities,” on page 13](#)
- ♦ [Section 3.4, “Removing Communities,” on page 15](#)
- ♦ [Section 3.5, “Updating Communities,” on page 15](#)

3.1 Managing Communities

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



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

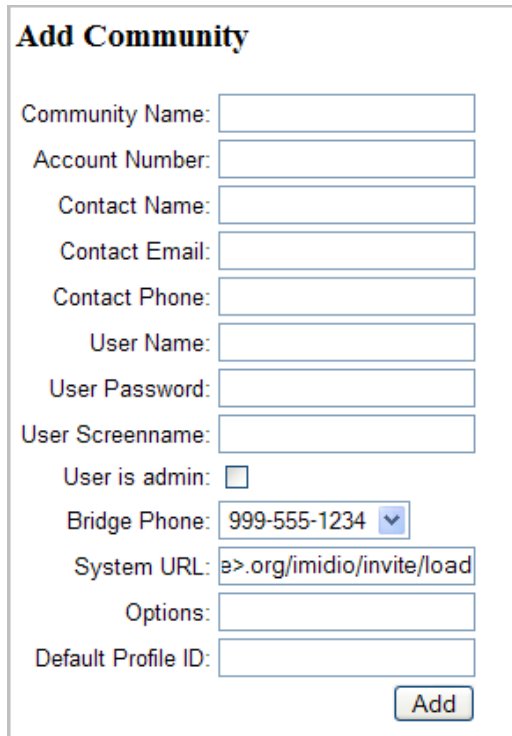
- ♦ Display all communities
- ♦ Search for specific communities
- ♦ Add a new community
- ♦ Remove an existing community
- ♦ Modify an existing community

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. When you install ICEcore Conference for the first time, you should create at least one new community. This community should have a Community Administrator, usually the first user that is created in the community.

3.2.1 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.

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

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

NOTE: 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 ICEcore Conference 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 ICEcore Conference users see for the community administrator when they access their ICEcore Conference 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 Once 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 and then select the *Show All* or 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:

The screenshot shows a web interface with three tabs at the top: "View Status", "Manage Communities" (which is selected), and "View Utilization". Below the tabs, there is a sidebar on the left titled "Operations" containing links for "show all", "find", "add", "remove", "update", and "Logout". The main content area is titled "Find Communities" and contains a text input field labeled "Community name:" followed by a "Search" button. Below the input field, there is a note: "Use '%' to match zero or more characters".

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:

The screenshot shows a web interface with a navigation bar at the top containing 'View Status', 'Manage Communities', and 'View Utilization'. On the left, there is a sidebar with 'Operations' and a 'Logout' link. The main area is titled 'Find Communities' and contains a search form and a table.

Search Form:

Community name:

Use '%' to match zero or more characters

Operations	Community ID	Community Name	Account Name	Contact Name	Contact Email	Contact Phone	User Name	User Password	Bridge Phone	System URL	Account Type	Account Status
show all find add remove update	21	Yoyodyne, Inc.	89	Buckaroo Bonzai	bbonzai@yoyodyne.com	999-555-3444	Buckaroo Bonzai	8thdimension	999-555-1234	http://zon.yoyodyne.com/imidio/imite	normal	Enabled

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

Operations – Operations provide 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 may 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 may be either normal or admin.

Account Status – This 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 either:

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

NOTE: In either case, each community in the table contains a *Remove* link that removes that community.

- a. Select *Show All* or *Find* (to search by community name).
The *Community Results* table appears.
- b. 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 either:

- ♦ 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 a *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 ICEcore Conference client to accomplish this task.

This chapter includes the following sections:

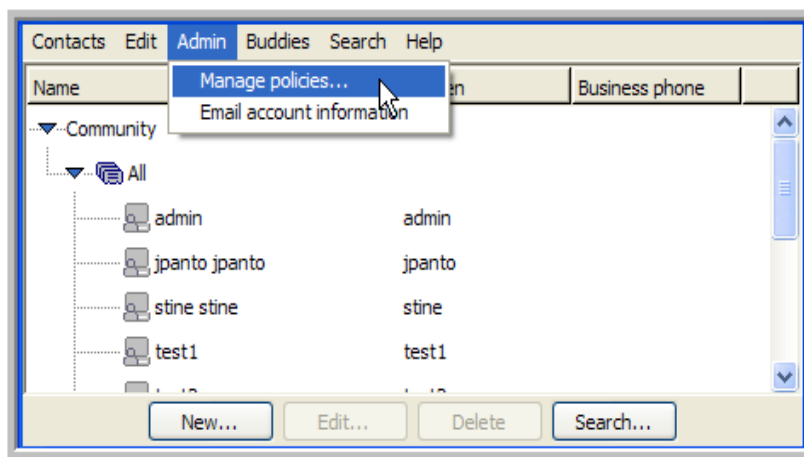
- ♦ Section 4.1, “Creating Policies,” on page 17
- ♦ Section 4.2, “Creating a New User,” on page 21
- ♦ Section 4.3, “Change the Policy for a User,” on page 23
- ♦ Section 4.4, “Reset the Password for a User,” on page 23

4.1 Creating Policies

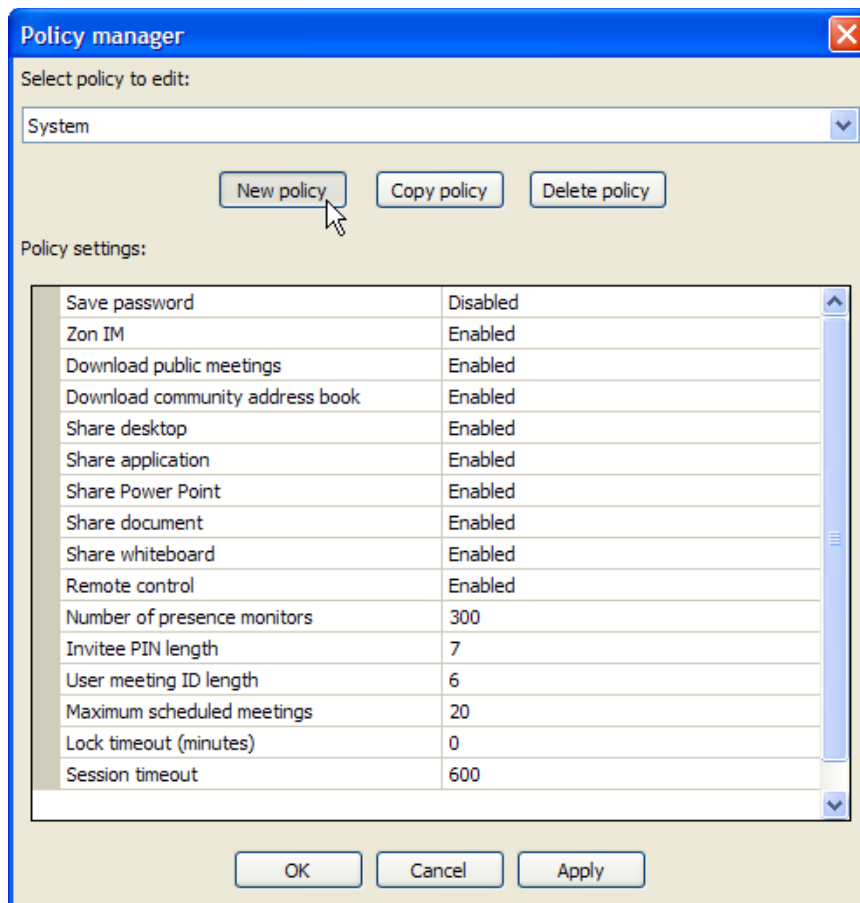
A policy is a set of privileges that governs the availability and limitations of certain features for a given user. Each user has a policy. Typically, an Administrator creates a small number of policies (appropriate for different levels of users) and assigns a policy to each user.

To create a new policy:

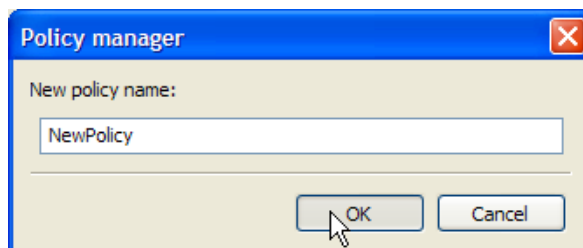
- 1 From the ICEcore Conference client’s *Manage Contacts* window, select the *Admin > Manage Policies* menu item.



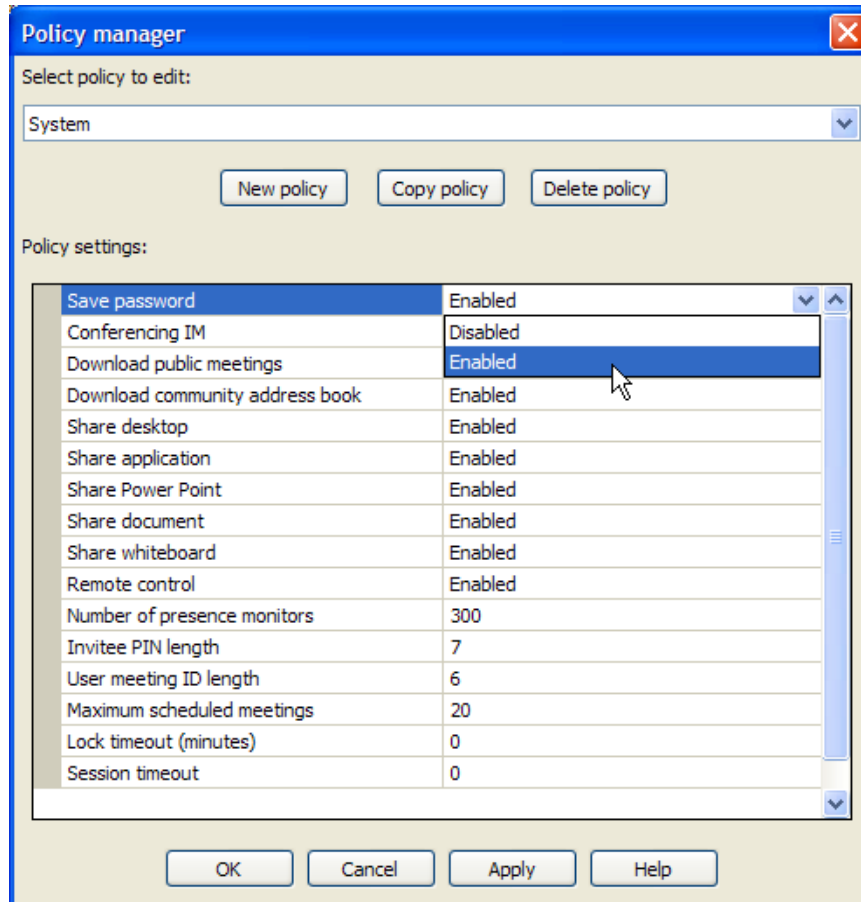
- 2 In the *Policy Manager* window, click the *New Policy* button.



- 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 wish to change.



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

NOTE: 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:

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

This Setting...	Means...
Download Public Meetings	Allows or disallows the display of public meetings in the <i>Meetings</i> 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 <i>Community Address Book</i> . 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	Is the number of digits in a meeting PIN.
User Meeting ID Length	Is 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)	Is the number of minutes of inactivity before the user is required to unlock the client by entering a password.
Session Timeout (minutes)	Is 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 may 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 ICEcore Conference Online Help or ICEcore Conference User Guide for detailed information on searching.

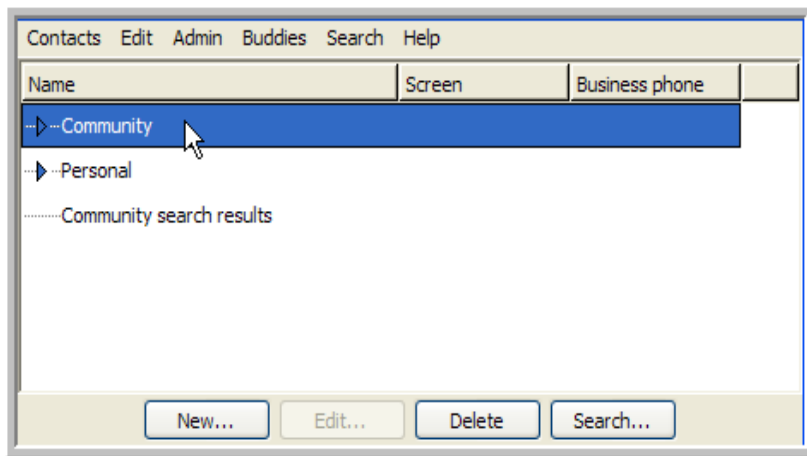
In summary, if you decide to disable the display of either the *Community Address Book* or public meetings, be sure that your users have the information or training they need to use search to locate contacts and public meetings of interest.

4.2 Creating a New User

Once 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.

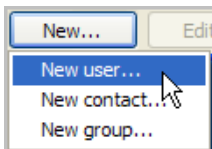
To create a user account:

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



NOTE: If the Download Community Address Book feature is disabled, you may 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 ICEcore Conference Online Help or ICEcore Conference User Guide for detailed information on these fields.

Address book:	Community Address Book
Group:	My contacts and buddies
Screen name:	NewUser
Password:	*****
Administrator:	No
Policy:	NewPolicy
Title:	
First name:	John
Middle name:	
Last name:	Smith
Suffix:	
Company:	MyCompany
Job title:	Programmer
Address 1:	
Address 2:	
City:	
State:	
Country:	
Postal code:	
Email 1:	jsmith@mycompany.com
Email 2:	
Email 3:	
Business phone:	999-999-9999
Home phone:	
Mobile phone:	
Other phone:	
AIM screen:	
Yahoo screen:	
Messenger screen:	
User 1:	
User 2:	

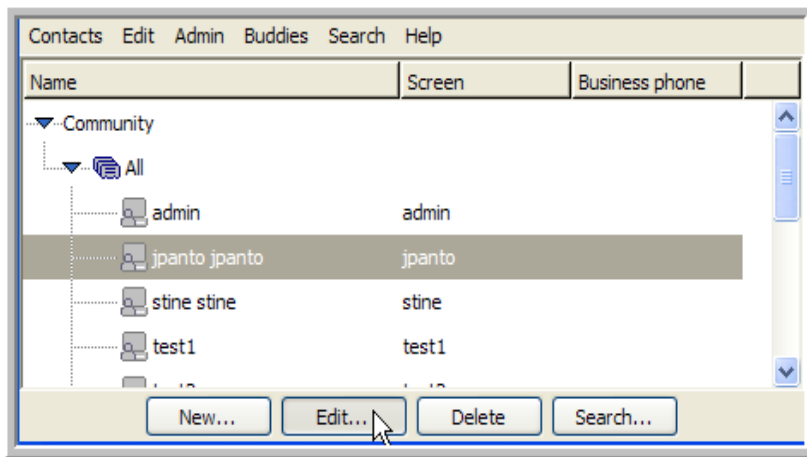
OK Cancel

5 Click *OK*.

ICEcore Conference 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.

Policy:	System
Title:	System
First name:	Restricted
Middle name:	NewPolicy
Last name:	jpanto

- 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.

Address book:	Community Address Book
Group:	My contacts and buddies
Screen name:	jpanto
Password:	•••••
Administrator:	No

- 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 chapters includes the following sections:

- ♦ [Section 5.1, “Viewing Components,” on page 25](#)
- ♦ [Section 5.2, “Viewing Active Meetings,” on page 26](#)
- ♦ [Section 5.3, “Determining Voice Port Status,” on page 28](#)
- ♦ [Section 5.4, “ICEcore Conference System Component Logging,” on page 28](#)
- ♦ [Section 5.5, “Assessing System Load,” on page 29](#)

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.

The screenshot shows the Administration Console interface. At the top, there are three tabs: "View Status" (selected), "Manage Communities", and "View Utilization". Below the tabs, the main content area is titled "Component Status". On the left side of this area, there is a sidebar with the heading "Status" and three links: "View Components", "View Active Meetings (3)", and "Logout". The main content area contains two tables. The first table, "Component Status", has columns: Operations, Service, ID, Via Router, Last Host, and Status. It lists seven services: controller, mailer, mtgarchiver, voice, addressbk, extapi, and share. All services have a status of "Online". The second table, "XML Router Status", has columns: Operations, Location, User Count, and Status. It shows one router at sm1286.hostcentric.net with 22 users and a status of "Online". At the bottom of the page, there is a timestamp: "Refreshed: Wednesday, 02 February 2005 01:16 pm".

Operations	Service	ID	Via Router	Last Host	Status
set logging	controller	controller.iic	sm1286.hostcentric.net	sm1286.hostcentric.net	Online
set logging	mailer	mailer.iic	sm1286.hostcentric.net	sm1286.hostcentric.net	Online
set logging	mtgarchiver	mtgarchiver.iic	sm1286.hostcentric.net	sm1286.hostcentric.net	Online
set logging view ports	voice	voice.iic	sm1286.hostcentric.net	iic2.homedns.org	Online
set logging	addressbk	addressbk.iic	sm1286.hostcentric.net	sm1286.hostcentric.net	Online
set logging	extapi	extapi.iic	sm1286.hostcentric.net	sm1286.hostcentric.net	Online
None	share	216.65.116.139::2182	N/A	N/A	Online

Operations	Location	User Count	Status
set logging	sm1286.hostcentric.net	22	Online

Refreshed: Wednesday, 02 February 2005 01:16 pm

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

Column	Description
Operations	These tools allow you to set the logging level for the XML router or in the case of voice bridges, 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:

Column	Description
Operations	The links under this column allows you to set the logging level for components and, in the case of voice bridges, 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 ICEcore Conference 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:

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.
Privacy	This is what privacy setting is in effect for the active meeting. It may 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.

Column	Description
Time	The start time of the active meeting.
Options	These are the meeting options in effect for the active meeting. (See table below 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 ICEcore Conference 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:

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.
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 where 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:

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: <code>board << 9 trunk << 7 channel</code> Board, trunk and channel are integers beginning with 0.
State	This value is either no call or 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 ICEcore Conference System Component Logging

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

There are three levels for logging:

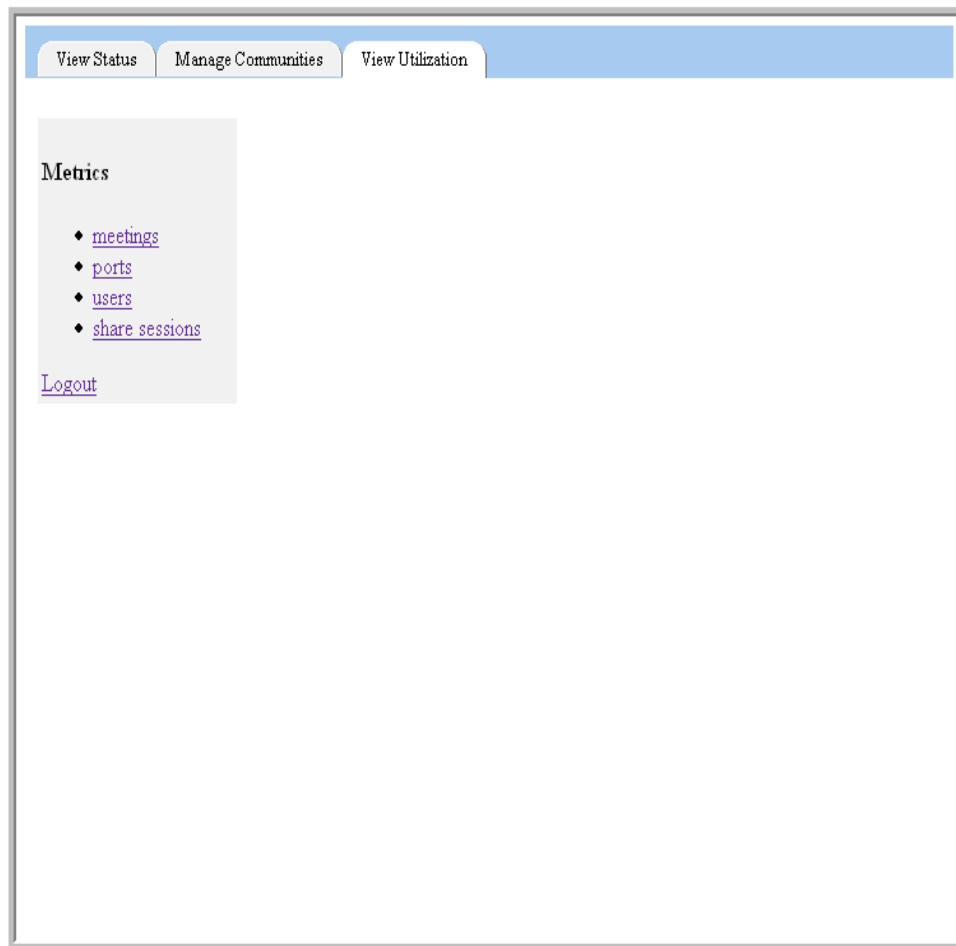
- ♦ **Error** - this is the default logging level and only logs error conditions (creates smaller files).
- ♦ **Info** - logs error conditions and also provides summary information on server tasks.
- ♦ **Debug** - logs error conditions, summary information, and detailed debugging information.

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 may 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.



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

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 ICEcore Conference 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:

View Status Manage Communities View Utilization		
<div> Metrics <ul style="list-style-type: none"> meetings ports users share sessions Logout </div>		
Users		
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 ICEcore Conference clients).

Auditing System Events

6

ICEcore Conference 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 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 timestamp of when the rotation was performed. If this file is not imported and deleted within 120 days, it is automatically removed.

This chapter includes the following sections:

- [Section 6.1, “Real-Time Event Logs,” on page 31](#)
- [Section 6.2, “User Record Format,” on page 32](#)
- [Section 6.3, “Call Data Records,” on page 34](#)
- [Section 6.4, “Reservation Data Records,” on page 36](#)
- [Section 6.5, “Chat Audit Log Configuration,” on page 37](#)

6.1 Real-Time Event Logs

You can configure the ICEcore Conference 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 occur so that third-party systems may 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 ICEcore Conference server hosts.

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 ICEcore Conference 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, re-run 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 ICEcore Conference host.

6.1.3 Call Record Host(s) and Port

The connected call record host(s) is specified by the `controller_host` array in the `global-config`. The port to use for the connection is specified by the `rt_call_port` variable.

6.1.4 User record host(s) 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(s) 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. Once 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 may want to place `/var/iic/cdr` on a network file system to facilitate the fetching of user records. Otherwise, you can fetch the call data records using tools such as `ssh/scp`.

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

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

Record	Type	Maximum Length
Event	Integer: 1 = Added 2 = Updated 3 = Deleted	1
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
User 1	String	128
User 2	String	128

Record	Type	Maximum Length
Default Phone	Integer: 0 - None 1 - Business 2 - Home 3 - Mobile 4 - Other	1
Default Email	Integer: 0 - None 1 - Email 1 2 - Email 2 3 - Email 3	1
Type	Integer: 0 - Registered User 1 - Admin	1
Modified Time	String: <YYYY>--<MM>--<DD>--<HH>--<mm>--<SS>	19
<p>NOTE: Updated user records have zeros for Default Phone and Default Email fields. Deleted records have only the following content fields: <i>Record ID</i>, <i>User ID</i>, <i>Event</i> and <i>Modified Time</i> (i.e. <i>Deleted Time</i>).</p>		

6.3 Call Data Records

Call data record files are created and stored by ICEcore Conference 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`. Once the call data record of one of the rotated files is exported, you may delete it. You may 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:

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 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	2
Event Info	String: DNIS (inbound call) Dialed number (outbound call) User name (IIC client)	297 + <max host name length>
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:

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 Reservation1 3 = Remove Meeting Reservation1 4 = Add Participant2 5 = Remove Participant2 6 = Remove All Participants3	
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 timestamp (e.g. `/var/iic/cdr/rsrv-2005-01-28-08-27.log`). Then a new RDR file is then 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 fetching 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 controller(s). ICEcore Conference IM and ICEcore Conference 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 timestamp 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:

Record	Type	Description
timestamp	String (YYYYMMDDTHH: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.
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 <code>delivery</code> is <code>ToOne</code> .
to_name	String	The display name of the meeting participant who received the chat message. This is empty unless <code>delivery</code> is <code>ToOne</code> .
message	String	The contents of the chat message.

ICEcore Conference Administration

7

Use the following commands to administer ICEcore Conference. Run these commands on the ICEcore Conference servers using the Command Line interface (not the ICEcore Conference *Administration Console*).

This chapter includes the following sections:

- ♦ [Section 7.1, “Starting and Stopping ICEcore Conference Services,” on page 39](#)
- ♦ [Section 7.2, “Backing Up the Database,” on page 40](#)
- ♦ [Section 7.3, “Restoring the Database,” on page 40](#)

7.1 Starting and Stopping ICEcore Conference Services

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

7.1.1 Starting and Stopping the Cluster

ICEcore Conference services for the entire cluster may be started and stopped using the `control-cluster.sh` script described in the ICEcore Conference Installation Guide.

To Stop ICEcore Conference Services:

Type:

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

To Start ICEcore Conference Services:

Type:

```
./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 script:
`/opt/iic/conf/control-services.sh`.

To Stop ICEcore Conference Services with `control-services.sh`:

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

To Start ICEcore Conference Services with `control-services.sh`:

Type:
`/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 `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 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 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



Configuring LDAP Authentication and Synchronization for ICEcore Conference

Currently you must manually configure this. Repeat this process if a server is re-installed or upgraded since a normal server install overwrites these changes.

An LDAP directory can be used as the data source for these two operations:

- ♦ Creation of ICEcore Conference users (via periodic synchronization against users in the LDAP directory)
- ♦ Authentication of ICEcore Conference users (password is checked against the directory as users sign on)

You can configure either or both of these as described below. If you are going to enable both, we recommend that you start with synchronization – once synchronization is complete, you can sign on and check that all users were created before moving onto the authentication step.

Address Book Configuration (Synchronization)

- ♦ Modify `/opt/iic/conf/config.xml` and remove the XML comment declaration around the `ldapConfig` element (remove `<!--` and `-->` from the lines preceding and following this line).
- ♦ Modify `/opt/iic/conf/ldap.xml`, setting the server URL and other fields as appropriate. Use `ldap:` for normal and `ldaps:` for SSL connections.
- ♦ The `communityid` configuration item indicates the community to which new users located in the LDAP directory are added. The available community ids can be found using the ICEcore Conference server console.
- ♦ The `attributes` configuration section controls how LDAP attributes are mapped to ICEcore Conference contact fields. The `screenname` ICEcore Conference field is the most important since that is how a user being updated is located in the address book.
- ♦ Execute `/etc/init.d/iicaddress stop` and `/etc/init.d/iicaddress start` to restart the address book service.
- ♦ Execute `/opt/iic/bin/ldap-sync.sh <portal-server-hname>` to perform the synchronization. This can be run manually as needed, or configured to run periodically using `cron`.

Jabber Configuration (Authentication)

- ♦ Modify LDAP section in `/opt/iic/jabberd/jabber.xml`, setting the server URL and other fields as appropriate. Use `ldap:` for normal and `ldaps:` for SSL connections.
- ♦ Add LDAP module (`mod_auth_ldap`) to module list in `/opt/iic/jabberd/jabber.xml`. See the example below.
- ♦ Remove `mod_auth_digest` from module list in `jabber.xml`.
- ♦ Execute `/etc/init.d/iicjabber stop` and `/etc/init.d/iicjabber start` to restart XML router service.

Web Server Configuration (Authentication)

- ♦ Copy `zon-docshare-ldap.conf` and `zonpasswd` from `/opt/iic/conf/webcontent` to `/usr/local/apache2/conf`.
- ♦ Edit `/usr/local/apache2/conf/zon-docshare-ldap.conf` and add ICEcore Conference XML router host name to `SetJabberHostName` parameter.
- ♦ Edit `/usr/local/apache2/conf/httpd.conf` and change the include for `zon-docshare.conf` to `zon-docshare-ldap.conf`.
- ♦ Execute `/etc/init.d/iicportal stop` and `/etc/init.d/iicportal start` to restart the web service.
- ♦ Test config by hitting `http://<server-portal>/repository/SharedDocuments/ping.html` and entering valid username and password.

Client Installer Rebuild (Authentication)

You need to build a ICEcore Conference client installer that enables plain text authentication. For testing purposes, install the client normally, then edit `<Program Files>/Zon/zon-def.opt` on Windows or `/opt/iic/share/meeting/zon-def.opt` on Linux and add or modify the following line:

```
"EnableExternalAuth", "yes"
```

Once this is known to work, see the ICEcore Conference Installation and Configuration Guide for information on rebuilding the installer. See the ICEcore Conference Package Kit for information on how to rebuild the Windows installer with this setting.

ICEcore Conference Field Names

Use these names to configure the mapping of LDAP attributes to ICEcore Conference 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" -  
"yahoscreen" - "aimscreen" - "user1" - "user2" - "defphone"
```

Notes:

- ♦ There is no way to map a single LDAP field with a user's full name into the separate ICEcore Conference contact fields (e.g. first name, last name, title). This will be added in a subsequent release. For now, map the LDAP name attribute to the ICEcore Conference first name field.
- ♦ If using LDAP over SSL, the server name in the certificate must match the server name configured in `jabber.xml`.
- ♦ The password for `admin` always comes from the ICEcore Conference 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 using SSL.
- ♦ `<cacertdir>path</cacertdir>` can be used in addition to or instead of `<cacertfile>`. This directory must contain certificate files with names specially hashed as described by the documentation for option `-CApath` from `man verify`.

Troubleshooting Strategies

B

This chapter presents several troubleshooting strategies in the following sections:

- ♦ Section B.1, “Verify That Everything is Running,” on page 43
- ♦ Section B.2, “Enable Debug Logging,” on page 43
- ♦ Section B.3, “Service watchdog,” on page 44
- ♦ Section B.4, “Error codes,” on page 44
- ♦ Section B.5, “More advanced checks,” on page 45
- ♦ Section B.6, “ICEcore Conference Client,” on page 46
- ♦ Section B.7, “Voice Bridge,” on page 47
- ♦ Section B.8, “Meeting Archiver,” on page 47

B.1 Verify That Everything is Running

Run the following command and verify that all services say running:

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

Run the following command and 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 Enable 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 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.
- ♦ Note that logs are rotated according to the size and number specified in `config.xml`, so in some cases these numbers must be made larger to capture enough tracing.
- ♦ Apache logs are in `/usr/local/apache2/logs`.

B.3 Service watchdog

Most system services are run by `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, e-mails are sent when any ICEcore Conference 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

May turn up 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 More advanced checks

To reveal jabber start-up errors that happened before normal logging was enabled (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 ICEcore Conference Client

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

Symptom: The client displays the error “*Unable to connect to server.*”

Possible Causes:

1. 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`.
2. The client concentrator, `jadc2s`, is not running.
 - a. Verify that the `jadc2s` process is running on all XML Router hosts.
 - b. Verify that port 5222 is in LISTEN state.
 - c. Look in `/var/log/iic/jadc2s.log` for more information.
3. The XML Router, `jabberd`, is not running.
 - a. Verify that the `jabberd` processes are running on all XML Router hosts.
 - b. Verify that a system component port is in LISTEN state.
 - c. Look in `/var/log/iic/xmlrouter_error.log` for more information.
4. The meeting controller is not running or not connected
 - a. 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`”.
 - b. 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.
5. The address book is not running or not connected
 - a. 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`”.
 - b. 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 Causes:

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: Voice bridge prompts “*Unable to join the meeting*” even though the meeting is available and both the password and the PIN are correct.

Possible Causes:

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 administrator receives e-mail notification.

Possible Causes:

1. The archiver may be out of disk space. Free up disk space by removing old files.
2. The archiver failed to fetch 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 Causes:

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. Once the file for the meeting instance has been renamed, restart the meeting archiver, as documented above.