

iVIEW Suite

Version 7.0



NOTICE

© 2000-2009 RADVISION Ltd. All intellectual property rights in this publication are owned by RADVISION Ltd and are protected by United States copyright laws, other applicable copyright laws and international treaty provisions. RADVISION Ltd retains all rights not expressly granted.

This publication is RADVISION confidential. No part of this publication may be reproduced in any form whatsoever or used to make any derivative work without prior written approval by RADVISION Ltd.

No representation of warranties for fitness for any purpose other than what is specifically mentioned in this guide is made either by RADVISION Ltd or its agents.

RADVISION Ltd reserves the right to revise this publication and make changes without obligation to notify any person of such revisions or changes. RADVISION Ltd may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this publication, it is furnished under a license agreement included with the product as a separate document. If you are unable to locate a copy, please contact RADVISION Ltd and a copy will be provided to you.

Unless otherwise indicated, RADVISION registered trademarks are registered in the United States and other territories. All registered trademarks recognized.

GoAhead WebServer is used by permission from GoAhead Software, Inc. GoAhead WebServer is used by permission from GoAhead Software, Inc. Copyright © 2006 GoAhead Software, Inc. All Rights Reserved.

For further information contact RADVISION or your local distributor or reseller.

iVIEW Suite version 7.0, June 2009

Publication 4

<http://www.radvision.com>

CONTENTS

About This Manual

Related Documentation	xix
Feedback	xix

1 *Introducing iVIEW Suite*

Overview	1
----------	---

iVIEW COMMUNICATIONS MANAGER

2 *iVIEW Communications Manager Overview*

iVIEW Communications Manager User Types	5
Administrative Permissions	6
Understanding Video Conferencing	7
Network Devices	7
Cascading for Flexible Conferencing	7
Login Screen Options	8
Service Provider Login	8
Single Sign-on (SSO)	8
Enabling Single Sign-on with Microsoft Vista and Internet Explorer	89
Interface Orientation	9
Configuration Workflow	10

3	<i>Managing Organizations in iCM</i>	
	How to Create an Organization Profile	13
	Defining Organization Contact Details	14
	Branding the User Interface	14
	Defining Concurrent Call Limits	15
	Defining a Billing Code	16
	Enabling Organization Meeting Types	16
	Defining Organization System Administrator Credentials	17
	Viewing an Organization Profile	17
	Searching for an Organization Profile	17
	How to Activate/Deactivate an Organization Profile	18
	Activating an Organization Profile	18
	Deactivating an Organization Profile	18
	Generating an Organization Report	19
	Removing an Inactive Organization Profile	20
4	<i>Managing Network Topologies in iCM</i>	
	How to Create a Network Topology with Device Islands	21
	Adding a Device Island	22
	Modifying Device Island Settings	23
	Removing Connectivity Between Device Islands	24
	Removing a Device Island	24
	Viewing IP and ISDN Network Topologies	24
	Modifying Your Network Topology View	25
5	<i>Configuring a Gatekeeper Profile in iCM</i>	
	About Gatekeeper Types	27
	Internal Gatekeeper	27
	Standalone RADVISION ECS Gatekeepers	28
	External Gatekeepers	28
	How to Create or Modify a Gatekeeper Profile	28
	Defining Gatekeeper Address Details	28
	Defining Dialing Plan Settings	29

	Defining iCM as the Gatekeeper Authorization Server	30
	Removing a Gatekeeper Profile	31
	Searching for a Gatekeeper Profile	31
	Accessing Meetings from an External Gatekeeper	32
6	<i>Configuring a SIP Server Profile in iCM</i>	
	Creating or Modifying a SIP Server Profile	35
	Removing a SIP Server Profile	36
	Searching for a SIP Server Profile	37
	Configuring the MCU to Work in SIP Mode	37
	Disabling the SIP Back-to-Back User Agent	38
7	<i>Managing an MCU Profile in iCM</i>	
	Configuring Cascading	39
	Creating or Modifying an MCU Profile	41
	Taking an MCU Offline	42
	Removing an MCU Profile	42
	Searching for an MCU Profile	43
	Synchronizing MCU Information with iVIEW Suite	43
	How to Manage Meeting Types	44
	Viewing Available Meeting Types on Network MCUs	44
	Viewing Built-in Meeting Types	45
	Removing a Meeting Type	46
	Searching for a Meeting Type	46
	Downloading a Meeting Type to iCM	47
	Resolving Meeting Type Conflicts Between MCUs	47
	Resolving Meeting Type Conflicts Between iCM and an MCU	48
	Uploading a Meeting Type to Network MCUs	48
	Viewing Meeting Type Details	49
	Modifying Meeting Type Details	49
	Accessing an MCU from the Meeting Type Details Screen	50
	Viewing a List of MCUs Containing a Specified Meeting Type	50
	Creating or Modifying a Meeting Type Group	50

	Removing a Meeting Type Group	51
	Customizing MCU Delimiters	51
	Designating a Service for IVR Use	52
8	<i>Configuring a Gateway Profile in iCM</i>	
	Creating or Modifying a Gateway Profile	53
	Taking a Gateway Offline	56
	Removing a Gateway Profile	57
	Searching for a Gateway Profile	57
9	<i>Configuring a SCOPIA Desktop Profile in iCM</i>	
	Creating or Modifying a SCOPIA Desktop Profile	59
	Removing a SCOPIA Desktop Profile	60
	Searching for a SCOPIA Desktop Profile	61
	How to Stream Meetings Using SCOPIA Desktop	61
	Enabling Streaming on SCOPIA Desktop	61
	Enabling Streaming for a Virtual Room	62
	Allowing Recording by Specified Roles	62
	Allowing Recording by Specified Users	62
	Enabling Recording for Specified Virtual Rooms	63
10	<i>Configuring a Meeting Room Profile in iCM</i>	
	Enabling Meeting Room Support	65
	Creating or Modifying a Meeting Room Profile	66
	Sending Meeting Details by Email	66
	Removing a Meeting Room Profile	67
	Searching for a Meeting Room Profile	67
11	<i>Configuring a Terminal Profile in iCM</i>	
	How to Create or Modify a Terminal Profile	69

	Defining H.323 IP Terminal Details	70
	Defining SIP IP Terminal Details	71
	Defining ISDN/PSTN H.320 Terminal Details	72
	Defining Mobile Terminal Details	73
	Defining Dual H.320 and H.323 Terminal Details	74
	Removing a Terminal Profile	75
	Searching for a Terminal Profile	75
12	<i>Defining iCM Call Routing Modes</i>	
	Call Routing in H.323 Deployments	77
	Call Routing in SIP Deployments	78
	Masking Conference Topology with the Virtual MCU Feature	78
	Creating a Centralized Conference	79
	Creating a Distributed Conference	79
13	<i>Viewing Network Device Performance and Availability</i>	
	Viewing Device Usage and Failure by Time Interval	81
	Viewing Device Usage and Failure by Time Interval and Period	82
	Viewing MCU Port Availability	83
	Generating a Report	84
14	<i>Viewing Real-time Meeting Statistics in iCM</i>	
	Viewing the Number of Ongoing Meetings and Calls	85
	Viewing Port Utilization Information	86
	Viewing Organization Meetings and Calls	86
	Viewing the Creation Status of Meetings	87
	Searching for a Meeting	88
	Monitoring a Meeting or Call	89
	Generating Reports	89
	Modifying Upcoming Meetings	91
	Viewing Host MCUs	92

Terminating Meetings	92
15 <i>Creating Statistical Reports of Meetings and Calls in iCM</i>	
Creating a Call Information Report	93
Creating a Port Usage Report	94
Creating a Resource Usage Report	95
Viewing the Use of Ad Hoc and Scheduled Meetings	96
Viewing Average Meeting Size	96
Viewing Average Meeting Duration	96
Generating Reports for Finished Meetings	97
Viewing Finished Meetings	99
Viewing the Termination Status of Meetings	99
Searching for a Finished Meeting	99
Viewing Host MCUs	100
Removing Meetings from the History Tab	101
16 <i>Managing iCM Users and User Groups without an External Directory</i>	
Creating or Modifying a User Profile	104
Removing a User Profile	105
Searching for a User Profile	105
Updating User Profiles	106
Creating a User Group	106
Modifying a User Group	107
Removing a User Group	107
Modifying a Service Provider Profile	108
Limiting Individual User Access to Meeting Types	109
Limiting Group Access to Meeting Types	109
Configuring Multiple Settings for User Groups	110

17	<i>Provisioning iCM Users via a Directory Server</i>	
	Synchronization of User Information	111
	Accessing User Information in Active Directory Server	112
	Synchronizing iCM with Active Directory Server	113
	Configuring a Connection to an LDAP Server	114
	Mapping iCM User Roles to ADS Users	115
	Defining Virtual Rooms for All LDAP Users	116
	Forcing iCM to Use a Virtual Room	117
	iCM LDAP Information Attributes	117
18	<i>Modifying Default Organization Settings for iCM Users and Meetings</i>	
	Settings Priorities	119
	How to Define Default Settings for Organization Users	119
	Defining Which Meeting Types are Available to New Users	120
	Defining a Default Time Zone for a User	120
	Defining Display Formats	121
	Defining Date Display Formats	121
	Defining Your Meeting Display Preferences	121
	Defining Bandwidth for SCOPIA Desktop Calls	122
	Defining SCOPIA Desktop Policies	122
	Defining Default Recording Permissions	123
	How to Define Default Settings for Meetings	123
	Defining a Default Meeting Type	124
	Defining the Default Cascading Mode	124
	Defining the Maximum Number of Ports for an Ad Hoc Meeting	125
	Defining How to End a Meeting	125
	Defining the Meeting Default Length	126
	Defining the Default Dialing Mode	126
	Defining a Billing Destination	127
	Defining Required Default Resources	127
	Defining the Auto Attendant Service Prefix	128
	Enabling Automatic Routing	128
	Customizing Invitation Email	129

Modifying the Look and Feel of the iCM Web User Interface	130
---	-----

19 *Using the iVIEW Suite Configuration Tool*

Setting Up the Java Runtime Environment	134
Launching the iVIEW Suite Configuration Tool	134
Retrieving an Administrator Password	135
Uninstalling the iVIEW Suite Configuration Tool	135
How to Modify General Settings	136
Defining Email Server Settings	136
Defining the Unconnected Endpoint Time Period	137
Defining User Provisioning Options	137
Defining Table Row Display	138
Defining the Command Delay	138
Defining the Parent Zone Authorization Filter	138
Defining the Log Level	139
Defining the iCM Server Name and Web Port	139
Defining the Online Help Host URL	140
How to Modify Scheduling Settings	140
Changing Call Authorization Settings	140
Dynamically Cascading Multiple MVPs for a Single Conference	142
Modifying iCM Default Meeting Settings	142
Modifying Default Recurring Meeting Settings	144
Hiding iCM User Interface Screens	144
How to Manage Custom Time Zones	145
Selecting a Time Zone Profile	145
Viewing a Time Zone Profile	146
Adding Daylight Saving to a Time Zone Profile	146
Creating a Customized Time Zone Profile	147
Removing a Customized Time Zone Profile	147
Reverting to Default Time Zone Settings	148
Customizing Product and Vendor Logos	148
Creating a Customized Billing Field	149
Defining Database Server Settings	149
How to Define Security Settings	150
Defining Password Settings	150

Defining a Login Message	151
Unlocking a User Account	151
How to Configure SNMP Trap Server Profiles	151
Adding an SNMP Trap Server Profile	152
Modifying an SNMP Trap Server Profile	152
Removing an SNMP Trap Server Profile	153
Defining Utilization Thresholds	153
How to Define Call Data Record (CDR) Settings	154
Creating CDR Information in XML Format	154
Defining Required Terminal Connection Duration	154
Defining a CDR File Prefix	155
Defining How Often CDRs Are Produced	155
Enabling Streaming to a RADIUS Server	156
20 <i>Configuring iVIEW Suite Redundancy</i>	
Introduction	157
Sample Configuration	158
Setup	159
After iVIEW Suite Installation	159
Defining Parameter Settings in Configuration Files	160
ha.xml	160
vnex.properties	162
vcs-core.properties	164
mssql-ds.xml	164
How to Configure Failover for Microsoft OCS 2007 Deployments	165
Configuring iVIEW Suite Servers for OCS Failover	165
Configuring the MCU for OCS Failover	165
Configuring the OCS 2007 Server for Failover	166
Configuring the OCS 2007 Client for Failover	166
Maintaining Consistency Between Live and Backup Servers	167
21 <i>iCM CDR XML Tags and Attributes</i>	
Accessing the CDR XML Files	170
Index of CDR XML Tags	170

Understanding the CDR XML Tags	182
22 <i>Enabling iCM to Use Secure Sockets Layer Connections on a JBoss Application Server</i>	
Component Identity via SSL	207
How to Generate Certificates	207
Methods for Creating a New Certificate	208
Prerequisites	208
Using Keytool to Generate a Certificate	209
Configuring JBoss to use SSL	210
Accessing iCM Using HTTPS	212
23 <i>Registering External Users with the iCM External Agent</i>	
Commands	213
Default Parameter Values	225
Modifying the Default Server	226
Sample Configuration	226

iVIEW NETWORK MANAGER

24 <i>iVIEW Network Manager Overview</i>	
About the iVIEW Network Manager	229
System Requirements	230
What the iVIEW Network Manager Provides	230
Viewing Network Status	230
Viewing Calls and Conferences	231
Using Auto-Detect	231
Configuring Basic Elements	231
Viewing Alarms and Events	232
Connecting to Element Managers	233
Connecting to Terminal Managers	233

Managing a Centralized Log	233
Viewing Multiple Networks	233
Configuring Offline Elements	233
ENC Functionality	234
Defining Network Subsets	234
Supporting ECS	234
Dragging and Dropping	234
Monitoring Calls	234
25 <i>Viewing Your Network in iVIEW Network Manager</i>	
How to View the Network as a Tree	235
Configuring Network Hierarchy	235
Creating a Custom Network Tree View	236
Viewing the Network as a Table	237
Viewing the Network as a Map	238
26 <i>Managing Elements in iVIEW Network Manager</i>	
Displaying General Element Information	240
Management Status of Elements	240
Viewing all Network Elements	241
Creating or Modifying an Element Profile	242
Removing an Element Profile	243
Searching for an Element Profile	243
Defining Default Element Access Settings	244
Defining Default PathFinder Access Settings	245
Overriding Default Element Access Settings	246
How to Upgrade Element Software	247
Adding a Software Upgrade File	247
Modifying a Software Upgrade File	247
Removing a Software Upgrade File	248
Cancelling Pending Offline Configuration Settings	248
How to Manage the Element Software Upgrade Upload Log	249
Viewing Your Software Upgrade Upload History	249

Uploading a File After a Failed Attempt	249
Removing Entries from the Upload Log	250
How to Automatically Detect New Elements on the Network	250
Running the Auto-detect Mechanism Manually	251
Running the Auto-detect Mechanism Automatically	251
Adding or Modifying Auto-detect Element Access Information	252
Removing an Element Type from the Auto-detect Mechanism	253
Accessing an Element Web User Interface	253
Accessing the Monitor Tab for a Specified Element	254

27 *Managing Endpoints in iVIEW Network Manager*

Defining Default Endpoint Access Settings	255
How to Override Default Endpoint Settings	256
Overriding Default Endpoint Addressing	256
Overriding Default Access Settings for a Selected Endpoint	257
Configuring Endpoint Dialing	257
Retrieving Configuration Parameters	258
How to Manage Endpoint Software Upgrade Files	259
Adding a Software Upgrade File	259
Modifying a Software Upgrade File	259
Removing a Software Upgrade File	260
How to Manage Endpoint Configuration Files	260
Viewing Saved Endpoint Configuration Files	261
Modifying an Endpoint Configuration File	261
Removing an Endpoint Configuration File	262
Upgrading Software for Selected Endpoints	262
Upgrading Software for Sony Endpoints	262
Upgrading Software for Polycom Endpoints	263
Updating Configuration for Selected Endpoints	264
Updating Configuration for Sony Endpoints	264
Updating Configuration for Polycom Endpoints	265
Setting the Managed Status of Polycom Endpoints	265
How to Manage the Endpoint Upload Log	266
Viewing Your Endpoint Configuration Upload History	266
Uploading a File After a Failed Attempt	266

Removing Entries from the Upload Log	267
--------------------------------------	-----

28 *Managing the ECS in iVIEW Network Manager*

How to Manage Services	269
Viewing ECS Supported Services	270
Creating or Modifying a Service	270
Viewing Global Services	271
Creating or Modifying a Global Service	272
Removing a Service	272
How to Manage Prefixes	273
Creating or Modifying a Prefix	273
Removing a Prefix	273
Bandwidth Tab (ECS version 3.5 or later)	274
How to Configure a Parent Gatekeeper	281
Enabling the Parent Tab	281
Adding a Parent Manually	281
Adding a Parent Automatically	282
How to Manage Parent Filters	282
Creating or Modifying a Parent Filter	282
Removing a Parent Filter	283
How to Configure a Child Gatekeeper	283
Enabling the Children Tab	283
Viewing Child Gatekeepers	284
Adding a Child Manually	284
Adding a Child Automatically	285
How to Manage Child Prefixes	285
Creating or Modifying a Child Prefix	285
Removing a Child Prefix	286
How to Configure a Neighbor Gatekeeper	286
Viewing Neighbor Gatekeepers	286
Adding or Modifying a Neighbor Gatekeeper	287
How to Manage Zones	288
Creating or Modifying a Local Zone	288
Creating or Modifying a Remote Zone	288
Removing a Zone	289

How to Manage Bandwidth Rules	289
Viewing Bandwidth Rules	289
Creating or Modifying a Bandwidth Rule	290
Removing a Bandwidth Rule	291
How to Manage Debug Flags	291
Creating or Modifying a Debug Flag	291
Removing a Debug Flag	291
Configuring an ECS	292
29 <i>Managing an MCU in iVIEW Network Manager</i>	
Setting Call Routing Devices	295
Viewing Registered Multipoint Processors	296
Viewing MCU Supported Services	297
How to Back Up and Restore MCU Configuration Settings	297
Backing Up MCU Configuration Settings	297
Restoring MCU Configuration Settings	298
Modifying MCU Configuration File Information	298
Deleting a Configuration File	298
Configuring MCU Unit Type and Addressing	299
30 <i>Managing a Gateway in iVIEW Network Manager</i>	
How to Manage Services	301
Viewing Gateway Supported Services	301
Creating or Modifying a Service	302
Removing a Service	302
Configuring Gateway Addressing	303
31 <i>Configuring a User Profile in iVIEW Network Manager</i>	
Creating or Modifying a User Profile	305
Removing a User Profile	306
How to Define Network Subsets	307
Creating or Modifying a Network Subset	307

	Removing a Network Subset	308
	Removing an Include or Exclude Criterion	308
32	<i>Managing Traps and Alarms in iVIEW Network Manager</i>	
	Sending Traps to iVIEW Network Manager	310
	Creating or Modifying a Trap Forwarding Rule	310
	Disabling a Trap Forwarding Rule	311
	Removing a Trap Forwarding Rule	311
	Creating or Modifying an Alert Recipient Profile	312
	Removing an Alert Recipient Profile	313
	Viewing Generated Events	313
	Filtering Generated Events	314
	Viewing Events per Network Item	314
	Viewing and Sorting Supported Alarms	315
	Modifying Alarms	315
	Viewing and Sorting Generated Alarms	316
	Viewing Generated Alarms per Network Item	316
33	<i>Managing Calls and Conferences in iVIEW Network Manager</i>	
	Viewing Current Call Details	319
	Viewing Current Call Details per Network Item	320
	Disconnecting Calls	320
	Searching for a Call	321
	Viewing Current Conferences	321
	Viewing Current Conferences per Network Item	322
	Searching for a Conference	323
	Accessing the Conference MCU	323
34	<i>Configuring Logging for iVIEW Network Manager</i>	
	Viewing Logs for a Selected Element	325

Defining iVIEW Network Manager Logging Activity	326
Saving Element Logs	326
Collecting Logs from a Cisco IOS H.323 Gatekeeper Element	327
<i>Index</i>	329

ABOUT THIS MANUAL

The [iVIEW Suite Administrator Guide](#) provides information for administrators about iVIEW Suite installation, configuration and the user interface. It includes detailed procedures about performing administrator-related tasks.

RELATED DOCUMENTATION

The iVIEW Suite documentation set is available on the RADVISION Utilities and Documentation CD-ROM supplied with the product and includes manuals and online helps. The manuals are in PDF format.

Note You require Adobe Acrobat Reader version 6.0 or later to open the PDF files. You can download Acrobat Reader free of charge from www.adobe.com.

FEEDBACK

The team at RADVISION constantly endeavors to provide accurate and informative documentation. If you have comments or suggestions regarding improvements to future publications, we would value your feedback.

Please send your comments to doc_comments@radvision.com.

We thank you for your contribution.

1

INTRODUCING iVIEW SUITE

OVERVIEW

RADVISION iVIEW Suite is a single-installation product that contains the following components:

- iVIEW Communications Manager is a simple-to-use, web-based application for managing visual communications in multi-site organization deployments. It provides resource management of network devices for video and audio meetings as well as scheduling, call-routing, and conference control functionalities.

iVIEW Communications Manager optionally includes an internal ITU-T H.323 version 4-compliant gatekeeper to provide call control for IP telephony and multimedia communication networks. This internal gatekeeper is a variation of the RADVISION Enhanced Communication Server (ECS).

iVIEW Communications Manager also contains an internal SIP Back-to-Back User Agent to provide call control for IP telephony and multimedia communication on the SIP network.

- iVIEW Network Manager provides a central management interface, enabling network administrators to easily and intuitively control, configure, and maintain collaborative RADVISION-based communication networks and equipment.

Overview

VIEW COMMUNICATIONS MANAGER

2

iVIEW COMMUNICATIONS MANAGER OVERVIEW

The iVIEW Communications Manager is a component in iVIEW Suite. This section provides an overview of this component.

- [iVIEW Communications Manager User Types](#) on page 5
- [Understanding Video Conferencing](#) on page 7
- [Login Screen Options](#) on page 8
- [Enabling Single Sign-on with Microsoft Vista and Internet Explorer 8](#) on page 9
- [Interface Orientation](#) on page 9
- [Configuration Workflow](#) on page 10

iVIEW COMMUNICATIONS MANAGER USER TYPES

The following user types are used by the system. Each user type has its own set of permissions.

- Service Provider Administrator—This user type is only available with multi-tenant support.
- Organization Administrator
- Meeting Operator
- Meeting Organizer
- Regular User

ADMINISTRATIVE PERMISSIONS

Each user type has a default set of permissions and a default view of the user interface. [Table 2-1](#) outlines the different permissions for the user types.

Table 2-1 *iCM User Types and Default Permissions*

	Service Provider Administrator	Organization Administrator	Meeting Operator	Meeting Organizer	Regular User
View and manage multiple organizations	Allowed				
View and manage all network devices across multiple organizations	Allowed				
View and manage all network devices, room terminals, and users and their virtual rooms within the organization		Allowed			
View and manage all meetings across multiple organizations	Allowed				
View and manage all meetings within the organization		Allowed	Allowed		
Create and manage meetings for others		Allowed	Allowed	Allowed	
Manage personal address book		Allowed	Allowed	Allowed	
Manage own virtual room		Allowed	Allowed	Allowed	
Create and manage own meetings		Allowed	Allowed	Allowed	Allowed
View scheduled meetings		Allowed	Allowed	Allowed	Allowed

	Service Provider Administrator	Organization Administrator	Meeting Operator	Meeting Organizer	Regular User
Receive and respond to meeting notices		Allowed	Allowed	Allowed	Allowed
Attend meetings		Allowed	Allowed	Allowed	Allowed
Moderate meetings		Allowed	Allowed	Allowed	Allowed
Modify own profile		Allowed	Allowed	Allowed	Allowed

UNDERSTANDING VIDEO CONFERENCING

This section describes the main aspects of video conferencing.

- [Network Devices](#) on page 7
- [Cascading for Flexible Conferencing](#) on page 7

NETWORK DEVICES

RADVISION network devices provide solutions for deploying high quality multipoint video meetings with video processing, audio transcoding and data-collaboration support over switched networks (ISDN) and packet-based networks (IP). RADVISION devices are modular and offer scalable solutions which can be deployed in large organizations in distributed environments. All devices provide easy to use and intuitive web-based interfaces for system management and configuration. RADVISION devices are fully compatible with third-party video network products, endpoints and terminals.

Entering complete information about each device attached to your network ensures that the iCM accurately predicts resource availability, reserves resource, and then schedules meetings accordingly.

CASCADING FOR FLEXIBLE CONFERENCING

With MCU cascading, iCM can combine meetings hosted on multiple MCUs, resulting in larger meetings with many more participants than can be supported by a single MCU. Cascading is also used to save network bandwidth by distributing network load over multiple MCUs.

With dynamic cascading, participants can join a meeting on-the-fly (that is, ad hoc) and if originally scheduled resources are not available, iCM can automatically schedule and assign MCU resources to accommodate the new participants. This means that a large conference can increase to a size greater than that of the conference originally scheduled, providing that sufficient network resources are available.

Cascading, in general, creates a distributed environment that reduces potential drain on network resources. Processing resources required in order to host a meeting are distributed among participating MCUs.

LOGIN SCREEN OPTIONS

The login screen offers the following options:

- Log in to the iCM user interface by providing the user ID and password.
- Click **Enter a Meeting** to open a new window from where you directly access the In-meeting Control interface of an ongoing meeting via meeting ID and PIN.
- Click **Network Management** to open a new window from where you can access the iVIEW Network Manager user interface.

SERVICE PROVIDER LOGIN

To log in to iCM with multi-tenant support as a service provider administrator, enter your user ID and password in the login screen. Leave the Organization field empty.

Note For iCM with multi-tenant support, users except the Service Provider Administrator need to supply a user ID, password and organization.

SINGLE SIGN-ON (SSO)

Single Sign-in (SSO) is only available for iCM without multi-tenant support. In other words, SSO only works in a single-enterprise setting. With SSO selected, users who log in to their Microsoft Windows account within their organization domain can log in to the iCM directly without having to enter their user names and passwords. iCM automatically authenticates the users using their Windows login ID, password, and domain name. For more information, refer to the Single Sign On (SSO) topic in the Installation Guide.

ENABLING SINGLE SIGN-ON WITH MICROSOFT VISTA AND INTERNET EXPLORER 8



The Single Sign-on (SSO) feature does not work with Internet Explorer 8 under Vista by default. Modify the Vista default security setting as described here to enable SSO.



Procedure






- 1 Go to **Administrative Tools > Local Security Policy > Security Options** on your computer.
- 2 Double-click **Network security: LAN Manager** or right-click and select **Properties**.
- 3 Select **Send LM & NTLM - use NTLMv2 session security if negotiated** in the Local Security Setting tab.
- 4 Click **Apply**.

INTERFACE ORIENTATION

The iCM toolbar is located in the upper-right corner of the window. The following table describes the graphic elements on the toolbar.

Table 2-2 *Toolbar Details*

Element Name	Icon	Description
Help About		Opens a window that contains license and version information about iVIEW Suite.
Customization		The Customization Tool icon is enabled in Configuration Tool > System Configuration > UI Settings > Customization Tool. Click the icon to open a new window and follow the steps to customize any Web interface display label in iVIEW Communications Manager according to your needs.

Element Name	Icon	Description
Help		Opens the online help window for iCM.
Show Log		Opens a window that contains iCM log files.
Event List		Opens a window that contains recent events.
Restart Server		Restarts the iVIEW Suite service from the web interface.
Login as a different user		Logs out of iCM.

CONFIGURATION WORKFLOW

We recommend that administrators configure iCM according to the following workflow:

- Organization Management—Optional (required only if multi-tenant support is enabled)
- Network Configuration—Optional (required only for distributed deployment)
 - IP topology
- Gatekeepers/SIP servers
- MCUs
 - meeting types
- Gateways
- SCOPIA Desktop Server

- Meeting rooms—optional
- Terminals
- Users
- Schedule first meeting

Note Some sections of the user-interface are hidden by default, according to settings in the Configuration Tool; however, these sections are included in the documentation.

Configuration Workflow

3

MANAGING ORGANIZATIONS IN ICM

This section is for Service Provider Administrators only.

- [How to Create an Organization Profile](#) on page 13
- [Viewing an Organization Profile](#) on page 17
- [Searching for an Organization Profile](#) on page 17
- [How to Activate/Deactivate an Organization Profile](#) on page 18
- [Generating an Organization Report](#) on page 19
- [Removing an Inactive Organization Profile](#) on page 20

HOW TO CREATE AN ORGANIZATION PROFILE

It is important to understand the distinction between the iVIEW Communications Manager *organization* and the iVIEW Communications Manager *user*.

An organization is a company, an enterprise or an individual that is registered with a Service Provider for video meeting services. An organization controls a discrete set of endpoints and a user group. An organization controls privileges for its users.

A user sits at the base of the iVIEW Communications Manager user pyramid. Users use iVIEW Communications Manager on a day-to-day basis to schedule meetings and invite attendees.

- [Defining Organization Contact Details](#) on page 14
- [Branding the User Interface](#) on page 14
- [Defining Concurrent Call Limits](#) on page 15
- [Defining a Billing Code](#) on page 16
- [Enabling Organization Meeting Types](#) on page 16
- [Defining Organization System Administrator Credentials](#) on page 17

DEFINING ORGANIZATION CONTACT DETAILS



Procedure

- 1 Click **Organization Management** in the sidebar menu.
 - 2 Click **Active**.
 - 3 Click **Add**.
 - 4 Enter the name of the organization in the **Organization Name** field.
Users in the organization use this name to access the iVIEW Communications Manager web user interface.
 - 5 Enter address information for the organization in the relevant fields.
 - 6 Enter contact information for the organization in the relevant fields.
The telephone number appears in the Active and Inactive tabs.
 - 7 Click **OK** to save your changes.
-

BRANDING THE USER INTERFACE

Use this procedure to enable the Organization Administrator to change the product logo that appears in the top left corner of the user interface.



Procedure

- 1 Click **Organization Management** in the sidebar menu.
- 2 Click **Active**.
- 3 Click **Add**.
- 4 Check **Allow Product Branding**.
When checked
 - The last product logo defined by the Organization Administrator appears in the user interface for all organization users.
 - The Branding tab appears in the Organization Settings section.When unchecked
 - The Branding tab does not appear in the Organization Settings section for the specified organization.
 - The product logo defined by the Service Provider Administrator appears in the top left corner of the user interface for all organization users.

- The Organization Administrator cannot change the product logo display.

Unselected by default.

Note Branding operations can also be performed via the iVIEW Suite Configuration Tool.

- 5 Click **OK** to save your changes.
-

DEFINING CONCURRENT CALL LIMITS



Procedure

- 1 Click **Organization Management** in the sidebar menu.
 - 2 Click **Active**.
 - 3 Click **Add**.
 - 4 Check **Limit Gateway Use to n Concurrent Calls** or **Limit MCU Use to n Concurrent Calls** to define the maximum number of concurrent gateway or MCU calls that can be scheduled for an organization.
During resource allocation, iVIEW Communications Manager checks if a newly scheduled meeting exceeds the defined limit.
 - 5 Check **If Over Limit: Refuse** to provide the user with a warning message if the meeting you are scheduling causes the allowed number of concurrent calls over the gateway/MCU to be exceeded, and to return the user to the scheduling interface.
If this option is not checked and the scheduled meeting causes the number of allowed concurrent calls over the gateway/MCU to be exceeded, the extra terminals in the meeting are recorded in the CDR.
 - 6 Click **OK** to save your changes.
-

DEFINING A BILLING CODE



Procedure

- 1 Click **Organization Management** in the sidebar menu.
 - 2 Click **Active**.
 - 3 Click **Add**.
 - 4 Enter a billing code for the organization in the **Billing Code** field.
 - 5 Click **OK** to save your changes.
-

ENABLING ORGANIZATION MEETING TYPES



Procedure

- 1 Click **Organization Management** in the sidebar menu.
 - 2 Click **Active**.
 - 3 Click **Add**.
 - 4 Locate the Meeting Type Groups field.
 - 5 Click **Select Groups** to select the meeting type groups for use by the organization.
Service Provider Administrators are advised to download and upload meeting types to/from iVIEW Communications Manager before creating organizations.
 - 6 Use the arrows in the Select Groups screen to select the required meeting types for the specified organization, and then click **OK**.
By default, all users in an organization have access to all meeting types of that organization.
 - 7 Click **OK** to save your changes.
-

DEFINING ORGANIZATION SYSTEM ADMINISTRATOR CREDENTIALS

This section is for Service Provider Administrators only for a multi-tenant.



Procedure

- 1 Click **Organization Management** in the sidebar menu.
 - 2 Click **Active**.
 - 3 Click **Add**.
 - 4 Locate the System Administrator Information section.
 - 5 Enter a login ID, password, and e-mail address for the system administrator of the organization in the relevant fields.
 - 6 Select a user provisioning option for synchronizing information about users defined in an external directory server.
 - 7 Click **OK** to save your changes.
-

VIEWING AN ORGANIZATION PROFILE



Procedure

- 1 Click **Organization Management** in the sidebar menu.
 - 2 Click the name of the organization whose details you want to display.
-

SEARCHING FOR AN ORGANIZATION PROFILE



Procedure

- 1 Click **Organization Management** in the sidebar menu.
- 2 Enter all or part of the name of the organization you want to find in the **Name** field.

How to Activate/Deactivate an Organization Profile

3 Click **Search**.

Search results are listed.

4 To return to the complete list of organizations, clear the Name field, and then click **Search**.

HOW TO ACTIVATE/ DEACTIVATE AN ORGANIZATION PROFILE

- [Activating an Organization Profile](#) on page 18

- [Deactivating an Organization Profile](#) on page 18

ACTIVATING AN ORGANIZATION PROFILE

An active organization is an organization to which you provide a service. The organization profile determines organization-specific parameters.



Procedure

1 Click **Organization Management** in the sidebar menu.

2 On the Inactive tab, click the check box beside the name of the organization profile you want to activate.

3 Click **Activate**.

The organization is removed from the Inactive tab and appears on the Active tab. All meeting types for the organization are restored.

4 Click **OK** to save your changes.

DEACTIVATING AN ORGANIZATION PROFILE

An active organization is an organization defined in the iVIEW Communications Manager but not currently receiving a service from you.



Procedure

1 Click **Organization Management** in the sidebar menu.

2 On the Active tab, click the check box beside the name of the organization profile you want to deactivate.

3 Click **Deactivate**.

A warning message appears, confirming if you want to deactivate the organization.

- 4 (Optional) Click **OK** if you do want to proceed.

The organization is deactivated and appears on the Inactive tab. The organization profile is maintained but the members of the organization cannot be used in the system unless they are reactivated.

GENERATING AN ORGANIZATION REPORT

You can generate a report in .xls format, showing information about organizations. Once you have saved the report, you can view it using Microsoft Excel.

The report contains the following information fields for each organization:

- Organization Name
- Address 1
- Address 2
- City
- State
- Zip Code
- Country
- Telephone #
- Meeting Type Groups
- Organization Since



Procedure

- 1 Click **Organization Management** in the sidebar menu.
 - 2 Click **Generate Reports** on the Active tab.
Information about each organization is included in the report.
 - 3 Click **Save** to save the report.
 - 4 Browse to the location at which you want to save the file, enter the file name and type, and then click **Save**.
-

REMOVING AN INACTIVE ORGANIZATION PROFILE



Procedure

- 1 Click **Organization Management** in the sidebar menu.
- 2 On the Inactive tab, click the check box beside the name of the organization profile you want to remove.
- 3 Click **Delete**.

The organization profile is deleted from the scheduler and information about the organization is removed from the database.

4

MANAGING NETWORK TOPOLOGIES IN iCM

This section is for Organization or Service Provider Administrators.

- [How to Create a Network Topology with Device Islands](#) on page 21
- [Viewing IP and ISDN Network Topologies](#) on page 24
- [Modifying Your Network Topology View](#) on page 25

HOW TO CREATE A NETWORK TOPOLOGY WITH DEVICE ISLANDS

IP network topology is the foundation of intelligent resource allocation. It allows iCM to model the video network by recording distance and bandwidth between device islands (IP locations where central and essential devices such as gatekeepers, MCUs, and gateways are placed) and to perform least-cost or best-performance routing over the IP network. An IP endpoint is also associated with its nearest device island when the endpoint is configured. This information is used by iCM to determine the best gatekeeper, MCU, and gateway resources to reserve and schedule for any call.

ISDN network topology intelligently manages ISDN/PSTN network connectivity and cost, gateway numbers, and PSTN/ISDN endpoint numbers that are assigned to ISDN device islands (similar to IP Network Topology). This allows iCM to perform least-cost routing over the ISDN network according to the topology configuration.

Within the same ISDN device island, PSTN/ISDN least-cost routing is also performed based on country codes, area codes of gateway numbers, and PSTN/ISDN endpoint numbers. Costly telephone or PSTN/ISDN line-usage is reduced by selecting the least costly gateway resources via telephone number.

- [Adding a Device Island](#) on page 22
- [Modifying Device Island Settings](#) on page 23
- [Removing Connectivity Between Device Islands](#) on page 24
- [Removing a Device Island](#) on page 24

ADDING A DEVICE ISLAND

In a large distributed deployment, create a device island for each location containing network devices, such as MCUs, gateways, and endpoints. The iCM monitors the bandwidth limitations and distance between each of the device islands.

In a multi-zone deployment where each ECS has its own zone prefix, define a device island for each zone and assign the ECS and the MCU/gateways registered to that ECS to the same device island.

The IP Topology tab displays distance and bandwidth information for all device islands within your video meeting network.

- **Distance**—The distance between the specified device islands relative to all other configured islands on the organization LAN. This setting is used to find and allocate the best available resources. The Distance value is a weight factor (from 1 to 100) that describes relative network delay between two device islands. The larger the distance, the larger the round trip delay caused by the network between two device islands. The distance should be an attribute proportional to the network delay. One logical way to model delay is to “ping” the connection between the two LANs and use the average delay results.
- **Bandwidth**—The bandwidth connection (in Kbps) between specified device islands. This setting is used in bandwidth control during resource allocation. The Bandwidth field represents the connection bandwidth (in Kbps) between any two device islands that can be used for video meetings. This is defined by the narrowest section of bandwidth, usually one of the outgoing connections from the LAN.

The ISDN Topology tab displays distance and cost information for all device islands within your PSTN/ISDN network.

- **Cost**—The cost of a PSTN/ ISDN call between the specified device islands relative to all other configured islands on the organization PSTN/ ISDN network. This setting is used to find and allocate best available resources.



Procedure

- 1 Click **Network Management** in the sidebar menu.
 - 2 Click **Add**.
An empty grid containing a single row appears. The row includes all of the existing device islands displayed in columns.
 - 3 For device islands on an IP network, enter the required distance and bandwidth in each column.
 - 4 For device islands on an ISDN network, enter the required distance and cost in each column.
 - 5 Click **OK** to save your changes.
-

MODIFYING DEVICE ISLAND SETTINGS



Procedure

- 1 Click **Network Management** in the sidebar menu.
 - 2 Modify the distance and bandwidth in the appropriate cell.
 - 3 Click **OK** to save your changes.
-

REMOVING CONNECTIVITY BETWEEN DEVICE ISLANDS



Procedure

- 1 Click **Network Management** in the sidebar menu.
 - 2 Delete the distance and bandwidth values for the required device island pair.
 - 3 Click **OK** to save your changes.
-

REMOVING A DEVICE ISLAND



Procedure

- 1 Click **Network Management** in the sidebar menu.
 - 2 Click the X above the device island that you want to delete.
The Reassign Device Island window appears if there are network devices currently assigned to this device island.
 - 3 Select the device island you want to reassign the devices to, and then click **OK**.
 - 4 Click **OK** in the Network Management screen to save your changes.
-

VIEWING IP AND ISDN NETWORK TOPOLOGIES

The Network Management section is hidden by default.



Procedure

- 1 Open the iVIEW Suite Configuration Tool.
- 2 Go to **System Configuration > UI Settings**.

- 3 Select the **IP Topology** and **ISDN Topology** fields.
 - 4 Click **Network Management** in the sidebar menu of the iCM web user interface.
-

MODIFYING YOUR NETWORK TOPOLOGY VIEW



Procedure

- 1 Click **Network Management** in the sidebar menu.
 - 2 Click **Display Locations**.
 - 3 Use the arrows to move the device islands that you want to display from the Available Locations column to the Assigned Locations column.
 - 4 Click **Search**.
 - 5 The selected device islands appear in the grid display.
-

Modifying Your Network Topology View

5

CONFIGURING A GATEKEEPER PROFILE IN ICM

- [About Gatekeeper Types](#) on page 27
- [How to Create or Modify a Gatekeeper Profile](#) on page 28
- [Removing a Gatekeeper Profile](#) on page 31
- [Searching for a Gatekeeper Profile](#) on page 31
- [Accessing Meetings from an External Gatekeeper](#) on page 32

ABOUT GATEKEEPER TYPES

iVIEW Suite supports the following types of gatekeeper:

- [Internal Gatekeeper](#) on page 27
- [Standalone RADVISION ECS Gatekeepers](#) on page 28
- [External Gatekeepers](#) on page 28

INTERNAL GATEKEEPER

If the version of iVIEW Suite that you are using is shipped with an internal gatekeeper for the SCOPIA bundle. Use the default gatekeeper configuration that is already configured after iVIEW Suite installation. The internal gatekeeper is a light version of the RADVISION ECS Gatekeeper. The internal gatekeeper is restricted to only work in authorization mode (whereas the standalone ECS Gatekeeper can work either in authorization mode or non-authorization mode).

iCM acts as the authorization server for any traffic going through the internal gatekeeper working in fully routed mode. In such cases, iCM can manage endpoint-initiated calls and point-to-point calls.

Register MCUs, gateways and endpoints (terminals) to the iVIEW Suite internal gatekeeper.

STANDALONE RADVISION ECS GATEKEEPERS

iCM can act as the authorization server for any traffic going through standalone ECSs working in a fully routed mode. With this mechanism, iCM can manage endpoint-initiated calls and point-to-point calls, and present a group of distributed, deployed MCUs as a single pool of video and audio resources. This feature is known as Virtual MCU.

Register MCUs, gateways, and endpoints (terminals) to ECS Gatekeepers.

EXTERNAL GATEKEEPERS

iCM supports external H.323 gatekeepers (such as the Cisco IOS H.323 Gatekeeper) when the external gatekeeper is configured as a neighbor to the iVIEW Suite internal gatekeeper or ECS.

Register only endpoints (terminals) to an external. Register gateways and MCUs to the internal gatekeeper or ECS.

HOW TO CREATE OR MODIFY A GATEKEEPER PROFILE

Only an Organization Administrator (or Service Provider Administrator when Multi-tenant support is enabled) has permission to configure an H.323 gatekeeper in the system for video conferences using the H.323 protocol.

- [Defining Gatekeeper Address Details](#) on page 28
- [Defining Dialing Plan Settings](#) on page 29
- [Defining iCM as the Gatekeeper Authorization Server](#) on page 30

DEFINING GATEKEEPER ADDRESS DETAILS



Procedure

- 1 Click **Resource Management** in the sidebar menu.
- 2 Click **Gatekeeper/SIP server**.
- 3 Click the link in the Name column for the gatekeeper you require, or click **Add** to create a new gatekeeper profile.
- 4 Locate the General section.
- 5 Enter the name and IP address of the gatekeeper in the relevant fields.
- 6 Select the gatekeeper model.
If you select **Other** in the Model field, select **H.323** in the Protocol field.

- 7 Select the device island to which the gatekeeper belongs from the Location list.

Each device island can have only one gatekeeper.

The Location field is visible only when the IP Topology tab is activated in the iCM Configuration Tool under System Configuration > UI Settings.

- 8 Click **OK** to save your changes.
-

DEFINING DIALING PLAN SETTINGS



Procedure

- 1 Click **Resource Management** in the sidebar menu.
- 2 Click **Gatekeeper/SIP server**.
- 3 Click the link in the Name column for the gatekeeper you require, or click **Add** to create a new gatekeeper profile.
- 4 Locate the Dialing Plan Information section.
- 5 (Optional) Select **Hierarchical** if the gatekeeper has a parent-child relationship with its neighbor in the dialing plan, rather than a flat peer relationship.

If you select Hierarchical, the Parent Gatekeeper list becomes active.

Select a parent zone for the gatekeeper from the list. **None** is automatically selected in the list if the gatekeeper is a parent at the top of the hierarchy.

Do not select Hierarchical for a root gatekeeper. The root gatekeeper in a hierarchical tree structure has no parent but may have peer neighbors.

- 6 (Optional) Select **Stripping** for a gatekeeper that is configured to strip (remove) zone prefixes.
 - 7 Click **Add Zone Prefix** to add a zone prefix that matches the configuration of the gatekeeper.
 - 8 Click **OK** to save your changes.
-

DEFINING ICM AS THE GATEKEEPER AUTHORIZATION SERVER



Procedure

- 1 Click **Resource Management** in the sidebar menu.
 - 2 Click **Gatekeeper/SIP server**.
 - 3 Click the link in the Name column for the gatekeeper you require, or click **Add** to create a new gatekeeper profile.
 - 4 Locate the Advanced section.
The Advanced section appears if you are using the internal gatekeeper or ECS.
 - 5 Select **Enable Gatekeeper advanced features (authorization and point-to-point)** to set iCM as the authorization server of the internal gatekeeper or ECS.
iCM will initiate a connection to the ECS for authorization and call control.
 - 6 If you are using the internal gatekeeper—You do not need to modify the internal gatekeeper default values for the Port, SNMP Get Community and SNMP Set Community fields.
 - 7 If you are using the ECS—Ensure the SNMP community names are correct.
iCM requires this to properly initiate the authorization connection with the ECS.
You can view the SNMP Get Community and SNMP Set Community fields on the ECS host server under Control Panel > Administrative Tools > Services > SNMP Service > Security.
 - 8 Ensure the following configuration options are set on the ECS or internal gatekeeper:
 - Under ECS > Settings > Calls, set the **Routing Mode** field to **Call Setup (Q.931) and Call Control (H.245)**.
 - Under ECS > Settings > External API:
 - Select **Allow Authorization servers to connect**.
 - 9 Click **OK** to save your changes.
-

REMOVING A GATEKEEPER PROFILE



Procedure

- 1 Click **Resource Management** in the sidebar menu.
- 2 Click **Gatekeeper/SIP server**.
- 3 Click the gatekeeper entry you want to delete in the Name column.
- 4 Click **Delete** and then **OK**.

The gatekeeper profile is deleted from the scheduler and information about the gatekeeper is removed from the database.

SEARCHING FOR A GATEKEEPER PROFILE



Procedure

- 1 Click **Resource Management** in the sidebar menu.
- 2 Click **Gatekeeper/SIP server**.
- 3 Enter all or part of the name of the gatekeeper you want to find in the **Name** field.
- 4 Click **Search**.

Search results are listed. If you are using the internal gatekeeper or ECS, the following information about connection status is available in the list of search results:

- Authorization Connection indicates whether or not iCM acts as the authorization server for the internal gatekeeper or ECS. This connection needs to appear as connected for advanced iCM features such as Virtual MCU and point-to-point call control to function correctly.
- Call Control Connection indicates whether or not a Call Control API connection is established between the gatekeeper and iCM. This corresponds to the Settings > Calls > Enable XML call control field in the ECS user interface.

- SNMP Connection indicates whether or not the SNMP connection between the iCM and the gatekeeper is established.
- 5 To return to the complete list of gatekeepers, clear the Name field, and then click **Search**.
-

ACCESSING MEETINGS FROM AN EXTERNAL GATEKEEPER



If iCM ECS is neighbored to an external gatekeeper (for example, a Cisco IOS Gatekeeper), perform the following configuration steps in the ECS web user interface to enable dial-in and dial-out to work properly between the ECS and the external gatekeeper:

Procedure

- 1 Add the external gatekeeper as a neighbor to this ECS at Hierarchy > Neighbors, and define the appropriate zone prefix according to the dial plan.
When iCM works in authorization mode with the ECS, meeting IDs start with the iCM meeting ID prefix (configured via the Meeting ID Prefix field at Configuration Tool > System Configuration > Scheduling Settings screen).
- 2 Add a new service to the Services tab and select **Conference Hunting**. The service prefix should be the same as the Meeting ID Prefix field in the iVIEW Suite Configuration Tool.
- 3 On the Endpoints tab, click **Add Predefined** to add a new dummy endpoint for routing purposes.
- 4 Enter dummy values in the **Registration IP** and **Call Signaling IP** fields.
- 5 Add the following two aliases:
 - Value = Fake Terminal, Type = Name
 - Value = Meeting ID Prefix value, Type = Phone number
- 6 Click **Upload** to save your changes.

Note iCM automatically performs the above steps on the internal gatekeeper, so no extra internal gatekeeper configuration is necessary.

- 7 In the external gatekeeper interface, add the ECS (or internal gatekeeper) as a neighbor to this external gatekeeper, and define the zone prefix for the ECS according to the dial plan.
- 8 Define the following forwarding rules in the external gatekeeper interface:
 - Forward any dial strings that begin with iCM Meeting ID Prefix to the ECS.
 - Forward any dial strings that begin with MCU service prefix or Gateway service prefix to the ECS.

Since terminals are registered to the external gatekeeper, these two forwarding rules allow these terminals to dial into the iCM meetings from the external gatekeeper.

Accessing Meetings from an External Gatekeeper

6

CONFIGURING A SIP SERVER PROFILE IN ICM

- [Creating or Modifying a SIP Server Profile](#) on page 35
- [Removing a SIP Server Profile](#) on page 36
- [Searching for a SIP Server Profile](#) on page 37
- [Configuring the MCU to Work in SIP Mode](#) on page 37
- [Disabling the SIP Back-to-Back User Agent](#) on page 38

CREATING OR MODIFYING A SIP SERVER PROFILE

iCM includes an embedded SIP Back-to-Back User Agent (B2BUA) component for managing SIP traffic to network devices (such as to MCUs) which are managed by iCM.

To enable iCM to operate with SIP endpoints, configure iCM with an external SIP server to which SIP endpoints are registered.



Procedure

- 1 Click **Resource Management** in the sidebar menu.
- 2 Click **Gatekeeper/SIP server**.
- 3 Click the link in the Name column for the SIP server you require, or click **Add** to create a new SIP server profile.
- 4 Enter the name and IP address or Fully Qualified Domain Name (FQDN) of the SIP server in the relevant fields.

- 5 Select the SIP server model.
You can select Microsoft LCS 2005/OCS 2007 or other third-party SIP servers. iCM is interoperable with the following external SIP servers:
 - ❑ Cisco Unified Communications Manager version 5.0 or later
 - ❑ Microsoft Live Communications Server 2005 with Service Pack 1
 - ❑ Broadsoft IPCentrix
 - 6 (Optional) If you select **Other** in the Model field, select **SIP** in the Protocol field.
 - 7 Select the device island to which the SIP server belongs from the Location list.
Each device island can have only one SIP server.
The Location field is visible only when the IP Topology tab is activated in the iVIEW Suite Configuration Tool under System Configuration > UI Settings.
 - 8 Enter the name of the SIP server in the **SIP Domain** field.
 - 9 (Optional) Enter the name of a preferred and an alternative DNS server in the relevant fields.
 - 10 Click **OK** to save your changes.
-

REMOVING A SIP SERVER PROFILE



Procedure

- 1 Click **Resource Management** in the sidebar menu.
- 2 Click **Gatekeeper/SIP server**.
- 3 Click the SIP server entry you want to delete in the Name column.
- 4 Click **Delete** and then **OK**.

The SIP server profile is deleted from the scheduler and information about the SIP server is removed from the database.

SEARCHING FOR A SIP SERVER PROFILE



Procedure

- 1 Click **Resource Management** in the sidebar menu.
 - 2 Click **Gatekeeper/SIP server**.
 - 3 Enter all or part of the name of the SIP server you want to find in the **Name** field.
 - 4 Click **Search**.
Search results are listed.
 - 5 To return to the complete list of SIP servers, clear the Name field, and then click **Search**.
-

CONFIGURING THE MCU TO WORK IN SIP MODE



Procedure

Perform the following configuration steps in the MCU web user interface.

- 1 Select **Configuration > Protocols > SIP**.
 - 2 Enter the iCM IP address in the SIP server **IP address** field.
Do not change the port number or the type (UDP/TCP). The default port is 5060 and type is UDP.
 - 3 If the external SIP server is LCS, select **Using Microsoft LCS/OCS**.
In this case, the type is always TCP.
 - 4 Click the **More** arrow near the bottom of the screen.
 - 5 Select Use **“Empty Invite” when sending messages to endpoints**.
-

Note We recommend using an empty invite when dialing out to a SIP endpoint.

- 6 Click **OK** to save your changes.

- 7 On the external SIP server, define a routing rule that forwards all calls whose dialing strings begin with the iCM meeting ID or service prefix to iCM.

The embedded SIP B2BUA can then forward the call to the appropriate MCU conference.

Note The default signalling port of the external SIP server is 5060.

DISABLING THE SIP BACK-TO-BACK USER AGENT

You can disable the B2BUA if iCM is currently not operating with an external SIP server to which SIP endpoints are registered.



Procedure

- 1 Go to **Control Panel > Administrative Tools > Services** on the iVIEW Suite server.
- 2 Locate the service named “SIP Server” and stop it.
- 3 Use a text editor to open the `vcs-core.properties` file located at `JBOSS_HOME\bin` on the iVIEW Suite server where `JBOSS_HOME` is the home directory of the JBOSS application server used in iVIEW Suite.

By default, `JBOSS_HOME` is `C:\Program Files\RADVISION\iVIEW Suite\iCM\jboss\bin`

- 4 Set the following line as shown:
`vnex.vcms.core.sip.serverAddress=`
 - 5 Save and close the `vcs-core.properties` file.
 - 6 Restart the SIP Server service for the change to take affect.
-

7

MANAGING AN MCU PROFILE IN ICM

- [Configuring Cascading](#) on page 39
- [Creating or Modifying an MCU Profile](#) on page 41
- [Taking an MCU Offline](#) on page 42
- [Removing an MCU Profile](#) on page 42
- [Searching for an MCU Profile](#) on page 43
- [Synchronizing MCU Information with iVIEW Suite](#) on page 43
- [How to Manage Meeting Types](#) on page 44
- [Customizing MCU Delimiters](#) on page 51
- [Designating a Service for IVR Use](#) on page 52

CONFIGURING CASCADING

iCM is able to manage multiple MCUs as a pool of resources. You can cascade MCUs to reduce potential drain on network resources, increase the efficiency of MCU usage, and allow large conferences to be held. The following points about cascading should be noted:

- The Meeting Type (MCU service) representing the required meeting must be available on all participating MCUs. For example, if the meeting uses MCU service 81, then 81 must exist on the master MCU and on the slave MCUs.
- A cascaded connection uses two ports—one on the master MCU conference, and one port on the slave MCU conference.
- Only one cascading stream exists between the master MCU and the slave MCU; therefore, only one participant from the slave MCU can send video for mixing and only one participant from the slave MCU can be seen by other participants in the meeting.

Configuring Cascading

- Only one level of cascading is supported. All slave MCU conferences must cascade to the same master MCU conference.
- The administrator must define a default system level property that determines the cascading behavior.

To configure the MCU cascading behavior, use the following procedure:



Procedure

- 1 Go to **Admin > Advanced Settings** from the sidebar menu.
 - 2 On the Default Meeting Settings tab you can enable or disable automatic cascading of MCU conferences by configuring the Allow Cascaded Meeting field.
 - 3 If Allow Cascaded Meeting is set to yes, select one of the following options from the Prioritize field:
 - **Bandwidth**—iCM allocates resources to conserve bandwidth. For example, at a site with two users and one MCU, iCM creates a local meeting. In some cases, this may cause a meeting to cascade to conserve bandwidth, even though a single MCU is available to host the meeting.
Using this option, iCM cascades a maximum of two MCUs.
 - **Delay (default)**—iCM allocates resources to ensure the best video quality. iCM invites all users directly to a main MCU, whatever their location. Since Delay can be costly in terms of bandwidth, it is recommended that you take topology into account before selecting the Delay option.
 - **Local MCU**—Select this option if iCM has more than one MCU and there are at least two meeting participants. iCM invites all of the participating terminals to meetings hosted on their respective local MCUs (according to IP Topology settings), and then cascades these meetings together to form a single conference.
 - 4 Click **OK** to save the preferred behavior as the default.
-

CREATING OR MODIFYING AN MCU PROFILE

The MCU is where a multipoint video conference is hosted. iCM reserves MCU resources, schedules MCU conferences, and controls in-session MCU meetings. In order for iCM to correctly manage the MCU, it needs to retrieve configuration information from the MCU via the profiles defined under Admin > Resource Management.



Procedure

- 1 Click **Resource Management** in the sidebar menu.
- 2 Click **MCU**.
- 3 Click the link in the Name column for the MCU you require, or click **Add** to create a new MCU profile.
- 4 Enter the name and IP address of the MCU in the relevant fields.
- 5 Select the MCU model.
- 6 If you want to register the MCU to operate in SIP mode only (without registering to an H.323 gatekeeper), select **MCU operates in SIP only mode**.
The MCU is not required to register to a gatekeeper and the Registered To field is inactive.
- 7 Select the device island from the **Location** list to which the MCU belongs.
The Location field is visible only when the IP Topology tab is activated in the iVIEW Suite Configuration Tool under System Configuration > UI Settings.
- 8 Enter the login name and login password of the MCU in the relevant fields.
These must match the MCU web interface login name and password.
- 9 Define SNMP communities, user name and password, communication port and signaling port in the relevant fields.
SNMP community information must match the settings defined in the MCU to enable iCM to retrieve information from the MCU.
- 10 Click **OK** to save your changes.
- 11 The MCU is added to the MCU tab and brought online by default.
If iCM cannot connect to a newly configured MCU, the MCU is added but its status is shown as Offline in the MCU tab.
To try to reconnect to the MCU, select **Online**, and then click **OK**.

TAKING AN MCU OFFLINE



Procedure

- 1 Click **Resource Management** in the sidebar menu.
- 2 Click **MCU**.
- 3 Click the link in the Name column for the MCU you require.
- 4 To take the MCU offline temporarily, select **Take this MCU offline and reschedule all meetings on this MCU up to this date** and set the date to bring the MCU online again.
- 5 To take the MCU offline permanently, select **Take this MCU offline and reschedule all meetings currently on this MCU**.
- 6 Click **OK** to save your changes.

When you take the MCU offline, the following changes occur:

- iCM cannot schedule meetings for the offline MCU.
 - All meetings currently in progress are terminated. iCM attempts to reschedule upcoming meetings for the offline MCU on other MCUs that use the same services and have sufficient, available resources. If no replacement MCUs are available when the MCU status is changed back to online, upcoming meetings are lost and not restored.
 - If the MCU goes offline temporarily, iCM attempts to reschedule all meetings scheduled to this MCU from the time the MCU goes offline to the specified date for its return online.
 - If the MCU goes offline permanently, iCM attempts to reschedule all future meetings scheduled to this MCU.
-

REMOVING AN MCU PROFILE



Procedure

- 1 Click **Resource Management** in the sidebar menu.
- 2 Click **MCU**.
- 3 Click the MCU entry you want to delete in the Name column.

You must take an MCU offline before you can remove it from the iVIEW Suite database.

- 4 Click **Delete** and then **OK**.

The MCU profile is deleted from the scheduler and information about the MCU is removed from the database.

SEARCHING FOR AN MCU PROFILE



Procedure

- 1 Click **Resource Management** in the sidebar menu.
 - 2 Click **MCU**.
 - 3 Enter the partial or complete name of the MCU in the **Name** field.
 - 4 Click **Search**.
Search results are listed.
 - 5 To return to the complete list of MCUs, clear the Name field, and then click **Search**.
-

SYNCHRONIZING MCU INFORMATION WITH IVIEW SUITE



Procedure

- 1 Click **Resource Management** in the sidebar menu.
- 2 Click **MCU**.
- 3 Click the MCU entry you want to update in the Name column.
- 4 Click **Synchronize**.

The information download includes the number of cards the MCU has and the resource capacity of each card.

HOW TO MANAGE MEETING TYPES

A meeting type in iCM is the equivalent of the MCU service definition. Services should be defined in the MCU first and then synchronized to iCM. In the Meeting Types section, retrieve services from MCUs configured in the system and then save them to iCM. iCM then distributes these services to other MCUs according to your specific deployment requirements. Meeting types in iCM are used to schedule meetings on the MCU. There are also built-in meeting types that are not retrieved from the MCU in iCM.

- [Viewing Available Meeting Types on Network MCUs](#) on page 44
- [Viewing Built-in Meeting Types](#) on page 45
- [Removing a Meeting Type](#) on page 46
- [Searching for a Meeting Type](#) on page 46
- [Downloading a Meeting Type to iCM](#) on page 47
- [Resolving Meeting Type Conflicts Between MCUs](#) on page 47
- [Resolving Meeting Type Conflicts Between iCM and an MCU](#) on page 48
- [Uploading a Meeting Type to Network MCUs](#) on page 48
- [Viewing Meeting Type Details](#) on page 49
- [Modifying Meeting Type Details](#) on page 49
- [Accessing an MCU from the Meeting Type Details Screen](#) on page 50
- [Viewing a List of MCUs Containing a Specified Meeting Type](#) on page 50
- [Creating or Modifying a Meeting Type Group](#) on page 50
- [Removing a Meeting Type Group](#) on page 51

VIEWING AVAILABLE MEETING TYPES ON NETWORK MCUS



Procedure

- 1 Click **Meeting Types** in the sidebar menu.
- 2 Ensure that the Active Meeting Types tab is displayed.

All meeting types available for meeting scheduling are displayed with the parameters listed in [Table 7-1](#).

If the name of a meeting type appears in red, the meeting type does not belong to any MCU and cannot currently be used for meeting scheduling.

Table 7-1 Meeting Type Parameters

Parameter	Description
Name	The name of a meeting type defined in iCM.
Prefix	The service prefix downloaded from the MCU.
Description	The service description downloaded from the MCU.
Media	The service media type downloaded from the MCU.
BW(Kbps)	The maximum service bandwidth (in kilobytes per second) for download from the MCU.
Lecture Mode	For MCU services that support exactly two views with the first view being single sub-frame and the second view being multiple sub-frames, you can set this service to support the lecture mode feature in which a meeting participant is set to one view and can be seen by all other participants, and the other participants are set to the other view and can be seen by the first participant.
In Use	Indicates whether or not there are currently or upcoming meetings in iCM that use the specified meeting type. If so, the meeting type is considered in use and cannot be deleted from the system until the meeting type is no longer in use.
MCUs	Click Details to display a list of all MCUs defined in iVIEW Suite containing the specified meeting type.

VIEWING BUILT-IN MEETING TYPES



You cannot modify, upload or download built-in meeting types.

Procedure

- 1 Click **Meeting Types** in the sidebar menu.
- 2 Ensure that the Active Meeting Types tab is displayed.
The built-in meeting types listed in [Table 7-2](#) are available.

Table 7-2 *Built-in Meeting Types*

Parameter	Description
Non Video Conference	This is a conference that involves only users and meeting rooms. There is no need for video conference devices. Use this meeting type to reserve users and room resources only.
Point to Point	This is a conference that involves only two endpoints (terminals) and no MCU resources. It can only be created if one endpoint dials another endpoint directly.

REMOVING A MEETING TYPE

You must deactivate an active meeting type before you can permanently remove it from the system. Once a meeting type is inactive, you can no longer use it to schedule a meeting; however, you must wait until all current or future meetings that use this meeting type are finished, or you must cancel them. When there are no longer any scheduled meetings that require this meeting type, the meeting type is marked not in use and you can remove it.

This process is irreversible. You can never reactivate a meeting type that you have deactivated. When you clear a deactivated meeting type from the iCM, the meeting type is also removed from all MCUs in the system which have a service with the same prefix as the deactivated meeting type.



Procedure

- 1 Click **Meeting Types** in the sidebar menu.
- 2 Select the meeting type you want to delete.
- 3 Click **Deactivate** and then **OK**.

The meeting type is removed from the Active Meeting Types tab and placed on the Inactive Meeting Types tab.

SEARCHING FOR A MEETING TYPE



Procedure

- 1 Click **Meeting Types** in the sidebar menu.
- 2 Enter the partial or complete name of the meeting type in the Name field.

- 3 Click **Search**.

Search results are listed.

- 4 To return to the complete list of meeting types, clear the Name field, and then click **Search**.
-

DOWNLOADING A MEETING TYPE TO iCM



Procedure

- 1 Click **Meeting Types** in the sidebar menu.

- 2 Click **Download**.

MCU services are downloaded from all network MCUs.

Because MCU services are downloaded via SNMP, the process might take some time if there are many MCUs to connect to.

- 3 Enter a unique name for each meeting type.

- 4 Click **OK**.
-

RESOLVING MEETING TYPE CONFLICTS BETWEEN MCUS



Procedure

- 1 Click **Meeting Types** in the sidebar menu.

- 2 Click **Download**.

MCU services are downloaded from all network MCUs.

Because MCU services are downloaded via SNMP, the process may take some time if there are many MCUs to connect to.

- 3 Scroll down to the Meeting Type (Service) Conflicts section on the Download Meeting Types (Services) screen.

- 4 Select the entry that you want to keep in the **Use Meeting Type Definition From** column for each service prefix listed.

iCM downloads the specified copy of the MCU service and overwrites all other MCU services that use the same prefix on other network MCUs.

This process enables iCM to ensure that all services with the same service prefix are identical on different MCUs in the network.

This process does not assign a service to MCUs that do not already have the service prefix defined.

- 5 Enter a unique name for each meeting type.

- 6 Click **OK**.
-

RESOLVING MEETING TYPE CONFLICTS BETWEEN ICM AND AN MCU

If a service downloaded from a network MCU conflicts with a service that already exists in iCM, the service stored in iCM is selected by default during conflict resolution.

If a service exists only on a single MCU that is removed from the network, that service can no longer be used for meeting scheduling. Such meeting types are displayed in the Missing Meeting Types table. When a user selects a service that already exists in iCM from the User Meeting Type Definition From list, this meeting type is uploaded to the MCU that formerly used this server.

UPLOADING A MEETING TYPE TO NETWORK MCUS

We recommend that you configure all network MCUs with exactly the same service definitions so that you can treat all your MCUs as a pool of interchangeable resources.

iCM supports mixed deployments of version 4 and version 5 MCUs. However, you cannot use the same MCU service prefix for both version 4 and version 5 MCUs in a mixed deployment. If you try to perform such an operation, you receive a warning message.

If you have defined MCU services to support High Definition Continuous Presence (HP CD) conferences, then you cannot synchronize to an MCU that is not enabled for HD CP. If you try to perform such an operation, you receive a warning message.



Procedure

- 1 Click **Meeting Types** in the sidebar menu.
- 2 Select the meeting types you want to upload from iCM on the Active Meeting Types tab.

- 3 Click **Upload**.
- 4 Use the arrows to select the target MCUs.
Only MCUs that support this type of service are available.
- 5 Click **OK**.

Since MCU services are uploaded via SNMP, the process may take some time if there are many MCUs to connect to.

VIEWING MEETING TYPE DETAILS



Procedure

- 1 Click **Meeting Types** in the sidebar menu.
 - 2 Click the link in the Name column for the meeting type you require on the Active Meeting Types tab.
-

MODIFYING MEETING TYPE DETAILS



Procedure

- 1 Click **Meeting Types** in the sidebar menu.
- 2 Click the link in the Name column for the meeting type you require on the Active Meeting Types.
- 3 (Optional) Enter a new name for the meeting type.
- 4 (Optional) Specify a default connection rate value.
The default connection rate value must be less than the maximum bandwidth value.
Use the default connection rate for any non-predefined terminals that you invited without specifying a bandwidth for those terminals during meeting scheduling process or in-meeting control operations.
- 5 (Optional) If the meeting type supports lecture mode, select **Select Lecture Mode** to enable this support.

- 6 (Optional) Select **Use in Auto Attendance sessions** to specify this meeting type as the Auto Attendant meeting type.
 - 7 Click **OK** to save your changes.
-

ACCESSING AN MCU FROM THE MEETING TYPE DETAILS SCREEN



Procedure

- 1 Click **Meeting Types** in the sidebar menu.
- 2 Click the link in the Name column for the meeting type you require on the Active Meeting Types tab.

A link is available for each MCU containing the specified meeting type.

VIEWING A LIST OF MCUs CONTAINING A SPECIFIED MEETING TYPE



Procedure

- 1 Click **Meeting Types** in the sidebar menu.
 - 2 Click **Detail** in the MCU column to see a list of MCUs containing the specified meeting type.
-

CREATING OR MODIFYING A MEETING TYPE GROUP

This function is only available with iVIEW Suite with Multi-tenant support. For iVIEW Suite that supports multi-tenant feature, the service provider administrator can define a Meeting Type Group on the Meeting Type Group tab. Each meeting type group is assigned multiple meeting types. A meeting type group can then in turn be assigned to an organization. This allows only a specific subset of all meeting types. The meeting types defined in the meeting type group assigned to the organization are available to that organization.

**Procedure**

- 1 Click **Meeting Types** in the sidebar menu.
 - 2 Click **Meeting Type Groups**.
 - 3 Click the link in the Group Name column for the group you require, or click **Add** to create a new meeting type group.
 - 4 Enter a name and, optionally, a description of the group in the appropriate fields.
 - 5 Use the arrows to select the meeting types included in this group.
 - 6 Click **OK** to save your changes.
-

REMOVING A MEETING TYPE GROUP

**Procedure**

- 1 Click **Meeting Types** in the sidebar menu.
 - 2 Click **Meeting Type Groups**.
 - 3 Select the meeting type group entry you want to delete.
 - 4 Click **Delete**.
- The meeting type group profile is deleted from the scheduler.
-

CUSTOMIZING MCU DELIMITERS

By default, ** is the MCU delimiter for inviting an endpoint to a meeting, and *** is the MCU delimiter for the meeting password.

If MCU delimiters are customized via the MCU web user interface configuration, you need to configure MCU delimiters accordingly in iCM.

**Procedure**

- 1 Open the vcs-core.properties file located at \JBOSS_DIR\BIN.
- 2 Locate the following string:
vnex.vcms.core.mcuPasswordDelimiter=###
- 3 Modify the delimiter to match the value configured in the MCU web user interface.

- 4 Save and close the vcs-core.properties file.

Note \JBOSS_DIR is the default JBOSS home directory path. The default path is C:\Program Files\Radvision\iVIEW Suite\iCM\jboss.

DESIGNATING A SERVICE FOR IVR USE

You can define the MCU service for entry into the IVR audio and video message utility. When users dial the auto attendant session number they receive video with a list of all active conferences on all MCU in the farm. iCM then routes calls based on input from users to an existing conference, or users can create a new conference.

When you download MCU services for the first time, iCM automatically selects the first audio and video service that you download for IVR entry.

When you use iCM with several MCUs (collectively known as a “farm”), you must define which MCU is the host for the video IVR.



Procedure

- 1 Click **Meeting Types** in the sidebar menu.
- 2 Click **Active Meeting Types**.
- 3 Select the name of the service you want to use for entry to the IVR.
- 4 Select **Use in Auto Attendance sessions** to specify this meeting type as the Auto Attendant meeting type.
- 5 When using ECS, create a remote zone prefix with the auto attendant session number that points to the iCM zone.
- 6 Click **OK** to save your changes.

The designated service is marked with an icon in the Name column of the Active Meeting Types screen.

8

CONFIGURING A GATEWAY PROFILE IN ICM

CREATING OR MODIFYING A GATEWAY PROFILE

- [Taking a Gateway Offline](#) on page 56
- [Creating or Modifying a Gateway Profile](#) on page 53
- [Removing a Gateway Profile](#) on page 57
- [Searching for a Gateway Profile](#) on page 57

Configure gateways in your network to enable PSTN/ISDN/mobile terminals to join a meeting. iCM uses the gateway information to provide proper dialing information for meeting participants, and to dial out to terminals to invite them to meetings. iCM also manages gateway resources to allow successful call scheduling using network gateways.

When you add a gateway, settings in iCM must be consistent with the actual gateway configuration. We recommend the following:

- If you make changes to the gateway, maintain the IVR and DID numbers in iCM.
- To ensure that there are no gateway ports available for scheduled and ad hoc calls, maintain capacity information.



Procedure

- 1 Click **Resource Management** in the sidebar menu.
- 2 Click **Gateway**.

- 3 Click the link in the Name column for the gateway you require, or click **Add** to create a new gateway profile.
- 4 Enter the name of the gateway in the Name field.
- 5 Select a gateway model and enter an IP address in the relevant fields.

Note If multiple gateways are pooled together in a local network with the same access phone number, you can enter multiple IP addresses in the IP Address field to indicate the gateways in the gateway pool. IP addresses are separated by a colon (:).

- 6 Select the gatekeeper from the Registered To list to which the gateway is registered.
- 7 Select the device island from the Location list to which the gateway belongs.

The Location field is visible only when the IP Topology tab is activated in the iVIEW Suite Configuration Tool under System Configuration > UI Settings.

- 8 Enter the bandwidth for the gateway or gateway pool. For example, for an E1 line, the bandwidth should be 30 B-channels (3940 Kbps).
- 9 Indicate in the Working Mode field whether the gateway operates in IVR or DID mode.

iCM works with the gateway in DID mode so that meeting participants can easily dial into a meeting. You can assign a range of DID numbers to the gateway. These numbers can be assigned to individual dial-in terminals (endpoints). If you dial one of the assigned DID numbers, you are automatically added to the meeting that the DID number is associated with. Only one terminal can dial a DID number at any given time.

If you configure the gateway in DID mode and set a DID number in the Telephone Number field, when a terminal dials this DID number iCM routes the call to the appropriate meeting based on the terminal number. If no associated meeting is found, then the dial-in call is routed back to the gateway for an IVR session. After entering the meeting ID using the IVR, the terminal is permitted to join the meeting.

- 10** Enter a gateway phone number.
 - a** Enter a description of the phone number for the gateway in the Description field.
 - b** Enter the numeric prefix required to make an international long distance call in the International Access Code field.
 - c** Enter the numeric prefix required to make a long distance call within the same country in the Domestic Long Distance Prefix field.
 - d** Enter the country code for the gateway phone number in the Country Code field. iCM adds this prefix when dial-out is performed from this gateway to a terminal located in a different country than the country in which the gateway is located.
 - e** If Allow Out of Area Calls is not selected, only endpoints with the same area code as the gateway are allowed to reach iCM via the gateway.
 - f** If you select Allow Out of Area Calls, the gateway accepts incoming calls to iCM from terminals with a different area code than that of the gateway.
 - g** Enter the domestic area code of the gateway number in the Area Code field.
 - h** Specify a local telephone number in the Telephone Number field that you want to assign to the specific port.
 - i** Enter a number in the To access an outside line for local calls, dial field for a gateway with no direct access to an outside line for local calls.
 - j** Enter a number in the To access an outside line for long distance calls, dial field, for a gateway with no direct access to an outside line for long distance calls.
 - k** Assign the ISDN device island that the gateway or gateway pool belongs to. If ISDN Topology is hidden, then this field is also hidden.

- 11** Define the DID range.

If DID is selected in the Working Mode field, define the DID range for the gateway or gateway pool.

- 12 Click **Add Service** to add or modify the gateway service.

Note If you select Restricted Mode in the Bandwidth section, 56 appears in the Kbps list. Multiples of 56 Kbps are used instead of multiples of 64. iCM does not support gateway services whose bandwidth is set to “auto” since iCM needs the specific bandwidth to perform resource reservation. If there is a gateway service with “auto” bandwidth, when you configure this service in iCM, select a bandwidth value to best approximate the average bandwidth endpoints use when dialing that service.

- 13 Set the Advanced Settings.
 - Set the gateway port used for signaling in the Signaling Port field. By default, it is left blank and signaling port will be negotiated dynamically on the fly.
 - Set the SNMP community name required by iCM to communicate with the gateway in the SNMP Get/Set Community fields.
 - Select **Dial-in Only** to mark the gateway for use only with terminals that users dial into. iCM does not schedule dial-out calls on this gateway.
 - 14 Click **OK** to save your changes.
-

TAKING A GATEWAY OFFLINE



Once a gateway is configured, it is automatically brought online so that iCM can schedule resources.

Procedure

- 1 Click **Resource Management** in the sidebar menu.
- 2 Click **Gateway**.
- 3 Click the link in the Name column for the gateway you require.
- 4 To take the gateway offline temporarily, select **Take this gateway offline and reschedule all meetings on this gateway up to this date** and set the date to bring the gateway online again.
- 5 To take the gateway offline permanently, select **Take this gateway offline and reschedule all meetings currently on this gateway**.

- 6 Click **OK** to save your changes.

When you take the gateway offline, the following changes occur:

- iCM cannot schedule meetings for the offline gateway.
 - All meetings currently in progress are terminated. iCM attempts to reschedule upcoming meetings for the offline gateway on other gateways that use the same services and have sufficient, available resources. If no replacement gateways are available when the gateway status is changed back to online, upcoming meetings are lost and not restored.
 - If the gateway goes offline temporarily, iCM attempts to reschedule all meetings scheduled to this gateway from the time the gateway goes offline to the specified date for its return online.
 - If the gateway goes offline permanently, iCM attempts to reschedule all future meetings scheduled to this gateway.
-

REMOVING A GATEWAY PROFILE



You must take a gateway offline before you can remove it from the iVIEW Suite database.

Procedure

- 1 Click **Resource Management** in the sidebar menu.
- 2 Click **Gateway**.
- 3 Click the gateway entry you want to delete in the Name column.
- 4 Click **Delete** and then **OK**.

The gateway profile is deleted from the scheduler and information about the gateway is removed from the database.

SEARCHING FOR A GATEWAY PROFILE



Procedure

- 1 Click **Resource Management** in the sidebar menu.
- 2 Click **Gateway**.
- 3 Enter the partial or complete name of the gateway in the Name field.

Searching for a Gateway Profile

4 Click **Search**.

Search results are listed.

The Status column indicates whether the gateway is online or not. iCM only uses an online gateway for meeting scheduling and creation.

The SNMP Connection column indicates whether or not iCM established an SNMP connection with the gateway.

5 To return to the complete list of gateways, clear the Name field, and then click **Search**.

9

CONFIGURING A SCOPIA DESKTOP PROFILE IN ICM

- [Creating or Modifying a SCOPIA Desktop Profile](#) on page 59
- [Removing a SCOPIA Desktop Profile](#) on page 60
- [Searching for a SCOPIA Desktop Profile](#) on page 61
- [How to Stream Meetings Using SCOPIA Desktop](#) on page 61

CREATING OR MODIFYING A SCOPIA DESKTOP PROFILE

Once a SCOPIA Desktop is configured, it is automatically brought online so that iCM can schedule resources.



Procedure

- 1 Click **Resource Management** in the sidebar menu.
- 2 Click **SCOPIA Desktop**.
- 3 Click the link in the Name column for the SCOPIA Desktop you require, or click **Add** to create a new SCOPIA Desktop profile.
- 4 Enter the name and IP address of the SCOPIA Desktop in the relevant fields.

When SCOPIA Desktop is installed with iCM, the name “Local Desktop Server” displays by default.

- 5 Enter the URL used by participants to join a meeting via SCOPIA Desktop in the **Web Access URL** field.
The URL must be in the format <http://<IP address>:<port number>/scopia>.
 - 6 Enter an H.323 ID used to identify connections from SCOPIA Desktop in MCU conferences in the H.323 ID field.
Ensure that the same H.323 ID is configured in the SCOPIA Desktop administrator web interface.
Configuring this field allows iCM to route calls from this SCOPIA Desktop Server based on the predefined IP topology.
 - 7 Select a topology setting from the Location drop-down list. The default value is Home.
The Location field is visible only when the IP Topology tab is activated in the iVIEW Suite Configuration Tool under System Configuration > UI Settings.
 - 8 Enter any text you want to associate with the web access URL in the Description Text field.
The description text is embedded in email invitations sent to meeting participants.
 - 9 Enter the maximum capacity allowed by your SCOPIA Desktop license in the Maximum Capacity field.
 - 10 (Optional) Select **Secure XML interface (SSL)** to use the Secure Sockets Layer (SSL) protocol to secure the transport link between iVIEW Suite and SCOPIA Desktop.
 - 11 Click **OK** to save your changes.
-

REMOVING A SCOPIA DESKTOP PROFILE



Procedure

- 1 Click **Resource Management** in the sidebar menu.
- 2 Click **SCOPIA Desktop**.
- 3 Click the SCOPIA Desktop entry you want to delete in the Name column.

- 4 Click **Delete** and then **OK**.

The SCOPIA Desktop profile is deleted from the scheduler and information about the SCOPIA Desktop is removed from the database.

SEARCHING FOR A SCOPIA DESKTOP PROFILE



Procedure

- 1 Click **Resource Management** in the sidebar menu.
 - 2 Click **SCOPIA Desktop**.
 - 3 Enter the partial or complete name of the SCOPIA Desktop in the **Name** field.
 - 4 Click **Search**.
Search results are listed.
 - 5 To return to the complete list of SCOPIA Desktops, clear the Name field, and then click **Search**.
-

HOW TO STREAM MEETINGS USING SCOPIA DESKTOP

- [Enabling Streaming on SCOPIA Desktop](#) on page 61
- [Enabling Streaming for a Virtual Room](#) on page 62
- [Allowing Recording by Specified Roles](#) on page 62
- [Allowing Recording by Specified Users](#) on page 62
- [Enabling Recording for Specified Virtual Rooms](#) on page 63

ENABLING STREAMING ON SCOPIA DESKTOP



Procedure

- 1 Click **Advanced Settings** in the sidebar menu.
- 2 Click **Look and Feel**.

- 3 Set Streaming to **Visible**.
 - 4 Click **OK** to save your changes.
-

ENABLING STREAMING FOR A VIRTUAL ROOM



Procedure

- 1 Click **User Management** in the sidebar menu.
 - 2 Click the link in the Name column for the user you require, or select **Add** to create a new user profile.
 - 3 Click **Virtual Room Setting**.
 - 4 Set Streaming to **Enabled**.
 - 5 Click **OK** to save your changes.
-

ALLOWING RECORDING BY SPECIFIED ROLES



Procedure

- 1 Click **Advanced Settings** in the sidebar menu.
 - 2 Click **Default User Settings**.
 - 3 Select the user types that you want to allow to record meetings from the list in the Default Recording Permissions section.
 - 4 Click **OK** to save your changes.
-

ALLOWING RECORDING BY SPECIFIED USERS



Procedure

- 1 Click **User Management** in the sidebar menu.
- 2 Click **Users**.

- 3 Click the link in the Name column for the user you require.
 - 4 Click **Advanced**.
 - 5 (Optional) Select **Allow user to record meetings** to enable this user to record meeting regardless of the global policy.
 - 6 Click **OK** to save your changes.
-

ENABLING RECORDING FOR SPECIFIED VIRTUAL ROOMS



Procedure

- 1 Click **User Management** in the sidebar menu.
- 2 Click **Users**.
- 3 Click the link in the Name column for the user you require.
- 4 Click **Virtual Room Setting**.
- 5 Select **Record the meeting when meeting starts**.

This option is available if

- Recording is allowed for the current user according to the recording policy.
- The Record Meeting field is set to Enabled under Admin > Advanced Settings > Look and Feel.

The meeting will not be recorded if there are not enough available recording ports on the SCOPIA Desktop when the meeting is scheduled.

- 6 Click **OK** to save your changes.
-

How to Stream Meetings Using SCOPIA Desktop

10

CONFIGURING A MEETING ROOM PROFILE IN ICM

A meeting room is the physical location of one or more terminals. Meeting rooms are also used for non-video conference meetings in which no terminals are involved.

- [Enabling Meeting Room Support](#) on page 65
- [Creating or Modifying a Meeting Room Profile](#) on page 66
- [Sending Meeting Details by Email](#) on page 66
- [Removing a Meeting Room Profile](#) on page 67
- [Searching for a Meeting Room Profile](#) on page 67

ENABLING MEETING ROOM SUPPORT

By default, the Meeting Rooms tab is hidden in iCM. Enable support for meeting rooms as follows:



Procedure

- 1 Click **Advanced Settings** in the sidebar menu.
 - 2 Click **Look and Feel**.
 - 3 Deselect **Hide Meeting Rooms**.
 - 4 Click **OK** to save your changes.
-

CREATING OR MODIFYING A MEETING ROOM PROFILE



Procedure

- 1 Click **Resource Management** in the sidebar menu.
 - 2 Click **Meeting Rooms**.
 - 3 Click the link in the Name column for the meeting room you require, or click **Add** to create a new meeting room profile.
 - 4 Enter the name and location of the meeting room in the relevant fields.
 - 5 Click **OK** to save your changes.
-

SENDING MEETING DETAILS BY EMAIL

You can define an email address to enable a terminal that participates in a meeting to receive notification email messages.

By default, this option is hidden.



Procedure

- 1 Click **Advanced Settings** in the sidebar menu.
 - 2 Click **Look and Feel**.
 - 3 Deselect **Hide Meeting Notification E-mail for meeting rooms and terminals**.
 - 4 Click **OK** to save your changes.
 - 5 Click **Resource Management** in the sidebar menu.
 - 6 Click **Meeting Rooms**.
 - 7 Click the link in the Name column for the meeting room you require.
 - 8 Select **Meeting e-mail notification address** and enter the email address for the meeting room.
 - 9 Select a time zone for the meeting room.
The default value is set at Advanced Settings > Default User Settings > Default Time Zone.
 - 10 Click **OK** to save your changes.
-

REMOVING A MEETING ROOM PROFILE



Procedure

- 1 Click **Resource Management** in the sidebar menu.
- 2 Click **Meeting Rooms**.
- 3 Select the meeting room entry you want to delete in the Name column.
- 4 Click **Delete** and then **OK**.

The meeting room profile is deleted from the scheduler and information about the meeting room is removed from the database.

SEARCHING FOR A MEETING ROOM PROFILE



Procedure

- 1 Click **Resource Management** in the sidebar menu.
 - 2 Click **Meeting Rooms**.
 - 3 Enter the partial or complete name of the meeting room in the Name field.
 - 4 Click **Search**.
Search results are listed.
 - 5 To return to the complete list of meeting rooms, clear the Name field, and then click **Search**.
-

Searching for a Meeting Room Profile

11

CONFIGURING A TERMINAL PROFILE IN ICM

HOW TO CREATE OR MODIFY A TERMINAL PROFILE

- [How to Create or Modify a Terminal Profile](#) on page 69
- [Removing a Terminal Profile](#) on page 75
- [Searching for a Terminal Profile](#) on page 75

The term “terminal” refers to any kind of endpoint (H.323, SIP, ISDN, or mobile) used for video conferencing.

- [Defining H.323 IP Terminal Details](#) on page 70
- [Defining SIP IP Terminal Details](#) on page 71
- [Defining ISDN/PSTN H.320 Terminal Details](#) on page 72
- [Defining Mobile Terminal Details](#) on page 73
- [Defining Dual H.320 and H.323 Terminal Details](#) on page 74

Note To avoid conflicts between endpoint-initiated point-to-point meetings and endpoint-initiated multipoint meetings, the names of endpoints and terminals registered to gatekeepers in iCM cannot start with the same prefix as the MCU service or as a meeting type ID in iCM.

DEFINING H.323 IP TERMINAL DETAILS



Define all H.323 terminals registered to gatekeepers that are configured in iCM.

Procedure

- 1 Click **Resource Management** in the sidebar menu.
- 2 Click **Terminals**.
- 3 Click the link in the Name column for the terminal you require, or click **Add** to create a new terminal profile.
- 4 (Optional) Click **Default Users** to associate this terminal as the default terminal for selected users defined in iCM.
- 5 Click **OK** to apply your selections and to close the Select Users window.
- 6 (Optional) Enter any description text that you may have for this terminal in the Description field.
- 7 Select **IP(H.323)** from the Terminal Type list.
- 8 Enter the E.164 IP phone number of the terminal registered on the gatekeeper in the IP Phone Number field as specified in the Registered to field.

If the terminal is not registered to a gatekeeper, enter the IP address of the terminal in the IP Phone Number field.

- 9 Select a topology setting from the Location drop-down list.
The Location field is visible only when the IP Topology tab is activated in the iVIEW Suite Configuration Tool under System Configuration > UI Settings.
 - 10 Define the default bandwidth for the terminal in the Bandwidth field. iCM uses the bandwidth number to reserve resources for this terminal.
 - 11 (Optional) Select an entry from the Meeting Room field to associate this terminal with a meeting room defined in iVIEW Suite.
 - 12 (Optional) Select **Display in global address book** (Enterprise edition only).
 - 13 Click **OK** to save your changes.
-

DEFINING SIP IP TERMINAL DETAILS



Define all SIP terminals registered to gatekeepers that are configured in iCM.

Procedure

- 1 Click **Resource Management** in the sidebar menu.
 - 2 Click **Terminals**.
 - 3 Click the link in the Name column for the terminal you require, or click **Add** to create a new terminal profile.
 - 4 (Optional) Click **Default Users** to associate this terminal as the default terminal for selected users defined in iCM.
 - 5 Click **OK** to apply your selections and to close the Select Users window.
 - 6 (Optional) Enter any description text that you may have for this terminal in the **Description** field.
 - 7 Select **IP(SIP)** from the Terminal Type list.
 - 8 Define the terminal name or terminal number in the SIP URI field, followed by the SIP server domain name and a suffix derived from the domain name of the SIP server.
For example, <terminal name>@<SIP server domain name> or “user@domain_name.com”.
 - 9 Define the default bandwidth for the terminal in the Bandwidth field. iCM uses the bandwidth number to reserve resources for this terminal.
 - 10 Select a topology setting from the Location drop-down list.
The Location field is visible only when the IP Topology tab is activated in the iVIEW Suite Configuration Tool under System Configuration > UI Settings.
 - 11 Click **OK** to save your changes.
-

DEFINING ISDN/ PSTN H.320 TERMINAL DETAILS

Define all H.320 terminals that you want iCM to automatically invite to a meeting and manage their availability.



Procedure

- 1 Click **Resource Management** in the sidebar menu.
 - 2 Click **Terminals**.
 - 3 Click the link in the Name column for the terminal you require, or click **Add** to create a new terminal profile.
 - 4 (Optional) Click **Default Users** to associate this terminal as the default terminal for selected users defined in iCM.
 - 5 Click **OK** to apply your selections and to close the Select Users window.
 - 6 (Optional) Enter any description text that you may have for this terminal in the Description field.
 - 7 Select **ISDN/PSDN(H.320)** from the Terminal Type list.
 - 8 Define the default bandwidth for the terminal in the Bandwidth field. iCM uses the bandwidth number to reserve resources for this terminal.
 - 9 Select a topology setting from the Location drop-down list.
The Location field is visible only when the IP Topology tab is activated in the iVIEW Suite Configuration Tool under System Configuration > UI Settings.
 - 10 Select **Restricted Mode** for a PSTN/ISDN network working in restricted mode.
 - 11 Enter the phone number of the terminal in the Country Code, Area Code and Number fields.
If you do not specify this information, iCM cannot find the optimal gateway for the terminal when scheduling a conference.
 - 12 (Optional) Select **Display in global address book** (Enterprise edition only).
 - 13 Click **OK** to save your changes.
-

DEFINING MOBILE TERMINAL DETAILS

Define all mobile terminals that you want iCM to automatically invite to a meeting and manage their availability.



Procedure

- 1 Click **Resource Management** in the sidebar menu.
 - 2 Click **Terminals**.
 - 3 Click the link in the Name column for the terminal you require, or click **Add** to create a new terminal profile.
 - 4 (Optional) Click **Default Users** to associate this terminal as the default terminal for selected users defined in iCM.
 - 5 Click **OK** to apply your selections and to close the Select Users window.
 - 6 (Optional) Enter any description text that you may have for this terminal in the Description field.
 - 7 Select **Mobile** from the Terminal Type list.
 - 8 Define the default bandwidth for the terminal in the Bandwidth field. iCM uses the bandwidth number to reserve resources for this terminal.
 - 9 Select a topology setting from the Location drop-down list.
The Location field is visible only when the IP Topology tab is activated in the iVIEW Suite Configuration Tool under System Configuration > UI Settings.
 - 10 Enter the phone number of the terminal in the Country Code, Area Code and Number fields.
If you do not specify this information, iCM cannot find the optimal gateway for the terminal when scheduling a conference.
 - 11 Select **3G** for 3G terminals.
 - 12 (Optional) Select **Display in global address book** (Enterprise edition only).
 - 13 Click **OK** to save your changes.
-

DEFINING DUAL H.320 AND H.323 TERMINAL DETAILS



Procedure

- 1 Click **Resource Management** in the sidebar menu.
- 2 Click **Terminals**.
- 3 Click the link in the Name column for the terminal you require, or click **Add** to create a new terminal profile.
- 4 (Optional) Click **Default Users** to associate this terminal as the default terminal for selected users defined in iCM.
- 5 Click **OK** to apply your selections and to close the Select Users window.
- 6 (Optional) Enter any description text that you may have for this terminal in the Description field.
- 7 Select **Dual(H.320 and H.323)** from the Terminal Type list.
- 8 Enter the E.164 IP phone number of the terminal registered on the gatekeeper in the IP Phone Number field as specified in the Registered to field.

If the terminal is not registered to a gatekeeper, enter the IP address of the terminal in the IP Phone Number field.

- 9 Define the default bandwidth for the terminal in the IP Bandwidth and ISDN Bandwidth fields. iCM uses the bandwidth number to reserve resources for this terminal.
- 10 Select a topology setting from the Location drop-down list.
The Location field is visible only when the IP Topology tab is activated in the iVIEW Suite Configuration Tool under System Configuration > UI Settings.
- 11 Select **Restricted Mode** for a PSTN/ISDN network working in restricted mode.
- 12 Enter the phone number of the ISDN terminal in the Country Code, Area Code and Number fields.
If you do not specify this information, iCM cannot find the optimal gateway for the terminal when scheduling a conference.

- 13 (Optional) Select **Display in global address book** (Enterprise edition only).
 - 14 Click **OK** to save your changes.
-

REMOVING A TERMINAL PROFILE



Procedure

- 1 Click **Resource Management** in the sidebar menu.
- 2 Click **Terminals**.
- 3 Click the terminal entry you want to delete in the Name column.
- 4 Click **Delete** and then **OK**.

The terminal profile is deleted from the scheduler and information about the terminal is removed from the database.

SEARCHING FOR A TERMINAL PROFILE



Procedure

- 1 Click **Resource Management** in the sidebar menu.
- 2 Click **Terminals**.
- 3 Enter the partial or complete name of the terminal in the Name field, or enter the partial or complete IP or ISDN phone number of the meeting room in the Dialing Info field.

The ISDN phone number of the terminal should not include dashes or spaces.

The ISDN phone number can only be used when you select ISDN/PSTN(H.320) or Dual(H.320 and H.323) in the Terminal Type field.

Both IP and ISDN numbers are displayed if the terminal is configured as a dual terminal.

Searching for a Terminal Profile

- 4 (Optional) Click **Display All** to include in the terminals displayed in the list all the terminals that are currently in the global address book.
Terminals in the global address book are indicated by a book icon after the terminal name.
 - 5 (Optional) Click **Conceal All** to remove from the terminals displayed in the list all the terminals that are currently in the global address book.
Terminals in the global address book are indicated by a book icon after the terminal name.
 - 6 Click **Search**.
Search results are listed.
 - 7 To return to the complete list of meeting rooms, clear the Name and Dialing Info fields, and then click **Search**.
-

12

DEFINING ICM CALL ROUTING MODES

iCM offers two call routing modes. This section describes these modes and explains their use in H.323 and SIP deployments.

- [Call Routing in H.323 Deployments](#) on page 77
- [Call Routing in SIP Deployments](#) on page 78
- [Masking Conference Topology with the Virtual MCU Feature](#) on page 78

CALL ROUTING IN H.323 DEPLOYMENTS

In Fully Routed H.323 Mode, iCM acts as an authorization server to the ECS. In this case, the Allow Authorization servers to connect and Enabled XML call control fields in the ECS Web interface at Settings > External API are both unchecked. iCM manages all traffic passing through the ECS and can control where incoming calls will go.

Fully Routed Mode enables the “Virtual MCU” feature where iCM can present multiple MCUs as a single pool of video and audio ports, or as a single virtual MCU.

For Fully Routed Mode, ensure you select the Enable Gatekeeper advanced features (authorization and point-to-point) option.



Procedure

- 1 Click **Resource Management** in the sidebar menu.
- 2 Click **Gatekeeper/SIP server**.
- 3 Click the link in the Name column for the gatekeeper you require, or click **Add** to create a new gatekeeper profile.

- 4 Locate the Advanced section.
The Advanced section appears if you are using the internal gatekeeper or ECS.
 - 5 Select **Enable Gatekeeper advanced features (authorization and point-to-point)**.
 - 6 Click **OK** to save your changes.
-

CALL ROUTING IN SIP DEPLOYMENTS

In SIP deployments, iCM works in Fully Routed Mode using the embedded SIP server to manage all traffic.

Because MCUs have iCM configured as the outbound proxy, and the external SIP server is configured to route incoming calls to the iCM embedded SIP server, iCM can control all calls going through the MCU.

Note iCM cannot manage SIP endpoint point-to-point traffic because these endpoints are registered to the external SIP server.

MASKING CONFERENCE TOPOLOGY WITH THE VIRTUAL MCU FEATURE

By controlling the call routing logic of the ECS, iCM can mask the complexity of the actual network deployment from end users. iCM can create a conference that spans multiple MCUs and present the conference to the end user as a single conference with a single dialing ID, a single PIN, and a single In-meeting Control interface to manage it. This is the iCM Virtual MCU feature.

- [Creating a Centralized Conference](#) on page 79
- [Creating a Distributed Conference](#) on page 79

CREATING A CENTRALIZED CONFERENCE

This section describes how to use the Virtual MCU feature to establish a centralized conference.



Procedure

- 1 Under **Admin > Advanced Settings > Default Meeting Settings**, set the Prioritize field to **Delay** to host a conference on a single MCU when possible.
iCM cascades multiple MCUs to create a conference only if the conference size is larger than the capacity of a single MCU.
 - 2 Click **OK** to save your changes.
-

CREATING A DISTRIBUTED CONFERENCE

This section describes how to use the Virtual MCU feature to establish a distributed conference.



Procedure

- 1 Under **Admin > Advanced Settings > Default Meeting Settings**, set the Prioritize field to **Local MCU** to force endpoints to cascade to their local MCU first, according to the IP topology configured in the Network Management section.
If there are endpoints from multiple locations, at least one MCU from each location is cascaded into the main MCU conference.
 - 2 Click **OK** to save your changes.
-

Masking Conference Topology with the Virtual MCU Feature

13

VIEWING NETWORK DEVICE PERFORMANCE AND AVAILABILITY

- [Viewing Device Usage and Failure by Time Interval](#) on page 81
- [Viewing Device Usage and Failure by Time Interval and Period](#) on page 82
- [Viewing MCU Port Availability](#) on page 83
- [Generating a Report](#) on page 84

VIEWING DEVICE USAGE AND FAILURE BY TIME INTERVAL

You can view historical usage and failure information for all MCUs and gatekeepers configured in iCM during a designated time period (the default time interval is 1 hour).



Procedure

- 1 Click **Device Monitoring** in the sidebar menu.
- 2 Click **Performance Monitor**.

[Table 13-1](#) describes the information displayed on the Performance Monitor tab.

Table 13-1 Performance Monitor Tab Parameters

Parameter	Description
Device Name	Displays the alias name of the MCU or gatekeeper.
Model	Displays the device model.
Total Meetings	Displays the total number of meetings hosted on the MCU during the designated time interval. These totals only include ad hoc and scheduled meetings created via iCM.
Failed Meetings	Displays the total number of meetings that were unable to start on the MCU during the designated time interval. These totals only include ad hoc and scheduled meetings created via iCM.
% Failed Meetings	Displays the number of failed meetings divided by the total number of meetings.
Total Connections	Displays the total number endpoints involved in meetings hosted on the MCU during the designated time interval. These totals only include ad hoc and scheduled meetings created via iCM.
Failed Connections	Displays the total number of endpoints involved in meetings on the MCU that were unable to start during the designated time interval. These totals only include ad hoc and scheduled meetings created via the iCM.
% Failed Connections	Displays the number of failed connections divided by the total number of connections.

VIEWING DEVICE USAGE AND FAILURE BY TIME INTERVAL AND PERIOD

You can view historical usage and failure information by time interval for all MCUs and gatekeepers configured in iCM during a designated time period. For example, usage per hour over a 15-day period.



Procedure

- 1 Click **Device Monitoring** in the sidebar menu.
- 2 Click **Statistics**.

[Table 13-2](#) describes the information displayed on the Statistics tab.

Table 13-2 *Statistics Tab Parameters*

Parameter	Description
Device Name	Displays the name of the MCU or gatekeeper.
Model	Displays the device model.
Start Time	Displays the beginning of the time interval.
End Time	Displays the end of the time interval.
Meetings	Displays the total number of multipoint meetings hosted on the MCU during the designated time interval. Totals include only ad hoc and scheduled meetings created via iCM. Gatekeeper information is not displayed.
Peak Connections	Displays the peak number of endpoint connections for MCU or gatekeeper during the designated time interval. Figures include only ad hoc and scheduled meetings created via iCM. Gatekeeper information is not displayed.
Failed Meetings	Displays the total number of meetings unable to start on the MCU during the designated time interval. Totals include only ad hoc and scheduled meetings created via iCM. Gatekeeper information is not displayed.
Failed Connections	Displays the number of endpoints involved in meetings that were unable to connect with the MCU during the designated time interval. Totals include only ad hoc and scheduled meetings created via iCM. Gatekeeper information is not displayed.

VIEWING MCU PORT AVAILABILITY



You can view MCU resource availability information during a designated time period.

Procedure

- 1 Click **Device Monitoring** in the sidebar menu.
- 2 Click **Resource Availability**.
- 3 Select a meeting type and a starting date.
- 4 Click **Previous** or **Next** to move between start times.

- 5 Select the time interval at which you want to view resource availability information.

Information about reserved MCU ports for a designated time interval is displayed in the Reserved MCU Ports section.

GENERATING A REPORT

You can generate a report in .xls format, showing statistics about device usage between selected dates. Once you have saved the report, you can view it using Microsoft Excel.



Procedure

- 1 Click **Device Monitoring** in the sidebar menu.
 - 2 Click **Resource Availability** or **Statistics**.
 - 3 Click the calendar icons by the From and To fields to select a start and end period within which to generate the report.
 - 4 Click **Generate Report**.
Information about each device is included in the report.
 - 5 Click **Save** to save the report.
 - 6 Browse to the location in which you want to save the file, enter the file name and type, and then click **Save**.
-

14

VIEWING REAL-TIME MEETING STATISTICS IN ICM

- [Viewing the Number of Ongoing Meetings and Calls](#) on page 85
- [Viewing Port Utilization Information](#) on page 86
- [Viewing Organization Meetings and Calls](#) on page 86
- [Viewing the Creation Status of Meetings](#) on page 87
- [Searching for a Meeting](#) on page 88
- [Searching for a Meeting](#) on page 88
- [Generating Reports](#) on page 89
- [Modifying Upcoming Meetings](#) on page 91
- [Viewing Host MCUs](#) on page 92
- [Terminating Meetings](#) on page 92

VIEWING THE NUMBER OF ONGOING MEETINGS AND CALLS

You can see the total number of meetings, multipoint calls and point-to-point calls currently in progress, and the following additional statistics:

- Meetings—scheduled, ad hoc and recorded
- Multipoint calls—audio, video and total bandwidth
- Point-to-point calls—audio, video and total bandwidth



Procedure

- 1 Click **Meeting Monitoring** in the sidebar menu.
- 2 Click **Overall Status**.

Viewing Port Utilization Information

- 3 (Optional) Click **Number of Meetings** in the Ongoing Meetings Status section to jump to the Ongoing Meetings tab where you can see further details of all meetings that are currently in progress.
 - 4 (Optional) Click **Number of Calls** in the Ongoing Point-to-Point Calls Status section to jump to the Ongoing Point-to-Point Calls tab where you can see further details of all point-to-point calls that are currently in progress.
-

VIEWING PORT UTILIZATION INFORMATION

You can see port utilization information for MCUs, Gateways and SCOPIA Desktops configured in the system.



Procedure

- 1 Click **Meeting Monitoring** in the sidebar menu.
 - 2 Click **Overall Status**.
 - 3 Locate the System Utilization Status section.
-

VIEWING ORGANIZATION MEETINGS AND CALLS



Procedure

- 1 Click **Meeting Monitoring** in the sidebar menu.
 - 2 Click **Ongoing Meetings** to see all meetings that are currently in progress.
 - 3 Click **Ongoing Point-to-Point Calls** to see all point-to-point calls that are currently in progress.
 - 4 Click **Upcoming** to see all meetings that have not yet started.
-

VIEWING THE CREATION STATUS OF MEETINGS



Procedure

- 1 Click **Meeting Monitoring** in the sidebar menu.
- 2 Click **Ongoing Meetings** to see all meetings that are currently in progress.
- 3 Click **Ongoing Point-to-Point Calls** to see all point-to-point calls that are currently in progress.
- 4 Click **Upcoming** to see all meetings that have not yet started.

The creation status of each of the displayed meetings is shown in the Status column.

- Green—Successful status
- Orange—Alert status
- Red—Failure status

There are three status indicators in each row.

- First (left) status icon—Indicates meeting creation status.
If meeting creation fails due to device failure, iCM attempts to recreate the meeting whenever it receives a dial-in call from a meeting participant. This allows the system multiple attempts at creating the meeting after the initial failure.
- Second (middle) status icon—Indicates participant/terminal status.
If the second status indicator is red, a participant/terminal is not connected.
If the second status indicator is orange, a participant/terminal is disconnecting from the meeting.
- Third (right) status icon—Indicates meeting termination status.

- 5 To view the Reason Failed error message, click the red status indicator, and then click **Retry** to resend the meeting information to the MCU.

Note If a terminal is disconnected correctly via the In-meeting Control interface, there is no red status indicator.

SEARCHING FOR A MEETING



Procedure

- 1 Click **Meeting Monitoring** in the sidebar menu.
 - 2 Click **Ongoing Meetings, Ongoing Point-to-Point Calls or Upcoming**, as required.
 - 3 Perform any of the following:
 - Enter the partial or complete subject of the meeting in the Subject field.
If any part of the meeting subject matches the search string, the meeting record is displayed in the search results.
 - Enter the E.164 number of an attending terminal in the E164 field.
If any part of the meeting subject matches the search string, the meeting record is displayed in the search results.
 - Click the calendar icon in the From field, and select a date and time in the window that opens.
Meetings scheduled after the selected time are listed.
 - Click the calendar icon in the To field, and select a date and time in the window that opens.
Meetings scheduled before the selected time are listed.
 - Enter the partial or complete meeting ID in the Meeting ID field.
If any part of the meeting ID matches the search string, the meeting record is displayed in the search results.
 - 4 Click **Search**.
Search results are listed.
 - 5 To return to the complete list of meetings, clear each of the fields.
 - 6 Click **Search**.
-

MONITORING A MEETING OR CALL



Procedure

- 1 Click **Meeting Monitoring** in the sidebar menu.
- 2 Click **Ongoing Meetings** or **Ongoing Point-to-Point Calls**.
- 3 Click the link in the Subject field for the meeting or call you want to monitor.
- 4 Enter the moderator PIN if one is used for this meeting or call.
- 5 Click the Take Control icon.

The In-meeting Control interface is not available for meetings or calls in which you are not a participant or the organizer.

GENERATING REPORTS



Procedure

- 1 Click **Meeting Monitoring** in the sidebar menu.
- 2 Click **Upcoming**.
- 3 Click the calendar icon in the From and To fields to choose a start and end date for information in the generated report.
- 4 Click **Generate Report**.

[Table 14-1](#) describes the information categories that are included in a generated report.

Table 14-1 *Generated Report Information Categories*

Category	Description
Virtual Meeting ID	Dialable meeting ID used by users to access a specific meeting.
Master Meeting ID	Corresponds to a physical meeting ID on the master MCU.
Slave Meeting ID	Corresponds to a physical meeting ID on the slave MCU.
iVIEW Suite Meeting ID	Internal database ID for the meeting.
Subject	Corresponds to Subject field in Meeting Scheduling.
Meeting Type	Corresponds to the Meeting Type field in Meeting Scheduling. The name of the meeting type is displayed.
Reference Code	Corresponds to the Reference Code field in Meeting Scheduling.
Start Time	Corresponds to the Start Time field in Meeting Scheduling.
Duration	Corresponds to the Duration field in the Meeting Scheduling.
Meeting Room	Meeting room used for scheduling a meeting.
Organizer Name	Corresponds to the Organizer field in Meeting Scheduling.
Service Prefix	MCU service prefix used for the meeting.
Services	MCU service used for the meeting.
MCU Name(s)	MCU(s) used for the meeting. For cascaded meetings, “(master)” appears after the MCU name.
Terminals	Number of terminals used for the meeting.
Number of Extra IP Ports Reserved	Corresponds to the Reserve additional ports field in Meeting Scheduling.
Dial-in IP Terminals	Number of dial-in IP terminals.
Dial-out IP Terminals	Number of dial-out IP terminals.

Category	Description
Dial-in ISDN Terminals	Number of dial-in PSTN/ISDN terminals.
Dial-out ISDN Terminals	Number of dial-out PSTN/ISDN terminals.
Gateway List	Gateways used for the meeting.
Device Failure Cause (Device Name, IP Failure, Cause)	Any failure on a network device such as an MCU or gateway.
Attendee Failure Cause (Name, Number, ISDN, Dial-in, Total Time, Failing Attempts, Last Failure Cause)	Any failures on attending terminals.

- 5 Click **Save** to save the report to a location of your choice.

MODIFYING UPCOMING MEETINGS

You can reschedule the meeting to another time, change the meeting parameters, or delete the meeting request.



Procedure

- 1 Click **Meeting Monitoring** in the sidebar menu.
- 2 Click **Upcoming**.
- 3 Click the subject of the meeting you want to modify in the In-meeting Control interface.
The In-meeting Control interface is not available for meetings in which you are not a participant or the organizer.
- 4 Enter the required information.

VIEWING HOST MCUs



Procedure

- 1 Click **Meeting Monitoring** in the sidebar menu.
- 2 Click **Ongoing Meetings**, **Ongoing Point-to-Point Calls** or **Upcoming**, as required.

All host MCUs are listed in the MCU column with an indication of whether the meeting is cascaded.

TERMINATING MEETINGS



Procedure

- 1 Click **Meeting Monitoring** in the sidebar menu.
 - 2 Click **Ongoing Meetings** or **Ongoing Point-to-Point Calls**.
 - 3 Click the icon in the Terminate column for the meeting you want to terminate.
-

15

CREATING STATISTICAL REPORTS OF MEETINGS AND CALLS IN ICM

- [Creating a Call Information Report](#) on page 93
- [Creating a Port Usage Report](#) on page 94
- [Creating a Resource Usage Report](#) on page 95
- [Viewing the Use of Ad Hoc and Scheduled Meetings](#) on page 96
- [Viewing Average Meeting Size](#) on page 96
- [Viewing Average Meeting Duration](#) on page 96
- [Generating Reports for Finished Meetings](#) on page 97
- [Viewing Finished Meetings](#) on page 99
- [Viewing the Termination Status of Meetings](#) on page 99
- [Searching for a Finished Meeting](#) on page 99
- [Viewing Host MCUs](#) on page 100
- [Removing Meetings from the History Tab](#) on page 101

CREATING A CALL INFORMATION REPORT

Organization Administrators can create a report for calls based on any one of these criteria:

- Multipoint calls
- Point-to-point calls
- Gateway calls
- Calls per terminal
- Calls per virtual room

Creating a Port Usage Report

Service Provider Administrators can create a report for calls based on any one of these criteria:

- Multipoint calls
- Point-to-point calls
- Gateway calls



Procedure

- 1 Click **Reports and Statistics** in the sidebar menu.
 - 2 Click **Create New Report**.
 - 3 Select an option from the Report Type field.
 - 4 Select the time period to be covered by the report in the Graph X-Axis field.
 - 5 Select a start and end time for the report in the relevant fields.
 - 6 Select **Total Number** or **Total Duration (Minutes)** in the Graph Y-Axis field.
 - 7 Select a week range and hour range where relevant.
 - 8 (Optional) Click **Recent Report** to see the last call report generated.
 - 9 Click **Generate**.
The report appears on the in the Usage tab.
 - 10 (Optional) Click **Generate PDF Report** to print your report to a PDF file.
 - 11 (Optional) Click **Generate Excel Report** to print your report to an Excel file.
-

CREATING A PORT USAGE REPORT

You can create a report of the ports used by these network elements:

- MCU
- Gateway
- SCOPIA Desktop
- All of these network elements



Procedure

- 1 Click **Reports and Statistics** in the sidebar menu.
- 2 Click **Utilization**.

- 3 Click **Create New Report**.
 - 4 Select an option from the Report Type field.
 - 5 Select the time period to be covered by the report in the Graph X-Axis field.
 - 6 Select a start and end time for the report in the relevant fields.
 - 7 Select a week range and hour range where relevant.
 - 8 (Optional) Click **Recent Report** to see the last port utilization report generated.
 - 9 Click **Generate**.
The report appears on the in the Utilization tab.
 - 10 (Optional) Click **Generate PDF Report** to print your report to a PDF file.
 - 11 (Optional) Click **Generate Excel Report** to print your report to an Excel file.
-

CREATING A RESOURCE USAGE REPORT



This section is for Organization Administrators only.

You can create a report of how terminals and virtual rooms are being used on your network.

Procedure

- 1 Click **Reports and Statistics** in the sidebar menu.
- 2 Click **Utilization**.
- 3 Click **Create New Report**.
- 4 Select **Terminals Utilization** or **Virtual Room Utilization** from the Report Type field.
- 5 Select up to 3 terminals or virtual rooms from the pop-up list and click **OK**.
- 6 Select the time period to be covered by the report in the Graph X-Axis field.
- 7 Select the start and end points for the report in the relevant fields.
- 8 (Optional) Click **Recent Report** to see the last port utilization report generated.
- 9 Click **Generate**.
The report appears on the in the Utilization tab.

Viewing the Use of Ad Hoc and Scheduled Meetings

- 10 (Optional) Click **Generate PDF Report** to print your report to a PDF file.
 - 11 (Optional) Click **Generate Excel Report** to print your report to an Excel file.
-

VIEWING THE USE OF AD HOC AND SCHEDULED MEETINGS



You can see the proportion of your network meetings that are ad hoc or scheduled.

Procedure

- 1 Click **Reports and Statistics** in the sidebar menu.
 - 2 Click **Statistics**.
-

VIEWING AVERAGE MEETING SIZE



Procedure

- 1 Click **Reports and Statistics** in the sidebar menu.
 - 2 Click **Statistics**.
-

VIEWING AVERAGE MEETING DURATION



Procedure

- 1 Click **Reports and Statistics** in the sidebar menu.
 - 2 Click **Statistics**.
-

GENERATING REPORTS FOR FINISHED MEETINGS

You can generate a report in .xls format which shows all meetings scheduled between selected dates (as specified in the To and From fields). Once you have saved a report, you can view it with Microsoft Excel.

If the generated report contains more than 10,000 records including meetings and calls, iVIEW Suite asks whether you want the report to contain only the last 10,000 entries, or whether you prefer to abandon the current generating operation.



Procedure

- 1 Click **Reports and Statistics** in the sidebar menu.
- 2 Click **History**.
- 3 Click the calendar icon in the From and To fields to choose a start and end date for information in the generated report.
- 4 Click **Generate Report**.

[Table 15-1](#) describes the information categories that are included in a generated report.

Table 15-1 *Generated Report Information Categories*

Category	Description
Virtual Meeting ID	Dialable meeting ID used by users to access a specific meeting.
Master Meeting ID	Corresponds to a physical meeting ID on the master MCU.
Slave Meeting ID	Corresponds to a physical meeting ID on the slave MCU.
iVIEW Suite Meeting ID	Internal database ID for the meeting.
Subject	Corresponds to Subject field in Meeting Scheduling.
Meeting Type	Corresponds to the Meeting Type field in Meeting Scheduling. The name of the meeting type is displayed.
Reference Code	Corresponds to the Reference Code field in Meeting Scheduling.
Start Time	Corresponds to the Start Time field in Meeting Scheduling.

Generating Reports for Finished Meetings

Category	Description
Duration	Corresponds to the Duration field in the Meeting Scheduling.
Meeting Room	Meeting room used for scheduling a meeting.
Organizer Name	Corresponds to the Organizer field in Meeting Scheduling.
Service Prefix	MCU service prefix used for the meeting.
Services	MCU service used for the meeting.
MCU Name(s)	MCU(s) used for the meeting. For cascaded meetings, “(master)” appears after the MCU name.
Terminals	Number of terminals used for the meeting.
Number of Extra IP Ports Reserved	Corresponds to the Reserve additional ports field in Meeting Scheduling.
Dial-in IP Terminals	Number of dial-in IP terminals.
Dial-out IP Terminals	Number of dial-out IP terminals.
Dial-in ISDN Terminals	Number of dial-in PSTN/ISDN terminals.
Dial-out ISDN Terminals	Number of dial-out PSTN/ISDN terminals.
Gateway List	Gateways used for the meeting.
Device Failure Cause (Device Name, IP Failure, Cause)	Any failure on a network device such as an MCU or gateway.
Attendee Failure Cause (Name, Number, ISDN, Dial-in, Total Time, Failing Attempts, Last Failure Cause)	Any failures on attending terminals.

5 Click **Save** to save the report to a location of your choice.

VIEWING FINISHED MEETINGS



Procedure

- 1 Click **Reports and Statistics** in the sidebar menu.
 - 2 Click **History**.
-

VIEWING THE TERMINATION STATUS OF MEETINGS



Procedure

- 1 Click **Reports and Statistics** in the sidebar menu.
 - 2 Click **History** to see all meetings that have already finished.
The termination status of each of the displayed meetings is shown in the Status column.
 - Green—Indicates successful termination and all participants successfully exited the meeting.
 - Red—Indicates unsuccessful meeting termination or the abnormal exit of a terminal from the meeting.
 - 3 Click the red status indicator to view the Reason Failed error message.
 - 4 Click **Retry** to resend the meeting information to the MCU.
-

SEARCHING FOR A FINISHED MEETING



Procedure

- 1 Click **Reports and Statistics** in the sidebar menu.
- 2 Click **History**.
- 3 Perform any of the following:

Viewing Host MCUs

- Enter the partial or complete subject of the meeting in the Subject field.
If any part of the meeting subject matches the search string, the meeting record is displayed in the search results.
 - Enter the E.164 number of an attending terminal in the E164 field.
If any part of the meeting subject matches the search string, the meeting record is displayed in the search results.
 - Click the calendar icon in the From field, and select a date and time in the window that opens.
Meetings scheduled after the selected time are listed.
 - Click the calendar icon in the To field, and select a date and time in the window that opens.
Meetings scheduled before the selected time are listed.
 - Enter the partial or complete meeting ID in the Meeting ID field.
If any part of the meeting ID matches the search string, the meeting record is displayed in the search results.
- 4 Click **Search**.
Search results are listed.
 - 5 To return to the complete list of meetings, clear each of the fields.
 - 6 Click **Search**.
-

VIEWING HOST MCUs



Procedure

- 1 Click **Reports and Statistics** in the sidebar menu.
 - 2 Click **History**.
All host MCUs are listed in the MCU column with an indication of whether the meeting is cascaded.
-

REMOVING MEETINGS FROM THE HISTORY TAB



You can define a rule to instruct iCM to automatically delete past meetings.

Procedure

- 1 Open the iVIEW Suite Configuration Tool.
 - 2 Go to **System Configuration > Scheduling Settings**.
 - 3 Select **Delete meetings older than** and enter a value in days up to a maximum of 9999 days.
Meetings older than this date are automatically deleted from the database.
 - 4 Click **Save**.
-

Removing Meetings from the History Tab

16

MANAGING ICM USERS AND USER GROUPS WITHOUT AN EXTERNAL DIRECTORY

- [Creating or Modifying a User Profile](#) on page 104
- [Removing a User Profile](#) on page 105
- [Searching for a User Profile](#) on page 105
- [Updating User Profiles](#) on page 106
- [Creating a User Group](#) on page 106
- [Modifying a User Group](#) on page 107
- [Removing a User Group](#) on page 107
- [Modifying a Service Provider Profile](#) on page 108
- [Limiting Individual User Access to Meeting Types](#) on page 109
- [Limiting Group Access to Meeting Types](#) on page 109
- [Configuring Multiple Settings for User Groups](#) on page 110

CREATING OR MODIFYING A USER PROFILE

You can add or modify a user profile if iCM uses its own database for storing user profiles.

If your organization is synchronized with an external directory server to provision users, you can only modify the settings stored in iCM, such as virtual room, default terminals, allowed meeting types, groups, and time zone.

You can modify user passwords, email, telephone and time zone settings at Users > My Profile if those settings are not stored in the external directory server.

Note Before configuring user profiles, set default settings for each user type at **Advanced Settings > Default User Settings**.



Procedure

- 1 Click **User Management** in the sidebar menu.
- 2 Click **Users**.
- 3 Click the link in the Name column for the user you require, or click **Add** to create a new user profile.
- 4 Enter the user ID and last name in the relevant fields.
- 5 (Optional) Enter the first name, email address and password for the user in the relevant fields, and confirm the password.
- 6 (Optional) Click **Virtual Room Setting** to add or modify virtual room settings for the user.
- 7 Click **Advanced**.
- 8 Select a user type and enter telephone numbers in the relevant fields.
- 9 Click **Select Terminal** to assign a default terminal to this user.
- 10 Select **Select** next to the Allowed Meeting Types field to restrict this user to a subset of all available meeting types.
By default, all active meeting types are allowed.
- 11 Select the group to which this user belongs from the Groups list.
- 12 Select a default time zone.
Local time zones are used by default at User > My Meetings and User > All Meetings.
- 13 Select **Enabled** in the Account Status field to activate the user account and allow the user to log in to iCM.

- 14 Select a recording policy option for this user from the Recording Policy list.
- 15 Select a location preference for this user.
- 16 Enable the user to log in to SCOPIA Desktop, if required.
- 17 Select an allowed bandwidth for SCOPIA Desktop calls.
- 18 Click **OK** to save your changes.

The user profile is saved and iCM sends the user a notification e-mail containing login access information.

REMOVING A USER PROFILE

You cannot remove a user profile if:

- You are provisioning users via an external directory server—The Delete button is disabled.
- The user is participating in an active meeting—You must wait for the user to leave the meeting.
- The user is the last user configured in the system with Organization Administrator privileges.



Procedure

- 1 Click **User Management** in the sidebar menu.
- 2 Click **Users**.
- 3 Click the user profile you want to delete in the Name column.
- 4 Click **Delete** and then **OK**.

The user profile is deleted from the scheduler and information about the user is removed from the database.

SEARCHING FOR A USER PROFILE



Procedure

- 1 Click **User Management** in the sidebar menu.
- 2 Click **Users**.

- 3 Enter the partial or complete name of the user in the Name field, or enter the partial or complete virtual room for the user in the Virtual Room field.
 - 4 Select the group in which you want to perform the search.
The default is All Groups.
 - 5 Click **Search**.
Search results are listed.
 - 6 To return to the complete list of users, clear the Name or Virtual Room field, and then click **Search**.
-

UPDATING USER PROFILES

If your organization uses an external directory server to provision users, you must update the list of iCM user profiles if users are removed from that directory server.

Meeting creation and meeting scheduling issues may arise if you do not update as required.



Procedure

- 1 Click **User Management** in the sidebar menu.
- 2 Click **Users**.
- 3 Click **Update** to import an up-to-date list of users from the external directory server.

The import process runs in the background enabling administrators to continue working with the system.

Once the new updated user database is created, users log in to iCM using a directory server login ID and password.

CREATING A USER GROUP



Procedure

- 1 Click **User Management** in the sidebar menu.
- 2 Click **Groups**.
- 3 Click **Add**.

- 4 Enter a name for the group in the Name field.
- 5 Select participants and terminals from the Available Contacts list and click the right-arrow button to move them to the Selected Contacts list.
- 6 Enter a cost code for group in the **Cost Code** field.

Note A cost code is required when an administrator includes catering services for a group.

- 7 Click **OK** to save your changes.
The group appears in the Groups tab list.
-

MODIFYING A USER GROUP



Procedure

- 1 Click **User Management** in the sidebar menu.
 - 2 Click **Groups**.
 - 3 Click the link in the Name column for the user group you require.
 - 4 Modify the name of the user group.
 - 5 Click **OK** to save your changes.
-

REMOVING A USER GROUP



Procedure

- 1 Click **User Management** in the sidebar menu.
 - 2 Click **Groups**.
 - 3 Select the group you want to delete.
 - 4 Click **Delete** and then **OK**.
The user group is deleted from the scheduler.
-

MODIFYING A SERVICE PROVIDER PROFILE



The Service Provider Administrator is a special kind of user. You can access and modify the profile of the service provider administrator of iVIEW Suite with multi-tenant support.

Procedure

- 1 Log in as the service provider administrator, and then go to **My Profile**.
 - 2 Modify the login ID in the **User ID** field.
 - 3 Click **Modify Password** to modify the service provider administrator password.
 - 4 You can configure the following information:
 - First name
 - Last name
 - Company
 - Department
 - Email
 - Branch
 - Telephone(Office)
 - Telephone(Mobile)
 - Time zone—Of the service provider administrator
 - 5 Set preferences for the service provider administrator:
 - Select a format from the **Date Display Format** list (for example, DD/MM/YY) to determine the date display in the user interface.
 - Select **User Full Screen Display** to display a window frame without a menu or title bar in the browser.

By default this option is selected. If the option is not selected, the standard browser display appears.
 - Select a name format from the **Name Display Format** list.

Depending on the default browser settings, the options are first name first or last name first.
 - Select a sort order (by last name or first name) in the Sort field.
 - Select the order in which the day, month, and year are displayed in the Date Display field.
 - 6 Click **OK** to save and apply changes.
-

LIMITING INDIVIDUAL USER ACCESS TO MEETING TYPES



Meeting types listed on the Active Meeting Types tab are automatically listed in the Meeting Type field at User > Meeting Scheduling > Meeting. You can limit which meeting types are accessible by users.

Procedure

- 1 Click **User Management** in the sidebar menu.
 - 2 Click **Users**.
 - 3 Click the link in the Name column for the user you require, or click **Add** to create a new user profile.
 - 4 Click **Advanced**.
 - 5 Click **Select** next to the Allowed Meeting Types field.
 - 6 Select the required meeting types and click **OK**.
 - 7 Click **OK** to save your changes.
-

LIMITING GROUP ACCESS TO MEETING TYPES



Procedure

- 1 Click **User Management** in the sidebar menu.
 - 2 Click **Provisioning**.
 - 3 Select one or any of the groups listed in the Available Groups list and click the right-pointing arrow.
 - 4 Select **Allowed Meeting Types** and click **Select**.
 - 5 Select the required meeting types and click **OK**.
 - 6 Click **OK** to save your changes.
-

CONFIGURING MULTIPLE SETTINGS FOR USER GROUPS

The Provisioning tab offers a convenient way to set multiple parameters for large groups of users.



Procedure

- 1 Click **User Management** in the sidebar menu.
- 2 Click **Provisioning**.
- 3 Select a group in the Available Groups list and click the right-pointing arrow to move the group to the Selected Groups list.

The following default groups are listed as well as any other groups that you have manually defined or imported from your directory server:

- All Users
- System Administrators
- Operators
- Meeting Organizers
- Regular Users

You can select more than one group at a time using the Ctrl button on your keyboard.

- 4 Select and configure the parameters you want to apply to the groups you have selected.
 - 5 Click **Update**.
-

17

PROVISIONING ICM USERS VIA A DIRECTORY SERVER

- [Synchronization of User Information](#) on page 111
- [Accessing User Information in Active Directory Server](#) on page 112
- [Synchronizing iCM with Active Directory Server](#) on page 113
- [Configuring a Connection to an LDAP Server](#) on page 114
- [Mapping iCM User Roles to ADS Users](#) on page 115
- [Defining Virtual Rooms for All LDAP Users](#) on page 116
- [Forcing iCM to Use a Virtual Room](#) on page 117
- [iCM LDAP Information Attributes](#) on page 117

SYNCHRONIZATION OF USER INFORMATION

If an organization uses an external directory server, iCM can synchronize user information with the directory server, minimizing user setup and maintenance. iCM supports Microsoft Active Directory Server (ADS) 2000 and 2003.

When iCM connects to an external directory server, each user defined in the directory server is included in iCM, along with the associated user type for that user. If no user type is defined, a user is assigned the user type defined at **Advanced Settings > LDAP Configurations > Advanced**. The default user type setting is Meeting Organizer.

During the organization account creation process, iCM registers the first user (the technical contact)—usually the administrator who performs the installation. This technical contact is automatically assigned the Organization Administrator user type, with permission to log in and provision the other users. The technical contact cannot be deleted from within iCM and should not be deleted from the directory server.

If the directory server is customized not to use standard schema attributes and class labels, the iCM installation application will not correctly configure the database to synchronize with the directory server.

ACCESSING USER INFORMATION IN ACTIVE DIRECTORY SERVER



This section describes how to access user information in Microsoft Active Directory Server (ADS) 2000 and 2003.

Procedure

- 1 Select one of the following paths to view information for a user in the host Active Directory Server (ADS), depending on the Active Directory version you are using:
 - Start > Programs > Administrative Tools > Active Directory Users and Computers
 - Start > Settings > Control Panel > Administrative Tools > Active Directory Users and Computers
 - 2 Open the **User** folder to access the user list.
 - 3 Right-click the required user in the user list and then select **Properties**.
 - 4 Select the **General** tab to view the user ID for the selected user.
 - 5 Select the **Account** tab to view the login name for the selected user.
-

SYNCHRONIZING ICM WITH ACTIVE DIRECTORY SERVER



For the purposes of this topic, assume that Active Directory Server (ADS) includes an organizational unit (OU) called “China” with a sub-OU called “User”.

Procedure

- 1 Create the following groups for users under China:
 - Organization Administrator
 - Meeting Organizer
 - Meeting Operator
 - Regular User

Note These groups can be used by users belonging to any OU(s) in ADS.

- 2 Create users in the organizational unit China > Users.
If you do not configure the following properties for each new user, iCM does not download the user from ADS:
 - Logon name
 - First name and/or last name
 - Email address.

Note iCM does not download users with no e-mail address configured if you select **Do not update users without an e-mail address from the LDAP server...** at Admin > Advanced Settings > LDAP Configurations > Advanced.

- 3 For a user to be downloaded from a directory server, the following properties must be defined for that user on the directory server:
 - User ID and password.
 - First name or last name.
 - Email address.
 - Belong to an OU.
 - Belong to a group (if you want to assign user role based on group).

- 4 In iCM, go to **Advanced Settings > LDAP Configurations > Advanced** and use the **Do not update users without an e-mail address from the LDAP server to...** and **Update Frequency** options to define record synchronization.
 - 5 To map specific iCM user roles to ADS users, see the [Configuring a Connection to an LDAP Server](#) section on page 114.
-

CONFIGURING A CONNECTION TO AN LDAP SERVER

To work with an LDAP server for user provisioning, you must select user provisioning using a directory server during the installation process (or when creating an organization profile if the multi-tenant feature is enabled).

To work with Microsoft Active Directory and the iCM Microsoft Outlook Add-on, select user provisioning using a directory server with Single Sign-on enabled.

After installation, configure video conferencing devices and terminals before defining LDAP server settings for user provisioning.



Procedure

- 1 Click **Advanced Settings** in the sidebar menu.
- 2 Click **LDAP Configurations**.
- 3 Click **Add** to add a new LDAP server, or click the required LDAP server entry to modify an existing LDAP server.
- 4 Select the type of LDAP server to connect iCM to in the Directory Server Type field.
- 5 Enter the directory server domain or directory server URL in the Domain/URL field.
- 6 Enter the directory server login ID and password in the relevant fields.

Note The user account needs to have read access to all user accounts that you want to synchronize to iCM. This user account does not have to be part of the search base.

- 7 Click **Configure** to configure the LDAP Search Base field.
A tree structure appears showing all OUs defined on the directory server.
- 8 Select the OUs that you want to download users from.

- 9 Click **Close**.
The selected OUs are displayed in the LDAP Search Base field.
 - 10 Click **OK** to save your changes.
-

MAPPING ICM USER ROLES TO ADS USERS



Procedure

- 1 Click **Advanced Settings** in the sidebar menu.
- 2 Click **LDAP Configurations**.
- 3 Click **Advanced**.
- 4 Click **Select** next to each user type to assign LDAP user groups to a specific iCM user role.

You can assign multiple LDAP user groups to each iCM user role.

The following user types are available:

- Organization Administrator
- Meeting Operator
- Meeting Organizer
- Regular User

By default, all users are assigned the Meeting Organizer role.

iCM maps all users that are not assigned to any listed iCM user role to the user role specified in the Default User Type field.

- 5 (Optional) Set the Default User Type field to **Don't download** to instruct iCM not to download users that are not assigned to any listed iCM user role.
 - 6 Click **OK** to save your changes.
-

DEFINING VIRTUAL ROOMS FOR ALL LDAP USERS

This section describes how to define a unique virtual meeting room for a specified LDAP user.

Each user can schedule a meeting in his/her own virtual room, or schedule a random meeting. A user cannot schedule a meeting in the virtual room of another user.

A virtual room is created for each user during LDAP synchronization.

To automatically create a virtual room, the following conditions must be met:

- The value of the LDAP field mapped to the virtual room must be numeric.
- The virtual room number for an LDAP server is not editable on the virtual room profile screen.
- If the same virtual room number is defined for two users in the LDAP server, the virtual room is created for only one of the users.

Each virtual room obeys the default settings defined at **Advanced Settings > Default Meeting Settings**.



Procedure

- 1 Click **Advanced Settings** in the sidebar menu.
 - 2 Click **LDAP Configurations**.
 - 3 Click **Advanced**.
 - 4 Check **Virtual Room Number** to create a virtual room for all LDAP users.
 - 5 Select a parameter that you want to use as the virtual room number.
By default, the `telephoneNumber` parameter is used since everyone within an organization should have a unique telephone number.
The resulting virtual room is the concatenation of the iCM Meeting ID prefix and the LDAP field that is used for generating the virtual room number.
 - 6 Click **OK** save your changes.
-

FORCING ICM TO USE A VIRTUAL ROOM



This section describes how to force endpoint-initiated ad hoc conferences to be hosted in a predefined virtual room.

Procedure

- 1 Go to **System Configuration > Scheduling Settings** in the iVIEW Suite Configuration Tool.
- 2 Select **Allow Only Endpoint Initiated Virtual Room Meetings** to ensure that endpoint-initiated ad hoc conferences can only be hosted within a predefined virtual room.

You cannot create random conferences when **Allow Only Endpoint Initiated Virtual Room Meetings** is selected.

This configuration prevents users from dialing into the system and randomly creating MCU conferences and using up MCU ports. If all virtual rooms are PIN protected, only users who know the virtual room PIN can create endpoint-initiated conferences.

Note The Allow Only Endpoint Initiated Virtual Room Meetings option is enabled only when the Allow Endpoint Initiated Multipoint Calls field is selected.

ICM LDAP INFORMATION ATTRIBUTES

Table 17-1 lists the LDAP information attributes used by iCM.

Table 17-1 *iCM LDAP Information Attributes*

Identifier	Attribute	Description
1	uid	User identifier
2	email	User email address
3	telephone	User telephone number
4	mobile	User mobile telephone number
5	fax	User fax number

iCM LDAP Information Attributes

Identifier	Attribute	Description
6	cn	Full name of user
7	givenName	Given name of user
8	sn	Surname of user
9	company	User company name
10	branch	Branch
11	department	Department
12	country	Country
13	state	State
14	city	City
15	description	Description
16	zipCode	Zip code
17	address	Address

18

MODIFYING DEFAULT ORGANIZATION SETTINGS FOR ICM USERS AND MEETINGS

- [Settings Priorities](#) on page 119
- [How to Define Default Settings for Organization Users](#) on page 119
- [How to Define Default Settings for Meetings](#) on page 123
- [Modifying the Look and Feel of the iCM Web User Interface](#) on page 130

SETTINGS PRIORITIES

When configuring advanced settings, note the following priority rules:

- Changes to an individual user profile override default settings
- Settings you make for a meeting during scheduling override settings in a virtual room
- Settings in a virtual room override default meeting settings

HOW TO DEFINE DEFAULT SETTINGS FOR ORGANIZATION USERS

- [Defining Which Meeting Types are Available to New Users](#) on page 120
- [Defining a Default Time Zone for a User](#) on page 120
- [Defining Display Formats](#) on page 121
- [Defining Date Display Formats](#) on page 121
- [Defining Your Meeting Display Preferences](#) on page 121
- [Defining Bandwidth for SCOPIA Desktop Calls](#) on page 122

- [Defining SCOPIA Desktop Policies](#) on page 122
- [Defining Default Recording Permissions](#) on page 123

DEFINING WHICH MEETING TYPES ARE AVAILABLE TO NEW USERS



Procedure

- 1 Click **Advanced Settings** in the sidebar menu.
- 2 Click **Default User Settings**.
- 3 Select a meeting type in the Available Meeting Types list that you want to make available to new users.
- 4 Use the right-pointing arrow to move the meeting type to the Selected Meeting Types list.

We recommended that you select all available meeting types.

Non-Video Conference, Point-to-Point, Continuous Presence and Voice Activated meeting types are default meeting types in iCM. They do not exist on the MCU.

- 5 Click **OK** to save your changes.
-

DEFINING A DEFAULT TIME ZONE FOR A USER



Procedure

- 1 Click **Advanced Settings** in the sidebar menu.
 - 2 Click **Default User Settings**.
 - 3 Select a default time zone for the selected meeting types.
 - 4 Click **OK** to save your changes.
-

DEFINING DISPLAY FORMATS



Procedure

- 1 Click **Advanced Settings** in the sidebar menu.
 - 2 Click **Default User Settings**.
 - 3 Select an option from the Name Display Format list to change the way user names are displayed in meeting-related information and in the meeting video display.
 - 4 Select **Last name** or **First name** from the Sort by list to change the sort order for participant name columns.
 - 5 Click **OK** to save your changes.
-

DEFINING DATE DISPLAY FORMATS



Procedure

- 1 Click **Advanced Settings** in the sidebar menu.
 - 2 Click **Default User Settings**.
 - 3 Select an option from the Date Display Format list to change the way dates are displayed in meeting-related information and in the meeting video display.
 - 4 Click **OK** to save your changes.
-

DEFINING YOUR MEETING DISPLAY PREFERENCES



Procedure

- 1 Click **Advanced Settings** in the sidebar menu.
- 2 Click **Default User Settings**.

- 3 Click **Display all meeting records on My Meetings** screens to display all meetings within the organization in My Meetings.
 - 4 Click **OK** to save your changes.
-

DEFINING BANDWIDTH FOR SCOPIA DESKTOP CALLS



Procedure

- 1 Click **Advanced Settings** in the sidebar menu.
 - 2 Click **Default User Settings**.
 - 3 Select a value from the **Maximum Allowed Bandwidth For SCOPIA Desktop Calls** field.
 - 4 Click **OK** to save your changes.
-

DEFINING SCOPIA DESKTOP POLICIES



Procedure

- 1 Click **Advanced Settings** in the sidebar menu.
 - 2 Click **Default User Settings**.
 - 3 Select **Enable SCOPIA Desktop users authentication** to instruct the SCOPIA Desktop Server to authenticate and authorize users.
 - 4 Select the options you require for defining which users can access meetings and webcasts, invite participants to meetings, and record meetings and access the recordings.
 - 5 Click **OK** to save your changes.
-

DEFINING DEFAULT RECORDING PERMISSIONS



Procedure

- 1 Click **Advanced Settings** in the sidebar menu.
 - 2 Click **Default User Settings**.
 - 3 Select any or all of the user roles in the Default Recording Permissions section.
 - 4 Click **OK** to save your changes.
-

HOW TO DEFINE DEFAULT SETTINGS FOR MEETINGS

On the Default Meeting Settings tab, the Organization Administrator sets which default values are available to users when scheduling meetings or defining virtual rooms.

When a new meeting is scheduled, default settings configured in the Default Meeting Settings tab also appear in the Meeting Scheduling tab.

- [Defining a Default Meeting Type](#) on page 124
- [Defining the Default Cascading Mode](#) on page 124
- [Defining the Maximum Number of Ports for an Ad Hoc Meeting](#) on page 125
- [Defining How to End a Meeting](#) on page 125
- [Defining the Meeting Default Length](#) on page 126
- [Defining the Default Dialing Mode](#) on page 126
- [Defining a Billing Destination](#) on page 127
- [Defining Required Default Resources](#) on page 127
- [Defining the Auto Attendant Service Prefix](#) on page 128
- [Enabling Automatic Routing](#) on page 128
- [Customizing Invitation Email](#) on page 129

DEFINING A DEFAULT MEETING TYPE



Procedure

- 1 Click **Advanced Settings** in the sidebar menu.
 - 2 Click **Default Meeting Settings**.
 - 3 Select a default meeting type from the Meeting Type list or all new meeting templates and new meetings.
We recommend that you select a default meeting type which is available to all users.
 - 4 Click **OK** to save your changes.
-

DEFINING THE DEFAULT CASCADING MODE



Procedure

- 1 Click **Advanced Settings** in the sidebar menu.
 - 2 Click **Default Meeting Settings**.
 - 3 Set Allow Cascaded Meeting to **Yes** to enable iCM to automatically create cascaded meetings on the MCUs.
Set to No to instruct iCM to create only meetings no larger than the capacity of a single MCU/MVP card. iCM will not cascade two MCU conferences together to increase conference size or save network bandwidth.
When set to No, the Prioritize field is disabled.
 - 4 Select the priority from the Prioritize list by which meetings are scheduled and which is used in meeting templates by default. This is an important factor in creating efficient conferences. The options are
 - Local MCU
 - Bandwidth
 - Delay
 - 5 Click **OK** to save your changes.
-

DEFINING THE MAXIMUM NUMBER OF PORTS FOR AN AD HOC MEETING



Procedure

- 1 Click **Advanced Settings** in the sidebar menu.
 - 2 Click **Default Meeting Settings**.
 - 3 Select a value from the Maximum number of ports option.
 - 4 Click **OK** to save your changes.
-

DEFINING HOW TO END A MEETING



Procedure

- 1 Click **Advanced Settings** in the sidebar menu.
- 2 Click **Default Meeting Settings**.
- 3 Locate the Default settings for scheduled meetings section.
- 4 Select **At scheduled time** in the Termination policy field to terminate the meeting according to the termination time define for the meeting.
- 5 Enter a value in the **Alert n minutes before the meeting ends** field to indicate the length of time before the scheduled termination of the meeting that terminals receive the end-of-meeting warning.

At the defined length of time before the end of the meeting, an audio alert message is played to the meeting participants. The only way to extend the meeting is to do it manually in the In-meeting Control screen.

- 6 Select **n minutes after all participants have left the meeting** to terminate the meeting only a defined period of time after the last terminal leaves.

iCM automatically extends the meeting as long as meeting participants are still connected to the meeting, and there is no resource conflict with upcoming scheduled meetings.

- 7 Enter the required value in the **n minutes after all participants have left the meeting** field.

By default, you cannot automatically extend iCM meetings to last more than 4 hours. Administrators can change this default via the iVIEW Suite Configuration Tool.

When iCM is configured to send an alert prior to the end of a meeting, users of Sony PCS endpoints can automatically extend the meeting.

When the alert reaches the Sony PCS endpoint, the user can press the Help button on the Sony PCS terminal remote control for 5 seconds to extend the meeting by the length of time specified in the Meeting Auto Extend Length field in the iVIEW Suite Configuration Tool.

- 8 Click **OK** to save your changes.
-

DEFINING THE MEETING DEFAULT LENGTH



Procedure

- 1 Click **Advanced Settings** in the sidebar menu.
 - 2 Click **Default Meeting Settings**.
 - 3 Enter the default length of a meeting in minutes in the Duration field.
 - 4 Click **OK** to save your changes.
-

DEFINING THE DEFAULT DIALING MODE



Procedure

- 1 Click **Advanced Settings** in the sidebar menu.
 - 2 Click **Default Meeting Settings**.
 - 3 Select **Dial-out** or **Dial-in** from the Default Dialing Mode list.
 - 4 Click **OK** to save your changes.
-

DEFINING A BILLING DESTINATION



Procedure

- 1 Click **Advanced Settings** in the sidebar menu.
- 2 Click **Default Meeting Settings**.
- 3 Select **Meeting host, Meeting organizer** or **All participants** in the Bill To field.

If the host and the organizer are the same person, the Meeting organizer option does not appear.

The cost of the meeting is billed accordingly.

The selection in the Bill To field determines the default setting in the Virtual Room and Meeting Scheduling screens.

- 4 Click **OK** to save your changes.
-

DEFINING REQUIRED DEFAULT RESOURCES



Procedure

- 1 Click **Advanced Settings** in the sidebar menu.
- 2 Click **Default Meeting Settings**.

Select the default resources from the Required list for the meeting to be confirmed. A meeting is not allowed if these resources are not available at the time of the meeting.

You can choose to require that participating users, rooms, or terminals cannot be double booked for a meeting before you can successfully schedule a meeting.

- 3 Click **OK** to save your changes.
-

DEFINING THE AUTO ATTENDANT SERVICE PREFIX

The Auto Attendant feature enables you to define the MCU service for entry into the IVR audio and video message utility.

This option is available only if you have selected the Use in Auto Attendant sessions option for one of the meeting types listed under Admin > Meeting Types > Active Meeting Types.



Procedure

- 1 Click **Advanced Settings** in the sidebar menu.
 - 2 Click **Default Meeting Settings**.
 - 3 Locate the Advanced Routing section.
 - 4 Select **Please specify the auto attendant number** and enter the service prefix for the Auto Attendant feature.
Verify that this number does not begin with any MCU or Gateway service or ECS zone prefix, or is the same as the number of an IP terminal
 - 5 (Optional) Select **Prompt for a meeting PIN while creating new meetings** if you want users to enter a PIN when creating or entering a conference using this service.
 - 6 (Optional) Select **Display all meeting records on the Auto Attendant menu** to enable users to see all meeting records when creating or entering a conference using this service.
 - 7 Click **OK** to save your changes.
-

ENABLING AUTOMATIC ROUTING



Procedure

- 1 Click **Advanced Settings** in the sidebar menu.
- 2 Click **Default Meeting Settings**.
- 3 Locate the Routing section.

- 4 Select **Automatically route incoming calls according to schedule. Please specify the auto route number.** and enter an e.164 number containing up to 10 characters.

When an endpoint dials to the specified e.164 number, iVIEW Suite reviews all ongoing meeting and meetings due to start in 5 minutes, and routes the call to the destination meeting according to the source number of the call and the meeting schedule.

- 5 Click **OK** to save your changes.
-

CUSTOMIZING INVITATION EMAIL



You can customize the content of the invitation email that participants receive when a meeting is scheduled, modified or cancelled.

Procedure

- 1 Click **Advanced Settings** in the sidebar menu.
- 2 Click **Default Meeting Settings**.
- 3 (Optional) Select **Customize the 'meeting invitation' introduction message** and then enter your text to override the introduction message in the initial meeting invitation email.
- 4 (Optional) Select **Customize the 'meeting update' introduction message** and enter your text to override the introduction message in the meeting update e-mail.
- 5 (Optional) Select **Customize the 'meeting cancellation' introduction message** and enter your text to override the introduction message in the meeting cancellation email.
- 6 (Optional) Select **Override IP Terminal Access Information** and enter your text to override default access information for IP terminals.
- 7 (Optional) Select **Meeting ID** to insert meeting ID placeholders into the text.
- 8 (Optional) Select **Override ISDN/PSTN/Mobile Terminal Access Information** and enter your text to override default access information for ISDN/PSTN/Mobile terminals.

Default access information for ISDN/PSTN/Mobile terminals consists of access information for all Gateways configured in iCM.

- 9 (Optional) Select **Meeting ID** to insert meeting ID placeholders into the text.

- 10 (Optional) Select **Hide the Attendees list** to hide the attendees section in the invitation email.
 - 11 (Optional) Select **Hide in-meeting control access information** to hide the instructions for accessing the meeting via the in-meeting control interface from the invitation email.
 - 12 (Optional) Select **Hide dial-in information for attendees** to hide only the dial-in access information for each attendee when Hide the Attendees list is deselected.
 - 13 Click **OK** to save your changes.
-

MODIFYING THE LOOK AND FEEL OF THE ICM WEB USER INTERFACE



Procedure

- 1 Click **Advanced Settings** in the sidebar menu.
- 2 Click **Look and Feel**.
- 3 Select **Visible** or **Hidden** to determine whether the following fields are displayed or hidden at Meeting Scheduling > Basic:
 - PIN
 - Waiting Room
 - Record Meeting
 - Streaming
 - Description
 - Bill To
 - Reference Code
 - Customize Reference Code Field Label—Determines the label used for the Reference Code field.
 - Enforce Reference Code Entry—Determines whether or not the reference code is mandatory.
 - Field Type—Determines the type of content that can be entered in the Reference Code Entry field.

- Field Length—Determines the length of the value entered in the Reference Code field.
 - Enforce Full Length—Determines whether or not the full Reference Code field length is used.
- 4 Select **Visible to Meeting Organizer** or **Hidden from Meeting Organizer** to determine whether the Attendees Settings tab, the Attendees Availability tab and the Advanced tab are displayed or hidden on the Meeting Scheduling tab.
 - 5 Use the Invite Attendees By field to indicate whether to invite attendees in groups or per terminal at Meeting Scheduling > Invite.
 - 6 Select **Visible** or **Hidden** to determine whether the Reserved Ports field is displayed or hidden at Meeting Scheduling > Invite.
 - 7 Select **Visible** or **Hidden** to determine whether the PSTN/ISDN and Dial-in columns are displayed or hidden at Meeting Scheduling > Attendees Settings.
 - 8 Determine whether attendee terminal settings are editable or read-only at Meeting Scheduling > Attendees Settings.
The Attendee Terminal Settings option determines whether or not a meeting organizer can change the default association between an attending user and his/her default terminal when scheduling a meeting.
 - 9 Select **Visible** or **Hidden** to determine whether the following are displayed or hidden in the In-meeting Control interface:
 - Statistics tab
 - Extend Meeting option
 - Terminal Invitation option
 - Advanced Invitation tab
 - Terminate Meeting option
 - Layout Control—Determines whether the layout control panel is displayed or hidden.
 - 10 Select the following options as required:
 - Hide Meeting Room—Determines whether or not the Meeting Room tab is hidden in the Resource Management section.
 - Hide Meeting Notification E-mail for meeting rooms and terminals—Determines whether or not email and time zone fields for meeting rooms and terminals are enabled. If meeting rooms and terminals are enabled, they can directly receive notification emails.

Modifying the Look and Feel of the iCM Web User Interface

- Show My Profile—Determines whether or not the My Profile section is displayed.
- Enable Personal Address Book—Determines whether or not the Address Book section is displayed.
- Play a sound upon scheduling failure—If chosen, there is a warning sound in the event of a meeting scheduling failure.
- Use Full Screen Display—Determines whether or not the iCM user-interface is displayed full-screen after login.

11 Click **OK** to save your changes.

19

USING THE iVIEW SUITE CONFIGURATION TOOL

During the initial installation of iVIEW Suite, defined network environment settings and other configurable elements, such as page length and meeting identifiers, are set to default values. This enables iCM to run upon installation without the need for additional configuration.

The iVIEW Suite Configuration Tool, a client-server application based on Java Web Start, enables the system administrator to configure iVIEW Suite system settings, set CDR preferences, and modify default value settings.

- [Setting Up the Java Runtime Environment](#) on page 134
- [Launching the iVIEW Suite Configuration Tool](#) on page 134
- [Retrieving an Administrator Password](#) on page 135
- [Uninstalling the iVIEW Suite Configuration Tool](#) on page 135
- [How to Modify General Settings](#) on page 136
- [How to Modify Scheduling Settings](#) on page 140
- [Hiding iCM User Interface Screens](#) on page 144
- [How to Manage Custom Time Zones](#) on page 145
- [Customizing Product and Vendor Logos](#) on page 148
- [Creating a Customized Billing Field](#) on page 149
- [Defining Database Server Settings](#) on page 149
- [How to Define Security Settings](#) on page 150
- [How to Configure SNMP Trap Server Profiles](#) on page 151

- [Defining Utilization Thresholds](#) on page 153
- [How to Define Call Data Record \(CDR\) Settings](#) on page 154

SETTING UP THE JAVA RUNTIME ENVIRONMENT

Install Java Runtime Environment on the client computer before using the iVIEW Suite Configuration Tool.



Procedure

- 1 Go to **http://server_host:port/icm-config**.
The first time you access the iVIEW Suite Configuration Tool, it detects whether or not Java Runtime Environment is installed on the client computer.
If Java Runtime Environment is not installed on the client computer, a download message appears.
 - 2 Click **Install Java Runtime Environment**.
 - 3 Click **download on the Java download web page**.
The Java Runtime Environment is installed on the client computer.
 - 4 To return to the iVIEW Suite Configuration Tool, click **previous page on the Java download web page**.
-

LAUNCHING THE iVIEW SUITE CONFIGURATION TOOL

The iVIEW Suite Configuration Tool is accessible from any client computer on which the Java Web Start application is installed.



Procedure

- 1 Go to **http://server_host:port/icm-config**.
The iVIEW Suite Configuration Tool launch page appears.
- 2 Click **Launch iVIEW Suite Configuration Tool**.
The iVIEW Suite Configuration Tool checks for the latest version of the Java Web Start application on the client computer, and then starts the iVIEW Suite Configuration Tool.

- 3 If a warning message appears stating that the digital signature is invalid and asking if you want to run the application, click **Run**.

To avoid the appearance of this message upon launch of the iVIEW Suite Configuration Tool from the same site address, in the message window, select **Always trust content from this publisher**, and then click **Run**.

- 4 Click **Launch iVIEW Suite Configuration Tool** on the iCM launch page.
- 5 Enter the login and password of the Service Provider Administrator or an Organization Administrator.
- 6 Click **Login**.

The iVIEW Suite Configuration Tool window opens.

RETRIEVING AN ADMINISTRATOR PASSWORD



Procedure

- 1 In the login window, click the down arrow to open the lower part of the login window in the iVIEW Suite Configuration Tool login window.
 - 2 Enter the administrator login ID in the Send Admin Password for Login ID field.
 - 3 Click **Send** to send the administrator password to the email address associated with the login ID.
-

UNINSTALLING THE iVIEW SUITE CONFIGURATION TOOL



Procedure

- 1 Go to **Settings > Control Panel > Add or Remove Programs** on the client computer.
 - 2 Select iVIEW Suite **Configuration Tool**, and click **Remove**.
-

HOW TO MODIFY GENERAL SETTINGS

- [Defining Email Server Settings](#) on page 136
- [Defining the Unconnected Endpoint Time Period](#) on page 137
- [Defining User Provisioning Options](#) on page 137
- [Defining Table Row Display](#) on page 138
- [Defining the Command Delay](#) on page 138
- [Defining the Parent Zone Authorization Filter](#) on page 138
- [Defining the Log Level](#) on page 139
- [Defining the iCM Server Name and Web Port](#) on page 139
- [Defining the Online Help Host URL](#) on page 140

DEFINING EMAIL SERVER SETTINGS

You can define settings that are used by iCM to send email notifications, such as meeting reservations and meeting updates, to users and administrators.



Procedure

- 1 Select **System Configuration > General Settings** in the iVIEW Suite Configuration Tool interface.
 - 2 Enter the email server IP address or domain name in the Host field.
 - 3 Enter the email server communications port number in the Port field.
 - 4 Enter the email server login ID and password in the relevant fields to enable access to the email server.
 - 5 Select **E-mail meeting organizer upon** to send an email notification to the meeting organizer in the event of a meeting failure.
 - 6 Select one or more of the following meeting-failure check boxes:
 - Meeting creation
 - EP abnormal connection
 - EP connection
 - Dial-in considered—This check box is only active if you select **EP connection**.

If you select **Dial-in considered**, dial-in connections are considered as endpoints and email notifications are sent in the case of a dial-in connection failure.
 - 7 Click **Save**.
-

DEFINING THE UNCONNECTED ENDPOINT TIME PERIOD

If an endpoint does not respond within the designated timeout period to a connection request, the system classifies the endpoint as unconnected.



Procedure

- 1 Select **System Configuration > General Settings** in the iVIEW Suite Configuration Tool interface.
 - 2 Enter a value in seconds in the EP Unconnected Time Out field.
 - 3 Click **Save**.
-

DEFINING USER PROVISIONING OPTIONS

This section is for Organization Administrators.



Procedure

- 1 Select **System Configuration > General Settings** in the iVIEW Suite Configuration Tool interface.
- 2 Select **Enable integration with directory server** to change the user provisioning mode if no integration was selected during iVIEW Suite installation.

Note Changing the user provisioning mode removes current users from the iVIEW Suite database.

- 3 Select **Enable Single Sign On (SSO)** to allow users to log in without entering a user name or password.
When SSO is enabled, a user who is logged into the organization domain and then tries to access the iVIEW Suite Web login window, is authenticated transparently according to the ADS domain account and password credentials that the user enters in the iVIEW Suite Web login window.
 - 4 Click **Save**.
-

DEFINING TABLE ROW DISPLAY

You can define the number of rows that are displayed in iCM tables.



Procedure

- 1 Select **System Configuration > General Settings** in the iVIEW Suite Configuration Tool interface.
 - 2 Enter a value in the Number of table rows per page field.
 - 3 Click **Save**.
-

DEFINING THE COMMAND DELAY

You can define the time interval that iCM waits when sending sequential internal messages to the MCU.



Procedure

- 1 Select **System Configuration > General Settings** in the iVIEW Suite Configuration Tool interface.
 - 2 Enter a value in milliseconds in the Delay between two commands from iCM to MCU field.
Enter 0 for deployments consisting of version 5.x MCUs only.
Enter 100 for deployments containing version 4.x MCUs.
 - 3 Click **Save**.
-

DEFINING THE PARENT ZONE AUTHORIZATION FILTER

The setting is only applicable when working with the ECS. In a hierarchical mode, this setting determines whether or not the parent zone prefix should be added when going from a child gatekeeper to a parent gatekeeper during multi-zone navigation. This is useful for iCM to determine the dial-out string when a terminal is invited.



Procedure

- 1 Select **System Configuration > General Settings** in the iVIEW Suite Configuration Tool interface.
 - 2 Select the Enable Parent Zone Authorization Filter field.
 - 3 Click **Save**.
-

DEFINING THE LOG LEVEL

You can select from three levels of detail for a log file. The more detailed a log file, the larger the log file.



Procedure

- 1 Select **System Configuration > General Settings** in the iVIEW Suite Configuration Tool interface.
 - 2 Select one of the following options in the Log Level field:
 - WARN—This is the standard setting that we recommend in most cases.
 - INFO—This setting includes more detailed information in the log file.
 - DEBUG—This setting includes issue details in the log file and produces the most detailed log.
 - 3 Click **Save**.
-

DEFINING THE ICM SERVER NAME AND WEB PORT

You can define the server name and Web port number after installation.



Procedure

- 1 Select **System Configuration > General Settings** in the iVIEW Suite Configuration Tool interface.
 - 2 Enter the server name, port, login ID and password in the relevant fields.
 - 3 Click **Save**.
-

DEFINING THE ONLINE HELP HOST URL

You can point the online help files to a remote URL. We recommend that you do not customize the online help host URL unless you have a copy of the online help files.



Procedure

- 1 Select **System Configuration > General Settings** in the iVIEW Suite Configuration Tool interface.
 - 2 Enter the remote URL in the Online Help Host URL field.
 - 3 Click **Save**.
-

HOW TO MODIFY SCHEDULING SETTINGS

- [Changing Call Authorization Settings](#) on page 140
- [Dynamically Cascading Multiple MVPs for a Single Conference](#) on page 142
- [Modifying iCM Default Meeting Settings](#) on page 142
- [Modifying Default Recurring Meeting Settings](#) on page 144

CHANGING CALL AUTHORIZATION SETTINGS

When iCM and ECS are working in authorization mode, iCM can restrict endpoint-initiated conferences with settings in this section to prevent uncontrolled and unmanaged access in a video conference network.



Procedure

- 1 Select **System Configuration > Scheduling Settings** in the iVIEW Suite Configuration Tool interface.
- 2 Deselect **Allow Endpoint Initiated Point to Point Calls** to prevent endpoint-initiated point-to-point calls.
- 3 Deselect **Allow Endpoint Initiated Multipoint Calls** to prevent endpoint-initiated MCU calls

- 4 Select **Allow Only Endpoint Initiated Virtual Room Meetings** to ensure that endpoint-initiated MCU calls must use a defined virtual room.

The Allow Only Endpoint Initiated Virtual Room Meetings option is enabled only when the Allow Endpoint Initiated Multipoint Calls field is selected.

Note You cannot create random endpoint-initiated conferences when Allow Only Endpoint Initiated Virtual Room Meetings is selected.

- 5 Select **Allow Advanced Virtual Room Management for Meeting Organizer** to enable Meeting Organizers to have multiple virtual rooms. When selected, a meeting organizer can have multiple virtual rooms under his or her user profile. The Basic and Invite tabs are also displayed under the Virtual Room Profile screens.

Only Administrators can add a new virtual room for a Meeting Organizer. A Meeting Organizer can only delete or modify his or her existing virtual rooms.

By default, **Allow Advanced Virtual Room Management for Meeting Organizer** is deselected. Each Meeting Organizer can have a single virtual room only, and only the virtual room Basic tab is displayed.

Administrators and Meeting Operators can always have multiple virtual rooms and the virtual room Basic and Invite tabs are both displayed by default.

Note If a Meeting Organizer already has more than one virtual room, even if the Allow Advanced Virtual Room Management for Meeting Organizer is deselected, a full list of the virtual rooms that belong to the user is displayed as well as all of the configuration tabs for each virtual room.

- 6 Click **Save**.
-

DYNAMICALLY CASCADING MULTIPLE MVPs FOR A SINGLE CONFERENCE

To allow an existing endpoint-initiated ad hoc meeting to grow beyond the size of a single MVP, you can instruct iCM to dynamically cascade additional MVPs to this meeting when the number of available ports on the MVP reaches the value you define.

On reaching this value, iCM creates a new meeting on another MVP when a new call joins the meeting. iCM then cascades this new meeting to the original meeting.

Dynamic cascading is only available for video meetings using MVPs. An endpoint-initiated ad hoc audio meeting will only grow to the size of a single MCU blade.



Procedure

- 1 Select **System Configuration > Scheduling Settings** in the iVIEW Suite Configuration Tool interface.
 - 2 Enter a positive number in the Reserve Port on MVP for dynamic cascading field.
We recommend 1 or 2 ports.
 - 3 Click **Save**.
-

MODIFYING ICM DEFAULT MEETING SETTINGS



Procedure

- 1 Select **System Configuration > Scheduling Settings** in the iVIEW Suite Configuration Tool interface.
- 2 Select **Use MCU Meeting ID** to work with the MCU conference ID instead of the iCM conference ID.
This option is meant to work when iCM and ECS are not working in authorization mode, and all meetings dial out to their meeting participants.
- 3 Enter a value for the number of characters allowed in meeting ID strings in the Meeting ID Length field.

- 4 Enter a numeric value for the meeting prefix in the Meeting ID Prefix field.

The prefix must be shorter than the number specified in the Meeting ID Length field.
- 5 Enter a value in minutes in the Duration of Endpoint Initiated Calls field to set the duration of endpoint-initiated calls.

The default value is 30 minutes. iCM uses this value in resource allocation and meeting creation.
- 6 Select **Dial-in** or **Dial-out** from the Default Dialing Mode list.

If you select Dial-in, meeting participants enter a meeting by dialing into the meeting.

If you select Dial-out, the iCM system dials out to meeting participants.
- 7 Select **Remove ad hoc participants when disconnected from conference** to enable ad hoc participants not on the original invited list to be removed from the In-Meeting Control screen after they disconnect.

This is useful for endpoint initiated ad-hoc conference where iCM will remove a participant from the conference list when the participant disconnects.

If you deselect this field, and disconnected participants remain in the In-Meeting Control participant list, such participants still use MCU ports even though they are no longer connected. This option is useful for managed conferences where a meeting operator can determine which disconnected participants should be removed from the meeting and do so manually.
- 8 Enter a value in minutes in the Launch Meetings <n> Minutes before scheduled start field to specify the amount of time prior to the scheduled start of a meeting that the meeting actually begins.

If the early start attempt fails, iCM attempts to create this meeting again at the regular scheduled start time.
- 9 Select **Delete meetings older than** and enter a value in days up to a maximum of 9999 days to define the length of time a meeting appears in the iVIEW Suite web interface.
- 10 Enter a value in minutes in the Meeting Auto Extend Length field to define the length of time that a meeting can be extended after the scheduled end of the meeting,.

- 11 Select **Waiting Room Timeout** and enter a value in the <n> Minutes After The Waiting Room Start field to define the length of time a meeting can remain in Waiting Room mode until the meeting host joins. The meeting ends if the host does not join within the specified time.
 - 12 Enter a value in the Maximum Length of Meeting Extension field to specify the maximum length of time that you want to allow for extending a meeting.
The maximum values that iCM allows are 10 days, 240 hours and 14400 minutes.
 - 13 Click **Save**.
-

MODIFYING DEFAULT RECURRING MEETING SETTINGS



You can modify the default number of days in advance that a recurring meeting can be scheduled.

Procedure

- 1 Select **System Configuration > Scheduling Settings** in the iVIEW Suite Configuration Tool interface.
 - 2 Enter a value in days in the Schedule Recurring Meetings field.
The maximum value is 730 days (2 years).
 - 3 Click **Save**.
-

HIDING iCM USER INTERFACE SCREENS

You can simplify the iCM web interface by defining which screens in the following sections of the iCM user interface are hidden from administrators and users.

- IP Topology in Admin > Network Management.
- Gatekeeper Definition > Gatekeeper/SIP server tab in Admin > Resource Management > Gatekeeper/SIP server.
- Gateway Definition tab in Admin > Resource Management.
- ISDN Topology tab in Admin > Network Management. The ISDN Topology tab is only displayed when the gateway is enabled.
- Terminal Definition tab in Admin > Resource Management.
- Meeting Monitoring section accessible via the Admin sidebar menu.
- User Management section accessible via the Admin sidebar menu.

- Advanced Settings section accessible via the Admin sidebar menu.
- Other Settings tab in the Scheduling a New Meeting and in Meeting Details windows.
- Customization Tool button on upper-right of the application window that provides access to the Customization Tool window in which you can customize terminology in the iCM web interface.
- Meeting Scheduling and Virtual Room sections accessible via the User sidebar menu.
- My Meetings section accessible via the User sidebar menu.



Procedure

- 1 Select **System Configuration > UI Settings** in the iVIEW Suite Configuration Tool interface.
 - 2 Select the screens you wish to show.
 - 3 Deselect the screens you wish to hide.
 - 4 Click **Save**.
-

HOW TO MANAGE CUSTOM TIME ZONES

- [Selecting a Time Zone Profile](#) on page 145
- [Viewing a Time Zone Profile](#) on page 146
- [Adding Daylight Saving to a Time Zone Profile](#) on page 146
- [Creating a Customized Time Zone Profile](#) on page 147
- [Removing a Customized Time Zone Profile](#) on page 147
- [Reverting to Default Time Zone Settings](#) on page 148

SELECTING A TIME ZONE PROFILE

Only selected time zones are displayed in the web interface in the user, terminal, and meeting time zone fields. You can define a subset of all available time zones in the Selected Time Zones list. This enables you to expose only the relevant time zones to the end users in the web interface.



Procedure

- 1 Select **System Configuration > Customized Settings** in the iVIEW Suite Configuration Tool interface.
- 2 Select a time zone in the Available Time Zones list.

- 3 Click the right-pointing arrow to move the time zone to the Selected Time Zones list.
 - 4 Click **Save**.
-

VIEWING A TIME ZONE PROFILE



Procedure

- 1 Select **System Configuration > Customized Settings** in the iVIEW Suite Configuration Tool interface.
 - 2 Double-click a time zone in either the Available Time Zones list or the Selected Time Zones list.
-

ADDING DAYLIGHT SAVING TO A TIME ZONE PROFILE



Procedure

- 1 Select **System Configuration > Customized Settings** in the iVIEW Suite Configuration Tool interface.
 - 2 Double-click a time zone in either the Available Time Zones list or the Selected Time Zones list.
 - 3 Select **Observer Daylight Saving**.
 - 4 Add a daylight saving duration in minutes.
 - 5 Configure daylight saving start and end dates and times.
 - 6 Click **Save**.
-

CREATING A CUSTOMIZED TIME ZONE PROFILE



Procedure

- 1 Select **System Configuration > Customized Settings** in the iVIEW Suite Configuration Tool interface.
 - 2 Click **New** below either the Available Time Zones list or the Selected Time Zones list.
 - 3 Enter a name and time difference from GMT for the new time zone. You cannot change a time zone name you have saved in the time zone profile.
If you create a custom time zone profile that has the same name as a default time zone profile, the new custom profile overrides the settings of the default time zone.
 - 4 (Optional) Select **Observer Daylight Saving**.
 - 5 (Optional) Add a daylight saving duration in minutes.
 - 6 (Optional) Configure daylight saving start and end dates and times.
 - 7 Click **Save**.
-

REMOVING A CUSTOMIZED TIME ZONE PROFILE



Procedure

- 1 Select **System Configuration > Customized Settings** in the iVIEW Suite Configuration Tool interface.
 - 2 Select a custom defined time zone from either the Available Time Zones list or the Selected Time Zones list.
 - 3 Click **Remove** below the Available Time Zones list or the Selected Time Zones list.
 - 4 Click **Yes**.
 - 5 Click **Save**.
-

You can remove a time zone profile that you have added to either the Available Time Zones list or the Selected Time Zones list.

REVERTING TO DEFAULT TIME ZONE SETTINGS

You can undo your changes if you have not yet clicked Save.



Procedure

- 1 Select **System Configuration > Customized Settings** in the iVIEW Suite Configuration Tool interface.
 - 2 Move, modify or create time zone profiles.
 - 3 Click **Reset** to undo your changes.
-

CUSTOMIZING PRODUCT AND VENDOR LOGOS

You can change the iCM product logo via Admin > Advanced Settings > Look and Feel.



Procedure

- 1 Select **System Configuration > Customized Settings** in the iVIEW Suite Configuration Tool interface.
 - 2 Enter the name of a file that contains the logo in the Product logo file name field, or click **Browse** to select the file.
The logo must be a .gif file with a maximum height of 45 pixels and a maximum width of 250 pixels.
 - 3 Enter a URL for the company that provides the branded logo and can authorize its use in the URL field.
 - 4 Select **Reset to Default** to restore the default vendor logo.
 - 5 Click **Save**.
-

CREATING A CUSTOMIZED BILLING FIELD



Procedure

- 1 Select **System Configuration > Customized Settings** in the iVIEW Suite Configuration Tool interface.
 - 2 Select a display rule for your billing field from the Billing Code Field Property list.
 - 3 Select **Customized Field Label** and enter a name for your billing field in the text box that becomes active.
 - 4 Enter the maximum number of characters allowed in your billing field in the Field Length field.
 - 5 Select **Enforce Full Length** to restrict the length of your billing field to the value set in the Field Length field.
 - 6 Select an input type for your billing field from the Field Type list.
 - 7 Enter an identifier for your billing field in the Field Value field.
 - 8 Click **Save**.
-

DEFINING DATABASE SERVER SETTINGS



Procedure

- 1 Select **System Configuration > Database Settings** in the iVIEW Suite Configuration Tool interface.
- 2 Enter the default database server name in the Server name field.
The port number in use by the database server automatically appears in the Server Port field.
- 3 Enter the account name used by iCM to connect to the database in the Connection Account field.
“Root” appears by default.
- 4 Enter a password in the Connection Password field for use by iCM when a connection to the database server is established.

- 5 Click **Test** to verify that the database configuration is correct. A message window shows the test results.
 - 6 Click **Reset** to revise your configured database server settings.
 - 7 Click **Save**.
 - 8 Restart iCM to apply your changes.
-

HOW TO DEFINE SECURITY SETTINGS

- [Defining Password Settings](#) on page 150
- [Defining a Login Message](#) on page 151
- [Unlocking a User Account](#) on page 151

DEFINING PASSWORD SETTINGS



Procedure

- 1 Select **System Configuration > Security Settings** in the iVIEW Suite Configuration Tool interface.
 - 2 (Optional) Select **Display password in user profile** and **Modify password in user profile** as required.
 - 3 (Optional) Select **Allow only secure passwords** if required.
 - 4 (Optional) Define the minimum allowed password length, password validity period, and number of allowed login attempts in the relevant fields.
 - 5 (Optional) Enter the number of previous passwords that are considered when processing a new password in the **Cannot be the same as the last <n> password(s)** field.
 - 6 Click **Save**.
-

DEFINING A LOGIN MESSAGE



Procedure

- 1 Select **System Configuration** > **Security Settings** in the iVIEW Suite Configuration Tool interface.
 - 2 Select **Display login message** and enter a login message in the text box that becomes active.
 - 3 Click **Save**.
-

UNLOCKING A USER ACCOUNT



Procedure

- 1 Select **System Configuration** > **Security Settings** in the iVIEW Suite Configuration Tool interface.
 - 2 Enter the login ID of the locked user account in the Please enter the User ID that you want to unlock field.
 - 3 Click **Unlock**.
 - 4 Click **Save**.
-

HOW TO CONFIGURE SNMP TRAP SERVER PROFILES

- [Adding an SNMP Trap Server Profile](#) on page 152
- [Modifying an SNMP Trap Server Profile](#) on page 152
- [Removing an SNMP Trap Server Profile](#) on page 153

ADDING AN SNMP TRAP SERVER PROFILE



Procedure

- 1 Select **System Configuration > SNMP Trap Servers Settings** in the iVIEW Suite Configuration Tool interface.
 - 2 Enter the required IP address for the SNMP trap server in the Server IP Address field.
 - 3 Enter the port used by the SNMP trap server in the Server Port field.
 - 4 Click **Add**.
 - 5 Click **Save** at the bottom of the screen.
 - 6 Click **Yes**.
-

MODIFYING AN SNMP TRAP SERVER PROFILE



Procedure

- 1 Select **System Configuration > SNMP Trap Servers Settings** in the iVIEW Suite Configuration Tool interface.
 - 2 Select the SNMP trap server entry that you want to modify.
 - 3 Enter the new SNMP trap server IP address and port number as required.
 - 4 Click **Edit**.
 - 5 Click **Save** at the bottom of the screen.
 - 6 Click **Yes**.
-

REMOVING AN SNMP TRAP SERVER PROFILE



Procedure

- 1 Select **System Configuration > SNMP Trap Servers Settings** in the iVIEW Suite Configuration Tool interface.
 - 2 Select the SNMP trap server that you want to remove.
 - 3 Click **Delete**.
You cannot delete a server if it is the only server in the list.
 - 4 Click **Save** at the bottom of the screen.
 - 5 Click **Yes**.
-

DEFINING UTILIZATION THRESHOLDS

You can define any of the following threshold limits:

- Utilization threshold for MCU audio ports
- Utilization threshold for MCU video ports
- Utilization threshold for Gateway ports
- Utilization threshold for SCOPIA Desktop ports
- Utilization threshold for net bandwidth



Procedure

- 1 Select **System Configuration > SNMP Trap Servers Settings** in the iVIEW Suite Configuration Tool interface.
 - 2 Locate the Utilization Threshold Settings section.
 - 3 Enter the required values in the relevant threshold fields.
 - 4 Click **Save** at the bottom of the screen.
 - 5 Click **Yes**.
-

HOW TO DEFINE CALL DATA RECORD (CDR) SETTINGS

iCM creates and stores Call Data Records (CDRs) in XML format. CDRs contain comprehensive records of each call. These records are useful for analyzing and tracking system use, as well as for supporting diagnostics and billing.

- [Creating CDR Information in XML Format](#) on page 154
- [Defining Required Terminal Connection Duration](#) on page 154
- [Defining a CDR File Prefix](#) on page 155
- [Defining How Often CDRs Are Produced](#) on page 155
- [Enabling Streaming to a RADIUS Server](#) on page 156

CREATING CDR INFORMATION IN XML FORMAT



Procedure

- 1 Click **CDR Configuration** in the iVIEW Suite Configuration Tool interface.
 - 2 Select **Enable XML CDR**.
 - 3 Enable CDRs for meeting scheduling, rescheduling and/or cancellation.
 - 4 Click **Save**.
-

DEFINING REQUIRED TERMINAL CONNECTION DURATION



Procedure

- 1 Click **CDR Configuration** in the iVIEW Suite Configuration Tool interface.
- 2 Enter a value in seconds in the Minimum connection required to produce CDR field for the minimum length of time a terminal must be

connected before an entry for that terminal is created in the Actual Information section of the CDR.

If the terminal is connected to a meeting for the specified minimum time or longer, the CDR records the actual connection time as the total connection time for that terminal.

If a terminal is connected to a meeting for less than the specified minimum time, the CDR records the total connection time for that terminal as zero.

- 3 Click **Save**.
-

DEFINING A CDR FILE PREFIX

A standard iCM installation creates a directory called iCM in the Program Files directory. For example, C:\Program Files\RADVISION iVIEW Suite\iCM.

CDR files are stored in a default sub-directory called cdrdata. For example, C:\Program Files\RADVISION iVIEW Suite\iCM\cdrdata\cdrfilename.xml.



Procedure

- 1 Click **CDR Configuration** in the iVIEW Suite Configuration Tool interface.
 - 2 Enter a prefix in the File prefix name field.
The prefix appears at the beginning of the CDR file name.
The default prefix is “cdr”.
 - 3 Click **Save**.
-

DEFINING HOW OFTEN CDRs ARE PRODUCED



Procedure

- 1 Click **CDR Configuration** in the iVIEW Suite Configuration Tool interface.
- 2 Select **One file per meeting** to create one CDR file for each meeting occurrence.

How to Define Call Data Record (CDR) Settings

- 3 Select **One file every day** to create a CDR file containing information for every scheduled meeting within a 24-hour period.
This is the default selection.
 - 4 Click **Save**.
CDR file names are labeled by date, followed by a sequential identifier. Filename suffixes are sequential regardless of how often a CDR is produced, and even if a different CDR production-time option is selected.
-

ENABLING STREAMING TO A RADIUS SERVER



Procedure

- 1 Click **CDR Configuration** in the iVIEW Suite Configuration Tool interface.
- 2 Select **Use RADIUS server**.
- 3 Define the RADIUS server IP address and port in the relevant fields.
- 4 Enter a password for the RADIUS server in the Shared Secret field.
iCM and the RADIUS server exclusively use the shared secret password as part of the security system.
- 5 Click **Save**.

If you do not select **Use RADIUS server**, the IP Address, Port and Shared Secret fields include read-only information by default.

20

CONFIGURING iVIEW SUITE REDUNDANCY

- [Introduction](#) on page 157
- [Sample Configuration](#) on page 158
- [Defining Parameter Settings in Configuration Files](#) on page 160
- [How to Configure Failover for Microsoft OCS 2007 Deployments](#) on page 165
- [Maintaining Consistency Between Live and Backup Servers](#) on page 167

INTRODUCTION

iVIEW Suite supports a 1+1 redundant deployment to provide high availability. The live iVIEW Suite server will be active, and the backup iVIEW Suite server will be in standby mode. Once a failure is detected, the backup iVIEW Suite server will become active, and the live iVIEW Suite server will be in standby mode after it recovers. The redundant deployment is symmetrical—there is no set live or backup server. The first iVIEW Suite server that finishes initialization process is the live server.

iVIEW Suite redundant deployment has the following characteristics and limitations:

- iVIEW Suite redundant deployment supports software failure of the iVIEW Suite service on the live server.
- iVIEW Suite redundant deployment supports hardware failure of the live server.
- iVIEW Suite redundant deployment supports network failure of the live server.

Sample Configuration

- The live and backup iVIEW Suite servers must be deployed on the same subnet.
- The live iVIEW Suite server will ping the Gateway to detect if it can connect to the network. If connection to the network is lost, the live iVIEW Suite server will reset itself in standby mode, and the backup iVIEW Suite server will take over.
- iVIEW Suite redundant deployment must work with a standalone ECS gatekeeper. In order to avoid single point of failure, redundant ECS deployment is also recommended when working with redundant iVIEW Suite deployment.
- Failover from the live iVIEW Suite server to the backup iVIEW Suite service is automatic. When failover takes place,
 - Users who are currently logged in to the Web interface need to log in again.
 - Existing H.323 calls are not affected since the SIP B2BUA component is hosted on the same server as the standalone iVIEW Suite. Failure of the live iVIEW Suite server causes an interruption of existing SIP calls.
 - After the live iVIEW Suite server has failed, and before the backup iVIEW Suite server is live, new calls cannot connect. Once the backup iVIEW Suite server is operational, new calls can connect again.

SAMPLE CONFIGURATION

This example uses two servers, each using a single NIC with an IP address. Assume iVIEW Suite Server A's IP address is 192.168.225.116, and iVIEW Suite Server B's IP address is 192.168.225.117.

Apply another unused IP address to be configured by iVIEW Suite to work as a public/virtual IP address. Users use this IP address to access the iVIEW Suite user interface. You could also bind this IP address to a DNS name. Assume the public IP address is 192.168.225.48.

We assume that the iVIEW Suite is installed under
C:\Program Files\RADVISION\iVIEW Suite\iCM.

In this example, we use `INSTALL_DIR` to refer to this directory.

SETUP

When you install iVIEW Suite, note the follow points:

- Installation Type—Do not select the iVIEW Suite with internal gatekeeper option, and use same the same installation type for the two servers.
- User Provisioning—Select the same user provisioning options on the two servers.
- iVIEW Suite Server Port—Select the same web server port on the two servers.
- iVIEW Suite Server Host Name—Set the same host name on the two servers. The host name should bind to the virtual IP address. End users can use the host name to access the server.
- Database Server—Select MSDE/MS-SQL for both iVIEW Suite instances.
- iVIEW Suite Database Information—Use different database names on the same database server for both iVIEW Suite instances.
- iVIEW Suite Database Account Login Information—Use different login IDs and passwords for the two iVIEW Suite instances.
- iVIEW Suite Account Login Information—Use the same login ID, password and email address on both servers.

AFTER iVIEW SUITE INSTALLATION

After finishing your iVIEW Suite installation, perform the following steps:



Procedure

- 1 Log in to the two servers separately and select the same User Provisioning option.
This screen is available after your initial login to iVIEW Suite. Perform the configuration of the two servers before they become live and backup instances. Once the two servers are configured as live and backup instances, the Web interface of the backup instance is no longer accessible.
- 2 Duplicate the configuration of the Configuration Tool on both iVIEW Suite instances.

- 3 Update the license with the same ports count for both servers.

If you have two NICs at the server, you should bind the license to the specify NIC. For example; if iVIEW Suite Server A has two NICs, the IP address for NIC 1 is 192.168.225.116, and for NIC 2 is 192.168.225.202. To configure 192.168.225.116 to work for a cluster, bind the iVIEW Suite license to NIC 1.

DEFINING PARAMETER SETTINGS IN CONFIGURATION FILES

This section describes how to configure the following files:

- [ha.xml](#) on page 160
- [vnex.properties](#) on page 162
- [vcs-core.properties](#) on page 164
- [mssql-ds.xml](#) on page 164

HA.XML

ON IVIEW SUITE SERVER A



Procedure

- 1 Open ha.xml INSTALL_DIR\jboss\bin in a text editor.

```
<config>
  <UDP
    bind_addr="${jgroups.bind_addr:192.168.225.116}"
    bind_port="7800"
    ip_mcast="false"
    tos="8"
    ucast_rcv_buf_size="20000000"
    ucast_send_buf_size="640000"
    mcast_rcv_buf_size="25000000"
    mcast_send_buf_size="640000"
    loopback="true"
    discard_incompatible_packets="true"
    max_bundle_size="64000"
    max_bundle_timeout="30"
    use_incoming_packet_handler="true"
```

```

use_outgoing_packet_handler="false"
ip_ttl="${jgroups.udp.ip_ttl:2}"
down_thread="false" up_thread="false"
enable_bundling="true" />
<PING timeout="2000"
down_thread="false" up_thread="false"
initial_hosts="${jgroups.tcpping.initial_hosts:
192.168.225.116[7800],192.168.225.117 [7800]}"
port_range="1"
num_initial_members="2" />
/>

```

-
- 2 Change the value of the *bind_addr* property to the IP address of the iVIEW Suite Server A.
 - 3 Change the *initial_hosts* to contain the IP addresses of the two servers.
 - 4 Ensure that port 7800 is not used on the two machines. If not so, select an unused port, and change above 7800 to use the selected port.
-

ON IVIEW SUITE SERVER B



Procedure

- 1 Open ha.xml in INSTALL_DIR\jboss\bin in a text editor.
- 2 Make the changes as described in the [On iVIEW Suite Server A](#) section on page 160.

```

<config>
  <UDP
    bind_addr="${jgroups.bind_addr:192.168.225.117}"
    bind_port="7800"
    ...
  <PING timeout="2000"
    down_thread="false" up_thread="false"
    initial_hosts="${jgroups.tcpping.initial_hosts:
192.168.225.116 [7800],192.168.225.117[7800]}"

```

Defining Parameter Settings in Configuration Files

- 3 The value of the *bind_addr* is the IP address of this machine.
 - 4 The *initial_hosts* contain the IP addresses of the two servers.
 - 5 Ensure the two servers use the same port.
-

VNEX.PROPERTIES

ON IVIEW SUITE SERVER A



Procedure

- 1 Open `vnex.properties` in `INSTALL_DIR\jboss\bin`.
- 2 Check the following properties according the example.
- 3 If the `vnex.properties` file does not contain these properties, add the following lines:

```
vnex.config.clustering=enabled
vnex.clustering.gateway=192.168.225.254
vnex.clustering.local.ip=192.168.225.116
vnex.clustering.virtual.ip=192.168.225.48
vnex.clustering.mask=255.255.255.0
```

ON IVIEW SUITE SERVER B



Procedure

- 1 Open `vnex.properties` in `INSTALL_DIR\jboss\bin`.
- 2 Check the following properties according the example.

- 3 If the `vnex.properties` file does not contain these properties, add the following lines:

```
vnex.config.clustering=enabled
vnex.clustering.gateway=192.168.225.254
vnex.clustering.local.ip=192.168.225.117
vnex.clustering.virtual.ip=192.168.225.48
vnex.clustering.mask=255.255.255.0
```

Property	Description	Default
<code>vnex.config.clustering</code>	Enable or disable the clustering. Its value can be disabled or enabled.	Disabled
<code>vnex.clustering.gateway</code>	This is the IP address with which the machine ping the connection to the network. It is better to use the IP address of the network default gateway. When there is no network default gateway, use the IP address of a server on the network that is always online. Configure the two machines with the same IP address.	No
<code>vnex.clustering.local.ip</code>	The local IP address. The virtual IP will bind to the network interface card that this local IP address bind to.	If no local IP address is defined, the virtual IP will be bound to the first network interface card.
<code>vnex.clustering.virtual.ip</code>	The virtual IP address that used by the users to access iVIEW Suite.	No
<code>vnex.clustering.mask</code>	The network mask.	255.255.255.0

VCS-CORE.PROPERTIES

ON BOTH
iVIEW SUITE
SERVERS



Procedure

- 1 Open vcs-core.properties in INSTALL_DIR\jboss\bin separately.
 - 2 Add the following line if it is not already present.
`vnex.vcms.core.startResourceActionListener=false`
 - 3 If it is present, change its value to false (as above).
-

MSSQL-DS.XML



Procedure

- 1 On the iVIEW Suite Server B, open mssql-ds.xml in INSTALL_DIR\jboss\server\default\deploy.
- 2 Change the connection URL and the database user name and password to be the same as that in iVIEW Suite Server A.

This allows iVIEW Suite Server B to use the database used by iVIEW Suite Server A.

For example

```
<connection-url>jdbc:microsoft:sqlserver:  
//192.168.225.198:1433;DatabaseName=icm_failover_M;  
SendStringParametersAsUnicode=  
false</connection-url>  
<user-name>icm_failover_M</user-name>  
<password>DES:DtlbXegPQnnRal00oetTOvs=</password>
```

Note CDR files are stored separately in INSTALL_DIR\cdrdata on the live and backup servers when CDR is enabled in the Configuration Tool.

HOW TO CONFIGURE FAILOVER FOR MICROSOFT OCS 2007 DEPLOYMENTS

The iVIEW Suite plug-in for Microsoft Office Communicator Server (OCS) 2007 enables OCS users to join MCU conferences.

This section describes how to configure the failover mechanism for Microsoft OCS 2007 Connector deployments.

For more information about the iVIEW Suite plug-in for OCS 2007, see the iVIEW Suite for Microsoft Office Communicator Server 2007 Deployment Guide.

- [Configuring iVIEW Suite Servers for OCS Failover](#) on page 165
- [Configuring the MCU for OCS Failover](#) on page 165
- [Configuring the OCS 2007 Server for Failover](#) on page 166
- [Configuring the OCS 2007 Client for Failover](#) on page 166

CONFIGURING iVIEW SUITE SERVERS FOR OCS FAILOVER



Procedure

- 1 Use a text editing tool to open the tab.xml file for both iVIEW Suite servers located by default under
`C:\Program Files\RADVISION\iVIEW Suite\iCM\jboss\server\default\deploy\vcs.ear\ocs.war\jsp\oc`
 - 2 Add the virtual host name for each iVIEW Suite server.
 - 3 Save and close each tab.xml file.
-

CONFIGURING THE MCU FOR OCS FAILOVER



Procedure

- 1 Go to MCU > Protocols > SIP in the MCU web user interface.
- 2 Select **Enable SIP protocol**.
- 3 Select **Using Microsoft OCS**.

- 4 Enter the virtual IP address of the iVIEW Suite server in the Specify address field.
 - 5 Click **OK** to save your changes.
-

CONFIGURING THE OCS 2007 SERVER FOR FAILOVER



Procedure

- 1 Go to Administrative Tools > Office Communicator 2007 in the OCS 2007 user interface.
 - 2 Expand the Standard Edition Servers tree view.
 - 3 Right click **rvcn-ocs2007.ocs2007.com** and select **Properties > Front End Properties**.
 - 4 Click the **Routing** tab and add the virtual IP address of the iVIEW Suite server in OCS 2007.
 - 5 Click **OK**.
 - 6 Click the **Host Authorization** tab and add the following IP addresses:
 - The IP address of Server A
 - The IP address of Server B
 - The virtual IP address of the iVIEW Suite server
 - The IP address of the MCU
 - 7 Click **OK** to save your changes.
-

CONFIGURING THE OCS 2007 CLIENT FOR FAILOVER



Procedure

- 1 Locate the ocs2007.reg registry file on the RADVISION Utilities and Documentation CD-ROM supplied with the product.
- 2 Open the file with a text editing tool.
- 3 Add the virtual host name.
- 4 Save and close the ocs2007.reg file.

- 5 Run the ocs2007.reg file.
 - 6 Go to Internet Explorer and confirm that the iVIEW Suite server is added as a trusted site. If not, manually add the iVIEW Suite server as a trusted site.
-

MAINTAINING CONSISTENCY BETWEEN LIVE AND BACKUP SERVERS

The backup iVIEW Suite instance is automatically set to waiting mode when the live instance is running. When in waiting mode, the Web interface of the backup instance is not accessible. The Configuration Tool interface is available.

Any changes to the Configuration Tool of the live instance must be reflected in the Configuration Tool of the backup instance.

Any changes to the system settings in the Web interface of the live instance are automatically synchronized in the backup instance.

Since the license is bound to the MAC address of the server NIC, the license for the live instance and backup instance are different. Individually update the licenses for the live and backup instances.

Maintaining Consistency Between Live and Backup Servers

21

ICM CDR XML TAGS AND ATTRIBUTES

The production and storage of Call Data Records (CDRs) in iCM is enabled via the iVIEW Suite Configuration Tool. A CDR file is generated each day by default.

CDR records are saved in XML format and provide comprehensive records of each call which can then be used for analysis of the system for diagnostic and billing purposes.

This section details the XML tags used to label data in the stored CDR .xml file, the attributes of each configurable tag, and the order in which the tags are arranged.

- [Accessing the CDR XML Files](#) on page 170
- [Index of CDR XML Tags](#) on page 170
- [Understanding the CDR XML Tags](#) on page 182

Note All references to “VCS” in this section are equivalent to “iVIEW Communications Manager”.

ACCESSING THE CDR XML FILES



Procedure

- 1 Select **Programs > iVIEW Suite > CDR files** from the Windows Start menu.
- 2 Open the relevant CDR file.

The information configured to appear is listed within the tags. For a list of the XML tags that can appear in the CDR, see the [Index of CDR XML Tags](#) section on page 170.

INDEX OF CDR XML TAGS

This section contains a list of all XML tags in the CDR, listed in their hierarchical relationship to each other.

Note In the tags, “conference” is equivalent to “meeting”, and “service” is equivalent to “meeting type”.

Table 21-1 *Index of CDR XML Tags*

<conferences>

<ConferenceData>

<Event>

<Scheduling-Data>

<Conference>

<Basic-Information>

<Conference-ID />

<Virtual-Conference-ID />

<Master-Conference-ID />

<Slave-Conference-ID-List>

<Slave-Conference-ID />

<Slave-Conference-ID-List />

<Subject />

<Reference-Code />

<Description />

<MultiPoint-PointToPoint />

<Scheduled-Adhoc />

<Start-Time />

<Duration />

<Server-TimeZone />

<Auto-Extend />

<Bill-To/>

<Billing-Code/>

<Basic-Information/>

<Advanced-Information>

<Extra-Ports-Reserved>>

<Priority />

<DateTime-Scheduled />

<DateTime-Cancelled />

<Streaming-Recording-Activated/>

<Export-Upon-Completion/>

<Streaming-Target-File-Name/>

<Streaming-Recording-View/>

<Advanced-Information/>

<Conference-Lifecycle-Summary>

<Resources-Scheduled>

<DateTime-Modified />

<Total-IP-Bandwidth />

<Total-ISDN-Bandwidth />

<Total-MCU-Connections-Number />

<Total-GW-Connections-Number />

</Resources-Scheduled>

</Conference-Lifecycle-Summary>

</Conference>

<Resources>

<Conference-Service>

<Service-Id />

<MCU-Service-Prefix />

<Min-Video-Layout />

<Max-Video-Layout />

<Max-Bit-Rate-In />

<Max-Bit-Rate-Out />

<Max-Frame-Rate-In />

<Max-Frame-Rate-Out />

<Max-Picture-Format-In />

<Max-Picture-Format-Out />

<Max-T120-Ports-Reserved />

<Max-Subconferences />

</Conference-Service>

<Resources-Scheduled-At-Time-Of-Conference>

<Total-IP-Bandwidth />

<Total-ISDN-Bandwidth />

<Total-MCU-Connections-Number />

<Total-GW-Connections-Number />

</Resources-Scheduled-At-Time-Of-Conference>

<Resources>

<Attendees-Terminals>

<Host>

<User-Id />

<Login-Id />

<First-Name />

<Last-Name />

<Email />

<Customer-Id />

<Company-Name />

<Customer-Profile-Type />

<Customer-Billing-Phone />

<Is-Controller />

</Host>

Index of CDR XML Tags

<Organizer>

<User-Id />

<Login-Id />

<First-Name />

<Last-Name />

<Email />

<Customer-Id />

<Company-Name />

<Customer-Profile-Type />

<Customer-Billing-Phone />

<Is-Controller />

</Organizer>

<Predefined-Attendees>

<Predefined-Attendee>

<User-Id />

<Login-Id />

<First-Name />

<Last-Name />

<Email />

<Customer-Id />

<Company-Name />

<Customer-Billing-Phone />

<Is-Controller />

</Predefined-Attendee>

</Predefined-Attendees>

<External-Attendees>

<External-Attendee>

<Email />

<First-Name />

<Last-Name />

</External-Attendee>

</External-Attendees>

<Predefined-Terminals>

<Predefined-Terminal>

<Terminal-Id />

<Alias />

<Dial-String />

<IP-ISDN-SIP />

<Dial-in-Dial-out />

<MCU />

<Gateway />

<Room />

<Gatekeeper />

<Zone-Prefix />

</Predefined-Terminal>

</Predefined-Terminals>

<External-Terminals>

<External-Terminal>

<Party-ID/>

<Name />

<Dial-String />

<IP-ISDN-SIP />

<Dial-in-Dial-out />

<MCU />

<Gateway />

<Room />

<Gatekeeper />

<Zone-Prefix />

<Desktop-Client/>

<Desktop-Server/>

<External-Terminal>

<External-Terminals>

<Attendees-Terminals-Association>

<Association />

</Attendees-Terminals-Association>

</Attendees-Terminals>

<Network-Devices>

<GKs>

<GK-Proxy-Information>

<ID />

<Name />

<Model />

<IP-Address />

<Zone-Prefix />

<SIP-Domain />

<GK-Device-Association>

<Association />

</GK-Device-Association>

</GK-Proxy-Information>

</GKs>

<MCUs>

<MCU-Information>

<ID />

<Alias />

<Model />

<Master-Slave />

<Zone-Prefix />

<Gatekeeper />

<Service-Prefix />

<List-of-Assigned-Terminals>

<Terminal />

</List-of-Assigned-Terminals>

Index of CDR XML Tags

</MCU-Information>

</MCUs>

<GateWays>

<Gateway-Information>

<ID />

<Phone-Number />

<Service-Prefix />

<Service-Bandwidth />

<Country-Code />

<Area-Code />

<Zone-Prefix />

<Terminal-Gateway-Association>

<Association />

</Terminal-Gateway-Association>

</Gateway-Information>

</GateWays>

<Rooms>

<Room-Information>

<ID />

<Name />

<Terminal-Room-Association>

<Terminal />

</Terminal-Room-Association>

<Room-Information>

<Rooms>

</Network-Devices>

</Scheduling-Data>

<Completed-Conference-Data>

<Conference-Status />

<Reason-Failed />

<Actual-Start-Time />

<Actual-End-Time />

<Actual-Predefined-Terminals>

<Actual-Predefined-Terminal>

<Terminal-Id />

<Alias />

<Dial-String />

<IP-ISDN-SIP />

<Source-IP-Address />

<Total-Connection-Time />

<Failing-Attempts />

<Last-Failure-Cause />

<List-of-Connection-Records />

<Connection />

<List-of-Connection-Records />

</Actual-Predefined-Terminal>

</Actual-Predefined-Terminals>

<Actual-External-Terminals>

<Actual-External-Terminal>

<Party-ID />

<Name />

<Dial-String />

<IP-ISDN-SIP />

<Desktop-Client />

<Desktop-Server />

<Total-Connection-Time />

<Failing-Attempts />

<Last-Failure-Cause />

<List-of-Connection-Records />

<Connection />

</List-of-Connection-Records >

</Actual-External-Terminal>

</Actual-External-Terminals>

<Connected-MCUs>

<MCU-information>

<ID />

<Alias />

<Model />

<Master-Slave />

<Zone-Prefix />

<Gatekeeper />

<Service-Prefix />

</ List-of-Assigned-Terminals>

</MCU-information>

<ConnectedMCUs>

<Connected-GWs>

<Gateway-information>

<ID />

<Phone-Number />

<Service-Prefix />

<Service-Bandwidth />

<Country-Code />

<Area-Code />

<Zone-Prefix />

<Terminal-Gateway-Association>

<Association />

</Terminal-Gateway-Association>

</Gateway-information>

</Connected-GWs>

</Completed-Conference-Data>

</Conference-Data>

</ conferences>

UNDERSTANDING THE CDR XML TAGS

Table 21-2 provides details about each CDR tag and includes a reference to information about configuring the tag in the CDR.

Note In the tags, “conference” is equivalent to “meeting”, and “service” is equivalent to “meeting type”.

Table 21-2 CDR XML Tag Details

Tag	Description	Attribute	Type	Example
<conferences> </conferences>	Defines the beginning of all conference data. Contains data for the conferences of an entire day or for a single conference depending on the configuration.			
<ConferenceData></ConferenceData>	Defines the beginning of data recording for a meeting instance.			
<Event></Event>	Defines the record type.	value	Schedule/ Reschedule/ Cancel/ Complete	
<Scheduling-Data></Scheduling-Data>	Contains data directly related to meeting scheduling, such as which resources are reserved and which attendees and/or terminals are invited as part of meeting scheduling.			
<Conference> </Conference>	Contains basic meeting scheduling information.			
<Basic-Information></Basic-Information>	Contains basic meeting scheduling information.			
<Conference-ID />	Contains the iVIEW Communications Manager internal ID of a specific conference.	value	String	<Conference-ID value="1307" / >

Tag	Description	Attribute	Type	Example
<Virtual-Conference-ID />	Contains the Virtual Conference ID number of a specific conference.	value	String	<Virtual-Conference-ID value="1307" />
<Master-Conference-ID />	Contains the ID used to identify the meeting on the master MCU.	value	String	<Master-Conference-ID value="N/A" />
<Slave-Conference-ID-List></Slave-Conference-ID-List>	Contains the meeting ID for a single slave MCU.			
<Slave-Conference-ID />	Contains the meeting ID for a single slave MCU.	value	Zone Number + Service Prefix ID + Physical Conference ID	<Slave-Conference-ID value="175-80-4417" />
<Subject />	Contains the meeting subject as entered during meeting scheduling.	value	String	<Subject value="Monthly Update" />
<Reference-Code />	Contains any internal department, billing, client or account numbers used to track resource use within a company, that are entered during meeting scheduling.	value	String	<Reference-Code value="A112" />
<Description />	Contains the description of the meeting, which is entered during meeting scheduling.	value	String	<Description value="N/A" />
<MultiPoint-PointToPoint />	Displays whether a multipoint meeting or a point-to-point meeting is scheduled. Possible values: Multipoint, PointToPoint.	value	String	<MultiPoint-PointToPoint value="MultiPoint" />

Understanding the CDR XML Tags

Tag	Description	Attribute	Type	Example
<Scheduled-Adhoc />	Displays whether the meeting is scheduled to start at a future time or if it is created immediately (ad hoc) via iVIEW Communications Manager or an endpoint. Possible values: Scheduled, Ad Hoc, Endpoint Initiated Ad Hoc.	value	String	<Scheduled-Adhoc value="Ad Hoc" />
<Start-Time />	Contains the scheduled start time of the meeting.	value	yyyy-mm-ddThh-mm-ssZ	<Start-Time value="2003-03-29T11:35:47Z" />
<Duration />	Contains the scheduled meeting duration.	value	String	<Duration value="30 Minutes"/>
<Server-TimeZone />	Contains time zone information of the iVIEW Communications Manager server.	value	GMT+/-XX:XX (Integer + 'Minutes')	<Server-Time Zone value="GMT+08:00"/>
<Auto-Extend />	Determines whether or not Auto Extend is selected during meeting scheduling.	value	Boolean	<AutoExtend value="true"/>
<Bill-To />	Contains information about who will be billed for the conference. Possible values: BILL_ALL_PARTICIPANTS, BILL_ORGANIZER, BILL_HOST, BILL_CONTROLLERS.	value	String	<Bill-To value="BILL_HOST"/>
<Billing-Code />	Contains the billing code relevant to the billing of the conference.	value	String	<Billing-Code value="1234" />
<Advanced-Information/></Advanced-Information>	Contains advanced meeting scheduling information.			

Tag	Description	Attribute	Type	Example
<Extra-Ports-reserved/>	Contains the number of additional ports that are reserved for the meeting during meeting scheduling	value	Integer	
<Priority />	Displays the Priority option selected during meeting scheduling. Possible values: Unspecified, Bandwidth, Delay.	value	String	<Priority value="Delay" />
<DateTime-Scheduled/>	Contains the date and time that the meeting is scheduled via the iVIEW Communications Manager.	value	yyyy-mm-ddThh-m m-ssZ	<DateTime-Scheduled value="2003-03-29T11:35:47Z" />
<DateTime-Cancelled/>	If a meeting is cancelled prior to its scheduled start time, the tag contains the date and time of cancellation.	value	yyyy-mm-ddThh-m m-ssZ	<DateTime-Cancelled value="N/A" />
<Streaming-Recording-Activated />	Indicates whether streaming recording is enabled or not.	value	Boolean	<Streaming-Recording-Activated value="false"/>
<Export-Upon-Completion-Activated/>	Indicates whether or not the recorded file should be exported upon conference completion.	value	Boolean	<Export-Upon-Completion-Activated value="false"/>
<Streaming-Target-File-Name/>	Contains the name of the recorded file, if specified by the user.	value	String	<Streaming-Target-File-Name value="N/A"/>
<Streaming-Recording-View/>	Contains the view chosen for recording.	value	String	<Streaming-Recording-View value="N/A"/>

Understanding the CDR XML Tags

Tag	Description	Attribute	Type	Example
<Conference-Lifecycle-Summary><Conference-LifeCycle-Summary/>	Contains lifecycle information for a single instance of a scheduled meeting, including basic statistics captured during meeting scheduling, as well as records of any modifications prior to the actual meeting.			
<Resources-Scheduled/>	Contains a list of resources scheduled when a meeting is created or modified.			
<DateTime-Modified/>	Contains the date and time of modification of a scheduled meeting.	value	yyyy-mm-ddThh-m m-ssZ	<DateTime-Modified value="2003-03-30T10:20:25Z" />
<Total-IP-Bandwidth/>	Contains the total amount of IP bandwidth, in Kbps, scheduled for the meeting	value	Integer	<Total-IP-Bandwidth value="768" />
<Total-ISDN-Bandwidth/>	Contains the total amount of ISDN bandwidth scheduled for a meeting, in Kbps.	value	Integer	<Total-ISDN-Bandwidth value="192"/>
<Total-MCU-Connections-Number/>	Contains the total number of MCU connections scheduled for a meeting (number of terminals, extra ports and cascading MCUs).	value	Integer	<Total-MCU-Connections-Number value="1" />
<Total-GW-Connections-Number/>	Contains the total number of Gateway connections scheduled for the conference (number of terminals and reserved ISDN ports).	value	Integer	<Total-GW-Connections-Number value="1" />
<Resources></Resources>	Contains a list of resources committed or required for a meeting.			

Tag	Description	Attribute	Type	Example
<Conference-Service></Conference-Service>	Contains a list of meeting types scheduled for use.			
<Service-Id/>	Lists the iVIEW Communications Manager ID (name) of the service selected for use during the meeting.	value	String	<Service-Id value="10045" />
<MCU-Service-Prefix />	Contains the MCU service prefix on the master MCU selected for use during the meeting.	value	String	<MCU-Service-Prefix value="80"/>
<Min-Video-Layout/>	Displays the minimal (smallest) video layout of all schemes associated with the scheduled meeting type.	value	Integer	<Min-Video-La yout value="1" />
<Max-Video-Layout/>	Displays the maximum (largest) video layout of all schemes associated with the scheduled meeting type.	value	Integer	<Max-Video- Layout value="1" />
<Max-Bit-Rate-In/>	Displays the maximum incoming video bit-rate available for the meeting type, In Kbps.	value	Integer	<Max-Bit-Rate -In value="384" />
<Max-Bit-Rate-Out/>	Displays the maximum outgoing video bit-rate available for the meeting type, in Kbps.	value	Integer	<Max-Bit-Rate -Out value="0" />
<Max-Frame-Rate-In/>	Displays the maximum incoming frame-rate available for the meeting type.	value	Integer	<Max-Frame-R ate- In value="30" />
<Max-Frame-Rate-Out/>	Displays the maximum outgoing frame-rate among all schemes available for the meeting type. Possible values: NONE, 5, 7.5, 10, 15, 25, 30, 50, 60.	value	String	<Max-Frame-R ate-Out value="30" />

Understanding the CDR XML Tags

Tag	Description	Attribute	Type	Example
<Max-Picture-Format-In/>	Displays the maximum incoming picture format available for the meeting type. Possible values: NONE, SQCIF, QCIF, SIF, CIF, VGA, 4SIF, 4CIF, SVGA, XGA, SXG A, 16CIF, UXGA, 4XGA.	value	String	<Max-Picture-Format-In value="4SIF" />
<Max-Picture-Format-Out/>	Displays the maximum outgoing picture format available for the meeting type. Possible values: NONE, SQCIF, QCIF, SIF, CIF, VGA, 4SIF, 4CIF, SVGA, XGA, SXG A, 16CIF, UXGA, 4XGA.	value	String	<Max-Picture-Format-Out value="4SIF" />
<Max-T120-Ports-Reserved />	Contains the total number of T120 ports reserved for the meeting.	value	Integer	<Max-T120-Ports-Reserved value="0"/>
<Max-Subconferences/>	Contains the number of breakout meetings (or sub-meetings) that are a part of the selected meeting type.	value	Integer	<Max-Subconferences value="0" />
<Resources-Scheduled-At-Time-Of-Conference></Resources-Scheduled-At-Time-Of-Conference>	Contains a list of resources at the time the meeting starts (including modifications made to the meeting reservation prior to the meeting start).			
<Total-IP-Bandwidth/>	Contains the total amount of IP bandwidth scheduled at the time of the meeting.	value	Integer	<Total-IP-Bandwidth value="768" />
<Total-ISDN-Bandwidth/>	Contains the total amount of ISDN bandwidth scheduled at the time of the meeting.	value	Integer	<Total-ISDN-Bandwidth value="192"/>
<Total-MCU-Connection-Number/>	Contains the total number of MCU connections scheduled at the time of the meeting.	value	Integer	<Total-MCU-Connections-Number value="5"/>

Tag	Description	Attribute	Type	Example
<Total-GW-Connections-Number />	Contains the total number of Gateway connections scheduled at the time of the meeting.	value	Integer	<Total-GW-Connections-Number value="5"/>
<Attendees-Terminals></Attendees-Terminals>	Contains lists of attendees and terminals scheduled for a conference.			
<Host></Host>	Contains information about the meeting host assigned during meeting scheduled.			
<User-Id/>	Contains the iVIEW Communications Manager ID number of the meeting host.	value	String	<User-Id value="75" />
<Login-Id />	Contains the iVIEW Communications Manager login ID of the meeting host.	value	String	<Login-Id value="Jsmith" />
<First-Name />	Contains the first name of the meeting host.	value	String	<First-Name value="Jennifer" />
<Last-Name />	Contains the last name of the meeting host.	value	String	<Last-Name value="Smith" />
<Email />	Contains the email address of the meeting host.	value	String	<Email value=jsmith@testco.com/>
<Customer-ID />	Contains the iVIEW Communications Manager customer ID of the meeting host.	value	String	<Customer-Id value="67" />
<Company-Name />	Contains the name of the company of the meeting host, which is associated with the Customer ID.	value	String	<Company-Name value="Testco" />

Understanding the CDR XML Tags

Tag	Description	Attribute	Type	Example
<Customer-Profile-Type />	Contains the customer profile-type for the company to which the meeting host belongs. For future use.	value	String	
<Customer-Billing-Phone/>	Contains the telephone number for the billing contact of the meeting host.	value	String	<Customer-Billing-Phone value="8499551" />
<Is-Controller/>	Notes whether the organizer, during meeting scheduling, granted the meeting host permission to control the meeting.	value	Boolean	
<Organizer></Organizer>	Contains information about the meeting organizer.			
<User-Id/>	Contains the iVIEW Communications Manager ID number of the meeting organizer.	value	String	<User-Id value="75" />
<Login-Id />	Contains the iVIEW Communications Manager login ID of the meeting organizer.	value	String	<Login-Id value="jsmith" />
<First-Name />	Contains the first name of the meeting organizer.	value	String	<First-Name value="Jennifer" />
<Last-Name />	Contains the last name of the meeting organizer.	value	String	<Last-Name value="Smith" />
<Email />	Contains the email address of the meeting organizer.	value	String	<Email value="jsmith@testco.com" />
<Customer-ID />	Contains the iVIEW Communications Manager customer ID of the meeting organizer.	value	String	<Customer-Id value="67" />

Tag	Description	Attribute	Type	Example
<Company-Name />	Contains the name of the company of the meeting organizer, which is associated with the Customer ID.	value	String	<Company-Name value="Testco" />
<Customer-Profile-Type />	Contains the customer profile-type for the company to which the meeting organizer belongs. For future use.	value	String	
<Customer-Billing-Phone/>	Contains the telephone number for the billing contact of the meeting organizer.	value	String	<Customer-Billing-Phone value="8499551"/>
<Is-Controller/>	Notes whether or not the organizer has permission to control the meeting.	value	Boolean	
<Predefined-Attendees></Predefined-Attendees>	Contains information about meeting attendees that are registered in the iVIEW Communications Manager.			
<Predefined-Attendee />	Contains information about a meeting attendee registered in iVIEW Communications Manager.			
<User-Id/>	Contains the iVIEW Communications Manager ID number of the attendee.	value	String	<User-Id value="75" />
<Login-Id />	Contains the iVIEW Communications Manager login ID of the attendee.	value	String	<Login-Id value="SPerkins" />
<First-Name />	Contains the first name of the attendee.	value	String	<First-Name value="Sam" />
<Last-Name />	Contains the last name of the attendee.	value	String	<Last-Name value="Perkins" />

Understanding the CDR XML Tags

Tag	Description	Attribute	Type	Example
<Email />	Contains the email address of the attendee.	value	String	<Email value="sperkins@testco.com"/>
<Customer-ID />	Contains the iVIEW Communications Manager customer ID of the attendee.	value	String	<Customer-Id value="73" />
<Company-Name />	Contains the name of the company of the attendee, which is associated with the Customer ID.	value	String	<Company-Name value="Testco" />
<Is-Controller/>	Notes whether the organizer, during meeting scheduling, granted the attendee permission to control the meeting.	value	Boolean	
<External-Attendees></External-Attendees>	Contains a list of external meeting attendees (attendees not registered to iVIEW Communications Manager).			
<External-Attendee></External-Attendee>	Contains information about an individual external meeting attendee who is not registered in iVIEW Communications Manager.			
<Email />	Contains the email address of an external meeting attendee.	value	String	<Email value="BJones@externalco.co/">
<First-Name />	Contains the first name of an external meeting attendee.	value	String	<First-Name value="Bill"/>
<Last-Name />	Contains the last name of an external meeting attendee.	value	String	<Last-Name value="Jones"/>

Tag	Description	Attribute	Type	Example
<Predefined-Terminals></Predefined-Terminals>	Contains a list of all iVIEW Communications Manager-registered terminals scheduled for the meeting.			
<Predefined-Terminal/>	Contains information about a single iVIEW Communications Manager registered terminal scheduled for the meeting.			
<Terminal-ID />	Contains the internal iVIEW Communications Manager ID string of a terminal.	value	String	<Terminal-Id value="0001-PARTY-10007" />
<Alias />	Contains the internal iVIEW Communications Manager name or the alias of a terminal.	value	String	<Alias value="T1" />
<Dial-String />	Contains the dial-string information of a terminal. For an ISDN phone number, the format is "CountryCode - AreaCode - PhoneNumber".	value	String	<Dial-String value="812518" />
<IP-ISDN-SIP />	Specifies the terminal type. Possible values: IP, ISDN, SIP.	value	String	<IP-ISDN-SIP value="IP" />
<Dial-in-Dial-out />	Contains the dialing mode of the terminal. Possible values: Dial-in, Dial-out.	value	String	<Dial-in-Dial-out value="Dial-out" />
<MCU />	Contains MCU information for an individual terminal registered to the iVIEW Communications Manager.	value	String	<MCU value="0001-MCU-10001" />
<Gateway />	Contains Gateway information for an individual terminal registered to the iVIEW Communications Manager.	value	String	<Gateway value="N/A" />

Understanding the CDR XML Tags

Tag	Description	Attribute	Type	Example
<Room />	Contains room information for a terminal registered to iVIEW Communications Manager, if that terminal is associated with a room in iVIEW Communications Manager.	value	String	<Room value="0001-ROOM-10001" />
<Gatekeeper />	Contains Gatekeeper information for an individual terminal registered to iVIEW Communications Manager.	value	String	<Gatekeeper value="001-GK-10001"/>
<Zone-Prefix />	Contains the zone prefix for an individual terminal registered to iVIEW Communications Manager.	value	String	<Zone-Prefix value="81" />
<External-Terminals></External-Terminals>	Contains a list of external terminals (terminals not registered to iVIEW Communications Manager) scheduled for the meeting.			
<External-Terminal></External-Terminal>	Contains information for an individual terminal scheduled for a meeting.			
<Party-ID/>	Contains the internal iVIEW Communications Manager ID string given to the external terminal.	value	String	<Party-Id value="EXTRA:2222" />
<Name/>	Contains the name of an external terminal as entered during meeting scheduling.	value	String	<Name value="Bob Baxton Mobile"/>
<Dial-String />	Contains the dial-string information of an external terminal. For an ISDN phone number, the format is "CountryCode - AreaCode - PhoneNumber".	value	String	<Dial-String value="8125199" />

Tag	Description	Attribute	Type	Example
<IP-ISDN-SIP />	Specifies the terminal type. Possible values: IP, ISDN, SIP.	value	String	<IP-ISDN-SIP value="IP" />
<Dial-in-Dial-out/>	Contains the dialing mode of the terminal. Possible values: Dial-in, Dial-out.	value	String	<Dial-in-Dial-out value="Dial-out" />
<MCU />	Contains MCU information of the external terminal.	value	String	<MCU value="0001-MCU-10001" />
<Gateway />	Contains Gateway information of the external terminal.	value	String	<Gateway value="N/A" />
<Room />	Contains room information of the external terminal (if relevant).	value	String	<Room value="N/A" />
<Gatekeeper />	Contains Gatekeeper information of the external terminal.	value	String	<Gatekeeper value="0001-GK-10001"/>
<Zone-Prefix />	Contains the zone prefix of the external terminal.	value	String	<Zone-Prefix value="81" />
<Desktop-Client />	Indicates whether or not this external terminal is a SCOPIA Desktop client. Only appears if value is True.	value	Boolean	<Desktop-Client value="true" />
<Desktop-Server />	Contains the internal iVIEW Communications Manager ID of the SCOPIA Desktop Server that is associated with this terminal.	value	String	<Desktop-Server value="0001-SDG-10002" />
<Attendees-Terminals-Association></Attendees-Terminals-Association />	Contains a list of attendee and terminal associations, allowing administrators to determine which users used which terminals for an individual meeting.			

Understanding the CDR XML Tags

Tag	Description	Attribute	Type	Example
<Association />	Associates an attendee with a terminal, login ID, email address, and terminal/dial string.	Dial-String, Email, LoginId	String	<Association Dial-String = "812518" Email = "Mjones@te stco.com" LoginId = "Mjones"/>
<Network-Devices> </ Network-Devices>	Contains information about network devices scheduled for use in a meeting during resource allocation.			
<GKs></GKs>	Contains a list of all gatekeepers reserved for use during a meeting.			
<GK-Proxy-Information></ GK-Proxy-Information />	Contains information about an individual gatekeeper that is reserved for use during the meeting.			
<ID />	Contains the internal gatekeeper ID in the iVIEW Communications Manager.	value	String	<ID value = "0001-GK-100 01"/>
<Name />	Contains the name of the gatekeeper in the iVIEW Communications Manager.	value	String	<Name value = "GK 58" />
<Model />	Contains gatekeeper model information.	value	String	<Model value = " ECS"
<IP-Address />	Contains the IP address of the gatekeeper.	value	String	<IP-Address value = "192.168.1.58"
<Zone-Prefix />	Contains the zone prefix of the gatekeeper.	value	String	<Zone-Prefix value = "58"/>
<SIP-Domain />	Contains the SIP domain of a gatekeeper.	value	String	<SIP-Domain = "N/A" />

Tag	Description	Attribute	Type	Example
<GK-Device-Association></GK-Device-Association>	Contains a list of gatekeeper and device associations, including all devices (terminals, MCUs, and Gateways) registered to the gatekeeper.			
<Association />	Associates an individual gatekeeper with devices registered to that gatekeeper.	Alias, E.164, device-Address, device-Type	String	<Association Alias="2509" E.164="2509" device-Address="N/A" device-Type="Terminal" />
<MCUs></MCUs>	Contains a list of all MCUs reserved for use during the meeting.			
<MCU-Information></MCU-Information>	Contains information about an individual MCU reserved for use during the meeting.			
<ID />	Contains the internal iVIEW Communications Manager ID of the MCU.	value	String	<ID value = "0001-MCU-1002" />
<Alias />	Contains the name of the MCU name in the iVIEW Communications Manager.	value	String	<Alias value="MCU82" />
<Model />	Contains model information for an individual MCU scheduled for use for the meeting.	value	String	<Model value="RADVISION MCU 3.0+" />
<Master-Slave />	Specifies whether or not this MCU is master or slave if the meeting is scheduled with cascading (set to True if the MCU served as Master in a cascaded conference).	value	String	<Master-Slave value="false" />

Understanding the CDR XML Tags

Tag	Description	Attribute	Type	Example
<Zone-Prefix />	Specifies the zone prefix of an MCU.	value	String	<Zone-Prefix value="58" />
<Gatekeeper />	Specifies the gatekeeper to which the MCU is registered.	value	String	<Gatekeeper value="0001-GK-10001" />
<Service-Prefix />	Specifies the service prefix of an MCU.	value	String	<Service-Prefix value="80" />
<List-of-Assigned-Terminals></List-of-Assigned-Terminals>	Contains a list of terminals assigned to the MCU for the meeting.			
<Terminal />	Contains information about a single terminal assigned to the MCU for the meeting. For an ISDN phone number, the format is "CountryCode - AreaCode - PhoneNumber".	Alias, Dial-String, IP-ISDN-SIP	String	<Terminal Alias="2518" Dial-String="812518" IP-ISDN-SIP="IP"/>
<Gateways></Gateways>	Contains a list of all Gateways reserved for use during the meeting.			
<Gateway-Information></Gateway-Information>	Contains information about an individual Gateway reserved for use during the meeting.			
<ID />	Contains the internal iVIEW Communications Manager ID of the Gateway.	value	String	<ID value = "0001-GW-10006" />
<Phone-Number />	Contains the Gateway phone number.	value	String	<Phone-Number value="88372361" />
<Service-Prefix />	Contains the prefix of the requested service.	value	String	<Service-Prefix value="9384" />

Tag	Description	Attribute	Type	Example
<Service-Bandwidth />	Specifies the bandwidth associated with the requested service configured on the Gateway.	value.	String	<Service-Bandwidth value="384" />
<Country-Code />	Specifies the country code of a Gateway.	value	String	<Country-Code value="86" />
<Area-Code />	Specifies the area code of a Gateway.	value	String	<Area-Code value="10" />
<Zone-Prefix />	Specifies the zone prefix of a Gateway.	value	String	<Zone-Prefix value="58" />
<Terminal-Gateway-Association ></ Terminal-Gateway-Association>	Contains a list of endpoints (terminals) assigned to the Gateway for the meeting.			
<Association />	Associates an ISDN terminal with the Gateway it will use for the meeting.	Alias, ISDN-Phone-Number, Scheduled-Service-Bandwidth, Scheduled-Service-Prefix	String, String, Integer, String	<Association Alias="ISDN002" ISDN-Phone-Number="22-55-88" Scheduled-Service-Bandwidth="64" Scheduled-Service-Prefix="9064" />
<Rooms></Rooms>	Contains a list of all rooms reserved for use during the meeting.			
<Room-Information></ Room-Information>	Contains information about an individual room reserved for use during the meeting.			
<ID />	Contains the iVIEW Communications Manager ID number of the room.	value	String	<ID value = "0001-ROOM-10003" />

Understanding the CDR XML Tags

Tag	Description	Attribute	Type	Example
<Name />	Contains the room name in iVIEW Communications Manager.	value	String	<Name value="Conference Room" />
<Terminal-Room-Association/ ></Terminal-Room-Association>	Contains a list of terminals and rooms to which they are assigned for the meeting.			
<Terminal />	Associates a room with any terminals that are located there for the meeting.	Alias, Dial-String, IP-ISDN-SIP	String	<Terminal Alias="ISDN001" Dial-String="44-55-66" IP-ISDN-SIP="ISDN"/>
<Completed-Conference-Data/ ></Completed-Conference-Data>	Contains actual conference data collected during the course of the meeting and at the conclusion of the meeting.			
<Conference-Status />	Contains information about the results of the meeting, such as whether or the meeting was canceled before its scheduled start time or started successfully. Possible values: STARTED, CANCELLED-BY-SERVER, CANCELLED-BY-USER, FAILED-TO-START.	value	String	<Conference-Status value="STARTED"/>
<Reason-Failed />	Describes the reason a meeting fails to start.	value	String	<Reason-Failed value="N/A" />
<Actual-Start-Time />	Contains the actual (versus scheduled) start time of the meeting.	value	yyyy-mm-ddThh-m m-ssZ	<Actual-Start-Time value = "2003-03-29T11:35:49Z" />

Tag	Description	Attribute	Type	Example
<Actual-End-Time />	Contains the actual (versus scheduled) end time of the meeting.	value	yyyy-mm-ddTh h-m m-ssZ	<Actual-End-Ti me value="2003-0 3-29T11:47:43 Z" />
<Actual-Predefined-Terminals>< /Actual-Predefined-Terminals>	Contains a list of terminals registered to iVIEW Communications Manager that actually participated in the meeting.			
<Actual-Predefined-Terminal></ Actual-Predefined-Terminal/>	Contains information on an individual terminal registered to iVIEW Communications Manager that actually participated in the meeting.			
<Terminal-ID />	Contains the internal iVIEW Communications Manager ID of a participating terminal.	value	String	<Terminal-Id value="0001- PARTY-10005" />
<Alias />	Contains the iVIEW Communications Manager alias of a participating terminal.	value	String	<Alias value="2518" / >
<Dial-String />	Contains the dial string of the participating terminal. For an ISDN phone number, the format is "CountryCode - AreaCode - PhoneNumber".	value	String	<Dial-String value="812518 " />
<IP-ISDN-SIP />	Defines the type of the participating terminal.	value	String	<IP-ISDN-SIP value="IP" />
<Source-IP-Address />	Contains the IP address of the participating terminal.	value	String	<Source-IP-Ad dress value="192.168 .223.23" />

Understanding the CDR XML Tags

Tag	Description	Attribute	Type	Example
<Total-Connection-Time />	Contains the total connection time of the participating terminal to the meeting, in seconds.	value	String (Integer + 's')	<Total-Connection-Time value="600s"/>
<Failing-Attempts />	Contains the number of times that this terminal attempted to join the conference and failed.	value	Integer	<Failing-Attempts value="2" />
<Last-Failure-Cause />	Contains the cause of failure of the last failed attempt.	value	String	<Last-Failure-Cause value="" />
<List-of-Connection-Records></List-of-Connection-Records />	Contains a list of records for each time the participating terminal connected to and disconnected from the meeting.			
<Connection />	Contains connection records for a specific terminal.	Connection Time; Dialin-Dialout; Disconnection-Time; Over-GW-port-limit; Over-MCU-port-limit; Reason-Disconnection	yyyy-mm-ddTh h-m m-ssZ; Dial-in/ Dial-out; yyyy-mm-ddTh h-m m-ssZ; Boolean; Boolean; String	<Connection ConnectionTime="2003-03-29T11:35:51Z" Dialin-Dialout="Dial-out" Disconnection-Time="2003-03-29T11:43:45Z" Over-GW-port-limit="false" Over-MCU-port-limit="true" Reason-Disconnection="Disconnect"/>
<Actual-External-Terminals></Actual-External-Terminals />	Contains a list of external terminals that actually participate in the meeting.			

Tag	Description	Attribute	Type	Example
<Actual-External-Terminal></Actual-External-Terminal/>	Contains information on an individual external terminal that actually participates in the meeting.			
<Party-ID />	Contains the internal iVIEW Communications Manager ID string given to the external terminal.	value	String	<Party-Id value="EXTRA:2222" />
<Name />	Contains the name of the external terminal.	value	String	<Name value="Bob Baxton Mobile"/>
<Dial-String />	Contains the dial-string information of the external terminal. For an ISDN phone number, the format is "CountryCode - AreaCode - PhoneNumber".	value	String	<Dial-String value="812519 9" />
<IP-ISDN-SIP />	Specifies the terminal type. Possible values: IP, ISDN, SIP.	value	String	<IP-ISDN-SIP value="IP" />
<Desktop-Client />	Indicates whether or not this external terminal is a SCOPIA Desktop client. Only appears if value is True.	value	Boolean	<Desktop-Client value="true" />
<Desktop-Server />	Contains the internal iVIEW Communications Manager ID of the SCOPIA Desktop Server that is associated with this terminal.	value	String	<Desktop-Server value="0001-S DG-10002" />
<Total-Connection-Time />	The overall time that the external terminal was connected in the conference, in seconds.	value	String (Integer+'s')	<Total-Connection-Time value="600s"/>
<Failing-Attempts />	Contains the number of times that this terminal attempted to join the conference and failed.	value	Integer	<Failing-Attempts value="0" />

Understanding the CDR XML Tags

Tag	Description	Attribute	Type	Example
<Last-Failure-Cause />	Contains the cause of failure of the last failed attempt.	value	String	<Last-Failure-Cause value="N/A" />
<List-of-Connection-Records></List-of-Connection-Records>	Contains a list of records for each time the participating terminal connected to and disconnected from the meeting.			
<Connection />	Contains connection records for a specific terminal.	Connection Time; Dialin-Dialout; Disconnection-Time; Over-GW-port-limit; Over-MCU-port-limit; Reason-Disconnection	yyyy-mm-ddTh h-m m-ssZ; Dial-in/ Dial-out; yyyy-mm-ddTh h-m m-ssZ; Boolean; Boolean; String	<Connection ConnectionTime="2003-03-29T11:35:51Z" Dialin-Dialout="Dial-out" DisconnectionTime="2003-03-29T11:43:45Z" Over-GW-port-limit="false" Over-MCU-port-limit="true" Reason-Disconnection="Disconnect" />
<Connected-MCUs></Connected-MCUs>	Contains a list of all MCUs actually used during the meeting.			
<MCU-Information></MCU-Information>	Contains information about an individual MCU used during the meeting.			
<ID />	Contains the internal iVIEW Communications Manager ID of the MCU.	value	String	<ID value = "0001-MCU-10002" />
<Alias />	Contains the name of the MCU name in the iVIEW Communications Manager.	value	String	<Alias value="MCU82" />

Tag	Description	Attribute	Type	Example
<Model />	Contains model information for an individual MCU scheduled for use for the meeting.	value	String	<Model value="RADVISION MCU 3.0+" />
<Master-Slave />	Specifies whether or not this MCU is master or slave, in case the meeting is scheduled with cascading (set to True if the MCU served as Master in a cascaded conference).	value	String	<Master-Slave value="false" />
<Zone-Prefix />	Specifies the zone prefix of an MCU.	value	String	<Zone-Prefix value="58" />
<Gatekeeper />	Specifies the gatekeeper to which the MCU is registered.	value	String	<Gatekeeper value="0001-GK-10001" />
<Service-Prefix />	Specifies the service prefix of an MCU.	value	String	<Service-Prefix value="80" />
<List-of-Assigned-Terminals></List-of-Assigned-Terminals>	Contains a list of terminals assigned to the MCU for the meeting.			
<Terminal />	Contains information about a single terminal assigned to the MCU for the meeting. For an ISDN phone number, the format is "CountryCode - AreaCode - PhoneNumber".	Alias, Dial-String, IP-ISDN-SIP	String	<Terminal Alias="2518" Dial-String="812518" IP-ISDN-SIP="IP"/>
<ConnectedGWs></ConnectedGWs>	Contains a list of all Gateways that actually participated in the meeting.			
<Gateway-Information></Gateway-Information>	Contains information about an individual Gateway used during the meeting.			

Understanding the CDR XML Tags

Tag	Description	Attribute	Type	Example
<ID />	Contains the internal iVIEW Communications Manager ID of the Gateway.	value	String	<ID value = "0001-GW-10006" />
<Phone-Number />	Contains the Gateway phone number.	value	String	<Phone-Number value="88372361" />
<Service-Prefix />	Contains the prefix of the requested service.	value	String	<Service-Prefix value="9384" />
<Service-Bandwidth />	Specifies the bandwidth associated with the requested service configured on the Gateway.	value	String	<Service-Bandwidth value="384" />
<Country-Code />	Specifies the country code of a Gateway.	value	String	<Country-Code value="86" />
<Area-Code />	Specifies the area code of a Gateway.	value	String	<Area-Code value="10" />
<Zone-Prefix />	Specifies the zone prefix of a Gateway.	value	String	<Zone-Prefix value="58" />
<Terminal-Gateway-Association ></ Terminal-Gateway-Association>	Contains a list of terminals assigned to the Gateway for the meeting.			
<Association />	Associates an ISDN terminal with the Gateway it will use for the meeting.	Alias, ISDN-Phone-Number, Scheduled-Service-Bandwidth, Scheduled-Service-Prefix	String, String, Integer, String	<Association Alias="ISDN002" ISDN-Phone-Number="22-55-88" Scheduled-Service-Bandwidth="64" Scheduled-Service-Prefix="9064" />

22

ENABLING ICM TO USE SECURE SOCKETS LAYER CONNECTIONS ON A JBOSS APPLICATION SERVER

- [Component Identity via SSL](#) on page 207
- [How to Generate Certificates](#) on page 207

COMPONENT IDENTITY VIA SSL

Secure Sockets Layer (SSL) connections rely on the existence of digital certificates. A digital certificate reveals information about its owner, including the identity of the owner.

During the initialization of an SSL connection, the server must present its certificate to the client for the client to determine the server identity. The client can also present the server with its own certificate for the server to determine the client identity. SSL is therefore, a means of propagating identity between components.

HOW TO GENERATE CERTIFICATES

- [Methods for Creating a New Certificate](#) on page 208
- [Prerequisites](#) on page 208
- [Using Keytool to Generate a Certificate](#) on page 209
- [Configuring JBoss to use SSL](#) on page 210
- [Accessing iCM Using HTTPS](#) on page 212

METHODS FOR CREATING A NEW CERTIFICATE

A client can trust the contents of a certificate if that certificate is digitally signed by a trusted third party. A Certificate Authority (CA) acts as a trusted third party and signs certificates on the basis of its knowledge of the certificate requester.

There are two options for creating a new certificate.

- Request that a CA generates the certificate on your behalf.
The CA creates a new certificate, digitally signs it, and delivers it to the requester. Popular web browsers are preconfigured to trust certificates that are signed by certain CAs. No further client configuration is necessary for a client to connect to the server through an SSL connection. Therefore, CA signed certificates are useful where configuration for each and every client that accesses the server is impractical.
- Generate a self-signed certificate.
This option is quicker and requires fewer details to create the certificate, but the certificate is not signed by a CA. Any client that connects to this server over an SSL connection needs to be configured by the administrator as a trusted signer of this certificate. Therefore, self-signed certificates are only useful when you can configure each of the clients to trust the certificate. It is possible in some cases to present a self-signed certificate to an untrusting client. In some web browsers, when the certificate is received and does not match any of those listed in the client trust file, a prompt appears that gives the user the option to trust the connection and add it to the trust file.

PREREQUISITES

iVIEW Suite uses the JBoss application server platform. The JBoss application server installs automatically with iVIEW Suite.

To use SSL with JBoss, the following conditions must be met:

- You have a certificate.
- You configure JBoss to use this certificate.
- You store the certificate in a JKS keystore.

USING KEYTOOL TO GENERATE A CERTIFICATE

Keytool is the command line Java utility. This section describes how to use keytool to create a private and public self-signed certificate key pair.



Procedure

- 1 Open a DOS window and set the path to point to the JDK or JRE bin directory. For example

```
D:\>set path= D:\jdk1.5.0\bin
```

- 2 Create a self-signed certificate key pair. For example

```
D:\>keytool -genkey -keyalg RSA
-dname "cn=scheduler,ou=users,ou=yourcountry,
DC=yourcompany,DC=com"
-alias scheduler -keypass yourcompany -keystore
scheduler.keystore
-storepass yourcompany
```

- 3 Specify RSA as the private key to ensure that the MD5 with RSA signature algorithm is used.

Not all web browsers support the DSA cryptograph algorithm, which is the default when RSA is not specified.

- 4 Set a password of at least six characters to protect the private key.
- 5 Specify the keystore file and keystore password (the option is storepass).

Enter each string on a single line.

- 6 If you do not want to send a certificate signing request, skip to [Configuring JBoss to use SSL](#) section on page 210.

- 7 Generate the certificate signing request. For example

```
D:\>keytool -certreq -v -alias scheduler -file
scheduler.csr -keypass yourcompany
-keystore scheduler.keystore -storepass yourcompany
```

This request generates the following output:

```
Certification request stored in file <scheduler.csr>
```

- 8 Send the scheduler.csr file to your selected CA for signing.
- 9 Save the content of the signed certificate to a file. For example, scheduler.cer.

- 10** Import the CA trusted root certificate into the keystore. For example
- ```
D:\>keytool -import -alias "Provider Test CA Root"
-file "Provider Test Root.cer"
-keystore scheduler.keystore -storepass yourcompany
where
```

- Provider Test CA Root is the directory containing the test CA root binary and text files.
- Provider Test Root.cer is the test CA root binary file.

When the command is successfully executed, the following output displays:

```
Certificate was added to keystore
```

- 11** Import the certificate responses from the CA into the keystore file using the same alias name that was first given to the self-signed certificates. In this example, the alias name is scheduler. Using an alternative alias name generates a new signed certificate and not a personal certificate chain.

```
D:\>keytool -import -trustcacerts -alias scheduler
-file scheduler.cer
-keystore scheduler.keystore -storepass yourcompany
```

When the command is successfully executed, the following output displays:

```
Certificate reply was installed in keystore
```

You have now created a keystore file that stores a valid certificate for use.

---

## CONFIGURING JBoss TO USE SSL



Configure the JBoss application server for use with SSL.

### Procedure

- 1** Copy the scheduler.keystore file to  
<i>CM installation directory</i>\jboss\server\default\conf
- 2** Open the server.xml file located in  
jboss\server\default\deploy\jbossweb-tomcat50.sar

- 3 Locate the section beginning with the line
 

```
<!-- SSL/TLS Connector configuration using the admin
devl guide keystore
```
- 4 Remove the comment indicators and make the following changes:
  - a Uncomment out the SSL/TLS connector.
  - b Change the keystore file from **chap8.keystore** to **scheduler.keystore**.
  - c Change the keystorePass from rmi+ssi to yourcompany.
  - d We recommend that you change the port from 8443 to 443 so that the user does not need to type the port when accessing iCM. Like port 80, port 443 is a known HTTPS port.

The amended text appears as follows:

```
<!-- A HTTP/1.1 Connector on port 8080 or 80 -->
<Connector port="8080"
address="${jboss.bind.address}"
maxThreads="150" minSpareThreads="25"
maxSpareThreads="75"
enableLookups="false" redirectPort="443"
acceptCount="100"
connectionTimeout="20000"
disableUploadTimeout="true"/>

<!-- A AJP 1.3 Connector on port 8009 -->
<Connector port="8009"
address="${jboss.bind.address}"
enableLookups="false" redirectPort="443" debug="0"
protocol="AJP/1.3"/>

<!-- SSL/TLS Connector configuration using the admin
devl guide keystore -->
<Connector port="443" address="${jboss.bind.address}"
maxThreads="100" minSpareThreads="5"
maxSpareThreads="15"
scheme="https" secure="true" clientAuth="false"
keystoreFile="${jboss.server.home.dir}/conf/
```

```
scheduler.keystore"
keystorePass="yourcompany" sslProtocol = "TLS" />
<!-- -->
```

- 5 Restart JBoss.
- 

## ACCESSING ICM USING HTTPS



### Procedure

- 1 Type a URL of the format `https://localhost`, or `https://localhost:8443` (if port 8443 is used instead of 443).  
If the certificate in use is a test root certificate or a self-signed certificate that is not trusted by Internet Explorer, a security alert appears.
  - 2 Click **Yes** to access iCM.
  - 3 Click **View Certificate** to avoid this message in future logins.
  - 4 Click **Install Certificate**.  
After the certificate is installed, the user will not see the security alert on subsequent logins.
-

# 23

## REGISTERING EXTERNAL USERS WITH THE ICM EXTERNAL AGENT

---

The iCM External Agent is a client-server application that enables you to register an external user or terminal to the iCM. You configure the required user or terminal using a series of commands via the Command Line Interface.

---

**Note** The External Agent application is not shipped with the main product by default. To obtain the External Agent, please contact Customer Support.

---

- [Commands](#) on page 213
- [Modifying the Default Server](#) on page 226
- [Sample Configuration](#) on page 226

### COMMANDS

This section introduces the commands supported by the iCM External Agent and describes their format. The iCM External Agent supports the following commands:

- iCMExt CreateConfRoom
- iCMExt ModifyConfRoom
- iCMExt DeleteConfRoom
- iCMExt CreateUser
- iCMExt ModifyUser
- iCMExt DeleteUser
- iCMExt CreateTerminal

## Commands

- iCMExt ModifyTerminal
- iCMExt DeleteTerminal

---

### Note

- The order in which you use the parameters is not significant.
  - All parameters are case-sensitive.
  - If a parameter value contains spaces, enclose that parameter with inverted commas. For example, *userid = "John Smith"*.
  - A Modify operation keeps the original attribute if you do not specify the parameter.
-

---

## iCMExt CreateConfRoom

| Parameter    | Type   | Compulsory /Optional | Notes                                                                                                                                          |
|--------------|--------|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| memberName   | string | optional             | iCM uses a default value if no value is specified. For more information, see the <a href="#">Default Parameter Values</a> section on page 225. |
| roomId       | string | optional             | iCM uses the <i>roomname</i> parameter value (assuming that this value is unique) if no value is set for the <i>roomId</i> parameter.          |
| roomname     | string | compulsory           |                                                                                                                                                |
| roomlocation | string | compulsory           |                                                                                                                                                |
| email        | string | optional             |                                                                                                                                                |
| mailenabled  | string | optional             | “true” or “false” (the default is “false”)                                                                                                     |

---

---

## iCMEExt ModifyConfRoom

---

| Parameter    | Type   | Compulsory /Optional | Notes                                                                                                                                          |
|--------------|--------|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| memberName   | string | optional             | iCM uses a default value if no value is specified. For more information, see the <a href="#">Default Parameter Values</a> section on page 225. |
| roomId       | string | compulsory           |                                                                                                                                                |
| roomname     | string | optional             |                                                                                                                                                |
| roomlocation | string | optional             |                                                                                                                                                |
| email        | string | optional             |                                                                                                                                                |
| mailenabled  | string | optional             | “true” or “false” (the default is “false”)                                                                                                     |

---

---

## iCMExt DeleteConfRoom

| Parameter  | Type   | Compulsory /Optional                                              | Notes                                                                                                                                          |
|------------|--------|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| memberName | string | optional                                                          | iCM uses a default value if no value is specified. For more information, see the <a href="#">Default Parameter Values</a> section on page 225. |
| roomId     | string | compulsory (if no value is set for the <i>roomname</i> parameter) | iCM uses the <i>roomname</i> parameter value (assuming that this value is unique) if no value is set for the <i>roomId</i> parameter.          |
| roomname   | string | optional                                                          |                                                                                                                                                |

---

---

## iCMEExt CreateUser

| Parameter  | Type        | Compulsory /Optional | Notes                                                                                                                                          |
|------------|-------------|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| memberName | string      | optional             | iCM uses a default value if no value is specified. For more information, see the <a href="#">Default Parameter Values</a> section on page 225. |
| userid     | string      | optional             | iCM uses the <i>login</i> parameter value (assuming that this value is unique) if no value is set for the <i>userid</i> parameter.             |
| login      | string      | compulsory           |                                                                                                                                                |
| password   | string      | compulsory           |                                                                                                                                                |
| firstname  | string      | optional             |                                                                                                                                                |
| lastname   | string      | compulsory           |                                                                                                                                                |
| email      | string      | optional             |                                                                                                                                                |
| timezone   | string      | optional             |                                                                                                                                                |
| role       | role option | optional             | For more information, see the <a href="#">Default Parameter Values</a> section on page 225.                                                    |
| terminalid | string      | optional             |                                                                                                                                                |

---

---

## iCMExt ModifyUser

| Parameter  | Type        | Compulsory /Optional | Notes                                                                                                                                          |
|------------|-------------|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| memberName | string      | optional             | iCM uses a default value if no value is specified. For more information, see the <a href="#">Default Parameter Values</a> section on page 225. |
| userid     | string      | optional             | iCM uses the <i>login</i> parameter value (assuming that this value is unique) if no value is set for the <i>userid</i> parameter.             |
| login      | string      | compulsory           |                                                                                                                                                |
| password   | string      | optional             |                                                                                                                                                |
| firstname  | string      | optional             |                                                                                                                                                |
| lastname   | string      | compulsory           |                                                                                                                                                |
| email      | string      | optional             |                                                                                                                                                |
| timezone   | string      | optional             |                                                                                                                                                |
| role       | role option | optional             | For more information, see the <a href="#">Default Parameter Values</a> section on page 225.                                                    |
| terminalid | string      | optional             |                                                                                                                                                |

---

**Warning** Setting the **iCMExt ModifyUser** command deletes *all* **iCMExt CreateUser** parameter values and replaces them with the configured **iCMExt ModifyUser** parameter values.

---

## Commands

iCMEExt DeleteUser

---

### iCMEExt DeleteUser

---

| Parameter  | Type   | Compulsory /Optional | Notes                                                                                                                                          |
|------------|--------|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| memberName | string | optional             | iCM uses a default value if no value is specified. For more information, see the <a href="#">Default Parameter Values</a> section on page 225. |
| userid     | string | compulsory           |                                                                                                                                                |

---

---

## iCMExt CreateTerminal

| Parameter        | Type   | Compulsory /Optional                                          | Notes                                                                                                                                                                                       |
|------------------|--------|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| memberName       | string | optional                                                      | iCM uses a default value if no value is specified. For more information, see the <a href="#">Default Parameter Values</a> section on page 225.                                              |
| terminalprotocol | string | optional                                                      | H.323/H.320/Dual/SIP                                                                                                                                                                        |
| terminalid       | string | optional                                                      | iCM uses the number parameter value (assuming that this value is unique) if no value is set for the <i>terminalid</i> parameter. Not used if a value is set for the <i>sipid</i> parameter. |
| sipid            | string | optional                                                      | Adds a SIP terminal. Not used if a value is set for the <i>terminalid</i> parameter.                                                                                                        |
| number           | string | compulsory                                                    |                                                                                                                                                                                             |
| name             | string | compulsory (if a value is set for the <i>sipid</i> parameter) | iCM uses the <i>number</i> parameter value (assuming that this value is unique) if no value is set for the <i>name</i> parameter.                                                           |
| roomid           | string | optional                                                      |                                                                                                                                                                                             |
| island           | string | optional                                                      |                                                                                                                                                                                             |
| connectionspeed  | string | optional                                                      |                                                                                                                                                                                             |
| billingtype      | string | optional                                                      |                                                                                                                                                                                             |
| sipuri           | string | compulsory                                                    | Used only in SIP terminals.                                                                                                                                                                 |

## Commands

### iCMExt CreateTerminal

| Parameter        | Type   | Compulsory /Optional | Notes                                                                                                                                                              |
|------------------|--------|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| userid           | string | optional             | The user ID for the new terminal created.                                                                                                                          |
| gatekeeper       | string | optional             | The name of the gatekeeper (if a value is set for the <i>terminalid</i> parameter), or the iCM SIP domain name (if a value is set for the <i>sipid</i> parameter). |
| countrycode      | string | compulsory           | Used for H.320 or Dual terminals.                                                                                                                                  |
| areacode         | string | compulsory           | Used for H.320 or Dual terminals.                                                                                                                                  |
| isdnumber        | string | compulsory           | Used for H.320 or Dual terminals.                                                                                                                                  |
| restrictmode     | string | optional             | Used for H.320 or Dual terminals.                                                                                                                                  |
| isdnconnectspeed | string | optional             |                                                                                                                                                                    |

---

## iCMExt ModifyTerminal

| Parameter      | Type   | Compulsory /Optional           | Notes                                                                                                                                          |
|----------------|--------|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| memberName     | string | optional                       | iCM uses a default value if no value is specified. For more information, see the <a href="#">Default Parameter Values</a> section on page 225. |
| terminalid     | string | compulsory (if an IP terminal) |                                                                                                                                                |
| sipid          | string | compulsory (if a SIP terminal) |                                                                                                                                                |
| number         | string | optional                       |                                                                                                                                                |
| name           | string | optional                       |                                                                                                                                                |
| roomid         | string | optional                       |                                                                                                                                                |
| island         | string | optional                       |                                                                                                                                                |
| connectionsper | string | optional                       |                                                                                                                                                |
| billingtype    | string | optional                       |                                                                                                                                                |
| sipuri         | string | compulsory                     | Used only in SIP terminals.                                                                                                                    |
| userid         | string | optional                       | The user ID for the new terminal created.                                                                                                      |
| gatekeeper     | string | optional                       | The name of the gatekeeper (if a value is set for the <i>terminalid</i> parameter).                                                            |
| countrycode    | string | compulsory                     | Used for H.320 or Dual terminals.                                                                                                              |
| areacode       | string | compulsory                     | Used for H.320 or Dual terminals.                                                                                                              |

---

## Commands

### iCMEExt ModifyTerminal

| Parameter        | Type   | Compulsory /Optional | Notes                             |
|------------------|--------|----------------------|-----------------------------------|
| isdnumber        | string | compulsory           | Used for H.320 or Dual terminals. |
| restrictmode     | string | optional             | Used for H.320 or Dual terminals. |
| isdnconnectspeed | string | optional             |                                   |

**Warning** Setting the **iCMEExt ModifyTerminal** command deletes *all* **iCMEExt CreateTerminal** parameter values and replaces them with the configured **iCMEExt ModifyTerminal** parameter values.

## iCMExt DeleteTerminal

| Parameter  | Type   | Compulsory /Optional           | Notes                                                                                                                                          |
|------------|--------|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| memberName | string | optional                       | iCM uses a default value if no value is specified. For more information, see the <a href="#">Default Parameter Values</a> section on page 225. |
| terminalid | string | compulsory (if an IP terminal) |                                                                                                                                                |
| sipid      | string | compulsory (if a SIP terminal) |                                                                                                                                                |

### DEFAULT PARAMETER VALUES

Default parameter values are stored in the *icm-external.properties* file in the iCMExternalAgent folder.

**Figure 23-1** *icm-external.properties* File Default Parameter Values

```

#####
#
RADVISION iCM-External properties files
#
NOTE:
You can only modify this file and not remove it,
otherwise it will not work with the external agent.
#
* Do not delete any lines.
* Do not change or delete any wording that is
before the = sign.
* You may modify wording that appears only after
the = sign.
#
DO NOT DELETE ANY LINES FROM THIS FILE
#
#####
icmexternal.memberName=ext
icmexternal.role=1
icmexternal.timeZone=Asia/Seoul
icmexternal.terminalConnectionSpeed=384
icmexternal.island=Home
icmexternal.terminalProtocol=H320
icmexternal.userPrefix=ext_
icmexternal.terminalPrefix=ext_
icmexternal.terminalZonePrefix=
icmexternal.terminalRegisterGK=gk

```

## MODIFYING THE DEFAULT SERVER

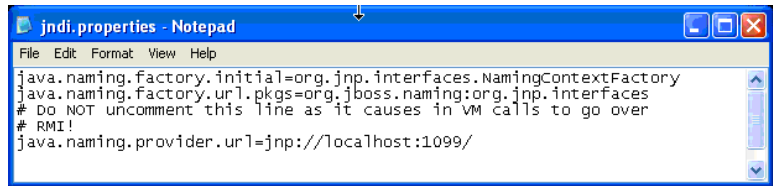


If your iCM client is not located on the same computer as the iCM, modify the default server accordingly.

### Procedure

- 1 In the ICMExternalAgent folder, open the jndi.properties file.

**Figure 23-2** *jndi.properties File*



- 2 Modify the localhost value as appropriate, then save and close the file.

## SAMPLE CONFIGURATION



This section describes a sample configuration using iCM External Agent commands.

### Procedure

- 1 In the ICMExternalAgent folder, run the iCMExt.cmd file.  
The iCM External Agent Command Line Interface displays.  
iCM External Agent Command Line Interface
- 2 Type the required parameter name followed by the relevant parameters and values. For example,
  - ❑ iCMExt CreateConfRoom roomid=1111 roomname=test roomlocation=beijing adminemail=aa@aa.aa
  - ❑ iCMExt CreateTerminal terminalid=88388 number=88388 name=Michael3 roomname=test
  - ❑ iCMExt CreateUser userid=88388 lastname="Michael3" login=88388 password=1111 terminalid=88388

# IVIEW NETWORK MANAGER



# 24

## iVIEW NETWORK MANAGER OVERVIEW

---

### ABOUT THE iVIEW NETWORK MANAGER

- [About the iVIEW Network Manager](#) on page 229
- [What the iVIEW Network Manager Provides](#) on page 230

The iVIEW Network Manager is a simple-to-use network management system for RADVISION IP video conferencing networks.

Designed with the network administrator in mind, the iVIEW Network Manager provides a unified interface for managing all the devices (elements) in your video conferencing network, including:

- RADVISION elements
  - MCU
  - ECS
  - Gateway
  - DCS
  - PathFinder
- Third-party elements and endpoints:
  - Polycom, Sony endpoints

### SYSTEM REQUIREMENTS

The iVIEW Network Manager communicates with RADVISION elements using a variety of industry-standard protocols, such as SNMP, XML, Telnet and FTP.

---

**Note** Ports supporting these protocols must be available in each element in order to be managed by the iVIEW Network Manager.

---

### WHAT THE iVIEW NETWORK MANAGER PROVIDES

The iVIEW Network Manager is a fully compliant network management system that provides network-wide functionality for RADVISION elements.

- [Viewing Network Status](#) on page 230
- [Viewing Calls and Conferences](#) on page 231
- [Using Auto-Detect](#) on page 231
- [Configuring Basic Elements](#) on page 231
- [Viewing Alarms and Events](#) on page 232
- [Connecting to Element Managers](#) on page 233
- [Connecting to Terminal Managers](#) on page 233
- [Managing a Centralized Log](#) on page 233
- [Viewing Multiple Networks](#) on page 233
- [Configuring Offline Elements](#) on page 233
- [ENC Functionality](#) on page 234
- [Defining Network Subsets](#) on page 234
- [Supporting ECS](#) on page 234
- [Dragging and Dropping](#) on page 234
- [Monitoring Calls](#) on page 234

### VIEWING NETWORK STATUS

The iVIEW Network Manager provides network administrators with the most critical network status information at a glance, including:

- Element information—Total number of elements, the number of faulty elements and the number of elements that are offline.
- Call information—Total number of calls in the network, the number of point-to-point calls and the number of conferences.
- Endpoint information.
- Bandwidth information—Inter-zone bandwidth usage.
- B-channel usage information.

All network status information is updated in real time by the iVIEW Network Manager database.

## VIEWING CALLS AND CONFERENCES

The iVIEW Network Manager provides network administrators with a view of all calls and conferences currently taking place over the network.

One-click control allows the network administrator to view call details or to access the source or destination gatekeeper element manager per call, and to link to the MCU Conference Control interface to assume full control of any conference in the list.

With these views, administrators can quickly determine:

- Call source and destination alias
- Call source and destination gatekeeper
- Call allocated resources
- The MCU controlling the conference
- Conference type.
- Conference video and bandwidth settings.
- Number of participants—including the current number, the number reserved and the number of local participants.

## USING AUTO-DETECT

The iVIEW Network Manager uses an automatic detection mechanism for discovering the RADVISION elements present on the network. This information is saved to the iVIEW Network Manager database and is used to create the various network views available via the iVIEW Network Manager interface. Auto-detect can be run at regular intervals and whenever the server is restarted. Auto-detect can also be manually initiated at any time.

PathFinder does not yet support auto-detect.

---

**Note** The access field definitions for SNMP communities and Telnet must correspond with the settings configured in the selected element in order to retrieve the information from the element. If these fields are not configured correctly, the required information cannot be displayed.

---

## CONFIGURING BASIC ELEMENTS

The iVIEW Network Manager provides network administrators with the ability to view and edit the most commonly used configuration parameters of various elements in the network, such as MCUs, gatekeepers, gateways, Polycom endpoints (configuration of the RADVISION PathFinder Server is not yet supported).

## What the iVIEW Network Manager Provides

### CONFIGURING AN MCU

Network administrators can configure the following MCU parameters, using the iVIEW Network Manager:

- IP address
- MCU type (such as MCU or MP Only)
- DCS parameters, if applicable

### CONFIGURING A GATEKEEPER

Using the iVIEW Network Manager, network administrators can configure the following Gatekeeper parameters:

- Dial plan version
- Registration and routing modes
- GKTMP port
- LRQ hop count

### CONFIGURING A GATEWAY

Using the iVIEW Network Manager, network administrators can configure the following Gateway parameters:

- Gatekeeper IP address
- Location

### CONFIGURING A POLYCOM ENDPOINT

Using the iVIEW Network Manager, network administrators can configure the following Polycom endpoint parameters:

- Endpoint IP address
- Gatekeeper IP address
- Endpoint alias name and E.164 number

### VIEWING ALARMS AND EVENTS

The iVIEW Network Manager provides network administrators with a list of the alarms currently active in any of the elements in the network. The list is constantly updated by the system, ensuring that any problems are located without delay. One-click access from any alarm directly to the administration interface of the device ensures that problems can be investigated and dealt with immediately. In addition, the iVIEW Network Manager provides a list of all events that have taken place in the network. This list can be filtered by the network administrator, as required.

## **CONNECTING TO ELEMENT MANAGERS**

The iVIEW Network Manager provides one-click access to the administration interfaces (element managers) of all the elements in the network, regardless of type, without the need to log in individually to each element. This gives network administrators the ability to perform a full range of management and configuration procedures on individual elements. Links to element managers can be found throughout the iVIEW Network Manager interface, including the Alarm and Event views, the Conferences view and the various network views.

## **CONNECTING TO TERMINAL MANAGERS**

In addition to providing one-click access to element managers, the Network Tree view of the iVIEW Network Manager also provides one-click access to the Web-based management systems of some common endpoints registered to the network.

## **MANAGING A CENTRALIZED LOG**

The iVIEW Network Manager provides centralized log management at both the network and element type levels. Using the Settings View, network administrators can define the size of the network log file, as well as the number of backups to maintain and the level of activity detail to include in the log. In addition, the iVIEW Network Manager can be used to keep logs for those elements types, such as MCU elements and Gateways, that do not maintain log files of their own.

## **VIEWING MULTIPLE NETWORKS**

The iVIEW Network Manager provides network administrators with multiple options for viewing the elements in the network, including a Network Tree view with elements arranged in a tree structure according to zone, a Network Table view that displays a single, unified list of all network elements, as well as a Network Map view that displays elements and network status information in a graphic, multi-layered format.

The Network Tree view features a default view based on the zones in the IP conferencing network. However, the iVIEW Network Manager also enables network administrators to create custom views. By creating folders and placing elements into them, administrators can view the network in whatever arrangement works best, such as dividing the network according to location. The views created in the Network Tree view can also be displayed in graphic format in the Network Map view.

## **CONFIGURING OFFLINE ELEMENTS**

The iVIEW Network Manager can hold configuration details for offline elements and apply settings as each element goes online. Both added elements and existing elements can be configured to allow offline configuration.

## **ENC FUNCTIONALITY**

The iVIEW Network Manager replaces the ENC functionality supported in some versions of the ECS and allows administrators to re-configure the ENC support settings globally so that all ECSs operate under the management of the iVIEW Network Manager. Administrators can manage and configure gatekeeper network hierarchy parent, child and neighbor relationships. Administrators can select each element node to view the relevant tables for defining the IP addresses of related elements.

This functionality is supported by the drag and drop management feature for automatic re-configuration of parent and child settings and by the offline management capability of the iVIEW Network Manager which allows pre-configuration of network hierarchy relationships.

## **DEFINING NETWORK SUBSETS**

The iVIEW Network Manager enables administrators to define subsets of the network and restrict users with specific profiles to control certain network areas. Administrators can configure the network subsets using criteria to include or exclude certain zones and element types.

## **SUPPORTING ECS**

The iVIEW Network Manager provides extensive monitoring, configuration and management capabilities of the ECS including local and remote zone setup, bandwidth policies, prefixes, logs, debugging and Telnet commands.

## **DRAGGING AND DROPPING**

The iVIEW Network Manager provides Network Tree drag and drop functionality for convenient element hierarchy management. Element addressing details are automatically updated in the tables of related elements. This feature can be used during offline configuration.

## **MONITORING CALLS**

The iVIEW Network Manager supports a comprehensive calls view detailing endpoint information, source and destination gatekeepers, bandwidth settings and call disconnection capabilities.

# 25

## VIEWING YOUR NETWORK IN iVIEW NETWORK MANAGER

---

- [How to View the Network as a Tree](#) on page 235
- [Viewing the Network as a Table](#) on page 237
- [Viewing the Network as a Map](#) on page 238

### HOW TO VIEW THE NETWORK AS A TREE

The Network Tree view organizes the information about the IP conferencing network into one or more tabbed views, each of which lists the elements in the network in a tree structure. By default, the tree divides the elements by zones.

- [Configuring Network Hierarchy](#) on page 235
- [Creating a Custom Network Tree View](#) on page 236

### CONFIGURING NETWORK HIERARCHY

The drag and drop feature enables quick configuration of the network hierarchy and reconfigures element relationships by automatically assigning and updating the appropriate details of the elements with which the managed element registers.

The following element relationships can be configured using the drag and drop feature:

- Gatekeeper Parent - Child
- Gatekeeper - MCU/Gateway
- MCU - DCS

iVIEW Network Manager automatically updates element tables for Gatekeeper parent and child elements in the relationship. iVIEW Network Manager updates MCU, Gateway and Polycom endpoint elements with the appropriate gatekeeper IP address. iVIEW Network Manager updates MVP and DCS elements with the relevant IP address and configuration details for registering with the MCU.



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Select an element in the network tree.
  - 3 Drag and drop the element to the required location in the hierarchy.
  - 4 Deselect the element.
- 

## CREATING A CUSTOM NETWORK TREE VIEW

You can create your own tree structures according to criteria you define, such as the physical location or other customer-specific criteria. You can add folders and elements to the custom views and organize them as needed.



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
- 2 Do one of the following:
  - Right-click a tab in the Network Tree view (above the tree) and select **Add tree view**
  - Select **Edit > New > New tree view**.

- 3 Enter a name for the new tree view and click **OK**.

The new tree view is added to the Network Tree view.

By default, the new tree view includes a Network root directory and an Unassigned folder. The Unassigned folder contains all the elements in the network organized by type.

- 4 Create folders for organizing the elements in the tree view by right-clicking the location in the tree where each folder should be located, and selecting **Add folder**.

- 5 Drag and drop elements from the Unassigned folder to the folders that you created.

---

**Note** To rename or remove tree views, either use the Edit menu or right-click the tree view. To rename or remove folders, right-click the folder and select the relevant option.

---

## VIEWING THE NETWORK AS A TABLE



The Network Table view displays information about all the elements in the IP conferencing network in a single table and provides element editing, search and auto-detect capabilities.

### Procedure

- 1 Click **Network Table** in the sidebar menu.

The Network Table view includes the following information about each element:

- Element status
  - Element type
  - Element name
  - IP address
  - Version number
  - Location
  - Resource usage versus capacity
- 2 Click the column headers to sort the information displayed.
  - 3 Double-click any element in the table to display the relevant element manager for that element.
-

## VIEWING THE NETWORK AS A MAP

The Network Map view displays information about the IP conferencing network in the form of graphic maps created for each node in the network hierarchy.



### Procedure

- 1 Click **Network Map** in the sidebar menu.

The top level of the **Network Map** view displays the network root and the zones into which the network is divided.

Each square represents either the network root, a zone (or user-defined folder) or a single element. Each square includes the following information:

- Current status
- Number of calls
- Number of conferences
- Number of registered participants versus capacity
- Number of B-channels handled by gateways versus capacity
- Total bandwidth handled by gatekeepers versus capacity

Inter-zone bandwidth information appears above the zones when relevant.

---

**Note** Call and conference statistics for OnLan Gateways and OnLan MCUs are not included in summary details for selected elements.

---

- 2 Use the Up and Down buttons to navigate between map levels.  
The Network Map view enables you to navigate from the zone level (or folder) to the element level by double-clicking a square.
  - 3 Use the list to select which view to display.
-

# 26

## MANAGING ELEMENTS IN iVIEW NETWORK MANAGER

---

- [Displaying General Element Information](#) on page 240
- [Management Status of Elements](#) on page 240
- [Viewing all Network Elements](#) on page 241
- [Creating or Modifying an Element Profile](#) on page 242
- [Removing an Element Profile](#) on page 243
- [Searching for an Element Profile](#) on page 243
- [Defining Default Element Access Settings](#) on page 244
- [Defining Default PathFinder Access Settings](#) on page 245
- [Overriding Default Element Access Settings](#) on page 246
- [How to Upgrade Element Software](#) on page 247
- [Cancelling Pending Offline Configuration Settings](#) on page 248
- [How to Manage the Element Software Upgrade Upload Log](#) on page 249
- [How to Automatically Detect New Elements on the Network](#) on page 250
- [Accessing an Element Web User Interface](#) on page 253
- [Accessing the Monitor Tab for a Specified Element](#) on page 254

## DISPLAYING GENERAL ELEMENT INFORMATION



The Monitor tab, which is the default tab displayed when an item is selected in the Network Tree view, displays general information about the item.

When the gatekeeper in a zone is unmanaged or inferred, the calls, bandwidth and registration information appears as zero.

The information displayed on the Monitor tab is dependent on the item selected in the tree.

### Procedure

- 1 Click **Network Tree** in the sidebar menu.
- 2 Select the element you require in the tree.
- 3 Click **Monitor**.
- 4 (Optional) Click the link to display the element manager for the selected element.

## MANAGEMENT STATUS OF ELEMENTS

Table 26-1 describes the different types of element management status.

**Table 26-1** *Element Management Status*

| Element Status | Description                                                                                                                                                                                                                                                                                                                           |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Managed        | The element exists in the iVIEW Network Manager database and provides monitoring information and access to configuration settings.                                                                                                                                                                                                    |
| Inferred       | The element does not exist in the iVIEW Network Manager database, but it might appear as an inferred element because a managed element refers to that element.<br>For example, a gatekeeper is inferred when a managed element is registered to that gatekeeper zone, but the gatekeeper is not managed by the iVIEW Network Manager. |

## VIEWING ALL NETWORK ELEMENTS

| Element Status | Description                                                                                                                                                                                                                                                                                                                                                             |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Unmanaged      | The element exists in the iVIEW Network Manager database but has no open communication channels with the iVIEW Network Manager and provides no monitoring information or access to configuration settings. An element might be unmanaged when the iVIEW Network Manager license limitations have been exceeded or when the user manually sets the element as unmanaged. |

The Elements tab displays a table of all elements related to the network, zone or folder selected in the tree.





Any element listed in the tree with a question mark (?) is considered to be an inferred element by the system. This means that the element is not listed in the database, but is presumed to exist because another known element refers to the element. Inferred elements cannot be managed, therefore we recommend that you either initiate auto-detect to discover an element, add an element manually or manually connect an inferred element.



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
- 2 Select Network root element.
- 3 Click **Elements**.

The table in the Elements tab includes the following information about each element:



- Element status, indicated by an icon, as follows:
  -  Online
  -  Unmanaged
  -  Offline
  -  Faulty
- Element type (MCU, gatekeeper and so on)
- Element name (acts as a link to its element manager)
- IP address
- Version number

- Location (as defined on the Configure tab of each element)
  - Traffic usage versus capacity
- 

## CREATING OR MODIFYING AN ELEMENT PROFILE



### Procedure

- 1 Click one of the network views (**Network Tree**, **Network Table** or **Network Map**) in the sidebar menu.
- 2 Do one of the following to modify an existing element profile:
  - Right-click the element you require and select **Edit element**.
  - Select the element you require and select **Edit > Modify > Modify element**.
  - Select the element you require and click **Edit element** .
- 3 Select the location in the **Network Tree or Network Map view where the new** element should be added, and do one of the following to create a new user profile:
  - Select **Edit > New > New element**.
  - Click **Add element** .
- 4 Enter the element name and IP address in the relevant fields.
- 5 Select the required element type.

The element type cannot be modified.
- 6 (Optional) Select **Managed element** to enable iVIEW Network Manager to manage the element.


This option is not available for endpoint elements.
- 7 (Optional) Select **Allow offline configuration** to allow offline configuration of the element.

This option is not available for MCU or endpoint elements.

The iVIEW Network Manager can hold configuration details for offline elements and apply settings as each element goes online. Both added elements and existing elements can be configured to allow offline configuration.


- 8 Select an option from the Gatekeeper IP field.  
You can select the IP address of a gatekeeper already configured in the system, or you can select **No Gatekeeper** or **Upon endpoint configuration**.
  - 9 (Optional) Select **Set iVIEW NMS as the default trap server** to use iVIEW Network Manager as the SNMP trap server for Polycom endpoint elements.
  - 10 Click **OK** to save your changes.
- 

## REMOVING AN ELEMENT PROFILE

Deleted elements are not added to the iVIEW Network Manager database in any subsequent auto-detect operations. You can only add a deleted element manually either by using the New element option in the Edit menu, selecting the Add element button  in the network views (Network Tree, Network Table or Network Map), or by connecting to a deleted element that is inferred.



### Procedure

- 1 Click one of the network views (**Network Tree**, **Network Table** or **Network Map**) in the sidebar menu.
- 2 Do one of the following to remove an existing element profile:
  - Right-click the element you require and select **Delete element**.
  - Select the element you require and select **Edit > Delete > Delete element**.
  - Select the element you require and click **Delete element** .
- 3 Click **Yes**.

The element profile is deleted from the scheduler and information about the element is removed from the database.


---

## SEARCHING FOR AN ELEMENT PROFILE



### Procedure

- 1 Click one of the network views (**Network Tree**, **Network Table** or **Network Map**) in the sidebar menu.
- 2 Do one of the following to search for an element profile:

- Right-click the element you require and select **Delete element**.
  - Select **Edit > Find > Find element**.
  - Click **Find element** .
- 3 Enter the IP address of the element or select the element type.
  - 4 Click **Find**.

The required element is highlighted in the Network Tree, Network Table or Network Map view.

---

## DEFINING DEFAULT ELEMENT ACCESS SETTINGS

Default access settings allow access to a network element for monitoring and configuration without having to first go through the login window for that element.

---

**Note** You can override default access settings for a specified element at Network Tree > Access.

---



### Procedure

- 1 Click **Settings** in the sidebar menu.
  - 2 Click **Element Management**.
  - 3 Click **Access**.
  - 4 Select an element type.
  - 5 Define SNMP read and write communities, user name and password, HTTP communication port and Telnet password in the relevant fields.  
The SNMP option is not available for endpoint or PathFinder Server elements.  
The HTTP option is not available for endpoint elements.  
SNMP community and Telnet information must match the settings defined in the selected element to enable iVIEW Network Manager to retrieve information from the element.
  - 6 Click **Upload** to save the information to the iVIEW Network Manager database.
-

## DEFINING DEFAULT PATHFINDER ACCESS SETTINGS



Default access settings allow access to a PathFinder Server network element for monitoring and configuration without having to first go through the login window.

### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Select the required PathFinder Server element.
  - 3 Click **Access**.
  - 4 Enter a collaborator user name and password in the relevant fields.  
This is the user account with which iVIEW Network Manager connects to the PathFinder Server. It should match the account details of a user defined on the PathFinder Server with the collaborator user type.  
Default values are *Collab* and *balloC* respectively.
  - 5 Enter an SFTP user name and password in the relevant fields.  
This is the user account with which iVIEW Network Manager connects to the PathFinder Server to download logs.  
Default values are *uadmin* and *admin* respectively.
  - 6 Enter the SFTP port number.  
The default value is 22.
  - 7 Enter an HTTP user name and password in the relevant fields.  
This is the user account with which iVIEW Network Manager accesses the PathFinder Server web user interface.  
Default values are *admin* and *admin* respectively.
  - 8 Enter the web server service port number of the PathFinder Server in the HTTP Port field.  
The default value is 8080.
  - 9 Enter an SSH user name and password in the relevant fields.  
This is the user account with which iVIEW Network Manager connects to the PathFinder Server platform.  
Default values are *admin* and *admin* respectively.
  - 10 Click **Upload** to save the information to the iVIEW Network Manager database.
-

## OVERRIDING DEFAULT ELEMENT ACCESS SETTINGS



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
- 2 Select the required network element.
- 3 Click **Access**.
- 4 Select **Use default** to use the default access settings for the element type.

When deselected, all other tab options are disabled.

Availability of the following access configuration parameters depends on the element type selected.

- 5 The Element type list appears when the selected element is an inferred gatekeeper. Select to display the appropriate access configuration parameters for the inferred gatekeeper.
  - 6 Select **Connect** to connect to an inferred element and add it to the iVIEW Network Manager database.  
SNMP community and Telnet information must match the settings defined in the selected element to enable iVIEW Network Manager to retrieve information from the element.
  - 7 Configure the following parameters:
    - SNMP read community
    - SNMP write community
    - User name
    - Password
    - HTTP port
    - Telnet password (Gateway, MCU, DCS, ECS)
    - Telnet user name (ECS only)
    - Enable Telnet (ECS only)
-

## HOW TO UPGRADE ELEMENT SOFTWARE

iVIEW Network Manager enables you to manage software upgrade files for MCUs, Gateways, and Polycom and Sony endpoints on your network.

- [Adding a Software Upgrade File](#) on page 247
- [Modifying a Software Upgrade File](#) on page 247
- [Removing a Software Upgrade File](#) on page 248

### ADDING A SOFTWARE UPGRADE FILE



#### Procedure

- 1 Click **Settings** in the sidebar menu.
  - 2 Click **Element Management**.
  - 3 Click **Software Upgrade Files**.
  - 4 Select the type of element you require in the Show field.
  - 5 Click **Add**.
  - 6 Enter the full path of the software upgrade file to be added to the iVIEW Network Manager database, or browse to the file.
  - 7 Enter a name and description for the upgrade file in the relevant fields.
  - 8 Click **OK** to save your changes.
- 

### MODIFYING A SOFTWARE UPGRADE FILE



#### Procedure

You can change the name and description of a software upgrade file that you have already added to iVIEW Network Manager.

- 1 Click **Settings** in the sidebar menu.
- 2 Click **Element Management**.
- 3 Click **Software Upgrade Files**.
- 4 Select the type of element you require in the Show field.
- 5 Do one of the following:
  - Double-click the software upgrade file you require.
  - Select the software upgrade file you require and click **Edit**.
  - Right-click the software upgrade file you require and select **Edit**.

## Canceling Pending Offline Configuration Settings

- 6 Enter a new name and description for the upgrade file in the relevant fields.
  - 7 Click **OK** to save your changes.
- 

## REMOVING A SOFTWARE UPGRADE FILE



### Procedure

- 1 Click **Settings** in the sidebar menu.
  - 2 Click **Element Management**.
  - 3 Click **Software Upgrade Files**.
  - 4 Select the type of element you require in the Show field.
  - 5 Do one of the following:
    - Select the software upgrade file you require and click **Delete**.
    - Right-click the software upgrade file you require and select **Delete**.
  - 6 Click **OK** to save your changes.
- The software upgrade file is removed from the database.
- 

## CANCELLING PENDING OFFLINE CONFIGURATION SETTINGS



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Right-click an offline element.
  - 3 Select **Clear offline updates**.
- The element configuration settings which existed before the offline modifications are restored.
-

## HOW TO MANAGE THE ELEMENT SOFTWARE UPGRADE UPLOAD LOG

- [Viewing Your Software Upgrade Upload History](#) on page 249
- [Uploading a File After a Failed Attempt](#) on page 249
- [Removing Entries from the Upload Log](#) on page 250

### VIEWING YOUR SOFTWARE UPGRADE UPLOAD HISTORY



#### Procedure

- 1 Click **Settings** in the sidebar menu.
- 2 Click **Element Management**.
- 3 Click **Upload Log**.
- 4 Select the type of element you require in the Show field.

The Upload Log tab displays the history of all your attempts to upload a software upgrade file, and shows all scheduled future upload attempts.

---

### UPLOADING A FILE AFTER A FAILED ATTEMPT



#### Procedure

- 1 Click **Settings** in the sidebar menu.
  - 2 Click **Element Management**.
  - 3 Click **Upload Log**.
  - 4 Select the type of element you require in the Show field.
  - 5 Do one of the following to attempt to upload a software upgrade file after a previous upload attempt has failed:
    - Select the log entry you require and click **Retry**.
    - Right-click the log entry you require and select **Retry**.
  - 6 Click **OK** to save your changes.
-

## REMOVING ENTRIES FROM THE UPLOAD LOG



### Procedure

- 1 Click **Settings** in the sidebar menu.
  - 2 Click **Element Management**.
  - 3 Click **Upload Log**.
  - 4 Select the type of element you require in the Show field.
  - 5 Do one of the following to remove a single log entry:
    - Select the log entry you require and click **Delete**.
    - Right-click the log entry you require and select **Delete**.
  - 6 Click **OK** to save your changes.
  - 7 Click **Delete All** to remove all entries from the log.
  - 8 Click **OK** to save your changes.
- 

## HOW TO AUTOMATICALLY DETECT NEW ELEMENTS ON THE NETWORK

Auto-detect enables you to search the network for elements and add them to the iVIEW Network Manager database.

Auto-detect is performed by broadcasting requests to all SNMP communities defined in the iVIEW Network Manager for RADVISION elements. The access field definitions for SNMP communities and Telnet must correspond with the settings configured in the selected element.

Once these elements respond to the requests, the iVIEW Network Manager can query the elements directly for full configuration and status details.

The auto-detect method of discovery might not find all the elements located behind equipment such as routers. Therefore, the iVIEW Network Manager interface enables you to complete the database by adding elements manually.

---

**Note** Elements manually deleted from the iVIEW Network Manager database are not detected in subsequent auto-detect procedures. These elements must be manually added to the iVIEW Network Manager database. For more information, see the [Creating or Modifying an Element Profile](#) section on page 242.


---

- [Running the Auto-detect Mechanism Manually](#) on page 251
- [Running the Auto-detect Mechanism Automatically](#) on page 251
- [Adding or Modifying Auto-detect Element Access Information](#) on page 252
- [Removing an Element Type from the Auto-detect Mechanism](#) on page 253

## RUNNING THE AUTO-DETECT MECHANISM MANUALLY



### Procedure

- 1 Click one of the network views (**Network Tree**, **Network Table** or **Network Map**) in the sidebar menu.
- 2 Do one of the following:
  - Select **Tools > Auto-detect elements**.
  - Click **Auto-detect elements** .
- 3 Click **Yes**.

The iVIEW Network Manager interface is updated accordingly.

The auto-detect procedure may take some time, depending on the size of the network.

---

## RUNNING THE AUTO-DETECT MECHANISM AUTOMATICALLY



### Procedure

- 1 Click **Settings** in the sidebar menu.
- 2 Click **Auto-detect**.
- 3 (Optional) Select **Run auto-detect on server startup** to instruct iVIEW Network Manager to look for new elements on the network whenever the iVIEW Suite server is restarted.

- 4 (Optional) Select **Run auto-detect every (hrs)** and set an hourly interval to instruct iVIEW Network Manager to look for new elements periodically.
  - 5 (Optional) Select **Use default access information in auto-detect routine** to instruct iVIEW Network Manager to use the default element access settings defined at Settings > Element Management > Access.
  - 6 Click **Upload** to save your changes.
- 

### ADDING OR MODIFYING AUTO-DETECT ELEMENT ACCESS INFORMATION



#### Procedure

- 1 Click **Settings** in the sidebar menu.
- 2 Click **Auto-detect**.
- 3 Do one of the following to modify existing access settings for a network element:
  - Double-click the element you require in the Type column.
  - Select the element you require and click **Edit**.
  - Right-click the element you require in the Type column and select **Edit**.
- 4 Do one of the following to create new access settings for a network element:
  - Click **Add**.
  - Right-click any link in the Recipient Name column and select **Add**.
- 5 Select the unit type you require.
- 6 Define an SNMP read community in the relevant field.  
SNMP community information must match the settings defined in the selected element to enable iVIEW Network Manager to retrieve information from the element.
- 7 (Optional) Define a description, SNMP write community, and user name and password in the relevant fields.

- 8 Click **Enabled** to activate the new access settings.
  - 9 Click **OK** to save the information to the iVIEW Network Manager database.
- 

## REMOVING AN ELEMENT TYPE FROM THE AUTO-DETECT MECHANISM



### Procedure

- 1 Click **Settings** in the sidebar menu.
  - 2 Click **Auto-detect**.
  - 3 Do one of the following:
    - Select the element type you require and click **Delete**.
    - Right-click the element type you require and select **Delete**.
  - 4 Click **OK** to save your changes.
- 

## ACCESSING AN ELEMENT WEB USER INTERFACE



### Procedure

- 1 Click one of the network views (**Network Tree**, **Network Table** or **Network Map**) in the sidebar menu.
  - 2 Right-click the element you require and select **Open element manager**  
–or–  
Click the link to the name or IP address of the element.
-

## ACCESSING THE MONITOR TAB FOR A SPECIFIED ELEMENT



### Procedure

- 1 Click **Network Table** in the sidebar menu.
  - 2 Double-click the element you require in the table.
-

# 27

## MANAGING ENDPOINTS IN iVIEW NETWORK MANAGER

---

- [Defining Default Endpoint Access Settings](#) on page 255
- [How to Override Default Endpoint Settings](#) on page 256
- [Retrieving Configuration Parameters](#) on page 258
- [How to Manage Endpoint Software Upgrade Files](#) on page 259
- [How to Manage Endpoint Configuration Files](#) on page 260
- [How to Manage Endpoint Software Upgrade Files](#) on page 259
- [Updating Configuration for Selected Endpoints](#) on page 264
- [Setting the Managed Status of Polycom Endpoints](#) on page 265
- [How to Manage the Endpoint Upload Log](#) on page 266

### DEFINING DEFAULT ENDPOINT ACCESS SETTINGS

This section applies to the Polycom and Sony endpoints only.

Default access settings for common endpoint types recognized by the iVIEW Network Manager allow elements such as MCUs and gateways to access these endpoints.

---

**Note** You can override default access settings for a specified endpoint at Network Tree > Endpoints.

---



### Procedure

- 1 Click **Settings** in the sidebar menu.
  - 2 Click **Endpoint Management**.
  - 3 Click **Access**.
  - 4 Select an element type.
  - 5 Define a user name and password in the relevant fields.
  - 6 Click **Upload** to save the information to the iVIEW Network Manager database.
- 

## HOW TO OVERRIDE DEFAULT ENDPOINT SETTINGS

- [Overriding Default Endpoint Addressing](#) on page 256
- [Overriding Default Access Settings for a Selected Endpoint](#) on page 257
- [Configuring Endpoint Dialing](#) on page 257

## OVERRIDING DEFAULT ENDPOINT ADDRESSING

This section applies to Polycom and Sony endpoints only.



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Select the endpoint you require in the tree.
  - 3 Click the **Configure** tab.
  - 4 Select a gatekeeper IP address from the list of gatekeepers available on the network.
  - 5 Enter an E.164 number for the endpoint.
  - 6 Enter an H.323 alias for the endpoint.
  - 7 Click **Upload** to add the new settings to the endpoint or **Refresh** to update the new settings.
-

## OVERRIDING DEFAULT ACCESS SETTINGS FOR A SELECTED ENDPOINT



This section applies to Polycom and Sony endpoints only.

### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Select the endpoint you require in the tree.
  - 3 Click the **Access** tab.
  - 4 Select **Use default** to use default access settings defined by the endpoint.  
When unchecked, Remote API port and Telnet prompt for Tandberg endpoints only can be modified.
  - 5 Set the endpoint API port (Tandberg endpoints only).
  - 6 Set the Telnet prompt character string (Tandberg endpoints only).
  - 7 Enter the user name required for communicating with the endpoint.
  - 8 Enter the password required for communicating with the endpoint.
  - 9 Click **Upload** to add the new settings to the endpoint or **Refresh** to update the new settings.
- 

## CONFIGURING ENDPOINT DIALING



This section applies to Polycom and Sony endpoints only.

### Procedure

- 1 Click **Network Tree** in the sidebar menu.
- 2 Click **Endpoints**.
- 3 Do one of the following:
  - Select the endpoint you require in the Endpoints tab and click **Configure**, then click the **Dial** tab in the Endpoint control screen.
  - Double-click the endpoint you require in the Endpoints tab and click the **Dial** tab in the Endpoint control screen.
  - Right-click the endpoint you require in the Endpoints tab and select **Dial**.

- 4 Enter the address that you want this endpoint to call in the Dial to address field.
  - 5 Enter the network endpoint that you want this endpoint to call in the Dial to network endpoint field.
  - 6 Click **Connect** to connect the endpoint to a call at the specified address or with the selected endpoint.
  - 7 Click **Dial Parameters** to specify the call type and whether the call is restricted to other incoming callers.
  - 8 Click **Upload** to add the new settings to the endpoint or **Refresh** to update the new settings.
- 

## RETRIEVING CONFIGURATION PARAMETERS



This section applies to Polycom and Sony endpoints only.

You can retrieve configuration parameters from an endpoint and save configuration information to a file accessed from Settings > Endpoint Management > Configuration Files.

### Procedure

- 1 Click **Network Tree** in the sidebar menu.
- 2 Select the endpoint you require in the tree.
- 3 Do one of the following:
  - Click **Endpoints**, select the endpoint you require in the Endpoints tab, and then click **Retrieve configuration file**.
  - Right-click the endpoint you require and select **Update > Retrieve configuration file**.

The Retrieve Configuration File window shows a list of the configuration files that were previously retrieved.

- 4 Enter the name that you would like to give to the configuration file.
  - 5 Enter a description of the file.
  - 6 Click **OK** to save the file in the iVIEW Network Manager database.
-

## HOW TO MANAGE ENDPOINT SOFTWARE UPGRADE FILES

iVIEW Network Manager enables you to manage software upgrade files for Polycom and Sony endpoints on your network.

- [Adding a Software Upgrade File](#) on page 259
- [Modifying a Software Upgrade File](#) on page 259
- [Removing a Software Upgrade File](#) on page 260

### ADDING A SOFTWARE UPGRADE FILE

This section applies to Polycom and Sony endpoints only.



#### Procedure

- 1 Click **Settings** in the sidebar menu.
  - 2 Click **Endpoint Management**.
  - 3 Click **Software Upgrade Files**.
  - 4 Select the type of endpoint you require in the **Endpoint type** field.
  - 5 Click **Add**.
  - 6 Enter the full path of the software upgrade file to be added to the iVIEW Network Manager database, or browse to the file.
  - 7 Enter a name and description for the upgrade file in the relevant fields.
  - 8 (Polycom endpoints only) Enter a related version number for the upgrade file.
  - 9 Click **OK** to save your changes.
- 

### MODIFYING A SOFTWARE UPGRADE FILE

This section applies to Polycom and Sony endpoints only.

You can change the name and description of a software upgrade file that you have already added to iVIEW Network Manager.



#### Procedure

- 1 Click **Settings** in the sidebar menu.
- 2 Click **Endpoint Management**.
- 3 Click **Software Upgrade Files**.
- 4 Select the type of endpoint you require in the Endpoint type field.

- 5 Do one of the following:
    - Double-click the software upgrade file you require.
    - Select the software upgrade file you require and click **Edit**.
    - Right-click the software upgrade file you require and select **Edit**.
  - 6 Enter a new name and description for the upgrade file in the relevant fields.
  - 7 Click **OK** to save your changes.
- 

### REMOVING A SOFTWARE UPGRADE FILE

This section applies to Polycom and Sony endpoints only.



#### Procedure

- 1 Click **Settings** in the sidebar menu.
- 2 Click **Endpoint Management**.
- 3 Click **Software Upgrade Files**.
- 4 Select the type of endpoint you require in the Endpoint type field.
- 5 Do one of the following:
  - Select the software upgrade file you require and click **Delete**.
  - Right-click the software upgrade file you require and select **Delete**.
- 6 Click **OK** to save your changes.

The software upgrade file is removed from the database.

---

### HOW TO MANAGE ENDPOINT CONFIGURATION FILES

iVIEW Network Manager enables you to manage endpoint configuration files for the Polycom and Sony endpoints on your network.

- [Viewing Saved Endpoint Configuration Files](#) on page 261
- [Viewing Saved Endpoint Configuration Files](#) on page 261
- [Removing an Endpoint Configuration File](#) on page 262

## VIEWING SAVED ENDPOINT CONFIGURATION FILES

This section applies to Polycom and Sony endpoints only.



### Procedure

- 1 Click **Settings** in the sidebar menu.
  - 2 Click **Endpoint Management**.
  - 3 Click **Configuration Files**.
  - 4 Select the type of endpoint you require in the Endpoint type field.  
The Configuration Files tab displays the configuration files previously retrieved from endpoints and saved in the iVIEW Network Manager database.
- 

## MODIFYING AN ENDPOINT CONFIGURATION FILE

This section applies to Polycom and Sony endpoints only.

You can change the name and description of an endpoint configuration file that you have already added to iVIEW Network Manager.



### Procedure

- 1 Click **Settings** in the sidebar menu.
  - 2 Click **Endpoint Management**.
  - 3 Click **Configuration Files**.
  - 4 Select the type of endpoint you require in the Endpoint type field.
  - 5 Do one of the following:
    - Double-click the endpoint configuration file you require.
    - Select the endpoint configuration file you require and click **Edit**.
    - Right-click the endpoint configuration file you require and select **Edit**.
  - 6 Enter a new name and description for the configuration file in the relevant fields.
  - 7 Click **OK** to save your changes.
-

## REMOVING AN ENDPOINT CONFIGURATION FILE



This section applies to Polycom and Sony endpoints only.

### Procedure

- 1 Click **Settings** in the sidebar menu.
- 2 Click **Endpoint Management**.
- 3 Click **Configuration Files**.
- 4 Select the type of endpoint you require in the Endpoint type field.
- 5 Do one of the following:
  - Select the log entry you require and click **Delete**.
  - Right-click the log entry you require and select **Delete**.
- 6 Click **OK** to save your changes.

The endpoint configuration file is removed from the database.

---

## UPGRADING SOFTWARE FOR SELECTED ENDPOINTS

This section applies to Polycom and Sony endpoints only.

The Upgrade software button enables you to upgrade the software version of selected endpoints with a software file that has been previously saved in the iVIEW Network Manager database Settings > Endpoint Management > Software Upgrade Files.

Only generic parameters are retrieved. Endpoint-specific parameters, such as the endpoint IP address, are not included.

- [Upgrading Software for Sony Endpoints](#) on page 262
- [Upgrading Software for Polycom Endpoints](#) on page 263

## UPGRADING SOFTWARE FOR SONY ENDPOINTS



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
- 2 Click **Endpoints** in the required zone.
- 3 Locate the endpoint you require from the list in the panel on the right.
- 4 Do one of the following:

- Right-click the endpoint and select **Update > Upgrade Software**.
- Select the endpoint and click the **Update software** button.

The Upgrade software window appears, showing a list of the software upgrade files stored in the iVIEW Network Manager database that are associated with the selected endpoint types.

- 5 Select the file with which to update the selected endpoints.
  - 6 Click **OK** to start upgrading endpoint software.
- 

## UPGRADING SOFTWARE FOR POLYCOM ENDPOINTS



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Click **Endpoints** in the required zone.
  - 3 Right-click the endpoint you require from below the Endpoints node in the network tree.
  - 4 Select **Update > Upgrade Software**.  
The Upgrade software window appears, showing a list of the software upgrade files stored in the iVIEW Network Manager database that are associated with the selected endpoint types.
  - 5 Select the file with which to update the selected endpoints.
  - 6 Click **OK** to start upgrading endpoint software.
-

### UPDATING CONFIGURATION FOR SELECTED ENDPOINTS

This section applies to Polycom and Sony endpoints only.

The Update configuration button enables you to update selected endpoints with a configuration file that has been previously retrieved and saved at Settings > Endpoint Management > Configuration Files.

- [Updating Configuration for Sony Endpoints](#) on page 264
- [Updating Configuration for Polycom Endpoints](#) on page 265

### UPDATING CONFIGURATION FOR SONY ENDPOINTS



#### Procedure

- 1 Click **Network Tree** in the sidebar menu.
- 2 Click **Endpoints** in the required zone.
- 3 Locate the endpoint you require from the list in the panel on the right.
- 4 Do one of the following:
  - Right-click the endpoint and select **Update > Update configuration**.
  - Select the endpoint and click the **Update configuration** button.

The Update configuration window shows a list of the configuration files stored in the iVIEW Network Manager database that are associated with the selected endpoint types.

Only generic parameters are retrieved. Endpoint-specific parameters, such as the endpoint IP address, are not included

- 5 Select the file with which to update the selected endpoints.
  - 6 Click **OK** to start updating endpoint configuration.
-

## UPDATING CONFIGURATION FOR POLYCOM ENDPOINTS



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Click **Endpoints** in the required zone.
  - 3 Right-click the endpoint you require from below the Endpoints node in the network tree.
  - 4 Select **Update > Update configuration**.  
The Update configuration window shows a list of the configuration files stored in the iVIEW Network Manager database that are associated with the selected endpoint types.  
Only generic parameters are retrieved. Endpoint-specific parameters, such as the endpoint IP address, are not included.
  - 5 Select the file with which to update the selected endpoints.
  - 6 Click **OK** to start updating endpoint configuration.
- 

## SETTING THE MANAGED STATUS OF POLYCOM ENDPOINTS



### Procedure

Managed endpoints are displayed below the Endpoints entry for each zone in the network.

- 1 Click **Network Tree** in the sidebar menu.
- 2 Click **Endpoints**.
- 3 Right-click the endpoint you require in the Endpoints tab.
- 4 Select **Manage**.
- 5 (Optional) Modify the endpoint display name.
- 6 (Optional) Select **Set iVIEW NMS as the default trap server** to use iVIEW Network Manager as the SNMP trap server for the endpoint.

- 7 Click **OK**.
  - 8 Click **Refresh** to update the new settings.
- 

## HOW TO MANAGE THE ENDPOINT UPLOAD LOG

iVIEW Network Manager enables you to manage the upload log for Polycom and Sony endpoints that support a software upgrade or an update configuration.

- [Viewing Your Endpoint Configuration Upload History](#) on page 266
- [Uploading a File After a Failed Attempt](#) on page 266
- [Removing Entries from the Upload Log](#) on page 267

## VIEWING YOUR ENDPOINT CONFIGURATION UPLOAD HISTORY

This section applies to Polycom and Sony endpoints only.



### Procedure

- 1 Click **Settings** in the sidebar menu.
- 2 Click **Endpoint Management**.
- 3 Click **Upload Log**.
- 4 Select the type of endpoint you require in the **Endpoint type** field.

The Upload Log tab displays the history of all your attempts to upload a software upgrade file, and shows all scheduled future upload attempts.

---

## UPLOADING A FILE AFTER A FAILED ATTEMPT

This section applies to Polycom and Sony endpoints only.



### Procedure

- 1 Click **Settings** in the sidebar menu.
- 2 Click **Endpoint Management**.
- 3 Click **Upload Log**.
- 4 Select the type of endpoint you require in the Endpoint type field.
- 5 Do one of the following to attempt to upload an endpoint configuration file after a previous upload attempt has failed:

- Select the log entry you require and click **Retry**.
  - Right-click the log entry you require and select **Retry**.
- 6 Click **OK** to save your changes.
- 

## REMOVING ENTRIES FROM THE UPLOAD LOG



This section applies to Polycom and Sony endpoints only.

### Procedure

- 1 Click **Settings** in the sidebar menu.
  - 2 Click **Endpoint Management**.
  - 3 Click **Upload Log**.
  - 4 Select the type of endpoint you require in the Endpoint type field.
  - 5 Do one of the following to remove a single log entry:
    - Select the log entry you require and click **Delete**.
    - Right-click the log entry you require and select **Delete**.
  - 6 Click **OK** to save your changes.
  - 7 Click **Delete All** to remove all entries from the log.
  - 8 Click **OK** to save your changes.
-

## How to Manage the Endpoint Upload Log

# 28

## MANAGING THE ECS IN iVIEW NETWORK MANAGER

---

- [How to Manage Services](#) on page 269
- [How to Manage Prefixes](#) on page 273
- [How to Configure a Parent Gatekeeper](#) on page 281
- [How to Manage Parent Filters](#) on page 282
- [How to Configure a Child Gatekeeper](#) on page 283
- [How to Manage Child Prefixes](#) on page 285
- [How to Configure a Neighbor Gatekeeper](#) on page 286
- [How to Manage Zones](#) on page 288
- [How to Manage Bandwidth Rules](#) on page 289
- [How to Manage Debug Flags](#) on page 291
- [Configuring an ECS](#) on page 292

### **HOW TO MANAGE SERVICES**

- [Viewing ECS Supported Services](#) on page 270
- [Creating or Modifying a Service](#) on page 270
- [Viewing Global Services](#) on page 271
- [Creating or Modifying a Global Service](#) on page 272
- [Removing a Service](#) on page 272

## VIEWING ECS SUPPORTED SERVICES

The Services tab displays the list of predefined and online services supported by the ECS selected in the tree.



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
- 2 Select the ECS you require in the tree.
- 3 Click **Services**.

[Table 28-1](#) describes the information displayed on the Services tab.

**Table 28-1** Services Tab Parameters

| Parameter          | Description                                                     |
|--------------------|-----------------------------------------------------------------|
| Prefix             | Prefix used to access the service                               |
| Description        | Service description                                             |
| Status             | Indicates whether the service is predefined or online           |
| Conference Hunting | Indicates whether conference hunting is enabled for the service |
| In-Zone Default    | Default policy for in-zone endpoints                            |
| Out of Zone        | Service policy for out-of-zone endpoints                        |

## CREATING OR MODIFYING A SERVICE



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
- 2 Select the ECS you require in the tree.
- 3 Click **Services**.
- 4 Do one of the following to modify an existing service:
  - ❑ Double-click the service you require.
  - ❑ Select the service you require and click **Edit**.

- Right-click the service you require and select **Edit**
  - 5 Do one of the following to create a new service:
    - Click **Add**.
    - Right-click any existing service and select **Add**.
  - 6 Enter the prefix used to access the service.
  - 7 Select the service type.
  - 8 Enter a description of the service.
  - 9 Select whether to enable conference hunting.
  - 10 Select whether to allow access to in-zone endpoints.
  - 11 Select whether to allow access to out-of-zone endpoints.
  - 12 Click **OK** to save your changes.
- 

## VIEWING GLOBAL SERVICES



The Global Services tab displays the list of global services which can be configured for the selected ECS.

### Procedure

- 1 Click **Network Tree** in the sidebar menu.
- 2 Select the ECS you require in the tree.
- 3 Click **Global Services**.

[Table 28-1](#) describes the information displayed on the Global Services tab.

---

**Table 28-2**      *Global Services Tab Parameters*

| Parameter        | Description                                                                         |
|------------------|-------------------------------------------------------------------------------------|
| Prefix           | Prefix used to access the service                                                   |
| Description      | Service description                                                                 |
| Central Database | Indicates whether or not the global service was retrieved from the central database |

---

## CREATING OR MODIFYING A GLOBAL SERVICE



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Select the ECS you require in the tree.
  - 3 Click **Global Services**.
  - 4 Do one of the following to modify an existing global service:
    - Double-click the service you require.
    - Select the service you require and click **Edit**.
    - Right-click the service you require and select **Edit**.
  - 5 Do one of the following to create a new global service:
    - Click **Add**.
    - Right-click any existing service and select **Add**.
  - 6 Enter the prefix used to access the service.
  - 7 Enter a description of the service.
  - 8 Click **OK** to save your changes.
- 

## REMOVING A SERVICE



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Select the ECS you require in the tree.
  - 3 Click **Services** or **Global Services**.
  - 4 Do one of the following:
    - Select the service you require and click **Delete**.
    - Right-click the service you require and select **Delete**.
  - 5 Click **OK** to save your changes.  
The service is removed from the database.
-

## HOW TO MANAGE PREFIXES

The Prefixes tab enables you to assign prefixes to local and remote ECS zones, configure the method for sending LRQ messages to each destination for address resolution and assign Gateway priorities.

- [Creating or Modifying a Prefix](#) on page 273
- [Removing a Prefix](#) on page 273
- [Bandwidth Tab \(ECS version 3.5 or later\)](#) on page 274

### CREATING OR MODIFYING A PREFIX



#### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Select the ECS you require in the tree.
  - 3 Click **Prefixes**.
  - 4 Select the prefix you require and click **Edit** to modify an existing prefix.
  - 5 Click **Add** to create a new prefix.
  - 6 Configure prefixes with which the ECS performs address resolution, sends LRQ messages simultaneously and configures Gateway priorities per zone.
  - 7 (Optional) Select a zone, enter a prefix number and select **Blast** to send LRQ messages simultaneously.
  - 8 Click **Upload** to save your changes to the ECS database.
- 

### REMOVING A PREFIX



#### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Select the ECS you require in the tree.
  - 3 Click **Prefixes**.
  - 4 Select the prefix you require and click **Delete**.
  - 5 Click **Yes** to remove the prefix from the ECS database.
-

**BANDWIDTH TAB  
(ECS VERSION 3.5  
OR LATER)**

The Bandwidth tab enables you to define subzones and subzone rules, and to determine bandwidth policy between zones and subzones for ECS version 3.5 or later.

**Figure 28-1** Network Tree—Bandwidth Tab (ECS version 3.5 or later)

| Monitor             | Alarms               | Events   | Calls     | Configure | Services  |        |        |
|---------------------|----------------------|----------|-----------|-----------|-----------|--------|--------|
| Global Services     | Parent               | Children | Neighbors | Subzones  | Bandwidth | Logs   | Access |
| Inter-subzone rules |                      |          |           |           |           |        |        |
| Name                | Description          | Allowed  | Used      | Available | Dedicated | Add    |        |
| Subzone Default     | Subzone default b... | 100000   | 0         | 100000    | no        | Edit   |        |
|                     |                      |          |           |           |           | Delete |        |
| Inter-zone rules    |                      |          |           |           |           |        |        |
| Name                | Description          | Allowed  | Used      | Available | Dedicated | Add    |        |
| ECS Default         | ECS default band...  | 100000   | 0         | 100000    | no        | Edit   |        |
| Test                | iView Test           | 200000   | 0         | 200000    | no        | Delete |        |

The Bandwidth tab displays the following information.

---

**Note** Details are displayed for both inter-subzone rules and for inter-zone rules.

---

- Name—Displays the name of the specified rule.
- Description—Displays the description of the specified rule.
- Allowed—Displays the total bandwidth (in Kbps) allowed by the specified rule.
- Used—Displays the bandwidth (in Kbps) currently used by calls governed by the specified rule.
- Available—Displays the free bandwidth (in Kbps) currently available to calls governed by the specified rule.  
Displays 0 when available minus used bandwidth < 0.
- Dedicated—Indicates whether or not the rule applies to a specific dedicated connection only.

## ADDING OR MODIFYING INTER-SUBZONE RULES



### Procedure

- 1 To create an inter-subzone bandwidth rule, click **Add**.

The Add Bandwidth Rules window appears.

-or-

To modify an existing inter-subzone rule, double-click the required inter-subzone rule, or select the required inter-subzone rule and click **Edit**.

The Edit Bandwidth Rules window appears.

---

**Note** If you select the **Subzone Default** entry, the **Edit Bandwidth Rule** window displays default settings only. For more information, see XREF.

---

**Figure 28-2** Add Bandwidth Rules Window (Inter-subzone)

The screenshot shows a Java Applet Window titled "Add Bandwidth Rule". It contains the following elements:

- Name:** An empty text input field.
- Description:** An empty text input field.
- Connection From:** A section with two checkboxes: "Subzone 1" and "Subzone 2".
- Connecting To:** A section with three checkboxes: "Subzone 1", "Subzone 2", and "Any non-dedicated subzone".
- Allowed:** An empty text input field.
- Dedicated:** A checkbox that is currently unchecked.
- Buttons:** "OK" and "Cancel" buttons at the bottom center.
- Footer:** The text "Java Applet Window" is located at the bottom left corner.

- 2 Configure the following in the Add Bandwidth Rules window:
    - ❑ Name—Enter the required name of the inter-subzone rule.
    - ❑ Description—Enter the required description of the inter-subzone rule.
    - ❑ Connecting—Select to apply the specified inter-subzone rule to specific subzones only. Select the required subzones from the lists displayed.
    - ❑ Any non-dedicated subzones—Check to apply the specified inter-subzone rule to all subzones within the zone.
    - ❑ Allowed—Enter the bandwidth (in Kbps) allowed by the specified inter-subzone rule.
    - ❑ Dedicated—When checked, the call is not included in the used bandwidth calculation. A dedicated rule applies to a specific dedicated connection only.
  - 3 To save the file in the iVIEW Network Manager database, click **OK** or to cancel the operation, click **Cancel**.
- 

### VIEWING OR MODIFYING THE DEFAULT INTER-SUBZONE RULE

The default inter-subzone rule applies to any intra-zone call that does not match any of the configured inter-subzone bandwidth rules.



#### Procedure

- 1 Double-click the subzone default inter-subzone rule, or select the subzone default inter-subzone rule and click **Edit**.  
The Edit Bandwidth Rules window appears showing the default settings.

**Figure 28-3** Edit Bandwidth Rules Window—Default

The screenshot shows a Java Applet Window titled "Edit Bandwidth Rule". The window contains the following fields and controls:

- Name:** Subzone Default
- Description:** Subzone default bandwidth rule
- Text Area:** Default inter-subzone rule. This rule applies to any i
- Allowed:** 100000
- Dedicated:**  Dedicated
- Buttons:** OK, Cancel
- Footer:** Java Applet Window

- 2 Configure the following in the Edit Bandwidth Rules window:
    - Name—Displays the name of the default inter-subzone rule.
    - Description—Displays the description of the default inter-subzone rule.
    - Allowed bandwidth—Enter the bandwidth (in Kbps) allowed by the default inter-subzone rule.
    - Dedicated—A default rule cannot be dedicated. Disabled for the default inter-subzone rule.
  - 3 To save the file in the iVIEW Network Manager database, click **OK** or to cancel the operation, click **Cancel**.
-

## ADDING OR MODIFYING INTER-ZONE RULES



The **Add Bandwidth Rules** window enables you to create an inter-zone bandwidth rule.

### Procedure

- 1 Click **Add**.

The Add Bandwidth Rule window appears.

-or-

To modify an existing inter-zone rule, double-click the required inter-zone rule, or select the required inter-zone rule and click **Edit**.

The Edit Inter-zone Bandwidth Rules window appears.

---

**Note** If you select the **Zone Default** entry, the **Edit Bandwidth Rule** window displays default settings only. For more information, see the [Viewing or Modifying the Default Inter-subzone Rule](#) section on page 276.

---

**Figure 28-4** Inter-zone Bandwidth Rules Window

| Gatekeeper IP | Add    |
|---------------|--------|
|               | Edit   |
|               | Delete |

- 2 Configure the following in the Inter-zone Bandwidth Rules window:
    - ❑ Name—Enter the required name of the inter-zone rule.
    - ❑ Description—Enter the required description of the inter-zone rule.
    - ❑ Gatekeeper IP—Select the required destination gatekeepers to which the rule is applied.
    - ❑ Add—To display the Add Gatekeeper window for adding additional gatekeepers to the displayed list, click **Add**.
    - ❑ Allowed—Enter the bandwidth (in Kbps) allowed by the specified inter-zone rule.
    - ❑ Outgoing—Enter the bandwidth (in Kbps) that you want you to reserve for outgoing calls only. Reserved bandwidth is deducted from the total allowed bandwidth.
    - ❑ Dedicated—When checked, the call is not included in the used bandwidth calculation.
  - 3 To save the file in the iVIEW Network Manager database, click **OK** or to cancel the operation, click **Cancel**.
- 

## VIEWING OR MODIFYING THE DEFAULT INTER-ZONE RULE

The default inter-zone rule applies to any inter-zone call that does not match any of the configured inter-zone bandwidth rules.

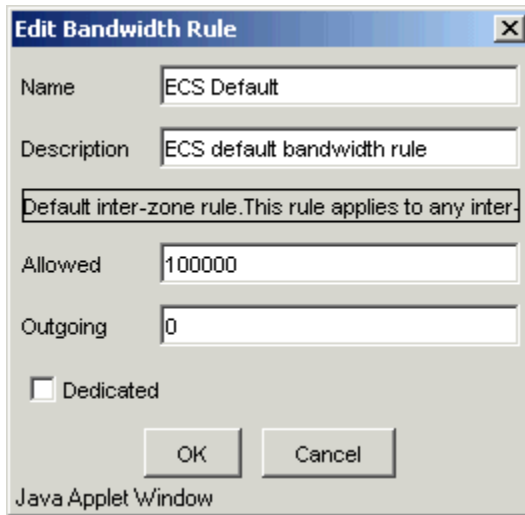


### Procedure

- 1 Double-click the ECS **Default** inter-zone rule, or select the ECS **Default** inter-zone rule and click **Edit**.

The Edit Bandwidth Rules window appears indicating default settings.

**Figure 28-5** *Inter-zone Bandwidth Rules Window—Default*



- 2 Configure the following in the default Inter-zone Bandwidth Rules window:
    - Name—Displays the name of the default inter-zone rule.
    - Description—Displays the description of the default inter-zone rule.
    - Allowed—Enter the bandwidth (in Kbps) allowed by the default inter-zone rule.
    - Outgoing—Enter the bandwidth (in Kbps) that you want you to reserve for outgoing calls only.
    - Dedicated—A default rule cannot be dedicated. Disabled for the default inter-zone rule.
-

## HOW TO CONFIGURE A PARENT GATEKEEPER

The ECS sends an LRQ to the parent gatekeeper when the zone prefix of the call matches one of the defined parent filters. If the ECS fails to match the zone prefix of the call with any of the defined parent filters, the ECS either rejects the call or forwards the call according to the Call Fallback settings configured in the ECS element manager. Where no filters are defined, the ECS passes the call to the parent gatekeeper. The ECS allows a maximum of ten parent filters.

- [Enabling the Parent Tab](#) on page 281
- [Adding a Parent Manually](#) on page 281
- [Adding a Parent Automatically](#) on page 282

## ENABLING THE PARENT TAB

The Parent tab is not available in ECS version 1.0 and INVISION ECS.



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Select the ECS you require in the tree.
  - 3 Click **Configure**.
  - 4 Select **Version 2** in the Dial plan version field.
  - 5 Ensure that Use Central Database is deselected.
  - 6 Click **Upload** to save your changes.
- 

## ADDING A PARENT MANUALLY



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Select the ECS you require in the tree.
  - 3 Click **Parent**.
  - 4 Select **Enabled**.
  - 5 Enter the IP address, port number and description of the parent gatekeeper in the relevant fields.
  - 6 (Optional) Add a parent filter.
  - 7 Click **Upload** to save your changes.
-

## ADDING A PARENT AUTOMATICALLY



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
- 2 Drag and drop the ECS element into the zone of the gatekeeper you want to configure as the parent gatekeeper.

The ECS Parent tab is automatically updated with the parent gatekeeper details.

---

## HOW TO MANAGE PARENT FILTERS

- [Creating or Modifying a Parent Filter](#) on page 282
- [Removing a Parent Filter](#) on page 283

## CREATING OR MODIFYING A PARENT FILTER



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Select the ECS you require in the tree.
  - 3 Click **Parent**.
  - 4 Locate the Parent Filters section.
  - 5 Select the parent filter you require and click **Edit** to modify an existing parent filter.
  - 6 Click **Add** to create a new parent filter.
  - 7 Enter a name for the parent filter and click **OK**.
  - 8 Click **Upload** to save the filter to the ECS database.
-

## REMOVING A PARENT FILTER



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Select the ECS you require in the tree.
  - 3 Click **Parent**.
  - 4 Locate the Parent Filters section.
  - 5 Select the parent filter you require and click **Delete**.
  - 6 Click **Yes** to remove the filter from the ECS database.
- 

## HOW TO CONFIGURE A CHILD GATEKEEPER

- [Enabling the Children Tab](#) on page 283
- [Viewing Child Gatekeepers](#) on page 284
- [Adding a Child Manually](#) on page 284
- [Adding a Child Automatically](#) on page 285

## ENABLING THE CHILDREN TAB

The Parent tab is not available in ECS version 1.0 and INVISION ECS.



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Select the ECS you require in the tree.
  - 3 Click **Configure**.
  - 4 Select **Version 2** in the Dial plan version field.
  - 5 Ensure that Use Central Database is deselected.
  - 6 Click **Upload** to save your changes.
-

## VIEWING CHILD GATEKEEPERS



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
- 2 Select the ECS you require in the tree.
- 3 Click **Children**.

[Table 28-1](#) describes the information displayed on the Children tab.

**Table 28-3** *Children Tab Parameters*

| Parameter        | Description                                                                                                      |
|------------------|------------------------------------------------------------------------------------------------------------------|
| Description      | Displays the child gatekeeper description in free text.                                                          |
| Prefixes         | Displays the zone prefix.                                                                                        |
| IP Address       | Displays the IP address of the child gatekeeper.                                                                 |
| Port             | Displays the port number of the child gatekeeper.                                                                |
| Proxy            | Indicates whether or not the ECS routes calls from this zone to the neighbor gatekeeper through the Cisco Proxy. |
| Central Database | Indicates whether or not the child gatekeeper was retrieved from the central database.                           |

## ADDING A CHILD MANUALLY



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
- 2 Select the ECS you require in the tree.
- 3 Click **Children**.
- 4 Click **Add**.
- 5 Enter the IP address, port number and description of the parent gatekeeper in the relevant fields.

- 6 (Optional) Select **Use Cisco Proxy** to route calls from this zone to the neighbor gatekeeper via the Cisco Proxy.
  - 7 Add required prefixes from the list of defined child prefixes.  
The ECS sends an LRQ to the child gatekeeper when the zone prefix of the call matches one of the defined child prefixes. If the ECS fails to match the zone prefix of the call with any of the defined child gatekeeper prefixes, the ECS passes the call to a neighbor gatekeeper.
  - 8 Click **Upload** to save your changes to the ECS database.
- 

## ADDING A CHILD AUTOMATICALLY



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Drag and drop the ECS element you want to configure as the child gatekeeper into the zone of the current ECS.  
The Children tab of the parent ECS is automatically updated with the child gatekeeper details.
- 

## HOW TO MANAGE CHILD PREFIXES

- [Creating or Modifying a Child Prefix](#) on page 285
- [Removing a Child Prefix](#) on page 286

## CREATING OR MODIFYING A CHILD PREFIX



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
- 2 Select the ECS you require in the tree.
- 3 Click **Children**.
- 4 Open the required child gatekeeper profile.
- 5 Select the prefix you require and click **Edit** to modify an existing prefix.
- 6 Click **Add** to create a new prefix.

- 7 Enter a name for the prefix and click **OK**.
  - 8 Click **Upload** to save the prefix to the ECS database.
- 

## REMOVING A CHILD PREFIX



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Select the ECS you require in the tree.
  - 3 Click **Children**.
  - 4 Open the required child gatekeeper profile.
  - 5 Select the prefix you require and click **Delete**.
  - 6 Click **Yes** to remove the prefix from the ECS database.
- 

## HOW TO CONFIGURE A NEIGHBOR GATEKEEPER

- [Viewing Neighbor Gatekeepers](#) on page 286
- [Adding or Modifying a Neighbor Gatekeeper](#) on page 287

## VIEWING NEIGHBOR GATEKEEPERS



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
- 2 Select the ECS you require in the tree.
- 3 Click **Neighbors**.

[Table 28-1](#) describes the information displayed on the Neighbors tab.

**Table 28-4** *Neighbors Tab Parameters*

| Parameter        | Description                                                                                                      |
|------------------|------------------------------------------------------------------------------------------------------------------|
| Description      | Displays the neighbor gatekeeper description in free text.                                                       |
| Prefixes         | Displays the zone prefix.                                                                                        |
| IP Address       | Displays the IP address of the neighbor gatekeeper.                                                              |
| Port             | Displays the port number of the neighbor gatekeeper.                                                             |
| Proxy            | Indicates whether or not the ECS routes calls from this zone to the neighbor gatekeeper through the Cisco Proxy. |
| GK ID            | Displays the neighbor gatekeeper identifier.                                                                     |
| Central Database | Indicates whether or not the child gatekeeper was retrieved from the central database.                           |
| LDAP             | Indicates whether or not the child gatekeeper was retrieved from the LDAP server.                                |

## ADDING OR MODIFYING A NEIGHBOR GATEKEEPER



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
- 2 Select the ECS you require in the tree.
- 3 Click **Neighbors**.
- 4 Do one of the following to modify an existing neighbor gatekeeper:
  - Double-click the ECS you require.
  - Select the ECS you require and click **Edit**.
  - Right-click the ECS you require and select **Edit**.
- 5 Do one of the following to create a new service:
  - Click **Add**.
  - Right-click any existing ECS and select **Add**.

- 6 Enter the neighbor gatekeeper zone prefix.
  - 7 Enter the description, IP address and port number of the neighbor gatekeeper in the relevant fields.
  - 8 (Optional) Select **Use Cisco Proxy** to route calls from this zone to the neighbor gatekeeper via the Cisco Proxy.
  - 9 Click **Upload** to save your changes to the ECS database.
- 

## HOW TO MANAGE ZONES

- [Creating or Modifying a Local Zone](#) on page 288
- [Creating or Modifying a Remote Zone](#) on page 288
- [Removing a Zone](#) on page 289

## CREATING OR MODIFYING A LOCAL ZONE



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Select the ECS you require in the tree.
  - 3 Click **Local Zones**.
  - 4 Select the zone you require and click **Edit** to modify an existing local zone.
  - 5 Click **Add** to create a new local zone.
  - 6 Enter a zone name and the zone domain.
  - 7 Click **Upload** to save your changes to the ECS database.
- 

## CREATING OR MODIFYING A REMOTE ZONE



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
- 2 Select the ECS you require in the tree.
- 3 Click **Remote Zones**.

- 4 Select the zone you require and click **Edit** to modify an existing remote zone.
  - 5 Click **Add** to create a new remote zone.
  - 6 Enter a zone name, zone domain, IP address and port.
  - 7 Click **Upload** to save your changes to the ECS database.
- 

## REMOVING A ZONE



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Select the ECS you require in the tree.
  - 3 Click **Local Zones** or **Remote Zones**.
  - 4 Select the zone you require and click **Delete**.
  - 5 Click **Yes** to remove the zone from the ECS database.
- 

## HOW TO MANAGE BANDWIDTH RULES

The BW Rules tab enables you control the bandwidth of H.323 traffic both in the ECS zone and between the ECS and other zones. Bandwidth rules per session or specific zones can also be specified. A default setting specifies a bandwidth rule for all zones with which the ECS operates.

- [Viewing Neighbor Gatekeepers](#) on page 286
- [Creating or Modifying a Bandwidth Rule](#) on page 290
- [Removing a Bandwidth Rule](#) on page 291

## VIEWING BANDWIDTH RULES



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
- 2 Select the ECS you require in the tree.
- 3 Click **BW Rules**.

[Table 28-1](#) describes the information displayed on the BW Rules tab.

**Table 28-5** *BW Rules Tab Parameters*

| Parameter | Description                                                                                  |
|-----------|----------------------------------------------------------------------------------------------|
| Total     | Indicates the total amount of bandwidth for H.323 traffic allowed in this zone.              |
| Remote    | Indicates the total amount of bandwidth for H.323 traffic from this zone to all other zones. |
| Interzone | Indicates the total amount of bandwidth for H.323 traffic from this zone to another zone.    |
| Session   | Indicates the maximum bandwidth allowed for a session in the zone.                           |
| Default   | Indicates whether or not the default value for all zones is configured in this rule.         |

## CREATING OR MODIFYING A BANDWIDTH RULE



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
- 2 Select the ECS you require in the tree.
- 3 Click **BW Rules**.
- 4 Select the rule you require and click **Edit** to modify an existing bandwidth rule.
- 5 Click **Add** to create a new bandwidth rule.
- 6 Select the scope of the bandwidth rule, indicate whether the rule is the default for all zones, select a zone and maximum bandwidth rate.
- 7 Click **Upload** to save your changes to the ECS database.

## REMOVING A BANDWIDTH RULE



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Select the ECS you require in the tree.
  - 3 Click **BW Rules**.
  - 4 Select the bandwidth rule you require and click **Delete**.
  - 5 Click **Yes** to remove the bandwidth rule from the ECS database.
- 

## HOW TO MANAGE DEBUG FLAGS

- [Creating or Modifying a Debug Flag](#) on page 291
- [Removing a Debug Flag](#) on page 291

## CREATING OR MODIFYING A DEBUG FLAG



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Select the ECS you require in the tree.
  - 3 Click **Debug Flags**.
  - 4 Select the flag you require and click **Edit** to modify an existing debug flag rule.
  - 5 Click **Add** to create a new debug flag.
  - 6 Enter the debug flag name, a description and enable the flag.
  - 7 Click **Upload** to save your changes to the ECS database.
- 

## REMOVING A DEBUG FLAG



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
- 2 Select the ECS you require in the tree.

- 3 Click **Debug Flags**.
  - 4 Select the debug flag you require and click **Delete**.
  - 5 Click **Yes** to remove the debug flag from the ECS database.
- 

## CONFIGURING AN ECS

The ECS **Configure** tab allows you to configure ECS addressing, registration mode, routing mode, physical location, dial plan version, prefix handling and allow access by the ECS to a central database for network hierarchy management by the ECS Network Configuration (ENC).



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
- 2 Select the ECS you require in the tree.
- 3 Click **Configure**.
- 4 Configure the parameters as follows:
  - ECS ID
  - Registration mode:
    - All—Open zone policy where the ECS accepts any legal registrations from any endpoint.
    - None—Closed zone policy that prevents the ECS from accepting any registrations.

If required, select **Merge predefined and online aliases upon registration** to enable the ECS to assign predefined aliases, identified either by alias or IP address/port number, to an endpoint when that endpoint registers.

- Routing mode:
  - Direct—Routes calls directly with ECS intervention.
  - Call Setup (Q.931)—Routes the Call Setup channel through the ECS.
  - Call Setup (Q.931) and Call control (H.245)—Enables the H.245 Proxy to route the Call Setup channel and the Control channel through the ECS.
  - Location—Enter a string specifying the physical device on which the ECS installed, for display purposes.
  - Dial plan version:

- Version 1—Default setting.
  - Version 2—Enables the parameters defined in the Dial Plan section of the Settings tab in the ECS and enables the Global Services tab, Parent tab and Children tab.
  - Strip prefixes—When selected, enables the ECS to strip zone prefixes in non-gateway calls (internal IP network calls).
  - Strip Gateway Prefixes—When selected, enables the ECS to strip zone prefixes in gateway calls (IP-to-ISDN network calls).
  - 
  - GKTMP port—The port via which the iVIEW Network Manager communicates with the ECS using the GKTMP communication protocol to get calls and registration information from the ECS.
  - 
  - Use Central Database—When selected, enables the ECS to access the central database used by the ENC for network hierarchy management. This option is deselected automatically if you select **Enable Central Hierarchy Management** in the Hierarchy tab.
-

## Configuring an ECS

# 29

## MANAGING AN MCU IN iVIEW NETWORK MANAGER

---

MCU configuration options vary according to MCU version.

- [Setting Call Routing Devices](#) on page 295
- [Viewing Registered Multipoint Processors](#) on page 296
- [Viewing MCU Supported Services](#) on page 297
- [How to Back Up and Restore MCU Configuration Settings](#) on page 297
- [Configuring MCU Unit Type and Addressing](#) on page 299

### SETTING CALL ROUTING DEVICES



#### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Select the MCU you require in the tree.
  - 3 Click **Protocols**.
  - 4 Select **Use H.323 Gatekeeper** or **Use SIP Server** to determine the MCU call routing device.
  - 5 Enter an IP address port value in the relevant fields.
  - 6 Click **Upload** to save your changes.
-

## VIEWING REGISTERED MULTIPOINT PROCESSORS



The term Multipoint Processors (MPs) refers to MCUs and MVPs.

### Procedure

- 1 Click **Network Tree** in the sidebar menu.
- 2 Select the MCU you require in the tree.
- 3 Click **Registered MPs** to view the list of MPs currently registered with the MCU.

[Table 29-1](#) describes the information displayed on the Registered MPs tab.

**Table 29-1** *Registered MPs Tab Parameters*

| Parameter   | Description                                                                                                                                                                  |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type        | Displays the type of MP unit registered with the current MCU. MP unit types supported include:                                                                               |
| MP          | The local MP component of the current MCU or MCU operating in MP Only mode. Performs basic media processing such as audio transcoding, video processing and video switching. |
| MVP         | Unit performing advanced media processing such as video processing and video switching.                                                                                      |
| DCS         | Providing T.120 data collaboration services.                                                                                                                                 |
| Address     | Address of the MP unit. This may be the same as the current MCU if the MP is the media processing component of the current unit.                                             |
| Description | Version number and type.                                                                                                                                                     |

## VIEWING MCU SUPPORTED SERVICES



The Services tab displays the list of services supported by the selected MCU. Services can be edited by clicking the link to the MCU element manager above the Services table.

### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Select the MCU you require in the tree.
  - 3 Click **Services**.
- 

## HOW TO BACK UP AND RESTORE MCU CONFIGURATION SETTINGS

This feature is available for SCOPIA Elite MCUs, but not for SCOPIA Classic MCUs.

- [Backing Up MCU Configuration Settings](#) on page 297
- [Restoring MCU Configuration Settings](#) on page 298
- [Modifying MCU Configuration File Information](#) on page 298
- [Deleting a Configuration File](#) on page 298

## BACKING UP MCU CONFIGURATION SETTINGS



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Select the MCU you require in the tree.
  - 3 Click **Backup & Restore**.
  - 4 Click **Backup**.
  - 5 Enter a description of the MCU configuration file in the Retrieve Configuration File window and click **OK**.
  - 6 Click **OK** in the “Configuration file backup successful” message window to complete the backup procedure.
-

## RESTORING MCU CONFIGURATION SETTINGS



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Select the MCU you require in the tree.
  - 3 Click **Backup & Restore**.
  - 4 Select a configuration file from the list.
  - 5 Click **Restore**.
  - 6 Click **Yes** when prompted by the “Are you sure you want to restore ...?” message.
- 

## MODIFYING MCU CONFIGURATION FILE INFORMATION



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Select the MCU you require in the tree.
  - 3 Click **Backup & Restore**.
  - 4 Select a configuration file from the list.
  - 5 Click **Edit**.
  - 6 Modify the name and description of the configuration file, as required.
  - 7 Click **OK**.
- 

## DELETING A CONFIGURATION FILE



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
- 2 Select the MCU you require in the tree.
- 3 Click **Backup & Restore**.

- 4 Select a configuration file from the list.
  - 5 Click **Delete**.
  - 6 Click **OK**.
- 

## CONFIGURING MCU UNIT TYPE AND ADDRESSING



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
- 2 Select the MCU you require in the tree.
- 3 Click **Configure**.

[Table 29-2](#) describes the information displayed on the Configure tab.

---

**Table 29-2** *Configure Tab Parameters*

| Parameter               | Description                                                                                                                                                                                                                                                                                                          |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Use internal gatekeeper | For use on Gateways and MCUs hosted on the INVISION platform.                                                                                                                                                                                                                                                        |
| Unit Type               | <ul style="list-style-type: none"> <li>■ MCU—The MCU and MP components in the unit work together to provide Call Setup, conference control and media processing.</li> <li>■ MP Only—The MP (Multipoint Processor) unit works in a clustered arrangement operating under the control of an individual MCU.</li> </ul> |
| Location                | Enter a string identifying the physical location of the MCU device.                                                                                                                                                                                                                                                  |
| MCU IP Address          | MCU IP address. Configurable only on MP units.                                                                                                                                                                                                                                                                       |
| Port                    | MCU communication port. Configurable only on MP units.                                                                                                                                                                                                                                                               |

## Configuring MCU Unit Type and Addressing

# 30

## MANAGING A GATEWAY IN iVIEW NETWORK MANAGER

---

### HOW TO MANAGE SERVICES

- [How to Manage Services](#) on page 301
- [Configuring Gateway Addressing](#) on page 303
- [Viewing Gateway Supported Services](#) on page 301
- [Creating or Modifying a Service](#) on page 302
- [Removing a Service](#) on page 302

### VIEWING GATEWAY SUPPORTED SERVICES



#### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Select the gateway you require in the tree.
  - 3 Click **Services**.
-

## CREATING OR MODIFYING A SERVICE



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Select the gateway you require in the tree.
  - 3 Click **Services**.
  - 4 Do one of the following to modify an existing service:
    - Double-click the service you require.
    - Select the service you require and click **Edit**.
    - Right-click the service you require and select **Edit**.
  - 5 Do one of the following to create a new service:
    - Click **Add**.
    - Right-click any existing service and select **Add**.
  - 6 Enter the service prefix description.
  - 7 Select the call type and bit rate.
  - 8 Click **OK**.
- 

## REMOVING A SERVICE



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Select the gateway you require in the tree.
  - 3 Click **Services**.
  - 4 Do one of the following:
    - Select the service you require and click **Delete**.
    - Right-click the service you require and select **Delete**.
  - 5 Click **OK** to save your changes.  
The service is removed from the database.
-

## CONFIGURING GATEWAY ADDRESSING



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Select the gateway you require in the tree.
  - 3 Click **Services**.
  - 4 Enter the IP address of the gatekeeper with which the gateway registers.
  - 5 (Optional) Enter a string identifying the physical location of the gateway.
-

## Configuring Gateway Addressing

# 31

## CONFIGURING A USER PROFILE IN iVIEW NETWORK MANAGER

---

### CREATING OR MODIFYING A USER PROFILE

- [Creating or Modifying a User Profile](#) on page 305
- [Removing a User Profile](#) on page 306
- [How to Define Network Subsets](#) on page 307

iVIEW Network Manager supports three types of network users:

- Administrator—Full read/write access to all managed elements and zones on the network.
- Read only—Read Only access to all elements and zones on the network.
- Local user—Restricted access to managed elements and zones on the network. This user profile is defined with specific read/write and read only access according to zones, elements and criteria for network subsets configured at Settings > Network Subsets.



### Procedure

- 1 Click **Settings** in the sidebar menu.
- 2 Click **Users**.
- 3 Do one of the following to modify an existing user profile:
  - Double-click the link in the User Name column for the user you require.
  - Select the user you require and click **Edit**.

## Removing a User Profile

- Right-click the link in the User Name column for the user you require and select **Edit**.
  - 4 Do one of the following to create a new user profile:
    - Click **Add**.
    - Right-click any link in the User Name column and select **Add**.
  - 5 Enter a name and password for the user in the relevant fields, and select the appropriate user access level.
  - 6 (For local users only) Select read/write access and read only access permissions according to zones and criteria for network subsets defined at Settings > Network Subsets.
  - 7 (For local users only) Select **Can add elements** to enable a local user to add new elements to the iVIEW Network Manager database throughout all network zones and subsets.
  - 8 Click **OK** to save your changes.
- 

## REMOVING A USER PROFILE



### Procedure

- 1 Click **Settings** in the sidebar menu.
  - 2 Click **Users**.
  - 3 Do one of the following:
    - Select the user you require and click **Delete**.
    - Right-click the link in the User Name column for the user you require and select **Delete**.
  - 4 Click **OK** to save your changes.
- The user profile is removed from the database.
-

## HOW TO DEFINE NETWORK SUBSETS

Network subsets enable you to define areas of the network according to zones and element types using include and exclude criteria for use with Local user access level profiles.

- [Creating or Modifying a Network Subset](#) on page 307
- [Removing a Network Subset](#) on page 308
- [Removing an Include or Exclude Criterion](#) on page 308

## CREATING OR MODIFYING A NETWORK SUBSET



### Procedure

- 1 Click **Settings** in the sidebar menu.
- 2 Click **Network Subsets**.
- 3 Do one of the following to modify an existing network subset:
  - Double-click the network subset you require.
  - Select the network subset you require and click **Edit**.
  - Right-click the network subset you require and select **Edit**.
- 4 Do one of the following to create a new network subset:
  - Click **Add**.
  - Right-click any network subset and select **Add**.
- 5 Enter a name for the network subset.  
A subset contains all elements which match at least one include criterion but do not match any exclude criterion.
- 6 Do one of the following to modify an existing include or exclude criterion:
  - Double-click the criterion you require.
  - Select the criterion you require and click **Edit**.
  - Right-click the criterion you require and select **Edit**.
- 7 Do one of the following to create a new include or exclude criterion:
  - Click **Add**.
  - Right-click any criterion and select **Add**.
- 8 Select a zone and element type in the relevant fields, and indicate whether or not child zones of the specified zone are contained in the criterion.

- 9 Click **OK** to add the criterion to the relevant list in the Add Network Subset window.
  - 10 Click **OK** to save your changes.
- 

## REMOVING A NETWORK SUBSET



### Procedure

- 1 Click **Settings** in the sidebar menu.
  - 2 Click **Network Subsets**.
  - 3 Do one of the following:
    - Select the network subset you require and click **Delete**.
    - Right-click the network subset you require and select **Delete**.
  - 4 Click **OK** to save your changes.
- 

## REMOVING AN INCLUDE OR EXCLUDE CRITERION



### Procedure

- 1 Click **Settings** in the sidebar menu.
  - 2 Click **Network Subsets**.
  - 3 Do one of the following:
    - Double-click the network subset you require.
    - Select the network subset you require and click **Edit**.
    - Right-click the network subset you require and select **Edit**.
  - 4 Do one of the following:
    - Select the criterion you require and click **Delete**.
    - Right-click the criterion you require and select **Delete**.
  - 5 Click **OK** to save your changes.
-

# 32

## MANAGING TRAPS AND ALARMS IN iVIEW NETWORK MANAGER

---

- [Sending Traps to iVIEW Network Manager](#) on page 310
- [Creating or Modifying a Trap Forwarding Rule](#) on page 310
- [Disabling a Trap Forwarding Rule](#) on page 311
- [Removing a Trap Forwarding Rule](#) on page 311
- [Creating or Modifying an Alert Recipient Profile](#) on page 312
- [Removing an Alert Recipient Profile](#) on page 313
- [Viewing Generated Events](#) on page 313
- [Filtering Generated Events](#) on page 314
- [Viewing Events per Network Item](#) on page 314
- [Viewing and Sorting Supported Alarms](#) on page 315
- [Modifying Alarms](#) on page 315
- [Viewing and Sorting Generated Alarms](#) on page 316
- [Viewing Generated Alarms per Network Item](#) on page 316

## SENDING TRAPS TO iVIEW NETWORK MANAGER



You can configure the managed elements in the network to send SNMP traps to the iVIEW Network Manager.

### Procedure

- 1 Click **Settings** in the sidebar menu.
  - 2 Click **Traps**.
  - 3 Select **Receive traps from elements**.
  - 4 Click **Upload** to save your changes.
- 

## CREATING OR MODIFYING A TRAP FORWARDING RULE



You can instruct iVIEW Network Manager to forward traps received from managed elements to an address specified by a trap forwarding rule.

### Procedure

- 1 Click **Settings** in the sidebar menu.
  - 2 Click **Traps**.
  - 3 Do one of the following to modify an existing trap forwarding rule:
    - Double-click the trap rule you require.
    - Select the trap rule you require and click **Edit**.
    - Right-click the trap rule you require and select **Edit**.
  - 4 Do one of the following to create a new trap forwarding rule:
    - Click **Add**.
    - Right-click any trap rule and select **Add**.
  - 5 Enter a description in the **Description** field.
  - 6 Specify the IP address and port number for iVIEW Network Manager to forward traps received from managed elements.
  - 7 Select **Enable trap forwarding**.
  - 8 Click **OK** to save your changes.
-

## DISABLING A TRAP FORWARDING RULE



### Procedure

- 1 Click **Settings** in the sidebar menu.
- 2 Click **Traps**.
- 3 Do one of the following to modify an existing trap forwarding rule:
  - Double-click the trap rule you require.
  - Select the trap rule you require and click **Edit**.
  - Right-click the trap rule you require and select **Edit**.
- 4 Deselect **Enable trap forwarding**.
- 5 Click **OK** to save your changes.

The trap forwarding rule is disabled but remains in the database.

---

## REMOVING A TRAP FORWARDING RULE



### Procedure

- 1 Click **Settings** in the sidebar menu.
- 2 Click **Traps**.
- 3 Do one of the following:
  - Select the trap rule you require and click **Delete**.
  - Right-click the trap rule you require and select **Delete**.
- 4 Click **OK** to save your changes.

The trap forwarding rule is removed from the database.

---

## CREATING OR MODIFYING AN ALERT RECIPIENT PROFILE



### Procedure

- 1 Click **Settings** in the sidebar menu.
- 2 Click **Alert Recipients**.
- 3 Do one of the following to modify an existing alert recipient profile:
  - Double-click the alert recipient you require in the Recipient Name column.
  - Select the alert recipient you require and click **Edit**.
  - Right-click the alert recipient you require in the Recipient Name column and select **Edit**.
- 4 Do one of the following to create a new alert recipient profile:
  - Click **Add**.
  - Right-click any link in the Recipient Name column and select **Add**.
- 5 Enter the name and email of the alert recipient in the relevant fields.
- 6 Select a user profile.

The options in the Select user profile field reflect the user details defined at Settings > Users.

If you select a user profile with Local user access level, the alert recipient receives notifications only for alarms that belong to elements that are part of the network subset defined for the user at Settings > Users.

If you select a user profile with Administrator or Read only access level, the alert recipient receives notification of all alarms.
- 7 Select the minimum severity level of the alerts to be sent to the alert recipient.

The severity level of alerts is defined by the profile selected in the Select user profile field.
- 8 (Optional) Select **Notify on alarms clearing** to enable the alarm recipient to receive an error report via email when the alarms have been cleared.
- 9 (Optional) Select **Use custom subject line** to include a custom subject line in the email and enter a string for the custom subject line.

- 10 (Optional) Select **Include element info** to include details of the elements reported in the alerts in the custom subject line.
  - 11 Select **Enable alert** to activate the recipient.
  - 12 Click **OK** to save your changes.
- 

## REMOVING AN ALERT RECIPIENT PROFILE



### Procedure

- 1 Click **Settings** in the sidebar menu.
  - 2 Click **Alert Recipients**.
  - 3 Do one of the following:
    - Select the alert recipient you require and click **Delete**.
    - Right-click the alert recipient you require in the Recipient Name column and select **Delete**.
  - 4 Click **OK** to save your changes.
- The alert recipient profile is removed from the database.
- 

## VIEWING GENERATED EVENTS



### Procedure

- 1 Click **Alarms** in the sidebar menu.
  - 2 Click **Events**.
- The Events tab displays the following information:
- Event severity level (Minor, Cleared, Information, Warning, Minor, Major, Critical).
  - Date and time of the event.
  - Text message describing the event.

- 3 Click the column headings in the alarms table to sort the information displayed.
  - 4 Double-click any element in the table to display the relevant element manager for that element.
- 

## FILTERING GENERATED EVENTS



### Procedure

- 1 Click **Alarms** in the sidebar menu.
  - 2 Click **Events**.
  - 3 Do one of the following:
    - Select **View > Filter events**.
    - Click the **Current filter** link above the table.
  - 4 Define the time period and minimum severity levels of the events to display.
  - 5 Enter filter criteria and click **OK**.
- The events that correspond to your selection are displayed in the table.
- 

## VIEWING EVENTS PER NETWORK ITEM



### Procedure

You can view a table of the events that have occurred in the system related to a specific item in your network.

- 1 Click **Network Tree** in the sidebar menu.
- 2 Click **Network** or a relevant custom view.
- 3 Select the network item you require.
- 4 Click **Events**.

The Events tab includes the event severity level, the date and time of the event and the event message.
- 5 (Optional) Double-click the link in the Element column to display the element manager for that element.

- 6 (Optional) Do one of the following to filter the events displayed by date and severity level:
    - ❑ Select **View > Filter events**.
    - ❑ Click the **Current filter** link above the table.
- 

## VIEWING AND SORTING SUPPORTED ALARMS



### Procedure

- 1 Click **Settings** in the sidebar menu.
  - 2 Click **Alarms**.
  - 3 Click the **Alarm** heading in the alarms table to view alarms generated by the managed elements in the network in alphabetical order.
  - 4 Click the **Severity** heading in the alarms table to sort the alarms by increasing or decreasing order of severity.
- 

## MODIFYING ALARMS



### Procedure

- 1 Click **Settings** in the sidebar menu.
- 2 Click **Alarms**.
- 3 Do one of the following to modify an alarm generated by the managed elements in the network:
  - ❑ Double-click the alarm you require.
  - ❑ Select the alarm you require and click **Edit**.
  - ❑ Right-click the alarm you require and select **Edit**.
- 4 Modify the severity level, and enable or disable the alarm in the relevant fields.

- 5 Select **Create event for this alarm** to instruct iVIEW Network Manager to create a report at Alarms > Events every time this alarm occurs.
  - 6 Use the **Apply to all users** option to indicate whether the alarm properties apply only to the current user or to all users.
  - 7 Click **OK** to save your changes.
- 

## VIEWING AND SORTING GENERATED ALARMS




The Alarms tab enables you to view and sort the alarms generated by the elements in the network according to alarm status, alarm message, date and time or element.



### Procedure

- 1 Click **Alarms** in the sidebar menu.
- 2 Click **Alarms**.

The Alarms tab includes the severity of each alarm, the time the event occurred and the alarm message that is related to the selected element. Alarm severity levels include the following:

-  Major/Minor/Critical
-  Information
-  Warning

- 3 Double-click any element in the table to display the relevant element manager for that element.
- 

## VIEWING GENERATED ALARMS PER NETWORK ITEM

You can view a table of all current alarms related to a specific item in your network. Alarms can be viewed per element, network zone or the entire network in one view.



### Procedure


- 1 Click **Network Tree** in the sidebar menu.
- 2 Click **Network** or a relevant custom view.
- 3 Select the network item you require.

4 Click **Alarms**.

The Alarms tab includes the severity of each alarm, the time the event occurred and the alarm message that is related to the selected element. Alarm severity levels include the following:

 Major/Minor/Critical

 Information

 Warning

---

## Viewing Generated Alarms per Network Item

# 33

## MANAGING CALLS AND CONFERENCES IN IVIEW NETWORK MANAGER

---

- [Viewing Current Call Details](#) on page 319
- [Viewing Current Call Details per Network Item](#) on page 320
- [Disconnecting Calls](#) on page 320
- [Searching for a Call](#) on page 321
- [Viewing Current Conferences](#) on page 321
- [Viewing Current Conferences per Network Item](#) on page 322
- [Searching for a Conference](#) on page 323
- [Accessing the Conference MCU](#) on page 323

### VIEWING CURRENT CALL DETAILS

The Calls tab displays a table providing details of each call currently taking place on the selected element including source and destination aliases, source and destination gatekeepers of the calling parties, call start time and allocated bandwidth.



#### Procedure

- 1 Click **Calls** in the sidebar menu.
  - 2 Click **GK Calls**.
  - 3 To display extended details per call, click on the table row and click **Show call details**.
-

## VIEWING CURRENT CALL DETAILS PER NETWORK ITEM



You can view the current status of all calls currently being hosted on the network, zone or selected MCU.

### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Click **Network** or a relevant custom view.
  - 3 Select the network item you require.
  - 4 Click **Calls**.
  - 5 To display extended details per call, click on the table row and click **Show call details**.
- 

## DISCONNECTING CALLS



### Procedure

- 1 Click **Calls** in the sidebar menu and then click **GK Calls**  
–or–  
Click **Network Tree** in the sidebar menu, select the network item you require, and then click **Calls**.
  - 2 Do one of the following:
    - Select the call(s) you want to disconnect and click **Disconnect selected call**.
    - Click **Disconnect all calls**.
-

## SEARCHING FOR A CALL



### Procedure

- 1 Click **Calls** in the sidebar menu and then click **GK Calls**  
–or–  
Click **Network Tree** in the sidebar menu, select the network item you require, and then click **Calls**.
  - 2 Click **Find**.
  - 3 Enter the call alias, IP address of the endpoint, or service ID.
  - 4 Click **Find**.
- 

## VIEWING CURRENT CONFERENCES



The Conferences tab provides a table for viewing the current status of all conferences being hosted on the network, zone or selected MCU.

### Procedure

- 1 Click **Calls** in the sidebar menu.
- 2 Click **Conferences**.

[Table 33-1](#) describes the information displayed on the Conferences tab.

**Table 33-1** *Conferences Tab Parameters*

| Parameter     | Description                                                                                                                                  |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| MCU           | IP address of the MCU on the which the conference is being hosted. Click on the link to view the element manager of the MCU (Administrator). |
| Conference ID | Conference ID number. Click on the link to view the conference manager of the MCU (Conference Control).                                      |
| Layout        | Video layout configuration of the conference.                                                                                                |
| Camera        | Indicates whether video is enabled for the conference.                                                                                       |
| Speaker       | Indicates whether audio is enabled for the conference.                                                                                       |

## Viewing Current Conferences per Network Item

| Parameter             | Description                                                   |
|-----------------------|---------------------------------------------------------------|
| Data                  | Indicates whether data support is enabled for the conference. |
| Total Participants    | Number of current participants.                               |
| Local Participants    | Number of local participants on this MCU.                     |
| Reserved Participants | Number of reserved participants.                              |
| Video Bit Rate        | Maximum bit rate for the conference.                          |
| Zone                  | Zone in which the conference is taking place.                 |

- 3 (Optional) Double-click the link in the MCU column to display the element manager for that element.

## VIEWING CURRENT CONFERENCES PER NETWORK ITEM



You can view the current status of all conferences currently being hosted on the network, zone or selected MCU.


### Procedure

- 1 Click **Network Tree** in the sidebar menu.
- 2 Click **Network** or a relevant custom view.
- 3 Select the network item you require.
- 4 Click **Conferences**.  
[Table 33-1](#) describes the information displayed on the Conferences tab.
- 5 (Optional) Double-click the link in the MCU column to display the element manager for that element.

## SEARCHING FOR A CONFERENCE



### Procedure

- 1 Click **Calls** in the sidebar menu and then click **Conferences**  
–or–  
Click **Network Tree** in the sidebar menu, select the network item you require, and then click **Conferences**.
  - 2 Click **Find** .
  - 3 Enter the conference ID or the zone prefix.
  - 4 (Optional) Use the [\*] wildcard to search for conferences.
  - 5 Click **Find**.
- The row in the table matching your search criteria is highlighted.
- 

## ACCESSING THE CONFERENCE MCU



### Procedure

- 1 Click **Calls** in the sidebar menu and then click **Conferences**  
–or–  
Click **Network Tree** in the sidebar menu, select the network item you require, and then click **Conferences**.
  - 2 To access the element manager of the MCU (Administrator), click the MCU link in the left-hand column of each table row.
  - 3 To access the MCU Conference Control interface, click the link in the Conference ID column.
- This enables you to manage and take control of the conference.
-

## Accessing the Conference MCU

# 34

## CONFIGURING LOGGING FOR iVIEW NETWORK MANAGER

---

- [Viewing Logs for a Selected Element](#) on page 325
- [Defining iVIEW Network Manager Logging Activity](#) on page 326
- [Saving Element Logs](#) on page 326
- [Collecting Logs from a Cisco IOS H.323 Gatekeeper Element](#) on page 327

### VIEWING LOGS FOR A SELECTED ELEMENT

The information displayed on the Logs tab is dependent on the type of element that is selected in the tree.

A log of operations is not available for endpoints supported by the iVIEW Network Manager. A log tab is not available for endpoints when selected in the Network Tree view.



#### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Select the required network element.
  - 3 Click **Logs**.
  - 4 Define the log details for the selected network element.
  - 5 Click **Open log view** to view the logs directory for the selected network element.
-

## DEFINING iVIEW NETWORK MANAGER LOGGING ACTIVITY



### Procedure

- 1 Click **Settings** in the sidebar menu.
- 2 Click **Logging**.
- 3 Click **Network Manager Logs**.
- 4 Select **Save iView Manager log** to enable logging.
- 5 (Optional) Define the log file name, the maximum file size, the number of backup files to maintain, and the level of log detail in the relevant fields.

The maximum log file size is 327,200 KB.

The maximum number of log files is 200.

iVIEW Network Manager overwrites the oldest file with the next new file when disk space is full.

- 6 Click the **View log directory** link to view a list of links to log files for iVIEW Network Manager and managed network elements.
  - 7 Click **Upload** to save your changes.
- 

## SAVING ELEMENT LOGS



### Procedure

- 1 Click **Settings** in the sidebar menu.
  - 2 Click **Logging**.
  - 3 Click **Element Logs**.
  - 4 Define the maximum size of each log file and the number of backup files to maintain in the relevant fields.
  - 5 Click **Upload** to save your changes.
- 

iVIEW Network Manager can locally save log files for those elements, such as MCUs, PathFinder Servers and Gateways, that do not maintain a log of their own.

## COLLECTING LOGS FROM A CISCO IOS H.323 GATEKEEPER ELEMENT



### Procedure

- 1 Click **Network Tree** in the sidebar menu.
  - 2 Select the Cisco IOS H.323 Gatekeeper you require in the tree.
  - 3 Click **Debug Flags**.
  - 4 Click **Add**.
  - 5 Enter **debug ip icmp** in the Debug Command field to generate traffic and confirm logging is configured properly.
  - 6 Enter **Enable ip icmp debugging** in the Description field.
  - 7 Select **Enable**.
  - 8 Click **OK**.  
A new alarm appears in the Alarms tab.
  - 9 Click **Logs**.
  - 10 Select **Save logs**.
  - 11 Enter a file name and set the log level to **Debugging**.
  - 12 Ping the Cisco IOS H.323 Gatekeeper to generate traffic to capture logs.
  - 13 Click **Open log view** to verify the result.
-

## Collecting Logs from a Cisco IOS H.323 Gatekeeper Element

# INDEX

---

## A

- ad hoc
  - participants 7
- Alarms view 232
- Auto-Detect 231

## B

- bandwidth 124
- Bandwidth Rules 289
- billing 127

## C

- cascading
  - dynamic 7
- Centralized Log Management 233
- columns
  - sorting 121
- concurrent call capacity 15
- Conferences and Calls view
  - Calls tab 319
  - Conferences tab 321
- Configuration Tool
  - e-mail server settings 136
  - MCU command delay 138
  - meeting settings 140
  - passwords 138
- Configuring
  - Gatekeeper 292
  - Terminal managers 233
- Configuring Protocols 295

## D

- Default Dialing Mode 126
- delay 124
- distributed environment 8
- dynamic cascading 7

## E

- Element configuration 231
- Element Managers
  - configuration 233
- endpoint
  - unresponsive to connection request 137

## G

- Gatekeeper
  - configuration 232
  - local zones 288
  - Prefixes 289
- Gateway
  - configuration 232

## H

- host 127

## I

- IP Topology tab 22
  - Bandwidth 22
  - Distance 22
- ISDN
  - cost of call 23

## M

### MCU

- command delay 138
- configuration 232
- local 124

MCU access 323

## N

Name Display Format 121

### Network Manager

- overview 230

Network Status 230

Network Tree view 235

- Elements tab 241

Network Views 233

## R

Registering MPs 296

### report

- information categories 19

### reports

- generating 19, 89, 97

### Requirements

- system 230

## S

### Services

- MCU 297

### Settings view

- Element Logs tab 326

## V

Viewing conferences 231

Viewing events 232

### Views

- Network Tree 235



[www.radvision.com](http://www.radvision.com)

---

#### About RADVISION

RADVISION (NASDAQ: RVSN) is the industry's leading provider of market-proven products and technologies for unified visual communications over IP and 3G networks. With its complete set of standards based video networking infrastructure and developer toolkits for voice, video, data and wireless communications, RADVISION is driving the unified communications evolution by combining the power of video, voice, data and wireless – for high definition video conferencing systems, innovative converged mobile services, and highly scalable video-enabled desktop platforms on IP, 3G and emerging next generation networks. For more information about RADVISION, visit [www.radvision.com](http://www.radvision.com)

---

USA/Americas  
T +1 201 689 6300  
F +1 201 689 6301  
[infoUSA@radvision.com](mailto:infoUSA@radvision.com)

EMEA  
T +44 20 3178 8685  
F +44 20 3178 5717  
[infoUK@radvision.com](mailto:infoUK@radvision.com)

APAC  
T +852 3472 4388  
F +852 2801 4071  
[infoAPAC@radvision.com](mailto:infoAPAC@radvision.com)