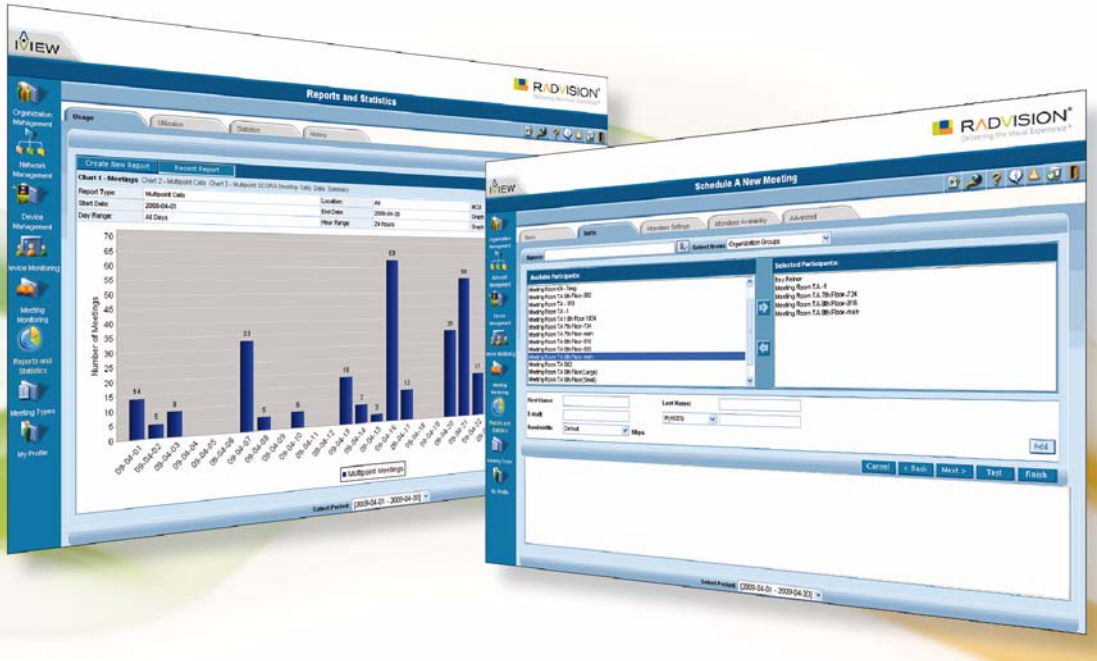
RADVISION®
Delivering the Visual Experience®

SCOPIA® MANAGEMENT

SCOPIA iVIEW Management Suite

Administrator Guide

Version 7.7



© 2000-2011 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.

All product and company names herein may be trademarks of their registered owners.

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.

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

Administrator Guide for SCOPIA iVIEW Management Suite Version 7.7, December 05, 2011

http://www.radvision.com

RADVISION®
Delivering the Visual Experience®

SCOPIA®

1 Table of Contents

1 Getting Started with the SCOPIA iVIEW Management Suite

About SCOPIA iVIEW Management Suite 1
Planning your SCOPIA iVIEW Management Suite Deployment 2
Ports to Open on SCOPIA iVIEW Management Suite 2
Localized Languages in iVIEW Management Suite 7
Defining SCOPIA iVIEW Management Suite Administrators 8
Accessing SCOPIA iVIEW Management Suite with Different User Types 8
Enabling Single Sign-on 9
Initial Configuration Workflow 9

2 Defining the Offices and Branches of your Enterprise

Adding Offices and Branches for the First Time 11
Defining a New Office or Branch 12
Defining Bandwidth Limits for the new Office or Branch 13

3 Defining your Video Network Devices

Planning Auto-detect of Network Devices 15
Running the Auto-detect Mechanism Automatically 16
Running the Auto-detect Mechanism Manually 16
Adding or Modifying Auto-detect Element Access Information 17
Planning and Configuring Gatekeeper Profiles 17
About the iVIEW Management Suite's Internal Gatekeeper 18
Defining a Gatekeeper in SCOPIA iVIEW Management Suite 19

Defining a Gatekeeper's Dial Plan in SCOPIA iVIEW Management Suite 20
Defining the Gatekeeper Authorization Server 20
Replicating SCOPIA Enhanced Communication Server Configurations in iVIEW Management Suite 21
Planning and Configuring MCUs in iVIEW Management Suite 22
Creating and Modifying an MCU Profile 22
Configuring MCU's Branch or Office 24
Choosing MCU Protocol: H.323 or SIP 25
Managing MCU Meeting Types 25
Increasing MCU Capacity by Cascading Multiple MCUs 26
Enabling the Auto-Attendant 27
Planning and Configuring a SCOPIA Desktop Server in iVIEW Management Suite 30
Adding a SCOPIA Desktop Profile in iVIEW Management Suite 30
Enabling Streaming on your Video Network 32
Defining Bandwidth for SCOPIA Desktop Pro to Pro Calls 32
Configuring Recording on your Video Network 32
Configuring the SCOPIA Desktop Profile to Include a Recording Server 33
Enabling Recording on iVIEW Management Suite 34
Allowing Recording for Specified User Types 34
Allowing Recording for Individual Users 35
Planning and Configuring Gateways in iVIEW 35
Adding a Gateway and its Services in iVIEW Management Suite 36
Adding or Editing a Service to an Existing Gateway 39
Registering a Gateway with a Gatekeeper 40
Adding and Configuring a SCOPIA Video Gateway in iVIEW Management Suite 40
Adding and Configuring SIP Gateway in iVIEW Management Suite 44
Adding Pathfinders in iVIEW Management Suite 49
Configuring and Planning Endpoints in iVIEW Management Suite 49
Importing Endpoints from the Gatekeeper 50
Importing Endpoints Registered to a Third-Party Gatekeeper 51
Downloading H.323 Endpoints from the LDAP Server 54
Importing SIP/H.323/H.320 Endpoints using the H.350 Search Base 56
Configuring your Endpoints to use iVIEW Management Suite as the LDAP Directory 56
Configuring the SCOPIA XT Series to use iVIEW Management Suite as LDAP Directory 56
Configuring the SCOPIA VC240 to use iVIEW Management Suite as the LDAP Directory 62
Configuring Third-Party Endpoints to use iVIEW Management Suite as LDAP Directory 66
Adding Endpoints in iVIEW Management Suite Manually 69

Adding H.323 IP Endpoints 70
Adding SIP IP Endpoints 71
Adding ISDN/PSTN H.320 Endpoints 72
Adding Mobile Endpoints 73
Adding Dual H.320 and H.323 Endpoints 73
Setting the Managed Status of Endpoints 75
Removing Endpoints 75
Searching for an Endpoint 76
Managing Endpoints Configuration Upload History 76
Adding a Lync Server or OCS Profile in iVIEW Management Suite 77
Enabling Remote Access to GUI of Video Network Devices 79
Configuring Remote Access to Network Devices and Endpoints 79
Configuring Remote Access to GUI of SCOPIA PathFinder 80
Defining Specific Information for Remote Access of Network Devices 81
Planning and Configuring Telepresence in iVIEW Management Suite 82
Understanding Telepresence Systems 82
Managing Telepresence in iVIEW Management Suite 83
Configuring Telepresence Endpoints 83
Calculating Resources for Telepresence 85
Scheduling Telepresence Systems 85
Configuring iVIEW Management Suite redundancy 86
Configuring Redundancy Mode 86
Monitoring Redundancy Status 90
Disabling Redundancy Mode 90

4 Defining and Managing Video Users

Adding Organization Profiles to iVIEW Management Suite 92
Creating a New Organization 93
Limiting Organization Access to Different Meeting Types 94
Defining Organization Administrators 95
Limiting the Number of Concurrent Calls per Organization 95
Allowing Calls between Organizations 96
Limiting the Number of SCOPIA Desktop Pro and SCOPIA Mobile Licenses 97
Dedicating the SCOPIA Video Gateway to an Organization 97
Removing Inactive Organization Profiles 97

Generating an Organization Report 98
Branding the User Interface 99
Managing Video Users 99
Managing Users from the LDAP Server 100
Connecting iVIEW Management Suite with the LDAP Server 100
iVIEW Management Suite LDAP Information Attributes 103
Securing the Connection between iVIEW Management Suite and an LDAP Server 103
Downloading Users from the LDAP Server 104
Updating User Profiles from the LDAP Server 105
Managing Users with a Local User Directory 105
Creating a User Profile within iVIEW Management Suite 105
Searching for a User Profile 106
Removing a User Profile 107
Defining SCOPIA Desktop User Authorization 108
Managing Virtual Rooms 108
Downloading Virtual Rooms from the LDAP Server 108
Creating a Virtual Room for an iVIEW Management Suite User 112
Enabling Recording for Specified Users Virtual Rooms 113
Enabling Streaming for a User Virtual Room 114
Managing User Groups 114
Creating a User Group 115
Modifying a User Group 115
Removing a User Group 116
Limiting Group Access to Meeting Types 116
Limiting User Access to Types of Meetings 116
Downloading Meeting Types to iVIEW Management Suite 117
Upload a Meeting Type to Network MCUs 117
Resolving Meeting Type Conflicts 118
Defining a Default Meeting Type 119
Configuring Meeting Type Details 119
Defining the Meeting Types Available for Users 120
Modifying Meeting Types 120
Modifying a Meeting Type Group 121
Searching for a Meeting Type 121
Removing a Meeting Type 122
Managing Your Own User Profile 122
Modifying Administrators Log in Information 123

Modifying Your Time Zone....124
Defining Your Meeting Display Preferences....124
Modifying a Service Provider Profile....125
Configuring Corporate Address Books....126
Enabling a Corporate Address Book....126
Configuring Endpoints to be Displayed in the Corporate Address Book....128

5 Securing your Video Network

Securing Web Access to iVIEW Management Suite Using HTTPS....129
Installing Certificates with Unique Keys on the Application Server....130
Configuring the Application Server to Use HTTPS....132
Accessing iVIEW Management Suite Using HTTPS....134
Securing Your Video Network Using TLS....134
Planning the Required Certificates for TLS....135
Generating the Certificate Signing Request for iVIEW Management Suite....141
Uploading iVIEW Management Suite Certificates into iVIEW Management Suite....144
Uploading Certificates for Other Devices into iVIEW Management Suite....146
Enabling the TLS Connection in iVIEW Management Suite....149

6 Real-time Monitoring

Managing iVIEW Management Suite Traps....151
Configuring iVIEW Management Suite to Receive Traps from Network Devices....151
How to Configure iVIEW to Forward Traps to a Specific Address....152
Creating or Modifying a Trap Forwarding Rule....152
Disabling a Trap Forwarding Rule....153
Removing a Trap Forwarding Rule....154
How to Send Alerts to a Specific User....154
Creating or Modifying an Alert Recipient Profile....154
Defining Network Subsets....155
Removing an Alert Recipient Profile....156
Monitoring Network Devices....156
About Management Status of Network Devices....157
About iVIEW Management Suite Monitoring Views....158
Creating your own Monitoring View....160

Monitoring Network Events 160
Monitoring Network Alarms 161
Changing the Severity Level of Alarms 162
Monitoring Device Usage and Utilization 162
Monitoring Device Usage and Failure by Time Interval 162
Monitoring Device Usage and Failure Statistics 163
Monitoring MCU Availability for a Meeting Type 164
Monitoring Meetings, Calls and Conferences 165
Monitoring Ongoing Meetings or Calls 165
Monitoring Bandwidth and Port Utilization 166
Checking the Status of Meetings 166
Managing Ongoing Calls 167
Managing Ongoing Calls per Network Device 168
Disconnecting Calls 168
Managing Ongoing Conferences 168
Monitoring Ongoing Conferences per Network Item 169

7 Maintaining your Videoconferencing Network

Upgrading, Backing up and Restoring iVIEW Management Suite Data 170
Backing Up iVIEW Management Suite 171
Restoring an iVIEW Management Suite Backup 172
Upgrading iVIEW Management Suite 172
Upgrading Network Device Software 173
Remotely Upgrading Endpoints and Other Devices from iVIEW Management Suite 173
Removing a Software Upgrade File 175
Backing Up and Duplicating an Endpoint's Configuration 176
Backing Up MCU Configuration Settings 177
Restoring MCU Configuration Settings 177
Updating the SCOPIA MCU License Keys 178
Upgrading the SCOPIA Video Gateway or RADVISION SIP Gateway 179
Restoring a Previous Software Version for the SCOPIA Video Gateway or RADVISION SIP Gateway 181
Maintaining Gateways 183
Downgrading your SCOPIA Video Gateway or RADVISION SIP Gateway 183
Daily Maintenance of your Video Network 183
Searching for Network Devices 184

Modifying a Network Device Profile 184
Removing a Network Device from iVIEW Management Suite 185
Taking a SCOPIA MCU or Gateway Offline 187
Cancelling Pending Offline Configuration Settings 187
Modifying Network Devices Hierarchy 188
Managing Bandwidth in your Network 188
Maintaining Scheduled Meetings 188
Searching for a Meeting 189
Modifying Upcoming Meetings 190
Uninstalling SCOPIA iVIEW Management Suite 191
Customizing your iVIEW Management Suite 191
Defining General Settings for iVIEW Management Suite 192
Defining Meeting Scheduling Settings 194
Defining the iVIEW Management Suite Web Interface 198
Defining Custom Time Zones 199
Defining Custom Branding for Vendors 200
Defining Database Server Settings 201
Defining Security Settings 202
Configuring SNMP Trap Server Profiles and Utilization Thresholds 202
Defining Call Data Record (CDR) 203
Customizing Meeting Invitation E-mails 204

8 Generating Reports for Statistics and Analysis

Generating Reports of Upcoming Meetings 206
Generating a Call Information Report 208
Generating a Port Usage Report 208
Generating a Resource Usage Report 209
Generating Statistic Report for Meetings 210
Generating Reports for Finished Meetings 210
Generating Bandwidth Utilization Reports 213
Generating a Report of Network Device Performance and Availability 214

1 Getting Started with the SCOPIA iVIEW Management Suite

Welcome to the Administrator Guide for SCOPIA iVIEW Management Suite.

This section provides an orientation for the iVIEW Management Suite, including its features, considerations for planning and implementing its deployment, and introduction to its user types:

- About SCOPIA iVIEW Management Suite ..... page 1
- Planning your SCOPIA iVIEW Management Suite Deployment ..... page 2
- Localized Languages in iVIEW Management Suite ..... page 7
- Defining SCOPIA iVIEW Management Suite Administrators ..... page 8
- Initial Configuration Workflow ..... page 9

About SCOPIA iVIEW Management Suite

SCOPIA iVIEW Management Suite is a set of management, control and scheduling applications which provide robust network management and easy-to-use conference scheduling.

The network management component, known as SCOPIA iVIEW Network Manager, provides enterprises with a single access point to managing all their videoconferencing network devices including SCOPIA Infrastructure components, through the call control software applications (SCOPIA Enhanced Communication Server, SIP Back-to-Back User Agents) and to the various endpoint devices deployed in the network, both RADVISION endpoints and 3rd party systems. Through the network management of iVIEW Management Suite, administrators can detect and monitor their systems, remotely configure and control them, and upgrade software/firmware to the various systems in the network.

The scheduling and resource component, known as SCOPIA iVIEW Communications Manager, allows administrators and conferencing operators to conveniently schedule, manage and control their conferences from a single access point. iVIEW Management Suite also provides scalability and redundancy capabilities of a large enterprise or application service provider's global deployment, with unique capabilities such as Virtual MCU with automatic cascading for bandwidth preservation, least cost routing for cross-site communications cost savings, Virtual Conference Room for ease-of-use and other features.

SCOPIA iVIEW Management Suite also integrates with enterprises' existing applications such as Microsoft Active Directory, IBM Lotus Domino for easy user provisioning, Microsoft Outlook or IBM Lotus Notes for an easy and intuitive calendar application scheduling. iVIEW Management Suite also provides the interface to market leading unified communication solutions such as Microsoft Lync Server, Microsoft Office Communications Server, and IBM Lotus Sametime.

The smooth integration with 3rd party SIP servers leverages existing network call control for the videoconferencing system. The SIP server manages the call control and network usage, while the SCOPIA Solution supplies the videoconferencing capabilities.

iVIEW Management Suite can be shipped with a built-in gatekeeper which supplies the correct destination IP and authorizes the appropriate bandwidth for the call. In this way, iVIEW Management Suite can manage endpoint-initiated calls and point-to-point calls.

MCUs, gateways and endpoints (terminals) can be registered with the iVIEW Management Suite's internal gatekeeper.

iVIEW Management Suite can also work with the standalone SCOPIA Enhanced Communication Server or third party gatekeepers.

Planning your SCOPIA iVIEW Management Suite Deployment

There are several solutions defined in the *SCOPIA Solution Guide*, each with its own deployment scenario and network topology. Decide on the type of deployment you need based on your video requirements and your existing network topology.

The *SCOPIA Solution Guide* includes details of the considerations for choosing each of the deployments, and the locations to place each of the solution components within the network topology.

When planning your deployment, it is also important to consider port security. For the list of ports to open, see "Ports to Open on SCOPIA iVIEW Management Suite" on page 2.

For installation procedures for each of the components of the SCOPIA Solution, see the product's *Installation Guide*. For installation procedures for the iVIEW Management Suite, see the *iVIEW Management Suite Installation Guide*.

Ports to Open on SCOPIA iVIEW Management Suite

SCOPIA iVIEW Management Suite is typically deployed in the enterprise network or the DMZ.

When opening ports to and from iVIEW Management Suite, use the following as a reference:

- If opening ports that are both to and from iVIEW Management Suite, see Table 1-1.
- For a list of outbound ports to open from iVIEW Management Suite, see Table 1-2.
- For a list of inbound ports to open to iVIEW Management Suite, see Table 1-3.

Note: The specific firewalls you need to open ports on depends on where your SCOPIA iVIEW Management Suite and other SCOPIA Solution products are deployed.

Table 1-1 Bidirectional Ports to Open on iVIEW Management Suite

Port Range	Protocol	Source/ Destination	Functionality	Result of Blocking Port	Required
23	Telnet (TCP)	Sony PCS address book, MCM, Endpoints	Enables you to use Sony PCS address book, retrieve element logs, and control MCM and endpoints.	Cannot use Sony PCS address book feature or retrieve logs from various devices (such as MCM)	Recommended
80	HTTP (TCP)	Web client	**In**: Provides access to the iVIEW Management Suite web user interface. When installed with the gatekeeper, this port defaults to 8080. **Out**: Provides access to the iVIEW Management Suite web user interface and TANDBERG MXP management (XML API via HTTP).	Cannot access the iVIEW Management Suite web user interface and TANDBERG MXP management	Mandatory This can be configured during installation. For more information, see the How to Install iVIEW Management Suite in the *Installation Guide for iVIEW Management Suite*.
161	SNMP (UDP)	Any managed element	Enables SNMP configuration	Cannot operate the SNMP service with devices, and forward trap events do not function.	Mandatory
162	SNMP (UDP)	Any third-party SNMP manager	Enables sending SNMP trap events from any managed element	Cannot operate the SNMP service with devices, and forward trap events do not function.	Recommended
389	LDAP (TCP)	LDAP servers	Enables connection to LDAP servers	Cannot work with LDAP Servers	Mandatory for LDAP authentication
3344	SOCKS (TCP/UDP)	iVIEW Management Suite	Enables object data synchronization between multiple iVIEW Management Suite installations (used only in distributed deployments)	Cannot operate in a distributed deployment	Mandatory in distributed deployments
4444, 4445	TCP	JBoss application server	Enables correct JBoss operation (required by the JBoss application server)	iVIEW Management Suite's underlying application server does not function properly	Mandatory

Port Range	Protocol	Source/ Destination	Functionality	Result of Blocking Port	Required
5060	SIP (TCP/ UDP)	B2B/ Other SIP components	Enables SIP signaling	Cannot connect SIP calls	Mandatory
5061	SIP (TLS)	B2B/ Other SIP components	Enables secure SIP signaling	No TLS connection available	Mandatory
7800-7802	UDP	iVIEW Management Suite	Enables master/slave data synchronization (used for iVIEW Management Suite redundant deployments)	Redundancy functionality is not available	Mandatory This can be configured during redundancy configuration. For more information, see the Configuring Redundancy Mode in the *Administrator Guide for iVIEW Management Suite*.
8011	HTTP (TCP)	Web client	Provides access to the internal ECS web user interface	iVIEW Management Suite client cannot access internal ECS web user interface	Mandatory for accessing the ECS web user interface
11098,11099	JNP/ RMI (TCP)	JBoss application server	Enables correct JBoss operation (required by the JBoss application server); this port is used by iVIEW Management Suite locally and is not connected from a remote host.	Cannot function if the port is occupied by another application	Mandatory

Table 1-2 Outbound Ports to Open from iVIEW Management Suite

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
7	Echo (TCP)	Video Network Devices	Detects online status of video network devices	Cannot detect online status of video network devices	Mandatory
21	FTP (TCP)	iVIEW Network Manager	Enables downloading logs from ECS or other devices that allow logs to be downloaded via FTP. Enables importing and exporting TANDBERG Local Address Book. Enables software upgrade.	Cannot download logs from ECS or from other devices via FTP, import or export TANDBERG Local Address Book, or perform software upgrades.	Mandatory

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
22	SSH (TCP)	iVIEW Network Manager	Detects LifeSize endpoints. Enables downloading SCOPIA PathFinder Server logs. Detects and manages SCOPIA VC240.	Cannot detect LifeSize endpoints, download SCOPIA PathFinder Server logs, or detect/ manage SCOPIA VC240	Mandatory
24	Telnet (TCP)	Polycom endpoints	Enables you to control Polycom endpoints	Cannot control Polycom endpoints	Optional
25	SMTP (TCP)	SMTP server	Enables connection to SMTP server for sending email notifications	Cannot send email notifications	Mandatory
53	DNS (UDP)	DNS server	Enables DNS queries	Cannot parse domain names	Mandatory
445	NTLM (TCP/UDP)	Active Directory Server	Enables connection to the Active Directory Server	NTLM SSO does not function	Mandatory
636	LDAP over SSL	Directory Server	Enables connection to the Directory Server	Cannot connect to the Directory Server	Mandatory
3089	TCP	SCOPIA PathFinder	Detects endpoints via SCOPIA PathFinder	Cannot detect endpoints via SCOPIA PathFinder	Mandatory
3336	XML (TCP)	SCOPIA Video Gateway/ SIP Gateway/ MCU	Enables connection to the SCOPIA Video Gateway/ SIP Gateway/ MCU via the moderator's XML API (used for managing meetings via iVIEW Management Suite)	Cannot connect to the SCOPIA Video Gateway/ SIP Gateway/ MCU via the XML API	Mandatory if deployed with SCOPIA Video Gateway/ SIP Gateway/ MCU
3338	XML (TCP)	SCOPIA Video Gateway/ SIP Gateway	Enables connection to SCOPIA Video Gateway/ SIP Gateway via the administrator's XML API (used for configuring devices via iVIEW Management Suite)	Cannot perform configuration for SCOPIA Video Gateway/ SIP Gateway via the XML API	Mandatory if deployed with SCOPIA Video Gateway/ SIP Gateway
3339	XML (TCP)	B2B	Enables you to use the iVIEW Management Suite XML API	Cannot communicate with the B2BUA component via iVIEW Management Suite XML API	Mandatory
3340	TCP/TLS	SCOPIA Desktop	Enables connection to SCOPIA Desktop	SCOPIA Desktop cannot use iVIEW Management Suite to place or manage calls	Mandatory if deployed with SCOPIA Desktop

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
3346	XML (TLS)	SCOPIA Video Gateway/ SIP Gateway	Enables secure connection to the SCOPIA Video Gateway/ SIP Gateway via the moderator's XML API (used for managing meetings via iVIEW Management Suite)	Cannot securely connect to the SCOPIA Video Gateway/ SIP Gateway/ MCU via the XML API	Mandatory for a secure XML API connection with SCOPIA Video Gateway/ SIP Gateway
3348	XML (TLS)	SCOPIA Video Gateway/ SIP Gateway	Enables secure connection to SCOPIA Video Gateway/ SIP Gateway via the administrator's XML API (used for configuring devices via iVIEW Management Suite)	Cannot securely connect to the SCOPIA Video Gateway/ SIP Gateway/ MCU via the administrator's XML API	Mandatory for a secure XML API connection with SCOPIA Video Gateway/ SIP Gateway
8089	XML (TCP)	SCOPIA PathFinder Server	Enables connection to SCOPIA PathFinder Server (v7.0 and later) via SCOPIA PathFinder Server XML API	Cannot connect to SCOPIA PathFinder Server via SCOPIA PathFinder Server XML API	Optional
50000	Telnet (TCP)	Sony endpoints	Enables you to control Sony endpoints	Cannot control Sony endpoints	Optional
55003	TCP	SCOPIA XT1000	Enables connection to the SCOPIA XT1000	Cannot connect to the SCOPIA XT1000	Mandatory if deployed with SCOPIA XT1000
63148	DIIOP (TCP)	Domino server	Enables connection with the Domino server	Cannot connect to the Domino Server	Mandatory if iVIEW Management Suite works with Domino Server

Table 1-3 Inbound Ports to Open on iVIEW Management Suite

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
443	HTTPS (TCP)	Web client	Enables Tomcat and JBoss to run over SSL	Cannot access iVIEW Management Suite web user interface via HTTPS	Mandatory if using HTTPS

Port Range	Protocol	Destination	Functionality	Result of Blocking Port	Required
3341	TCP	IBM Sametime	Enables connection to IBM Sametime application	Cannot work with IBM Sametime	Mandatory if iVIEW Management Suite works with IBM Sametime
8080	HTTP (TCP)	Web client	Provides access to the SCOPIA PathFinder and iVIEW Management Suite web user interface	Cannot access the SCOPIA PathFinder web user interface	Mandatory if deployed with SCOPIA PathFinder or iVIEW Management Suite internal Gatekeeper. This can be configured during installation. For more information, see the How to Install iVIEW Management Suite in the *Installation Guide for iVIEW Management Suite*.

Localized Languages in iVIEW Management Suite

The menus and input fields of the iVIEW Management Suite can be viewed in the these languages:

Languages	iVIEW Communications Manager	iVIEW Network Manager	Microsoft Outlook Add-on	IBM Lotus Notes Plug-in
Chinese (simplified)	Yes	Yes	Yes	Yes
Chinese (traditional)	Yes	No	Yes	Yes
English (US)	Yes	Yes	Yes	Yes
French	Yes	No	Yes	Yes
German	Yes	No	Yes	Yes
Italian	Yes	No	Yes	Yes
Japanese	Yes	Yes	Yes	Yes
Korean	Yes	Yes	Yes	Yes
Portuguese (Brazilian)	Yes	No	Yes	Yes
Russian	Yes	No	Yes	Yes
Spanish (international)	Yes	No	Yes	Yes

Defining SCOPIA iVIEW Management Suite Administrators

There are a number of types of users that can be defined within the SCOPIA iVIEW Management Suite. The most important user type is the administrator, to access iVIEW Management Suite's full functionality. After installation, a default admin user is created, and you can use it to create other admin users. You can also configure users in iVIEW Management Suite to use the Windows credentials:

- Accessing SCOPIA iVIEW Management Suite with Different User Types ..... page 8
- Enabling Single Sign-on ..... page 9

Accessing SCOPIA iVIEW Management Suite with Different User Types

You can log in to SCOPIA iVIEW Management Suite as one of several types of users. Each type has its own set of rights and privileges, and influences the screen layout of iVIEW Management Suite and its available features.

The SCOPIA iVIEW Communications Manager module has five user types:

- Regular Users

  Regular Users can view, manage, and moderate their own meetings, as well as modify their own profile. They cannot manage their own virtual rooms.

- Meeting Organizers

  Organizers have all the abilities of regular users, but they can also manage their own virtual rooms and personal address books. They can also create and manage meetings for others.

- Meeting Operators

  Meeting operators have all the rights of organizers, and additionally they can view and manage all meetings in an organization.

- Administrators

  Administrators have all the rights of an operator, and additionally they can view and manage all network devices, room terminal and users with their virtual rooms.

- The service provider installation of iVIEW Management Suite divides the Administrator user type into two separate user types:

  - Organization Administrators

    Administrators have all the rights of an operator, and additionally they can view all network devices within their organization only, and manage room terminals, and users with their virtual rooms only within that organization.

  - Service Provider Administrators

    This category of users can manage devices and meeting types across multiple organizations, but cannot assign users within an organization.

The iVIEW Network Manager module has three user types:

- Read Only users

  Read only users can view all elements and zones on the network.

- Administrators

  Administrators have full read/write access to all managed elements and zones on the network.

- Local Users

  Each local user can be defined with different rights to each different predefined area. For example, if you have already defined a network subset called NS1, you can define a local user to have read/write access to all elements in this area. Another subset, NS2, can be defined with read-only access to the elements there. You can also determine whether this user has the privilege of adding new elements to the network. Network subsets are configured by selecting **Settings > Network Subsets**.

Enabling Single Sign-on

By default, the Single Sign-on (SSO) feature does not work with Internet Explorer 8 under Microsoft Vista and Windows 7. Modify the default security setting as described here to enable SSO.

Procedure

Step 1 Go to **Administrative Tools > Local Security Policy > Local Policies > Security Options** on your computer.

Step 2 Double-click **Network security: LAN Manager** or right-click and select **Properties**.

Step 3 Select **Send LM & NTLM - use NTLMv2 session security if negotiated** in the **Local Security Setting** tab.

Step 4 Select **Apply**.

Initial Configuration Workflow

The initial configuration sets up the network in iVIEW Management Suite and prepare the system for daily management.

Before you start configuring your iVIEW Management Suite, make sure you have your network planned and all devices are installed and ready to run. Verify that you have the right administrator permissions. For more information see "Accessing SCOPIA iVIEW Management Suite with Different User Types" on page 8.

We recommend that the initial configuration follows this workflow:

Note: The first step is relevant for service providers and for administrators of a distributed deployment. For centralized deployments, the office or branch is automatically configured during installation.

1. Define the offices and branches of your enterprise in iVIEW Management Suite.
2. Define video network devices in iVIEW Management Suite.

- Gatekeepers/SIP Servers
- SCOPIA MCUs and SCOPIA Elite MCUs
- SCOPIA Desktop Servers
- Gateways
- SCOPIA Video Gateways
- SCOPIA PathFinder Servers
- Endpoints

3. Define organizations and their administrator.

Note: This step only applies to service providers.

4. Define video users within each organizations. This is performed by organization administrators only.

2 Defining the Offices and Branches of your Enterprise

Offices and branches are locations where network devices such as gatekeepers, MCUs, endpoints and gateways are placed.

According to the bandwidth threshold defined for each office or branch, iVIEW Management Suite can perform least-cost or best-performance allocation of resources.

This section describes how to create offices and branches within your network. This procedure is relevant for service providers and for administrators of a distributed deployment only. Once you define offices and branches, you can start building your network by adding devices to specific offices and branches.

- Adding Offices and Branches for the First Time ..... page 11
- Defining a New Office or Branch ..... page 12
- Defining Bandwidth Limits for the new Office or Branch..... page 13

Adding Offices and Branches for the First Time

The Network Management tab is hidden by default. When adding offices and branches for the first time, enable the Network Management tab in your iVIEW Management Suite. The Network Management tab allows you to add and modify locations within iVIEW Management Suite.

The iVIEW Management Suite Configuration tool is a client-server application, based on Java Web Start, that enables service providers and administrators of a distributed deployment to configure iVIEW Management Suite system settings, and modify default settings defined automatically during iVIEW Management Suite installation.

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

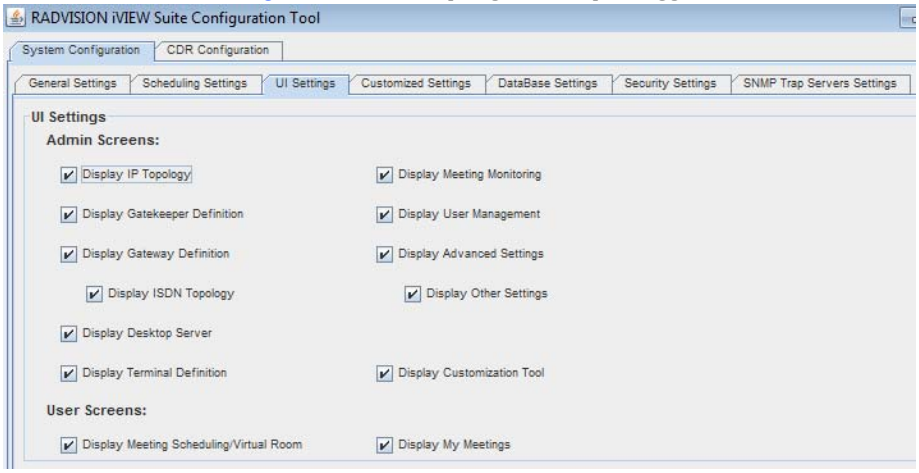
Procedure

Step 1 Go to http://iview-url:port/icm-config/ to launch the iVIEW Management Suite Configuration Tool.

Step 2 Log in as a service provider or as an administrator.

Step 3 Select the **UI Settings** tab and check the **Display IP Topology** box to enable network management capabilities.

Figure 2-1 Display IP Topology



Step 4 Select **OK**. and close the Configuration Tool.

Step 5 Log in to iCM.
To configure offices and branches see "Defining a New Office or Branch" on page 12

Defining a New Office or Branch

When configuring your videoconferencing network in iVIEW Management Suite, the first step for a distributed deployment or for a service provider deployment is to divide the network in offices and branches. Once you define the offices and branches of your network, you can start building the infrastructure by adding device elements such as gatekeepers, MCUs, gateways, and endpoints to specific offices and branches.

This procedure is relevant for service providers and for administrators of a distributed deployment.

Procedure

Step 1 Log in to iCM.

Step 2 Select the **Network Management** icon.

Step 3 In the Locations tab, select a location name or select the **Add** button.

The system displays the Location Profile window (Figure 2-2 on page 13).

Step 4 Define the **Location Name** and the **Domain Name**.

The location name is used to identify offices or branches within the network. The same naming conventions should be use to identify zones when adding gatekeepers to the network. See "Defining a Gatekeeper in SCOPIA iVIEW Management Suite" on page 19.

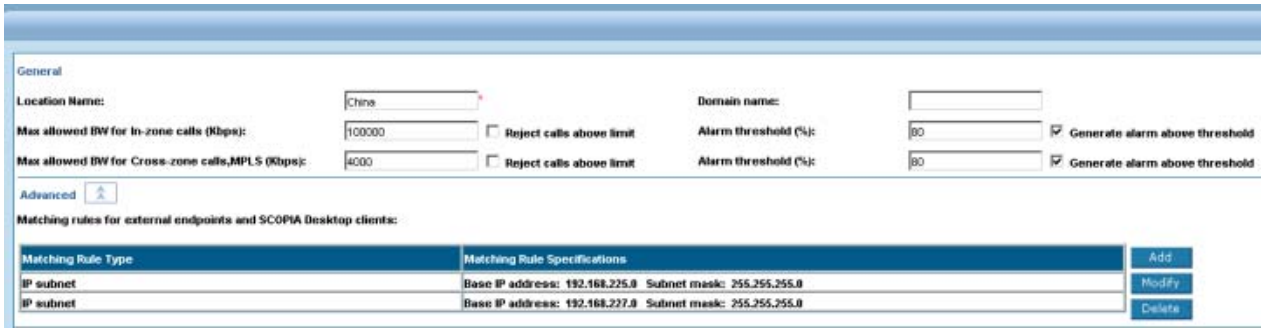
Step 5 Define the distance and bandwidth thresholds for the new office or branch. See "Defining Bandwidth Limits for the new Office or Branch" on page 13 for details.

You can define the maximum bandwidth for calls across offices or branches to another location, or the bandwidth dedicated to calls within an office or branch.

When calling across offices or branches, for example via an MPLS connection, you can define the maximum bandwidth usage and set alerts to be triggered if the maximum designated bandwidth is close to being exceeded.

The bandwidth threshold calculations include SCOPIA Desktop calls. When setting up a new office or branch, use the Location Profile screen (Figure 2-2 on page 13) to define the bandwidth thresholds.

Figure 2-2 Defining bandwidth thresholds for a new office or branch



Procedure

Step 1 Log in to iCM.

Step 2 Select the **Network Management** icon.

Step 3 In the Locations tab, select a location name.

The system displays the Location Profile window (Figure 2-2 on page 13).

Step 4 Define the maximum bandwidth for internal calls with **Max allowed BW for In-zone calls (Kbps)**.

Step 5 Define the maximum bandwidth for calls between two defined locations with the **Max allowed BW for Cross-zone calls (Kbps)** field.

Step 6 You can define the system's behavior when the maximum has been exceeded. Select **Reject calls above limit** to automatically disallow calls that exceed the defined maximum.

Use the check box next to the in-zone calls for internal calls, or the check box next to cross-zone calls for automatic rejections between zones.

If a call is rejected because of bandwidth limits, the system triggers a Call Rejected alert.

Step 7 You can set a system alert when the maximum bandwidth is close to being exceeded. Enter the percentage bandwidth usage that would trigger the with the **Alarm threshold (%)** field. The default value is **80%**. The alert is called BW Utilization.

Step 8 In the **Advanced** pane (Figure 2-2 on page 13), select the **Add** button to define a location with rules to determine what is considered within a zone and what is considered a cross-zone call. There are three ways to define a location:

- Any device with an IP address within a range, for example between 192.168.1.1 and192.168.1.110.
- Any device within an IP subnet, for example to specify 192.168.x.x, enter a base IP of 192.168.1.1 and a subnet of 255.255.0.0.
- A dial prefix, for example any call dialled beginning with the prefix 85.

You can modify a rule by selecting the **Modify** button, or delete it by selecting **Delete**.

3 Defining your Video Network Devices

This section provides step-by-step procedures for adding network devices and configuring your videoconferencing network. Note that the procedures require logging in to both NMS and iCM.

- Planning Auto-detect of Network Devices ..... page 15
- Planning and Configuring Gatekeeper Profiles ..... page 17
- Planning and Configuring MCUs in iVIEW Management Suite ..... page 22
- Planning and Configuring a SCOPIA Desktop Server in iVIEW Management Suite .... page 30
- Planning and Configuring Gateways in iVIEW ..... page 35
- Adding Pathfinders in iVIEW Management Suite ..... page 49
- Configuring and Planning Endpoints in iVIEW Management Suite ..... page 49
- Adding a Lync Server or OCS Profile in iVIEW Management Suite ..... page 77
- Enabling Remote Access to GUI of Video Network Devices ..... page 79
- Planning and Configuring Telepresence in iVIEW Management Suite ..... page 82
- Configuring iVIEW Management Suite redundancy ..... page 86

Planning Auto-detect of Network Devices

The SCOPIA iVIEW Network Manager uses an automatic detection mechanism for discovering the RADVISION device elements present on the network. This information is saved to the SCOPIA iVIEW Network Manager database and is used to create the various network views available via the SCOPIA 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.

SCOPIA PathFinder, SCOPIA XT Series and SCOPIA Video Gateway does not yet support auto-detect.

Elements manually deleted from the SCOPIA iVIEW Network Manager database are not detected in subsequent auto-detect procedures. These elements must be manually added to the SCOPIA iVIEW Network Manager database.

- Running the Auto-detect Mechanism Automatically ..... page 16
- Running the Auto-detect Mechanism Manually ..... page 16
- Adding or Modifying Auto-detect Element Access Information ..... page 17

Running the Auto-detect Mechanism Automatically

You can define the auto-detect mechanism to run automatically at regular intervals and whenever the server is restarted, so iVIEW Management Suite is updated with new device elements added to the network.

Procedure

Step 1 Log in to NMS.

Step 2 Select **Settings** in the sidebar menu.

Step 3 Select **Auto-detect**.

Step 4 (Optional) Select **Run auto-detect on server startup** to instruct SCOPIA iVIEW Network Manager to look for new elements on the network whenever the iVIEW Management Suite server is restarted.

Step 5 (Optional) Select **Run auto-detect every (hrs)** and set an hourly interval to instruct SCOPIA iVIEW Network Manager to look for new elements periodically.

Step 6 (Optional) Select **Use default access information in auto-detect routine** to instruct SCOPIA iVIEW Network Manager to use the default element access settings defined at **Settings > Element Management > Access** or **Settings > Endpoint Management > Access**.

Step 7 Select **Upload** to save your changes.

Running the Auto-detect Mechanism Manually

You can run auto-detect at any time by manually initiating it.

Procedure

Step 1 Log in to NMS.

Step 2 Select one of the network views (**Network Tree**, **Network Table** or **Network Map**) in the sidebar menu.

Step 3 Select **Tools** > **Auto-detect elements**

Step 4 Select **OK**.

The SCOPIA iVIEW Network Manager interface is updated accordingly.
The auto-detect procedure may take some time, depending on the size of the network.

Adding or Modifying Auto-detect Element Access Information

You can define log in information for network devices so that iVIEW Management Suite can discover and connect to these devices, to retrieve basic and advance configuration parameters. The information retrieved is displayed in the NMS Network Tree view. You can also configure default parameters for connecting to devices. See "Enabling Remote Access to GUI of Video Network Devices" on page 79.

Procedure

Step 1 Log in to NMS.

Step 2 Select **Settings** in the sidebar menu.

Step 3 Select **Auto-detect**.

Step 4 Do one of the following to modify existing access settings for a network element:

- Double-click the type you require in the Type column.
- Select the type you require and select **Edit**.
- Right-click the type you require in the Type column and select **Edit**.

Step 5 Do one of the following to create new access settings for a network element:

- Select **Add**.
- Right-click the type you require and select **Add**.

Step 6 Select the unit type you require.

Step 7 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.

Step 8 (Optional) Define a description, SNMP write community, and user name and password in the relevant fields.

Step 9 Select **Enabled** to activate the new access settings.

Step 10 Select **OK** to save the information to the SCOPIA iVIEW Network Manager database.

Planning and Configuring Gatekeeper Profiles

Only administrators of a distributed deployment and service providers have permission to configure gatekeepers in the videoconferencing network.

Before adding a gatekeeper to the network, make sure you have all the offices and branches defined in iVIEW Management Suite. See "Defining a New Office or Branch" on page 12.

- About the iVIEW Management Suite's Internal Gatekeeper ..... page 18
- Defining a Gatekeeper in SCOPIA iVIEW Management Suite..... page 19
- Defining a Gatekeeper's Dial Plan in SCOPIA iVIEW Management Suite ..... page 20

- Defining the Gatekeeper Authorization Server ..... page 20
- Replicating SCOPIA Enhanced Communication Server Configurations in iVIEW Management Suite page 21

About the iVIEW Management Suite's Internal Gatekeeper

Gatekeepers are similar to a PBX for an IP video network. After you register the network devices with iVIEW Management Suite's internal gatekeeper, it can perform a number of key features including:

- Translate the alias of an address to its actual IP address. There are three types of aliases:
  - E.164 aliases are numeric addresses representing the endpoint, like a phone number.
  - H.323 aliases are alphanumeric addresses that represent endpoints, like 'user_endpoint'.
  - URI aliases are similar to email addresses, like 'user@radvision.com'.

  In each case, the gatekeeper translates the alias into its corresponding IP address and routes the call successfully.
- Gatekeepers negotiate the connecting and disconnecting of calls.
- Gatekeepers implement an organization's dial plan. A dial plan is the set of call routing rules based on the pre-defined prefixes of a number. The format can determine the location and/or the services you want.

  The most common example of a dial plan comes from the traditional telephony world, where locations are determined by the format of the phone number:
  - Numbers which do not begin with a zero are local calls.
  - Numbers starting with a single zero denote an inter-city call.
  - Numbers starting with a double-zero indicate an international call.

  Similarly, a gatekeeper can be configured to determine locations in an organization's dial plan. For example, all numbers beginning with '5' might be located in Europe, '6' routes to the west coast of the US, '7' to the east coast and so on.

  In addition to locations, gatekeepers can also invoke services from a number format (dial plan). For example, a number beginning with '88' might be chosen to access a person's video virtual room.

iVIEW Management Suite is shipped with a built-in gatekeeper which supplies the correct destination IP and authorizes the appropriate bandwidth for the call. In this way, iVIEW Management Suite can manage endpoint-initiated calls and point-to-point calls.

MCUs, gateways and endpoints (terminals) can be registered with the iVIEW Management Suite's internal gatekeeper.

iVIEW Management Suite can also work with the standalone SCOPIA Enhanced Communication Server or third party gatekeepers when they are configured as neighbors to its internal gatekeeper, including the Cisco IOS H.323 Gatekeeper and the TANDBERG (Cisco) Video Communications Server (VCS). Only endpoints (terminals) can be registered to a third party gatekeeper.

Defining a Gatekeeper in SCOPIA iVIEW Management Suite

You can define and configure third-party external gatekeepers or a standalone SCOPIA Enhanced Communication Server in SCOPIA iVIEW Management Suite. You do not need to define SCOPIA Gatekeeper since it is iVIEW Management Suite's internal gatekeeper.

This procedure is for service providers and administrators only.

When configuring a redundant gatekeeper, use the same settings as those on the main gatekeeper.

Note: Once a gatekeeper is defined in iVIEW Management Suite, basic and advanced configuration parameters can be retrieved from the device, including the MCUs and gateways registered on the gatekeeper.

Procedure

Step 1 Log in to iVIEW Network Manager.

Step 2 Select one of the network views (**Network Tree**, **Network Table** or **Network Map**) in the sidebar menu.

Step 3 Select **Add** > **New** > **New element** or select **Add element**  to create a new gatekeeper profile.

Step 4 Select the gatekeeper type and enter the element name and IP address.

Step 5 (Optional) Select **Allow offline configuration** to allow the iVIEW Network Manager to hold configuration details for an offline element and apply the settings when the element goes online.

Step 6 Select **OK** to add the gatekeeper to the iVIEW Network Manager.

Step 7 Log in to iVIEW Communications Manager.

Step 8 Select **Resource Management** in the sidebar menu.

Step 9 Select **Gatekeeper/SIP server/Presence server**.

Step 10 Select **Add** to create a new gatekeeper profile.

Step 11 Select the **General** tab and enter the name and the management IP address of the gatekeeper.

Step 12 Select the gatekeeper model.

If you selected **Other Model** in the Model field, select **H.323** in the Protocol field.

Step 13 Select the office or branch to which the gatekeeper belongs from the **Location** list.

Each location can have only one gatekeeper.

The Location field is visible only when the IP Topology tab is activated in the iVIEW Communications Manager. See "Adding Offices and Branches for the First Time" on page 11 for details.

Step 14 Select **OK** to add the new gatekeeper to iVIEW Communications Manager.

Step 15 Define a dial plan for the gatekeeper. See "Defining a Gatekeeper's Dial Plan in SCOPIA iVIEW Management Suite" on page 20.

Step 16 Define the gatekeeper authorization server. See "Defining the Gatekeeper Authorization Server" on page 20.

Defining a Gatekeeper's Dial Plan in SCOPIA iVIEW Management Suite

An organization's dial plan must be implemented in SCOPIA iVIEW Management Suite and also configured in any standalone gatekeepers to ensure the dial plan is managed effectively.

A dial plan is the set of call routing rules based on pre-defined number prefixes. The number prefixes are used to determine the location and/or the services a user needs. For more information and examples on dial plans, see "About the iVIEW Management Suite's Internal Gatekeeper" on page 18.

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **Resource Management** in the sidebar menu.

Step 3 Select **Gatekeeper/SIP server/Presence server**.

Step 4 Select the link in the Name column for the gatekeeper you require, or select **Add** to create a new gatekeeper profile.

Step 5 Locate the **Dialing Plan Information** section.

Step 6 (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.

Step 7 (Optional) Select **Stripping** for a gatekeeper that is configured to strip (remove) zone prefixes.

Step 8 Select **Add Zone Prefix** to add a zone prefix that matches the configuration of the gatekeeper.

Step 9 Select **OK** to save your changes.

Defining the Gatekeeper Authorization Server

Define the SCOPIA iVIEW Management Suite as an authorization server to SCOPIA Enhanced Communication Server to ensure that every call that is routed by the gatekeeper is authorized by iVIEW Management Suite, in terms of bandwidth management and other IT policies.

The built-in gatekeeper gets its authorization from iVIEW Management Suite by default.

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **Resource Management** in the sidebar menu.

Step 3 Select **Gatekeeper/SIP server/Presence server**.

Step 4 Select the link in the **Name** column for the gatekeeper you require.

Step 5 Locate the **Advanced** section.

The **Advanced** section appears if you are using iVIEW Management Suite's built-in gatekeeper or a standalone SCOPIA Enhanced Communication Server.

Step 6 Select **Enable Gatekeeper advanced features (authorization and point-to-point)** to set iVIEW Communications Manager as the authorization server of the internal gatekeeper or ECS.

This option is checked by default if you are using the built-in gatekeeper or ECS.

iVIEW Communications Manager will initiate a connection to the ECS for authorization and call control.

Step 7 If you are using the built-in gatekeeper, do not modify the default values for the **Port**, **SNMP Get Community** and **SNMP Set Community** fields.

Step 8 If you are using ECS, ensure the SNMP community names correspond to the settings on 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**.

On the ECS or built-in gatekeeper:

a. Under **ECS > Settings > Calls**, set the **Routing Mode** field to **Call Setup (Q.931) and Call Control (H.245)**.

b. Under **ECS > Settings > External API**, select **Allow Authorization servers to connect**.

Step 9 Select **OK** to save your changes.

Replicating SCOPIA Enhanced Communication Server Configurations in iVIEW Management Suite

In deployments which include a standalone gatekeeper such as the SCOPIA Enhanced Communication Server, iVIEW Management Suite should also manage this device to ensure comprehensive management of your video network.

To manage a standalone ECS, you must replicate the ECS settings within iVIEW Management Suite.

Parameters to be replicated include:

- Services: enables you to view, add and update service information on built-in and user-defined services.
- Global Services: enables you to view, add and update service information on global services common to all gatekeepers defined within the network. This tab is used for distributed deployments with multiple gatekeepers.
- Parent: enables you to configure a parent gatekeeper for the ECS, to define a list of parent filters and to choose whether or not to route calls to unresolved zones via a Cisco proxy.
- Children: enables you to view, configure and modify child gatekeeper of the ECS.
- Neighbors: enables you to view, configure and modify neighbor gatekeepers of the ECS.
- Subzones: enables you to view and configure subzones settings and rules.
- Bandwidth: enables you to view and configure bandwidth policy settings which determine the bandwidth available between specific zones and subzones.

For more information on these parameters and how to configure them in ECS, see the *Reference Guide for SCOPIA Enhanced Communication Server*.

Note: Fields and values are identical to those documented in the *Reference Guide for* SCOPIA Enhanced Communication Server.

To access these parameters in iVIEW Management Suite, follow this procedure.

Procedure

Step 1 Log in to NMS.

Step 2 Select **Network Tree** in the sidebar menu.

Step 3 Select the Gatekeeper you require in the tree.

Step 4 Select the tab that represents the parameter you want to configure. Refer to the *Reference Guide for* SCOPIA Enhanced Communication Server for details.

Planning and Configuring MCUs in iVIEW Management Suite

The SCOPIA MCU is a hardware unit which houses videoconferences from multiple endpoints, both H.323 and SIP. MCUs are added to a specific office or branch, according to pre-defined network topology.

This section describes how to add MCU profiles to iVIEW Management Suite and how to configure and manage MCU services, known as meeting types.

- Creating and Modifying an MCU Profile ..... page 22
- Configuring MCU's Branch or Office ..... page 24
- Choosing MCU Protocol: H.323 or SIP ..... page 25
- Managing MCU Meeting Types ..... page 25
- Increasing MCU Capacity by Cascading Multiple MCUs ..... page 26
- Enabling the Auto-Attendant ..... page 27

Creating and Modifying an MCU Profile

The MCU is where a multipoint video conference is hosted. iVIEW Communications Manager reserves MCU resources, schedules MCU conferences, and controls in-session MCU meetings. iVIEW Communications Manager

The procedure of adding a new MCU to iVIEW Management Suite involves adding the device to both iVIEW Network Manager and iVIEW Communications Manager.

Procedure

Step 1 Log in to iVIEW Network Manager.

Step 2 Select one of the network views (**Network Tree**, **Network Table** or **Network Map**) in the sidebar menu.

Step 3 To create a new MCU element profile, do the following:

a. Select the **Add element** icon.

b. Select MCU from the element type list and enter the element name and IP address.

c. Select **OK** to add the MCU element profile to the NMS.

Step 4 To modify an existing MCU element profile, do the following:

a. Select the MCU you want to modify.

b. Select the **Edit element** icon.

c. Modify the element name.

d. Select **OK** to update the MCU in the NMS.

Step 5 Log in to iVIEW Communications Manager.

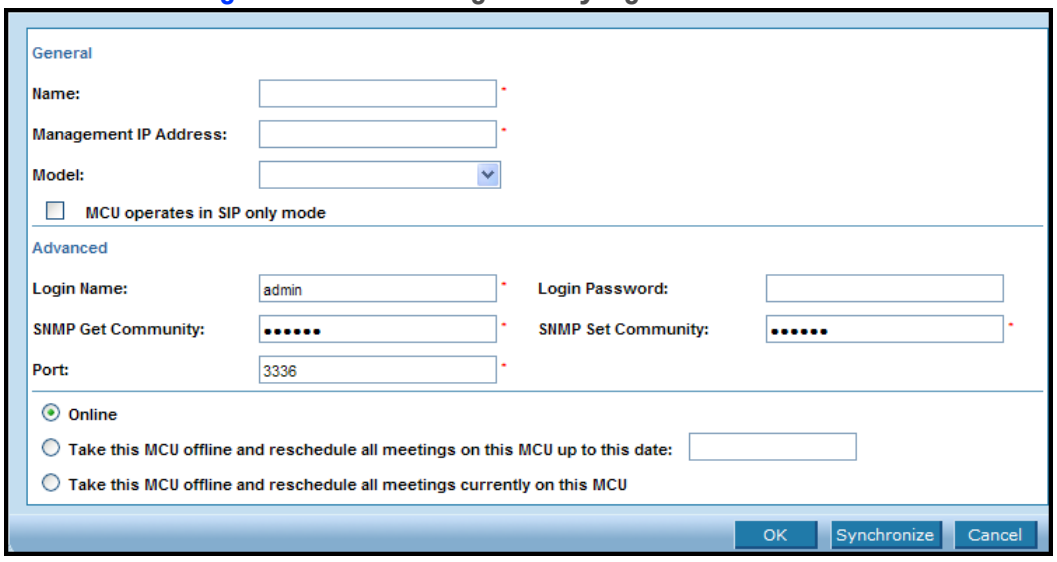
Step 6 Select **Resource Management** in the sidebar menu.

Step 7 Select **MCU**.

Step 8 Select **Add** to create a new MCU profile. If your MCU profile already exists, select the link of the MCU you want to modify in the **Name** column.

Step 9 Enter the name and the management IP address of the MCU in the relevant fields.

Figure 3-1 Creating/Modifying an MCU Profile



Step 10 Select the MCU model.

Step 11 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.

Step 12 Select the MCU's branch or office 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 Communications Manager Configuration Tool under **System Configuration** > **UI Settings**.

Step 13 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.

Step 14 Define SNMP communities, port, and bandwidth in the relevant fields.

SNMP community information must match the settings defined in the MCU to enable iVIEW Communications Manager to retrieve information from the MCU.

Step 15 Select **OK** to either add the new MCU profile to iCM, or to update the existing profile.

The MCU appears on the MCU tab and is brought online by default.

Note: If iVIEW Communications Manager 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 select **OK**.

After modifying an MCU profile, you can take the MCU offline and reschedule meetings on the MCU by selecting the relevant option.

Configuring MCU's Branch or Office

Once the MCU is added to the iVIEW Management Suite, you can modify the office or branch to which the MCU was registered to, according to your network requirements and topology. This procedure is relevant for service providers and administrators of a distributed deployment.

Procedure

Step 1 Log in to iCM.

Step 2 Select **Resource Management** in the sidebar menu.

Step 3 Select **MCU**.

Step 4 Select the link in the Name column for the MCU you want to configure.

Step 5 Select the MCU's branch or office 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 Communications Manager Configuration Tool under **System Configuration** > **UI Settings**.

Step 6 Select **OK** to save your changes.

Choosing MCU Protocol: H.323 or SIP

The MCU can operate in dual-protocol mode, supporting both SIP and H.323 devices easily and transparently. Choose the appropriate gatekeeper to rout MCU calls according to the selected protocol mode.

Procedure

Step 1 Log in to NMS.

Step 2 Select **Network Tree** in the sidebar menu.

Step 3 Select the MCU you require in the tree.

Step 4 Select **Protocols**.

Step 5 Select **Use H.323 Gatekeeper** or **Use SIP Server** to determine the MCU call routing device.

Step 6 Enter an IP address port value in the relevant fields.

Step 7 Select **Upload** to save your changes.

Note: When you select SIP as the MCU protocol mode, make sure the MCU is configured to communicate with the SIP proxy. For details, see the *Installation Guide for SCOPIA Elite MCU*.

Managing MCU Meeting Types

There are two types of meetings in iVIEW Management Suite, MCU meetings and iVIEW Management Suite built-in meetings.

MCU meetings, also known as MCU services, are used for scheduling meetings on the MCU. To view the supported services of an MCU, go to iVIEW Network Manager > Network Tree > MCU > Services. MCU meeting types are defined in the MCU and then synchronized with iVIEW Management Suite. Once iVIEW Management Suite retrieves meeting types from MCUs, these meeting types can be uploaded and distributes to other MCUs according to your specific deployment requirements. Each meeting type is identified by a unique prefix number, to avoid conflicts when synchronizing with MCUs. See "Resolving Meeting Type Conflicts" on page 118. For details on how to create MCU meeting types, see *the Installation Guide for SCOPIA MCU*.

iVIEW Management Suite has two built-in meeting types; non video conference and point-to-point. Built-in meeting types cannot be modified, uploaded or downloaded.

- 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.

This section explains how to download, upload and configure meeting types.

- Downloading Meeting Types to iVIEW Management Suite ..... page 117
- Upload a Meeting Type to Network MCUs ..... page 117
- Resolving Meeting Type Conflicts..... page 118
- Defining a Default Meeting Type ..... page 119
- Configuring Meeting Type Details ..... page 119
- Modifying Meeting Types..... page 120

Increasing MCU Capacity by Cascading Multiple MCUs

iVIEW Management Suite can 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.
- 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 procedure below:

Procedure

Step 1 Log in to iCM.

Step 2 Go to **Admin** > **Advanced Settings** from the sidebar menu.

Step 3 On the Default Meeting Settings tab you can enable or disable automatic cascading of MCU conferences by configuring the Allow Cascaded Meeting field.

Step 4 If Allow Cascaded Meeting is set to yes, select one of the following options from the Prioritize field:

- Bandwidth—iVIEW Communications Manager allocates resources to conserve bandwidth. For example, at a site with two users and one MCU, iVIEW Communications Manager 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, iVIEW Communications Manager cascades a maximum of two MCUs.
- Delay (default)—iVIEW Communications Manager allocates resources to ensure the best video quality. iVIEW Communications Manager 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 iVIEW Communications Manager has more than one MCU and there are at least two meeting participants. iVIEW Communications Manager 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.

Step 5 Select **OK** to save the preferred behavior as the default.

Enabling the Auto-Attendant

The auto-attendant allows users to access a video menu and select menu options using DTMF. In video networks, this functionality is typically used to provide quick access to meetings currently running on an RADVISION MCU.

The process of enabling the auto-attendant includes creating an Active Directory (AD) user dedicated to the auto attendant.

The auto-attendant is available only in video networks where a SCOPIA Elite MCU is deployed.

Before You Begin

1. Choose a number you want to assign to the auto-attendant feature.

   This number must be different from these numbers:

   - MCU service
   - SCOPIA Gateway service
   - ECS zone prefix
   - IP terminal number
2. Verify the e-mail of the Active Directory user that represents the auto-attendant feature.

Procedure

Step 1 Download the meeting types from MCUs.

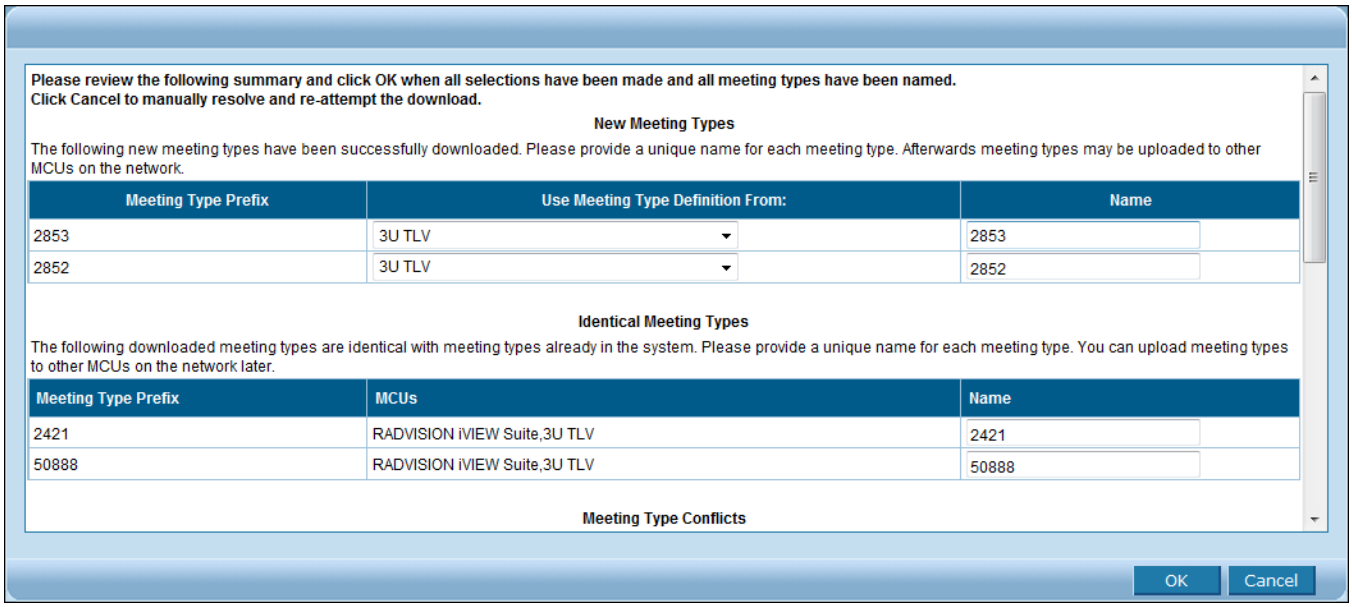
a. Access the iVIEW Communications Manager user interface.

b. Select **Meeting types** in the sidebar.

c. Select **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 in your deployment.

Figure 3-2 Meeting types downloaded into the iVIEW Management Suite from MCUs



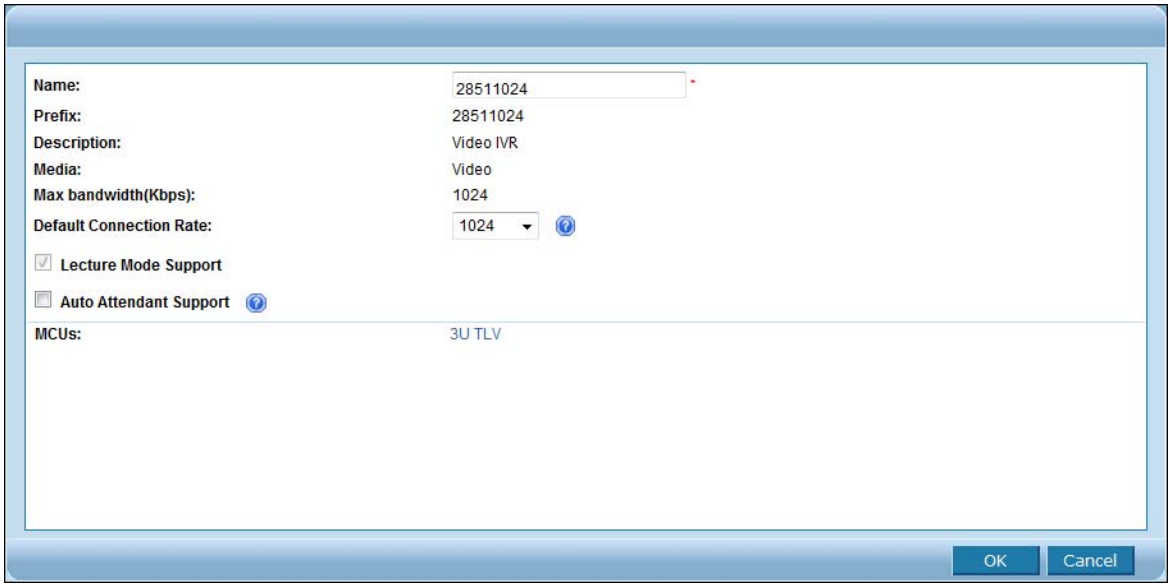
d. Enter a unique name for each meeting type.

e. Select **OK**.

Step 2 Enable the auto-attendant for the meeting type you want to use for the auto-attendant functionality:

a. Select the meeting type on the Active Meeting Types tab.

Figure 3-3 Enabling the auto-attendant feature for a meeting type



b. Select **Auto Attendant Support**.

> **Note:** When enabling auto-attendant support, if your deployment uses a third party gatekeeper, ensure that the gatekeeper has a prefix configured to direct calls to the auto-attendant.

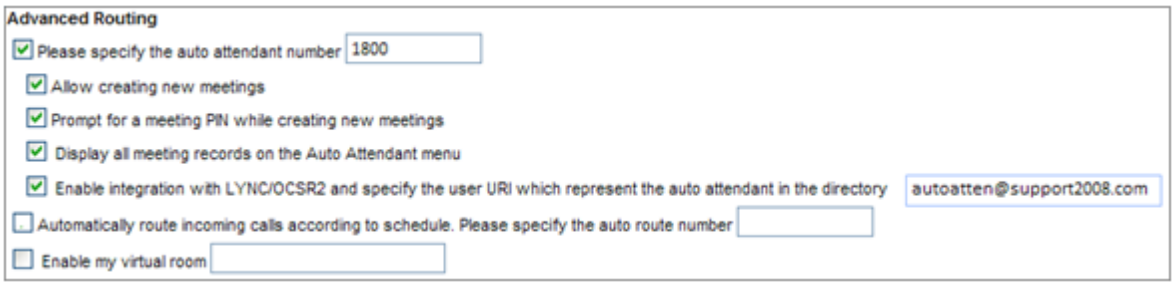
c. Select **OK**.

Step 3 Assign an auto attendant number to the meeting you configured with auto-attendant support:

a. Select **Advanced Settings** in the sidebar.

b. Select the **Default Meeting Settings** tab.

Figure 3-4 Selecting the auto-attendant number



c. Select **Please specify the auto attendant number**.

d. Enter the number for accessing the auto-attendant.

Typically, the number 1800 is used as the auto-attendant number.

In a multi-tenant deployment, add the prefix of the SCOPIA Video Gateway to the auto-attendant number (for example: 193 1800).

e. Select **Enable integration with MS Lync/OCS R2 and specify the user URI which represent the auto attendant in the directory**.

   In our example, it is AutoAtten@support2008.com.

f. Select **OK**.

Planning and Configuring a SCOPIA Desktop Server in iVIEW Management Suite

SCOPIA Desktop is a client/server application that provides video conferencing to remote and desktop users. The SCOPIA Desktop Server acts as a gateway from SCOPIA Desktop clients to the MCU and handles all media connections.

When adding and configuring SCOPIA Desktop Server in iVIEW Management Suite, a web access URL is defined so users can simply click on a link to connect to a conference.

- Adding a SCOPIA Desktop Profile in iVIEW Management Suite ..... page 30
- Enabling Streaming on your Video Network..... page 32
- Defining Bandwidth for SCOPIA Desktop Pro to Pro Calls..... page 32
- Configuring Recording on your Video Network ..... page 32

Adding a SCOPIA Desktop Profile in iVIEW Management Suite

SCOPIA Desktop profiles are manually added to the iVIEW Management Suite. Once a SCOPIA Desktop is configured, it is automatically brought online so that iVIEW Communications Manager can schedule resources.

When configuring the SCOPIA Desktop server IP address in iVIEW Management Suite, the iVIEW Management Suite IP address must be configured in the SCOPIA Desktop server to allow connection and communication between them. For more information on how to configure iVIEW Management Suite IP address in the SCOPIA Desktop server, see the *Installation Guide for SCOPIA Desktop Server*.

Procedure

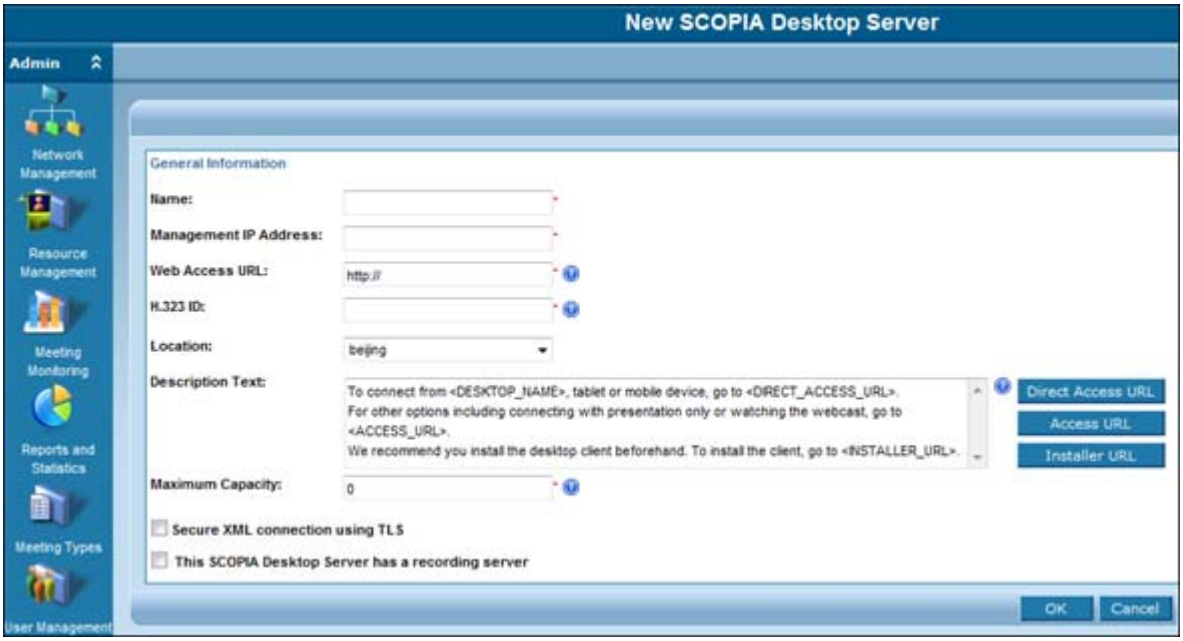
Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **Resource Management** in the sidebar menu.

Step 3 Select SCOPIA Desktop.

Step 4 Select the link in the Name column for the SCOPIA Desktop Server you require, or select **Add** to create a new SCOPIA Desktop Server profile. The **New SCOPIA Desktop Server** page appears (Figure 3-5 on page 31).

Figure 3-5 Adding a SCOPIA Desktop profile



Step 5 Enter the name and IP address of the SCOPIA Desktop Server in the relevant fields.

Step 6 Enter the URL used by participants to join a meeting via SCOPIA Desktop Server in the **Web Access URL** field.

The URL must be in the format http://<web URL>:<port number>/scopia.

Step 7 Enter an H.323 ID used to identify connections from SCOPIA Desktop Server 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 iVIEW Communications Manager to route calls from this SCOPIA Desktop Server based on the predefined IP topology.

Step 8 Select a topology setting from the **Location** list. The default value is **Home**.

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

Step 9 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.

Step 10 Enter the maximum capacity allowed by your SCOPIA Desktop license in the Maximum Capacity field.

Step 11 (Optional) Select **Secure XML connection using TLS** to use the Transport Layer Security (TLS) protocol to secure the transport link between iVIEW Management Suite and SCOPIA Desktop.

Step 12 To configure this SCOPIA Desktop Server with a recording server, select the **This SCOPIA Desktop Server has a recording server** checkbox.

Step 13 Select **OK** to save your changes.

Enabling Streaming on your Video Network

Streaming can be configured in iVIEW Management Suite to provide broadcast of a point-to-point or multipoint videoconference to an audience of listeners and viewers who are not active participants in the conference. Streamed video and audio can be played using a client PC with any media playing application.

To enable streaming, make sure SCOPIA Desktop Server is configured to support streaming. See the *Administrator Guide for SCOPIA Desktop Server*.

Procedure

Step 1 Log in to iCM.

Step 2 Select **Advanced Settings** in the sidebar menu.

Step 3 Select **Look and Feel**.

Step 4 Set Streaming to **Visible**.

Step 5 Select **OK** to save your changes.

Defining Bandwidth for SCOPIA Desktop Pro to Pro Calls

When defining bandwidth for your office or branch, you define the in-zone and cross-zone calls, including SCOPIA Desktop calls bandwidth thresholds.

iVIEW Management Suite does not manage pro to pro calls, although you can configure bandwidth for SCOPIA Desktop Pro calls within iVIEW Management Suite. This setting is retrieved by the SCOPIA Desktop that actually manages pro to pro calls.

Procedure

Step 1 Log in to iVIEW Communications Manager

Step 2 Select **Advanced Settings** in the sidebar menu.

Step 3 Select **Default User Settings**.

Step 4 (Optional) If a single SCOPIA Desktop Server or multiple SCOPIA Desktop Servers are configured to work with iVIEW Management Suite, select a value from the **Maximum Allowed Bandwidth for SCOPIA Desktop Calls** field.

Step 5 Select **OK** to save your changes.

Configuring Recording on your Video Network

You can configure iVIEW Management Suite and SCOPIA Desktop to support recording of audio, video and data of on-going meetings. Recording is performed by a SCOPIA Desktop Server with a recording license installed. See the *Administrator Guide for SCOPIA Desktop* for details on how to configure recording on SCOPIA Desktop Server according to your deployment.

To configure iVIEW Management Suite and SCOPIA Desktop to support recording on your video network, perform the following procedures in the order that they are listed:

- Configuring the SCOPIA Desktop Profile to Include a Recording Server ..... page 33
- Enabling Recording on iVIEW Management Suite..... page 34
- Allowing Recording for Specified User Types ..... page 34
- Allowing Recording for Individual Users ..... page 35
- Enabling Recording for Specified Users Virtual Rooms..... page 113

Configuring the SCOPIA Desktop Profile to Include a Recording Server

You can configure your SCOPIA Desktop profile to include a recording server. This requires you to have the recording license. For more information about the license, see the *Installation Guide for SCOPIA Desktop*.

Procedure

Step 1 Access the iVIEW Communications Manager.

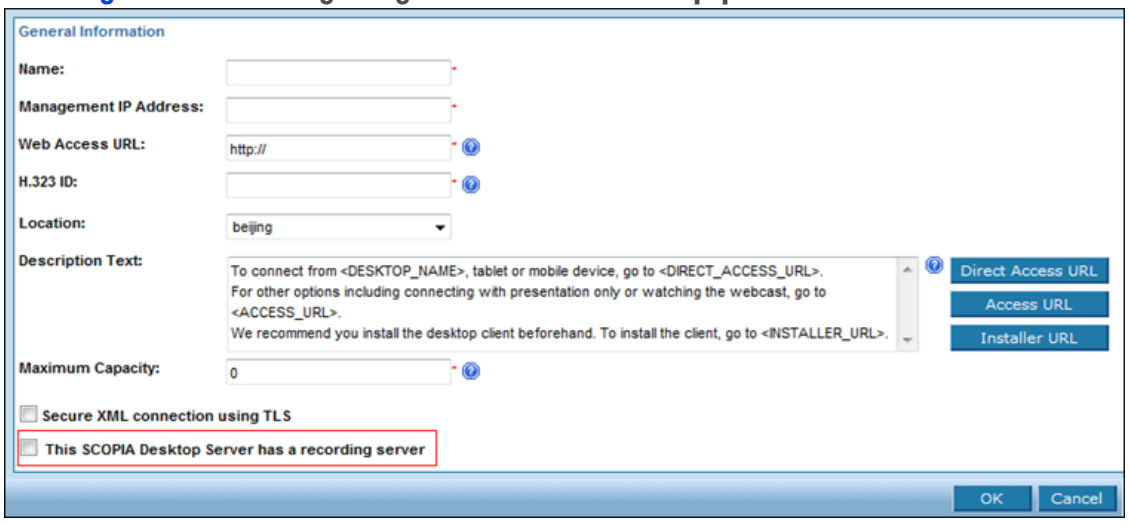
Step 2 Select **Resource Management**.

Step 3 Select the **SCOPIA Desktop** tab.

Step 4 Select the SCOPIA Desktop profile you want to modify in the **Name** column.

Step 5 To configure this SCOPIA Desktop with a recorder, select the **This SCOPIA Desktop Server has a recording server** checkbox (Figure 3-6 on page 33).

Figure 3-6 Configuring the SCOPIA Desktop profile with a recorder



Step 6 Select **OK**.

Step 7 Enable recording on iVIEW Management Suite, as described in "Enabling Recording on iVIEW Management Suite" on page 34.

Enabling Recording on iVIEW Management Suite

You can configure iVIEW Management Suite SCOPIA Desktop Server.

After recording is enabled in iVIEW Management Suite, you can:

- Specify the types of users to which recording will be available upon meeting scheduling, as described in "Allowing Recording for Specified User Types" on page 34 and "Allowing Recording for Individual Users" on page 35.

  By default, all users types have recording permissions.

- Enable automatic recording of a meeting for specified users virtual rooms, as described in "Enabling Recording for Specified Users Virtual Rooms" on page 113.

Before You Begin

Make sure your SCOPIA Desktop profile includes a recorder. See "Configuring the SCOPIA Desktop Profile to Include a Recording Server" on page 33.

Procedure

Step 1 Log in to iCM.

Step 2 Select **Advanced Settings** in the sidebar menu.

Step 3 Select **Look and Feel**.

Step 4 Set Recording to **Visible**.

Step 5 Select **OK** to save your changes.

Allowing Recording for Specified User Types

When recording is enabled in iVIEW Management Suite, by default all user types have permission to record meetings. You can narrow the recording service by granting recording permissions to specific user types.

Before You Begin

Make sure recording is enabled in iVIEW Management Suite. See "Enabling Recording on iVIEW Management Suite" on page 34.

Procedure

Step 1 Select **Advanced Settings** in the sidebar menu.

Step 2 Select **Default User Settings**.

Step 3 Select the user types that you want to allow to record meetings from the list in the Default Recording Permissions section.

Step 4 Select **OK** to save your changes.

Allowing Recording for Individual Users

When recording is enabled in iVIEW Management Suite, by default all users have permission to record on-going meetings. You can narrow the availability of this service by configure recording permission for specific users.

Before You Begin

- Make sure recording is enabled in iVIEW Management Suite. See "Enabling Recording on iVIEW Management Suite" on page 34.
- If you want to manually allow specific users to be able to record meetings, make sure you remove recording permissions from all users. See "Allowing Recording for Specified User Types" on page 34.

Procedure

Step 1 Select **User Management** in the sidebar menu.

Step 2 Select **Users**.

Step 3 Select the link in the Name column for the user you require.

Step 4 Select **Advanced**.

Step 5 (Optional) Select **Allow user to record meetings** to enable this user to record meeting regardless of the global policy.

Step 6 Select **OK** to save your changes.

Planning and Configuring Gateways in iVIEW

Configure gateways in your network to enable non-H.323 endpoints, such as SIP, PSTN, ISDN, and mobile endpoints, to join a meeting. iVIEW Management Suite uses the gateway information to provide proper dialing information for meeting participants, and to dial out to endpoints to invite them to meetings. In addition, iVIEW Management Suite manages gateway resources to allow successful call scheduling using network gateways.

- Adding a Gateway and its Services in iVIEW Management Suite ..... page 36
- Adding or Editing a Service to an Existing Gateway ..... page 39
- Registering a Gateway with a Gatekeeper ..... page 40
- Adding and Configuring a SCOPIA Video Gateway in iVIEW Management Suite ..... page 40
- Adding and Configuring SIP Gateway in iVIEW Management Suite ..... page 44

Gateways extend your video capabilities to include protocols outside of your main video network. The SCOPIA Gateway, for example, extends your H.323-based network to include ISDN endpoints.

The resource management features of iVIEW Management Suite keeps track of the gateway's available ports to enable the successful scheduling of calls.

When you add a gateway, the settings in iVIEW Management Suite must be consistent with the configuration of the gateway device itself. This includes specifying all the services on that gateway.

A service maps a numeric dial prefix to a type of call. When the gateway receives a call with the designated prefix, it determines the properties of that call:

- Whether it is voice only or video, and
- The bandwidth allocated for this kind of call.

This procedure details how to add a gateway to the iVIEW Management Suite including detailing the gateway's services.

Procedure

Step 1 Log in to iVIEW Network Manager.

Step 2 Select one of the network views (**Network Tree**, **Network Table** or **Network Map**) in the sidebar menu.

Step 3 Select the location in the network view at which you want to add the new element, and do one of the following to create a new element profile:

- Select **Add** > **New** > **New element**.
- Select **Add element** .

Step 4 Select the gateway type from the element type list and enter the element name and IP address.

Step 5 (Optional) Select **Allow offline configuration** to allow The SCOPIA iVIEW Network Manager to hold configuration details for an offline element and apply settings as the element goes online.

Step 6 Select **OK** to add the gateway.

Step 7 Log in to iVIEW Communications Manager.

Step 8 Select **Resource Management** in the sidebar menu.

Step 9 Select **Gateway**.

Step 10 Select a link for an existing gateway to edit, or select **Add** to create a new gateway profile.

Step 11 Enter the field values as required.

Field Name	Description
Name	The name of the gateway.
Model	The type of gateway. Choose from a list of predefined gateway types.
Registered To	Select the gatekeeper to which the gateway is registered.

Field Name	Description
Location	Select the office or branch from the list to which the gateway belongs. The **Location** field is visible only when the **IP Topology** tab is activated in the iVIEW Communications Manager Configuration Tool under **System Configuration** > **UI Settings**.
Management IP Address	The IP address of the management stream of the gateway. iVIEW Communications Manager communicates with the gateway via its management stream, and does not need the media stream if different. If multiple gateways are pooled together in a local network with the same access phone number, enter all the IP addresses separated by a semi-colon (;).
Bandwidth	The total bandwidth allocated to this gateway. For example, for an E1 line or 30 B-channels, the bandwidth is 64 x 30 = 1920 Kbps per network interface. For gateways with two PRI interfaces, the total bandwidth would be 1920 x 2 = 3840kbps. If multiple gateways are pooled together in a local network with the same access phone number, enter the bandwidth of a single gateway unit in the pool.
Working Mode	Choose **IVR** if the gateway routes calls using an Interactive Voice Response (IVR) system. Choose **DID** if call routing is direct to an endpoint without operator intervention using Direct Inward Dialing. For more information see the User Guide of the gateway.
Description	A description of the phone number for the gateway.
International Access Code	The numeric dial prefix required to make an international call.
Country Code	The numeric dial prefix to dial a terminal located in a different country than the country.
Domestic Long Distance Prefix	The numeric dial prefix required to make a long distance call within the same country.
Allow Out of Area Calls	If selected, endpoints can reach iVIEW Communications Manager via the gateway even when they have a different area code to that of the gateway.
Area Code	The domestic area code of the gateway number.
Telephone Number	A local telephone number to be assigned to the specific port.
To access an outside line for local calls, dial	The dial prefix required for the gateway to access an outside line.
To access an outside line for long distance calls, dial	The dial prefix required for the gateway to make a long distance call.

Step 12 Select **Add Service** to create an additional service entry for this gateway. You can add multiple services. The list of services must be identical to the services on the gateway itself.

A service maps a numeric dial prefix to a type of call. When the gateway receives a call with the designated prefix, it determines the properties of that call:

- Whether it is voice only or video, and
- The bandwidth allocated for this kind of call.

Step 13 For each service, enter the field values as required:

Field Name	Description
Service Prefix	The numeric dial prefix used by the gateway to identify this service.
Bandwidth	The properties of this service, both bandwidth and whether it is voice only or video. Choose from a predefined list. If this service's bandwidth is set to **Auto** on the device itself, in iVIEW Management Suite enter the average bandwidth endpoints use when dialing that service.
Restricted Mode	Select this field to indicate the ISDN line is a restricted type. This is a property of the line's PBX, which reserves the top 8k of each packet for control data.

Note: If you select **Restricted Mode**, the bandwidth appears as multiples of 56 Kbps instead of multiples of 64, since 8k of each packet is reserved for control data on an ISDN line operating in restricted mode.

Step 14 Set the advanced settings.

Field Name	Description
Signaling Port	The gateway port used for signaling. Leave this field blank to negotiate the signaling port dynamically.
SNMP Set/Get Community	The shared password between iVIEW Management Suite and the gateway to enable encrypted SNMP communications.
Dial-in Only	Indicates the gateway is used for incoming calls only. iVIEW Management Suite would not schedule outgoing calls on this gateway.

Step 15 Select **OK** to save your changes.

Adding or Editing a Service to an Existing Gateway

A gateway profile in iVIEW Management Suite must be consistent with the settings on the gateway device itself. This includes specifying all the services on that gateway.

A gateway service maps a numeric dial prefix to a type of call. When the gateway receives a call with the designated prefix, it determines the properties of that call:

- Whether it is voice only or video, and
- The bandwidth allocated for this kind of call.

This section explains how to edit or add new services to a gateway already defined in iVIEW Management Suite.

Procedure

Step 1 Log in to iVIEW Network Manager.

Step 2 Select **Network Tree** in the sidebar menu.

Step 3 Select the gateway you require in the tree.

> Note: If the gateway has not yet been added to iVIEW Management Suite, you must first add the gateway. For more information, see "Adding a Gateway and its Services in iVIEW Management Suite" on page 36.

Step 4 Select **Services**.

Step 5 To create a new service:

- Select **Add**.
- Right-click any existing service and select **Add**.

Step 6 To modify an existing service:

- Double-click the service
- Right-click the service and select **Edit**.

Step 7 To delete a gateway service, right-click the service and select **Delete**.

Step 8 Enter the numeric dial prefix used by the gateway to identify this service.

Step 9 Enter a short description.

Step 10 Select the call type and bit rate.

Step 11 Select **OK**.

Registering a Gateway with a Gatekeeper

Gatekeepers, which maintain the register of aliases in a video network, sometimes include endpoints working under a different network protocol, and therefore must be routed through a gateway. Gateways bridge between the H.323 protocol and other video protocols, like ISDN.

Therefore the gatekeeper must register a network's gateways, to ensure safe call routing across different protocols.

Procedure

Step 1 Log in to SCOPIA iVIEW Network Manager.

Step 2 Select **Network Tree** in the sidebar menu.

Step 3 Select the gateway you require in the tree.

Step 4 Select **Configure**.

Step 5 Enter the IP address of the gatekeeper with which the gateway registers.

Step 6 (Optional) Enter a string identifying the physical location of the gateway.

Step 7 Select **Upload**.

Adding and Configuring a SCOPIA Video Gateway in iVIEW Management Suite

This section explains how to add the SCOPIA Video Gateway into the iVIEW Management Suite and configure its settings. For more information on adding a Lync Server or OCS profile to iVIEW Management Suite, see "Adding a Lync Server or OCS Profile in iVIEW Management Suite" on page 77.

Perform this procedure after your Microsoft Lync Server or Microsoft Office Communications Server is configured.

Since the SCOPIA Video Gateway does not have a direct GUI of its own, its configuration is performed in the iVIEW Management Suite.

First add the gateway to the iVIEW Network Manager to configure it, and then add it as a resource to the iVIEW Communications Manager to manage it as a network resource.

The iVIEW Management Suite and SCOPIA Video Gateway communicate in XML over TCP for control and configuration commands. You can secure the connection by configuring it to the TLS protocol. Make sure to generate the SCOPIA iVIEW Management Suite and SCOPIA Video Gateway certificates before configuring the connection to TLS.

The SCOPIA Video Gateway is configured by default to switch to the presentation channel whenever an H.323 endpoint shares content during a video call. The SCOPIA Video Gateway sends the shared content to the Lync client. If this feature does not suit the needs of the video call, you can disable it in iVIEW Management Suite.

Procedure

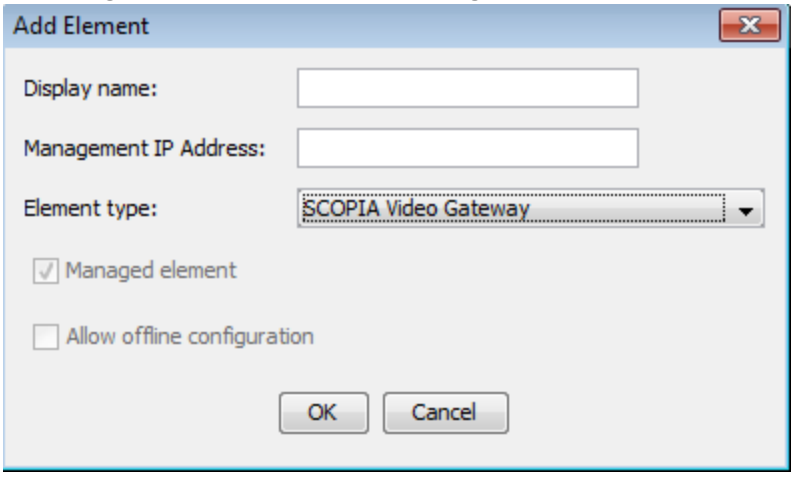
Step 1 Log into the iVIEW Network Manager.

Step 2 Add SCOPIA Video Gateway to the iVIEW Network Manager:

a. Select **Add** button  in the left pane.

The Add Element dialog box opens.

Figure 3-7 Adding a SCOPIA Video Gateway to the iVIEW Network Manager



b. Enter the name for this SCOPIA Video Gateway.

c. Enter the Management IP address for SCOPIA Video Gateway.

d. Select **SCOPIA Video Gateway** from the list.

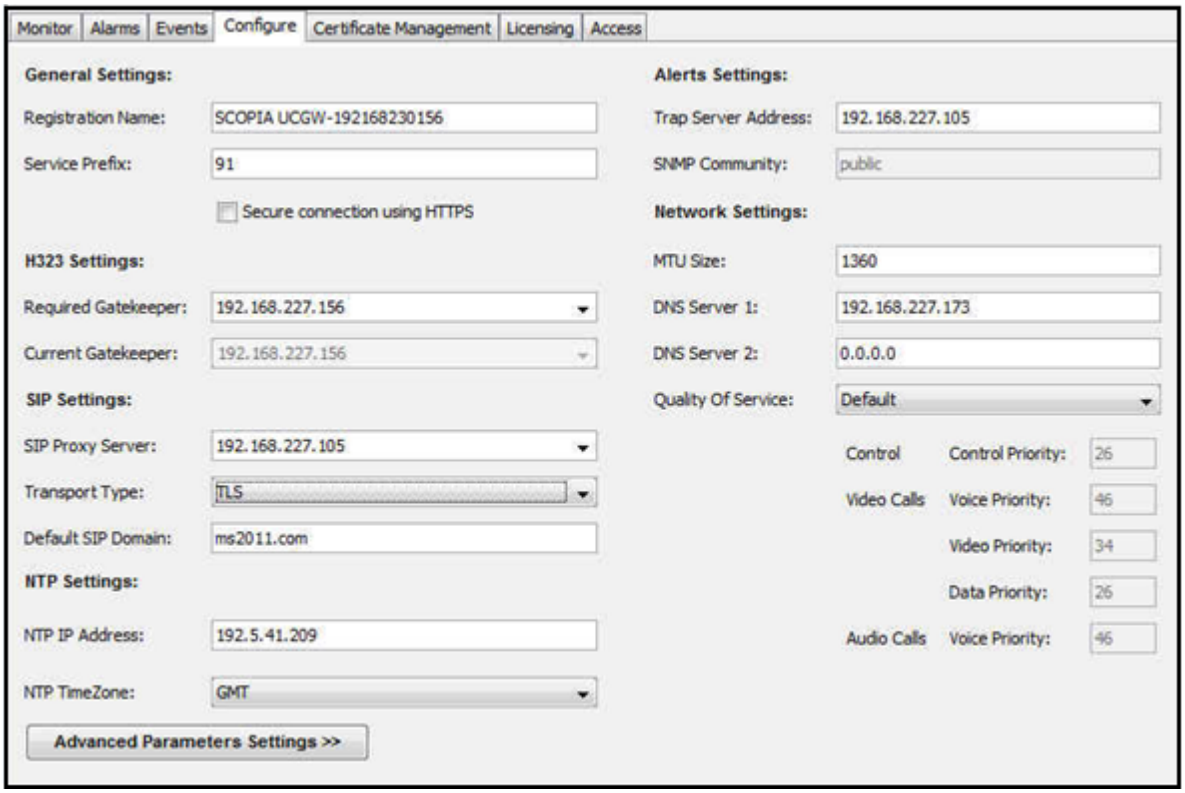
e. Select **OK**.

Step 3 Configure the SCOPIA Video Gateway settings:

a. Select the SCOPIA Video Gateway in the tree view.

b. Select the **Configure** tab.

Figure 3-8 The Configure Tab



c. Enter the following values:

Field Names	Description
Registration Name	The name of this gateway is automatically generated by the system.
Service Prefix	The prefix to dial to access this gateway.
Secure connection using HTTPS	Select this setting to encrypt the communication between the gateway and the iVIEW Network Manager. Before selecting HTTPS, you must generate the gateway certificates.
Required Gatekeeper	The gatekeeper to which you want to register the gateway.
SIP Proxy Server	The IP of the SIP Server for this gateway. Typically iVIEW Management Suite acts as the SIP server.
Transport Type	The default setting is TCP. Choose **TLS** for encrypted communications with the SIP server. TLS requires correctly issued certificates from a CA for the gateway and the SIP server.
Default SIP Domain	The SIP domain of your organization.

Field Names	Description
NTP IP Address	The IP address of a Network Time Protocol server which sets the time for the gateway's clock. External NTP servers ensure the same clock throughout all devices on the network. If you have no NTP server, enter **0.0.0.0**.
NTP Time Zone	The time zone of the NTP server.
Trap Server Address	The IP address of the server which receives the SNMP traps from the gateway, including alarms and events. Typically the iVIEW Management Suite acts as the gateway's SNMP traps server.
SNMP Community	The SNMP Server group setting.
MTU size	The size of the packets received from the gateway. Only change this if a router uses a non-standard MTU size.
DNS Server 1, 2	The IP address(es) of the organization's DNS server(s).
Quality of Service	Typically this setting remains on **Default**. You can customize the priority given to the different elements of the gateway communication if required.

d. Select **Upload**.

Step 4 Add the SCOPIA Video Gateway as an iVIEW Management Suite resource:

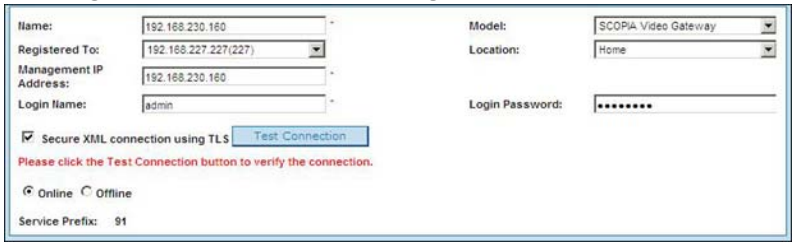
a. Access the iVIEW Management Suite administrator interface.

b. Select **Resource Management** in the sidebar.

c. Select the **Gateway** tab.

d. Select **Add**.

Figure 3-9 Adding SCOPIA Video Gateway to iVIEW Communications Manager



e. Enter a name for your SCOPIA Video Gateway in the **Name** field.

f. Select **SCOPIA Video Gateway** from the **Model** list.

g. Select the IP address of the gatekeeper that the SCOPIA Video Gateway is registered to in the **Registered To** field.

h. Enter the IP address of the SCOPIA Video Gateway in the **Management IP Address** field.

i. If there is more than one location in your deployment, assign your SCOPIA Video Gateway to a location by selecting an option from the **Location** list.

j. Enter the login name and password of the SCOPIA Video Gateway. The default username is **admin** and the default password is **password**.

k. If required, select **Secure XML Connection using TLS** to use TLS and thus secure the exchange of XML messages and commands between the SCOPIA Video Gateway and iVIEW Management Suite.

> Note: Before selecting TLS, you must generate the SCOPIA iVIEW Management Suite and SCOPIA Video Gateway certificates.

After you select that checkbox, click **Test Connection**. When the test is successful, the **OK** button is enabled.

l. Select **OK**.

m. Select **Synchronize**.

Adding and Configuring SIP Gateway in iVIEW Management Suite

This section explains how to add the RADVISION SIP Gateway into the iVIEW Management Suite and configure its settings. Since the SIP Gateway does not have a direct GUI of its own, its configuration is performed in the iVIEW Management Suite.

First add the gateway to the iVIEW Network Manager to configure it, and then add it as a resource to the iVIEW Communications Manager to manage it as a network resource.

The iVIEW Management Suite and SIP Gateway communicate in XML over TCP for control and configuration commands. You can secure the connection by configuring it to the TLS protocol. Make sure to generate the SCOPIA iVIEW Management Suite and SIP Gateway certificates before configuring the connection to TLS.

Procedure

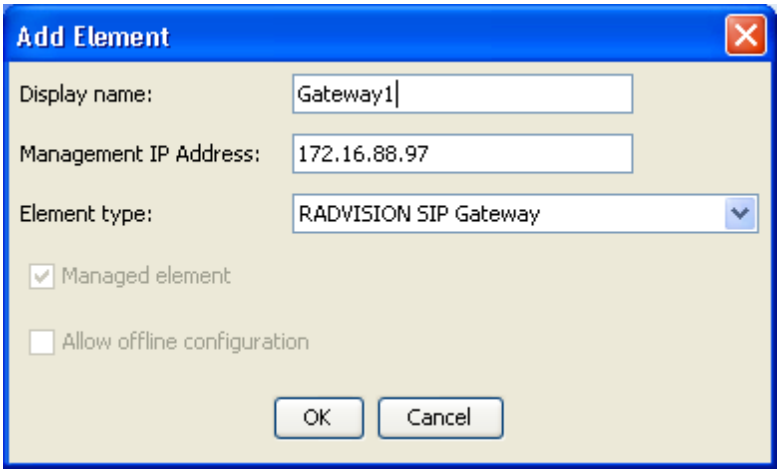
Step 1 Log into the iVIEW Network Manager.

Step 2 Add this gateway to the iVIEW Network Manager:

a. Select the **Add** button  in the left pane.

The Add Element dialog box opens.

Figure 3-10 Adding an SIP Gateway to the iVIEW Network Manager



b. Enter the name for this gateway.

c. Enter its Management IP Address.

d. Select **RADVISION SIP Gateway** from the list.

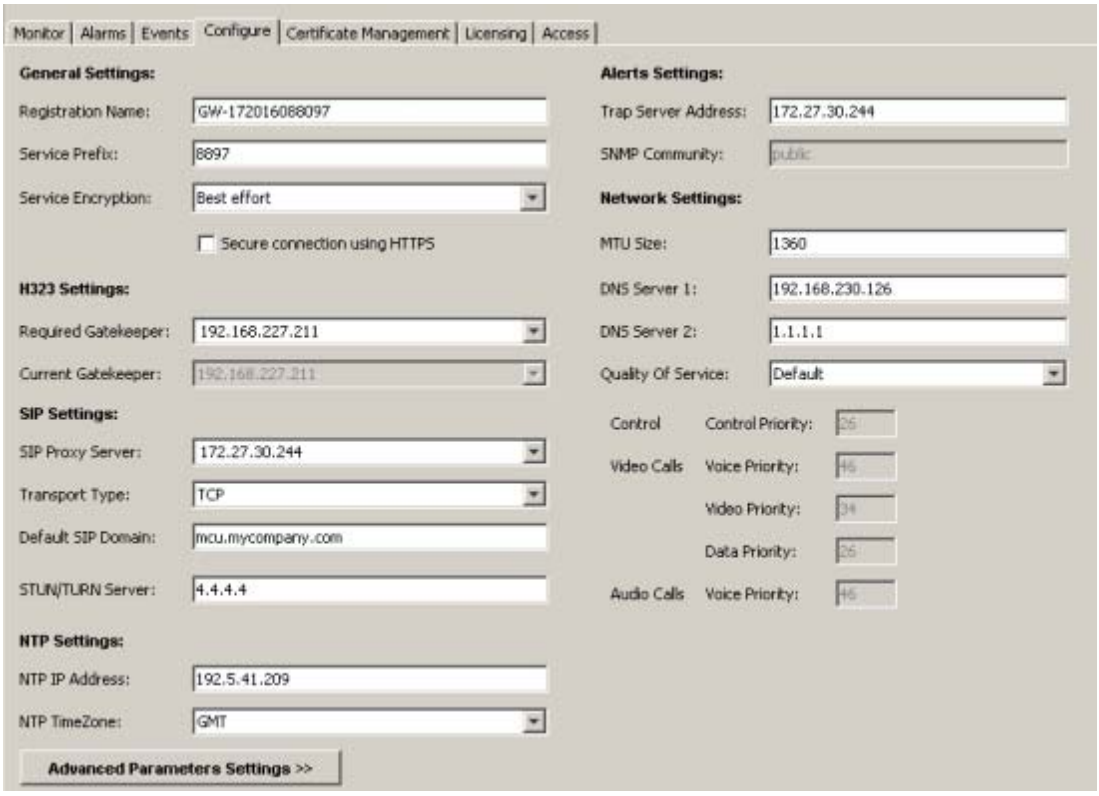
e. Select **OK**.

Step 3 Configure the gateway settings:

a. Select the new gateway in the tree view.

b. Select the **Configure** tab.

Figure 3-11 Setting the gateway's addresses and encryption



c. Enter the following values:

Field Names	Description
Registration Name	The name of this gateway is automatically generated by the system.
Service Prefix	The prefix to dial to access this gateway. Use the dial prefix when attempting to dial a remote SIP ICE client like the IBM Sametime client using a numeric dial.
Service Encryption	Determines the level of encryption used when communicating with the remote SIP ICE client. Choose between: • **None** - Encryption is not required to connect the call. • **Best Effort** - Connects the call encrypted if the other party supports that encryption. This may lead to only part of the route being encrypted, for example only the portion from the SIP ICE client to the gateway is encrypted. • **Mandatory** - The SIP ICE client's communications to the gateway must be encrypted with TLS for the call to be connected, while the connection to the MCU can also be encrypted with H.235 (optional).
Required Gatekeeper	The gatekeeper to which you want to register the gateway.
Current Gatekeeper	The current IP of the gatekeeper as it is registered on the network. This value is taken from the gatekeeper device, and cannot be edited in this window.
SIP Proxy Server	The IP of the SIP Server for this gateway. Typically iVIEW Management Suite acts as the SIP server.
Transport Type	The default setting is **TCP**. Choose **TLS** for encrypted communications with the SIP server. TLS requires correctly issued certificates from a CA for the gateway and the SIP server.
Default SIP Domain	The SIP domain of your organization.
STUN/TURN Server	The IP address or FQDN of the IBM Sametime STUN/TURN server.
NTP IP Address	The IP address of a Network Time Protocol server which sets the time for the gateway's clock. External NTP servers ensure the same clock throughout all devices on the network. If you have no NTP server, enter **0.0.0.0**.
NTP Time Zone	The time zone of the gateway.

Field Names	Description
Trap Server Address	The IP address of the server which receives the SNMP traps from the gateway, including alarms and events. Typically the iVIEW Management Suite acts as the gateway's SNMP traps server.
SNMP Community	The SNMP Server group setting.
MTU size	The size of the packets received from the gateway. Only change this if a router uses a non-standard MTU size.
DNS Server 1, 2	The IP address(es) of the organization's DNS server(s).
Quality of Service	Typically this setting remains on **Default**. You can customize the priority given to the different elements of the gateway communication if required.

Step 4 Add the gateway as an iVIEW Management Suite resource:

a. Access the iVIEW Communications Manager administrator interface.

b. Select **Resource Management** in the sidebar.

c. Select the **Gateway** tab.

d. Select **Add**.

Figure 3-12 Adding SIP Gateway to iVIEW Communications Manager



e. Enter a name for your gateway in the **Name** field.

f. Select **RADVISION SIP Gateway** from the **Model** list.

g. Enter the IP address of the gateway in the **Management IP Address** field.

h. If there is more than one location in your deployment, assign your gateway to a location by selecting an option from the **Location** list.

i. Enter the login name and password of the gateway. The default username is **admin** and the default password is **password**.

j. Select **Secure XML Connection using TLS** to use TLS and thus secure the exchange of XML messages and commands between the gateway and iVIEW Management Suite.

> Note: Before selecting TLS, you must generate certificates for the gateway and for iVIEW Management Suite.

k. Select **OK**.
l. Select **Synchronize**.

Adding Pathfinders in iVIEW Management Suite

The SCOPIA PathFinder provides a complete firewall and NAT traversal solution enabling secure connectivity between enterprise networks and remote sites.

Pathfinders do not yet support auto-detect, therefore, all pathfinders need to be added to the network manually.

Procedure

Step 1 Log in to iVIEW Network Manager.

Step 2 Select one of the network views (**Network Tree**, **Network Table** or **Network Map**) in the sidebar menu.

Step 3 Select the location in the network view at which you want to add the new element, and do one of the following to create a new element profile:

- Select **Add** > **New** > **New element**.
- Select **Add element** .

Step 4 Select **Pathfinder Server** from the element type list and enter the element name and IP address.
Step 5 Select **OK** to add the SCOPIA PathFinder Server to the iVIEW Network Manager.

Configuring and Planning Endpoints in iVIEW Management Suite

iVIEW Management Suite supports RADVISION endpoints and third-party endpoints. You can configure iVIEW Management Suite to manage the following endpoint types: SCOPIA XT Series, SCOPIA VC240, Polycom, Tandberg, and LifeSize.

Endpoints are defined first in the iVIEW Network Manager and then in the iVIEW Communications Manager. When a gatekeeper is defined in the iVIEW Network Manager, all SCOPIA XT Series, SCOPIA VC240, and LifeSize endpoints registered to this gatekeeper are automatically added to the system and displayed in the tree view under the gatekeeper. Other endpoints need to be manually added to the iVIEW Network Manager, as described in "Setting the Managed Status of Endpoints" on page 75.

In the iVIEW Communications Manager, endpoints registered to the gatekeeper must be imported. There are three different ways to import endpoints in the iVIEW Communications Manager. In addition, you can manually add endpoints to the videoconferencing network.

Note: Before you import endpoints defined in an LDAP server, make sure the connection to an LDAP server is configured. See Connecting iVIEW Management Suite with the LDAP Server page 100.

- Importing Endpoints from the Gatekeeper ..... page 50
- Importing Endpoints Registered to a Third-Party Gatekeeper ..... page 51
- Downloading H.323 Endpoints from the LDAP Server ..... page 54
- Importing SIP/H.323/H.320 Endpoints using the H.350 Search Base ..... page 56
- Configuring your Endpoints to use iVIEW Management Suite as the LDAP Directory page 56
- Adding Endpoints in iVIEW Management Suite Manually ..... page 69
- Setting the Managed Status of Endpoints ..... page 75
- Removing Endpoints ..... page 75
- Searching for an Endpoint ..... page 76
- Managing Endpoints Configuration Upload History..... page 76

Importing Endpoints from the Gatekeeper

This procedure describes how to import all endpoints registered to SCOPIA Enhanced Communication Server, SCOPIA Gatekeeper, and Tandberg VCS to iVIEW Management Suite. Before you can import endpoints registered to SCOPIA Enhanced Communication Server or Tandberg VCS, you must define the gatekeeper in the iVIEW Communications Manager (see "Defining a Gatekeeper in SCOPIA iVIEW Management Suite" on page 19). You do not need to define the SCOPIA Gatekeeper since it is iVIEW Management Suite's internal gatekeeper.

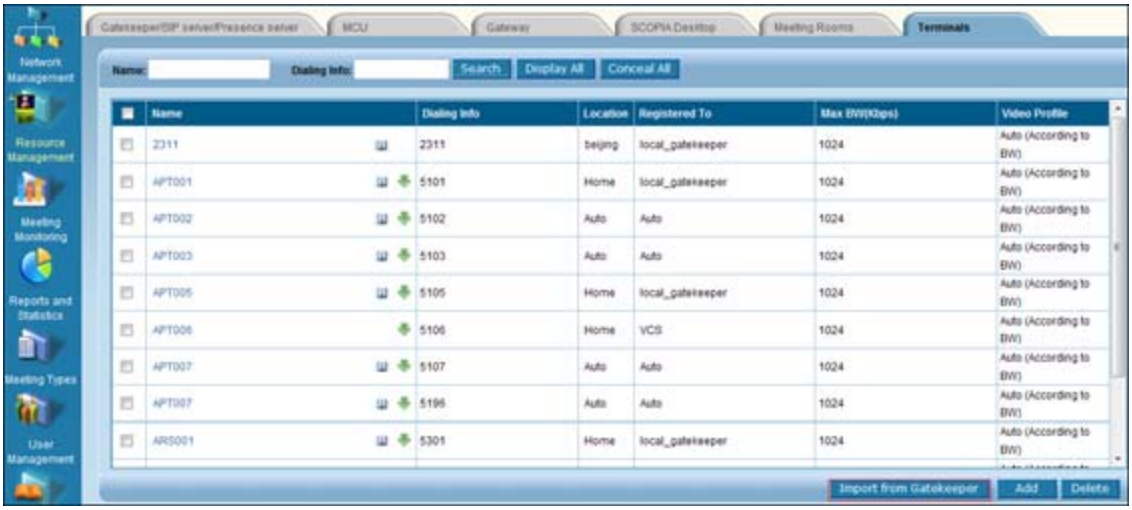
To import endpoints registered to a third-party gatekeeper, see "Importing Endpoints Registered to a Third-Party Gatekeeper" on page 51.

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **Resource Management** in the sidebar menu (see Figure 3-13 on page 51).

Figure 3-13 Importing Endpoints from ECS, SCOPIA Gatekeeper, and Tandberg VCS



Step 3 Select the **Terminals** tab.

Step 4 Select **Import from Gatekeeper**. A gatekeeper list is displayed.

Step 5 Select the gatekeeper from which endpoints should be imported and select **OK**. A list of all endpoints registered to the gatekeeper is displayed.

Step 6 Select the endpoints you want to import.

Step 7 Select **Import** to import the endpoints. Endpoints are displayed in the **Terminals** tab.

Importing Endpoints Registered to a Third-Party Gatekeeper

When you use a third-party gatekeeper in your deployment and there are endpoints registered to this gatekeeper, you need to import these endpoints. Before you can import endpoints registered to third-party gatekeeper, you must define the gatekeeper in the iVIEW Communications Manager.

Note: If you have a Tandberg VCS gatekeeper and want to register your endpoints, follow the procedure described in "Importing Endpoints from the Gatekeeper" on page 50.

Procedure

Step 1 Access the iVIEW Management Suite user interface.

Step 2 Select **Advanced Settings** in the left pane.

Step 3 Select the **LDAP Configurations** tab.

Step 4 Select the relevant LDAP link.

Step 5 Select **Advanced**.

Step 6 Navigate to the **Terminals** section of the tab.

Step 7 In the **Registered to third party gatekeeper** area, define the endpoints registered to the third-party gatekeeper in the iVIEW Management Suite as described in Table 3-1:

Figure 3-14 Registered to third-party gatekeeper area of the LDAP Configurations tab

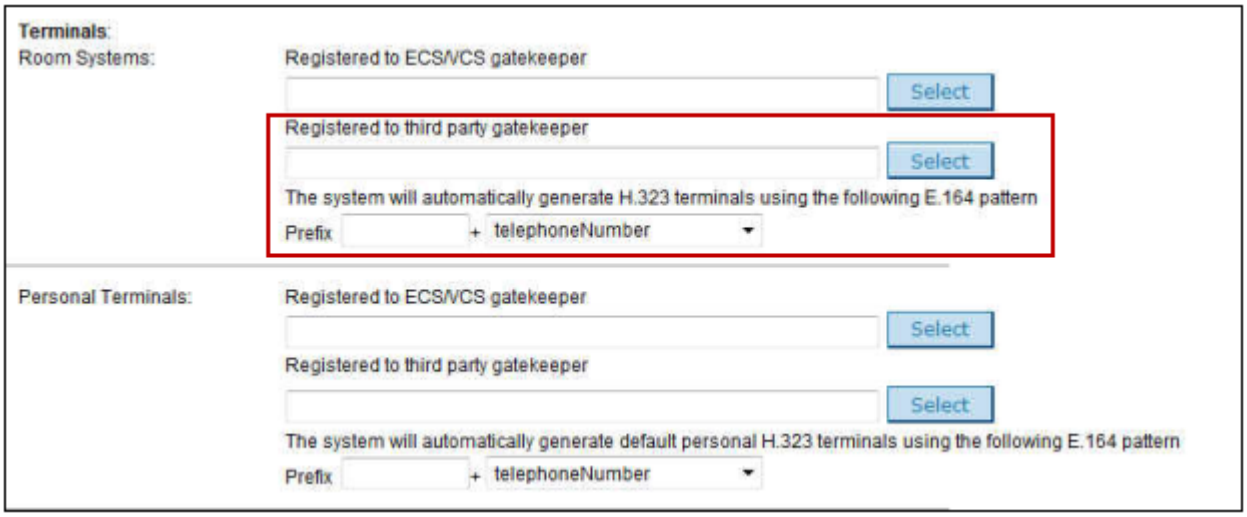


Table 3-1 Configuring settings in the Registered to third-party gatekeeper area

Field	Description
The **Select** button	Select the Active Directory user group to which you assigned the endpoints in the Meeting Rooms field.
The **Prefix** field	Enter a number that you want to use for a prefix. Use any number that is shorter than 11 digits and is not used as a prefix for the auto attendant or for other deployment components.
The **telephoneNumber** list	Verify that the telephoneNumber options is selected.

Step 8 Select **OK**.

Step 9 Select **Synchronize**.

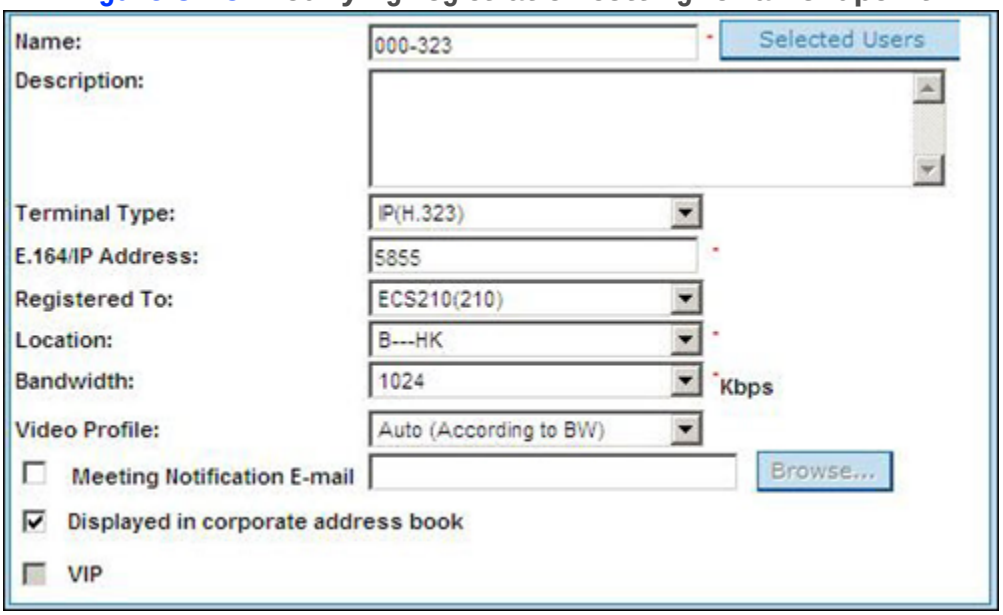
Step 10 Select **Resource Management** in the left pane.

Step 11 Select the **Terminals** tab.

Step 12 Select an endpoint that is registered to the third-party gatekeeper in the table.

The **Modify Terminal** page opens.

Figure 3-15 Modifying registration setting for an endpoint



Step 13 Select the third-party gatekeeper from the **Registered To** list.

Step 14 Select **OK**.

Step 15 Repeat Step 12 - Step 14 for all endpoints that are registered to the third-party gatekeeper.

Endpoints are predefined in the LDAP server and imported to iVIEW Management Suite as room systems and personal terminals.

Personal terminals are added to iVIEW Management Suite as default personal H.323 endpoints. Room systems can be registered to a RADVISION gatekeeper or to a third party gatekeeper.This section explains how to import endpoints registered to the SCOPIA Enhanced Communication Server. For information about importing endpoints registered to a third-party gatekeeper, see "Importing Endpoints Registered to a Third-Party Gatekeeper" on page 51.

In SCOPIA Video Gateway deployments the LDAP Server is your Active Directory Server.

During this procedure you define a prefix for endpoints you import. The prefix is part of the unified string that is defined by a dial plan and is added to the endpoint number. The prefix helps to route a call to a specific endpoint. Defining prefixes is optional.

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **Advanced Settings** in the sidebar.

Step 3 Select the **LDAP Configurations** tab.

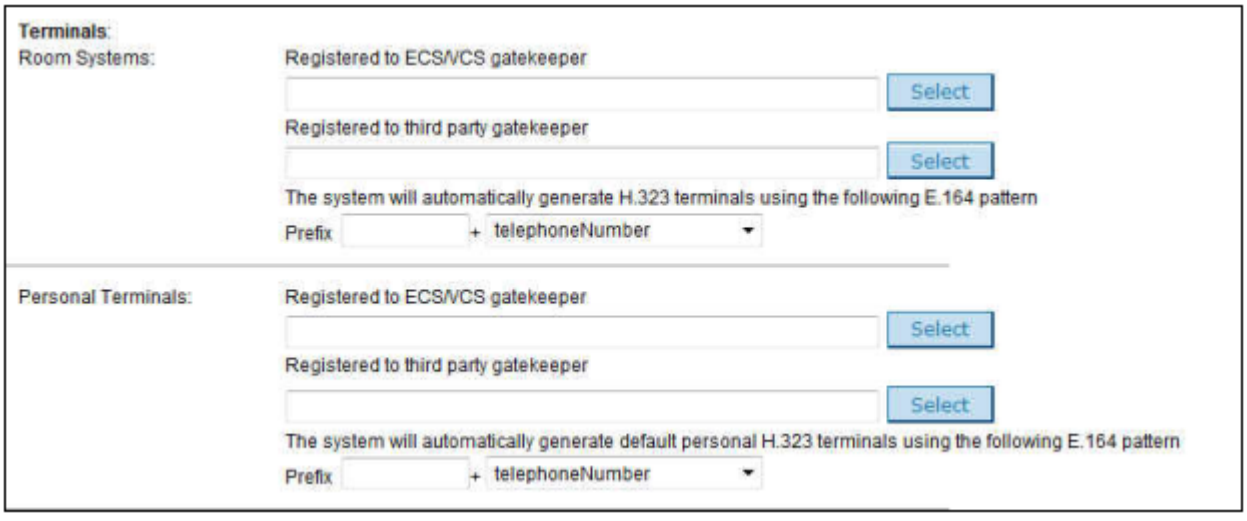
Step 4 Verify that you selected the LDAP server where the organization users were defined, including the defined **Users Search Base** and the **Terminals Search Base**.

For more information on configuring these settings, see the *Administrator Guide for SCOPIA iVIEW Management Suite*.

Step 5 Select **Advanced**. The **Advanced** section of the screen is displayed.

Step 6 Navigate to the **Terminals** section of the tab.

Figure 3-16 Terminals section of the LDAP Configurations tab



Step 7 Configure room systems in the Room Systems area of the Terminals section of the LDAP Configurations tab as described in Table 3-2.

Table 3-2 Configuring settings for downloading virtual meeting rooms and endpoints

Field	Description
The **Select** button	Select the Active Directory user group to which you assigned the room systems in the Meeting Rooms field. When configuring endpoints in a multi-tenant deployment, only select user groups belonging to the tenant that you are currently configuring.
The **Prefix** field	Enter a number that you want to use for a prefix. Use any number that is that is shorter than 11 digits and not used as a prefix for the auto attendant, auto routing, or for other deployment components. You cannot use the same prefix for personal virtual rooms and personal endpoints when configuring the same LDAP attribute (such as **telephoneNumber**). When configuring settings for virtual rooms, you do not need to enter a prefix. If you do enter a prefix for the virtual room, you can use any number not used as a prefix for the auto attendant, auto routing, personal endpoint, or for other deployment components.
The **telephoneNumber** list	Verify that the telephoneNumber options is selected.

Step 8 Configure personal endpoints in the Personal Terminals area of the Terminals section as described in Table 3-2.

Step 9 Define how often iVIEW Management Suite is synchronized with the LDAP server by selecting a value from the **Update Frequency** list.

Step 10 Select **OK**. The LDAP Configurations tab is displayed.

Step 11 Select **Synchronize**.

Endpoints defined in the LDAP server are downloaded and saved in the iVIEW Management Suite as room systems and personal endpoints.

Step 12 Verify that endpoints were downloaded correctly:

a. Select **Resource Management** in the sidebar.

b. Select the **Terminals** tab.

c. Verify that all endpoints defined in the LDAP server were downloaded and appear on the Terminals tab. The download icon is displayed next to all downloaded endpoints to differentiate endpoints from the LDAP server from endpoints added manually to the network.

Importing SIP/H.323/H.320 Endpoints using the H.350 Search Base

H.350 is a standard protocol to retrieve endpoints from an LDAP server.

You can define a schema with specific user parameters to be downloaded from the LDAP server to iVIEW Management Suite, for example, you can define the type of endpoint to be downloaded. The H.350 search base supports SIP, H.323 and H.320 endpoints. In addition, you can define new fields in the LDAP server to extend details, for example, you can define a schema to download endpoints with a specific video profile.

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **Advanced Settings**.

Step 3 Select **LDAP Configurations**.

Step 4 In the Terminals Search Base (H.350) section, select **Configure** to define the LDAP search base.

A tree structure is displayed showing all the users defined on the LDAP server.

Step 5 Select the relevant user groups you want to download.

Step 6 Select **OK**.

Step 7 (Optional) Select Secure User Credential at the bottom of the Advanced section.

Configuring your Endpoints to use iVIEW Management Suite as the LDAP Directory

You can manage the user directory of your endpoints using either an external LDAP server like SCOPIA iVIEW Management Suite or the local built-in LDAP server.

Use the following procedures to use SCOPIA iVIEW Management Suite as the LDAP directory for your endpoints:

- Configuring the SCOPIA XT Series to use iVIEW Management Suite as LDAP Directory page 56
- Configuring the SCOPIA VC240 to use iVIEW Management Suite as the LDAP Directory page 62
- Configuring Third-Party Endpoints to use iVIEW Management Suite as LDAP Directory page 66

Configuring the SCOPIA XT Series to use iVIEW Management Suite as LDAP Directory

You can manage the user directory of your XT Series using either an external LDAP server like SCOPIA iVIEW Management Suite or the local built-in LDAP server. You can configure the XT Series to use iVIEW Management Suite as the LDAP directory by configuring the LDAP settings in one of the following interfaces:

- XT Series endpoint
- XT Series web interface
- SCOPIA iVIEW Management Suite web interface

Typically your deployment would use iVIEW Management Suite as the external LDAP server which stores the contacts. A centralized solution like iVIEW Management Suite enables synchronizing the same list of contacts across all the endpoints in your organization, and has other benefits like remote centralized upgrading and backing up of all endpoints in your video network.

In deployments without iVIEW Management Suite, you can use the local built-in LDAP server that comes within every XT Series unit.

LDAP servers are accessed using the H.350 protocol, which enhances the LDAP standard to include video endpoint information.

Note: When using SCOPIA iVIEW Management Suite, associate LDAP contacts to video endpoints otherwise these contacts are not displayed on the XT Series.

Each LDAP contact on the XT Series can only be mapped to a maximum of ten video endpoints.

iVIEW Management Suite of version 7.5 or upgraded to version 7.6, it uses the objectClass=inetOrgPerson filter that causes all contacts to be loaded. In this case you need to change the filter manually as described in this procedure.

Note: New installations of iVIEW Management Suite version 7.6 do not use this filter.

Before You Begin

Make sure you know how to configure these parameters for your iVIEW Management Suite LDAP server:

- **Base** - the name of the root of the remote LDAP server tree.
- **Filter** - The phrase required to navigate the remote LDAP tree, which depends on the way the tree was structured. For example, if the LDAP tree is built from objects known as inetOrgPerson, the filter is `objectclass=inetOrgPerson`.
- **User** - The username and password for accessing information on the remote LDAP server. If you select XT Series as the remote server, you do no need to enter the username and password as they are already pre-defined in the server. For the iVIEW Management Suite or a third party LDAP server, refer to the system administrator for the username.
- When connecting to a third party LDAP server, the server administrator must verify that the video endpoint information is stored in the h323Identity and SIPidentity objects, according to the H.350 protocol.

Note: When the endpoint is under the management of iVIEW Management Suite, it sets parameters like the Gatekeeper address and the name of the LDAP server.

Procedure

Step 1 To configure the LDAP server via the XT Series endpoint:

a. In the XT Series **Administrator settings** menu, select **System**.

b. Scroll to **LDAP**.

c. Select the **General** page.

d. Choose whether to add, edit or remove the link to an LDAP server:

- To add a new link to iVIEW Management Suite or another remote LDAP server, press **Add server**.
- To modify parameters related to an existing link to a server, press **Modify server**.
- To delete a stored link to a server, press **Delete server**.

Note: The local LDAP server is embedded in the XT Codec Unit and cannot be deleted.

Figure 3-17 Adding a link to a remote LDAP server, in this case, another XT Series



e. Set the fields as required and press **Save**.

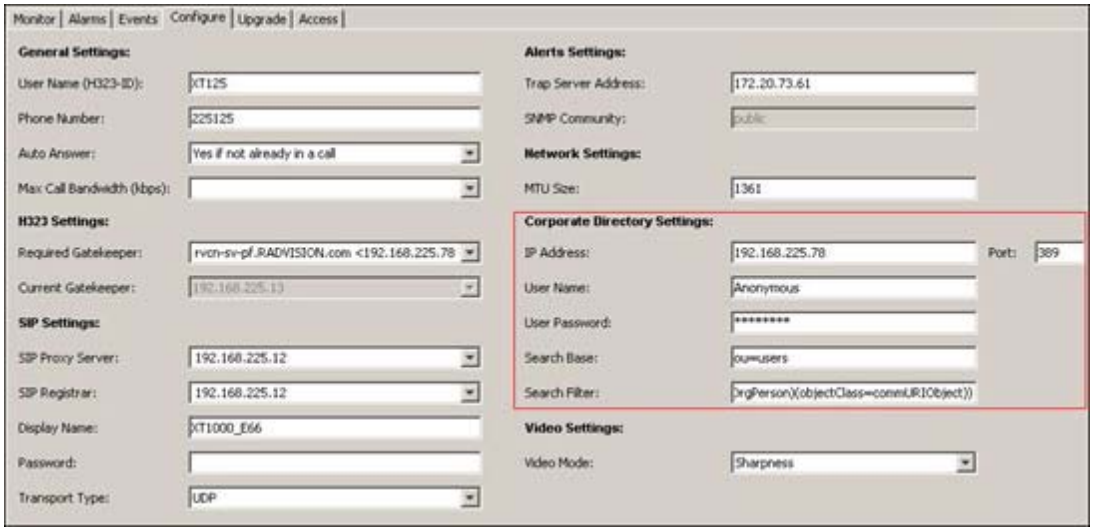
Table 3-3 Configuring LDAP server settings

Field Name	Description
Type	Allows to define the LDAP server.
Address	Indicates the LDAP server address.
Port	Indicates the port used to connect to the LDAP server.
User	The username and password with access to the information required in the remote LDAP server. The format of the username is in the form of a Distinguished Name (DN). The LDAP user of a XT Series is predefined, so when pointing to an XT Series this value cannot be edited. Some standard components of DN are: domain controller (dc), organizational unit (ou), common name (cn), country (c), state or province (st), locality (l), organization (o).
Password	The **User**'s password to authenticate with the server.
Base	The root of the LDAP tree where the contacts' records are defined. This value is predefined when the LDAP server is an XT Series.
Filter	The phrase required to navigate the remote LDAP tree, which depends on the way the tree was structured. For example, if the LDAP tree is built from objects known as inetOrgPerson, the filter would be `objectclass=inetOrgPerson`. This value is predefined when the LDAP server is an XT Series.

f. In deployments using iVIEW Management Suite version 7.5 or upgraded to version 7.6, do the following in the iVIEW Network Manager web interface:

1. Navigate to the endpoint in the network tree and select the **Configure** tab.

Figure 3-18 Corporate Directory Settings



2. Change the objectClass filter in the **Search filter** field of the **Corporate Directory Settings** area to (&(objectClass=inetOrgPerson)(objectClass=commURIObject)).

3. Select **Upload**.

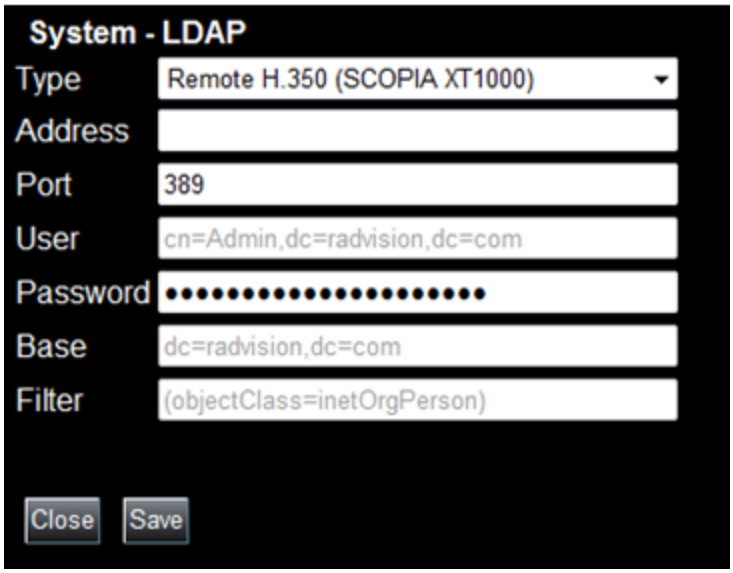
--Or--

Step 2 To configure the LDAP server via the XT Series web interface:

a. Access the XT Series web interface.

b. Select **Settings > System > LDAP**.

c. Select **Add Server**.



d. Configure LDAP server settings as described in Table 3-3.

e. Select **Save**.

f. In deployments using iVIEW Management Suite version 7.5 or upgraded to version 7.6, do the following in the iVIEW Network Manager web interface:

1. Navigate to the endpoint in the network tree and select the **Configure** tab (see Figure 3-18 on page 59).
2. Change the objectClass filter in the **Search filter** field of the **Corporate Directory Settings** area to (&(objectClass=inetOrgPerson)(objectClass=commURIObject)).
3. Select **Upload**.

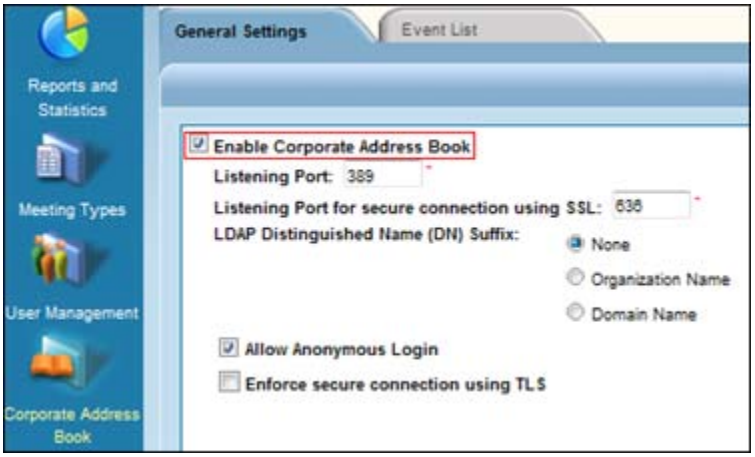
--Or--

Step 3 To configure the LDAP server settings via the SCOPIA iVIEW Management Suite web interface:

a. Access the iVIEW Communications Manager.

b. Select **Corporate Address Book** from the left-hand side.

Figure 3-19 Corporate Address Book Settings



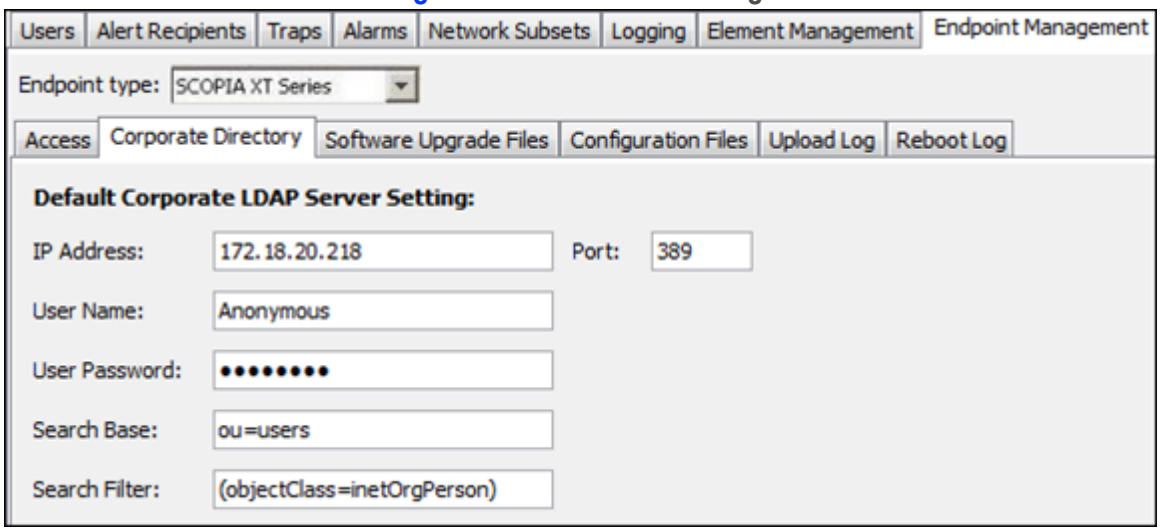
c. Select **Enable Corporate Address Book**.

d. Select **OK**.

e. Access the iVIEW Network Manager components of the iVIEW Management Suite.

f. Select **Setting > Endpoint Management > SCOPIA XT Series > Corporate Directory**.

Figure 3-20 LDAP Settings



g. Set the fields as described in Table 3-4.

Table 3-4 Configuring LDAP server settings

Field Name	Description
IP Address	Indicates the LDAP server address.
Port	Indicates the port used to connect to the LDAP server.
User Name	The username and password with access to the information required in the remote LDAP server. The format of the username is in the form of a Distinguished Name (DN). The LDAP user of a XT Series is predefined, so when pointing to an XT Series this value cannot be edited. Some standard components of DN are: domain controller (dc), organizational unit (ou), common name (cn), country (c), state or province (st), locality (l), organization (o).
Password	The **User**'s password to authenticate with the server.
Search Base	The root of the LDAP tree where the contacts' records are defined. This value is predefined when the LDAP server is an XT Series.
Search Filter	The phrase required to navigate the remote LDAP tree, which depends on the way the tree was structured. For example, if the LDAP tree is built from objects known as inetOrgPerson, the filter would be `objectclass=inetOrgPerson`. This value is predefined when the LDAP server is an XT Series.

h. In deployments using iVIEW Management Suite version 7.5 or upgraded to version 7.6, change the objectClass filter to (&(objectClass=inetOrgPerson)(objectClass=commURIObject)) in the **Search filter** field.

> Note: This prevents loading contacts which are not associated with video endpoints.

i. Select the **Upload** button.

Configuring the SCOPIA VC240 to use iVIEW Management Suite as the LDAP Directory

You can manage the user directory of your SCOPIA VC240 using either an external LDAP server like SCOPIA iVIEW Management Suite or the local built-in LDAP server.

Typically your deployment would use iVIEW Management Suite as the external LDAP server which stores the contacts. A centralized solution like iVIEW Management Suite enables synchronizing the same list of contacts across all the endpoints in your organization, and has other benefits like remote centralized upgrading and backing up of all endpoints in your video network.

In deployments without iVIEW Management Suite, you can use the local built-in LDAP server that comes with the unit.

LDAP servers are accessed using the H.350 protocol, which enhances the LDAP standard to include video endpoint information.

When using SCOPIA iVIEW Management Suite, associate LDAP contacts to video endpoints in order to display these contacts on the endpoint. Each LDAP contact on the SCOPIA VC240 can only be mapped to a maximum of ten video endpoints.

Note: iVIEW Management Suite of version 7.5 or version 7.5 upgraded to a higher version uses the **objectClass=inetOrgPerson** filter that causes all contacts to be loaded. In this case you need to change the filter manually as described in this procedure.

New installations of iVIEW Management Suite version 7.6 and higher do not use this filter.

Before You Begin

Make sure you know how to configure these parameters for your iVIEW Management Suite LDAP server:

- **Search Base** - the name of the root of the remote LDAP server tree.
- **Search Filter** - The phrase required to navigate the remote LDAP tree, which depends on the way the tree was structured. For example, if the LDAP tree is built from objects known as inetOrgPerson, the filter is `objectclass=inetOrgPerson`.
- **User** - The username and password for accessing information on the remote LDAP server. If you select SCOPIA VC240 as the remote server, you do no need to enter the username and password as they are already pre-defined in the server. For the iVIEW Management Suite or a third party LDAP server, refer to the system administrator for the username.
- When connecting to a third party LDAP server, the server administrator must verify that the video endpoint information is stored in the h323Identity and SIPidentity objects, according to the H.350 protocol.

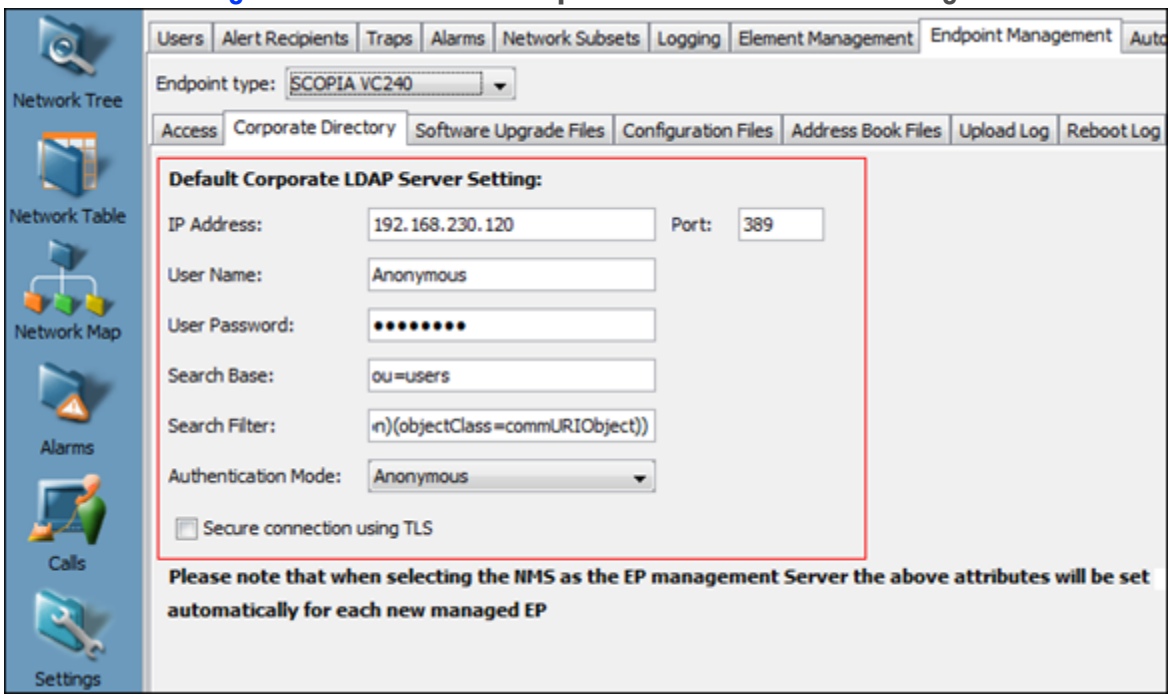
Note: When the endpoint is under the management of iVIEW Management Suite, it sets parameters like the Gatekeeper address and the name of the LDAP server.

Procedure

Step 1 Access the iVIEW Network Manager components of the iVIEW Management Suite.

Step 2 Select **Settings > Endpoint Management > SCOPIA VC240> Corporate Directory** (Figure 3-21 on page 64).

Figure 3-21 Default Corporate LDAP Server Settings



Step 3 Set the fields described in Table 3-5, as required.

Table 3-5 Configuring LDAP server settings

Field Name	Description
IP Address	Indicates the LDAP server address.
Port	Indicates the port used to connect to the LDAP server.
User Name	The username with access to the information required in the remote LDAP server. The format of the username is in the form of a Distinguished Name (DN). The LDAP user of a SCOPIA VC240 is predefined, so when pointing to an SCOPIA VC240. this value cannot be edited. Some standard components of DN are: domain controller (dc), organizational unit (ou), common name (cn), country (c), state or province (st), locality (l), organization (o).
User Password	The **User**'s password to authenticate with the server.
Search Base	The root of the LDAP tree where the contacts' records are defined. This value is predefined when the LDAP server is a SCOPIA VC240.
Search Filter	The phrase required to navigate the remote LDAP tree, which depends on the way the tree was structured. For example, if the LDAP tree is built from objects known as inetOrgPerson, the filter would be `objectclass=inetOrgPerson`. This value is predefined when the LDAP server is a SCOPIA VC240. Note: In deployments using iVIEW Management Suite version 7.5 or upgraded from 7.5 to a higher version, change the objectClass filter value to **(&(objectClass=inetOrgPerson)(objectClass=commURIObject))** in the **Search filter** field.
Authentication Mode	Select one of the following modes used to authenticate the SCOPIA VC240: • **Anonymous**: The SCOPIA VC240 connects with the following credentials: Username: Anonymous Password: password • **Basic**: The SCOPIA VC240 connects with the username and password selected by the administrator.

Note: To enable a secure connection via TLS, select the check box.

Step 4 Select the **Upload** button.

Use the settings detailed in this section to configure third-party endpoints to use iVIEW Management Suite as their LDAP server (H.350 protocol). This process synchronizes each endpoint's contacts list with the corporate address book. Configure the LDAP settings via the endpoint's web user interface.

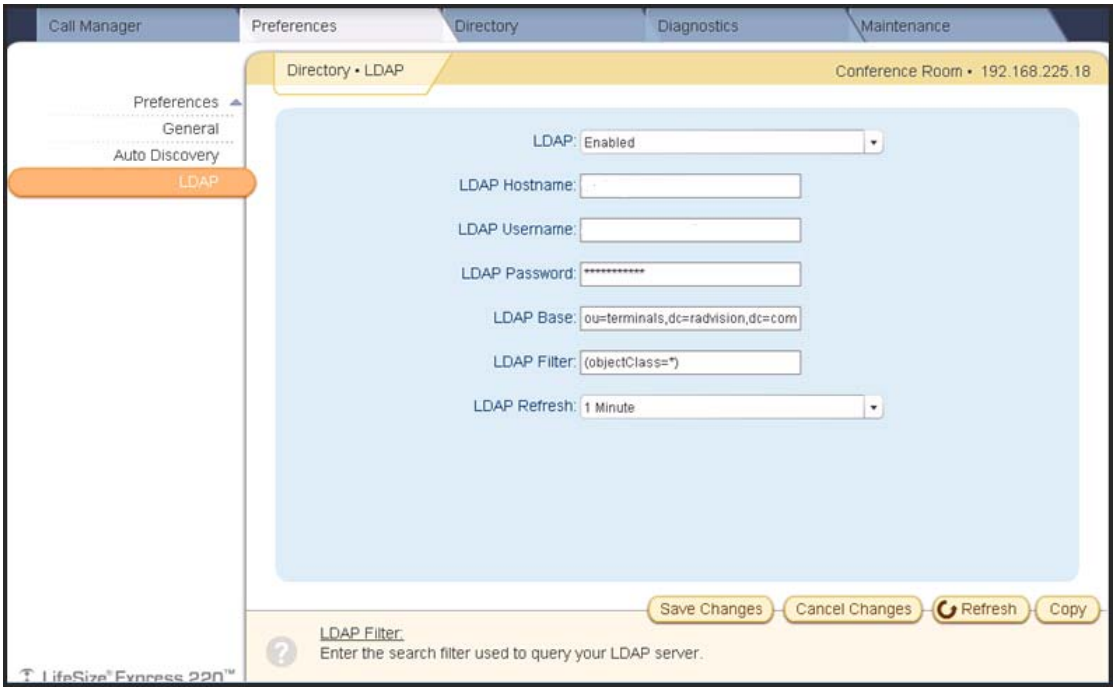
For LifeSize endpoints apply these settings (Figure 3-22 on page 67):

- **LDAP Enable**: This must be enabled.
- **LDAP Host name**: The iVIEW Management Suite address.
- **LDAP Username**: Set this field to the iVIEW Management Suite's user, or set this to anonymous.
- **LDAP Password**: Set to the user's password.
- **LDAP Base**: The data input in one of the fields is the suffix of the LDAP Distinguished Name of an entry supplied by the LDAP service. LifeSize searches the terminals by **ou=endpoints**.

  For example:

  - If iVIEW Management Suite configured the LDAP Distinguished Name (DN) Suffix as **None**, in LifeSize the Base DN should be **ou=endpoints**.
  - If iVIEW Management Suite configures the LDAP Distinguished Name (DN) Suffix as **mycompany** for the Organization Name, in LifeSize the Base DN would be: **ou=endpoints,o=mycompany**.
  - If iVIEW Management Suite configured the LDAP Distinguished Name (DN) Suffix as: **mycompany.com**, in LifeSize the Base DN would be: **ou=endpoints,dc=radvision,dc=com**.
- **LDAP Filter**: Set its value to **(objectClass=*)**.

Figure 3-22 LifeSize Endpoint Settings



Note: You can perform this configuration via iVIEW Network Manager by entering the LDAP settings in **Setting > Endpoint Management > Lifesize > Corporate Directory**.

For Polycom endpoints, apply these settings (Figure 3-23 on page 68):

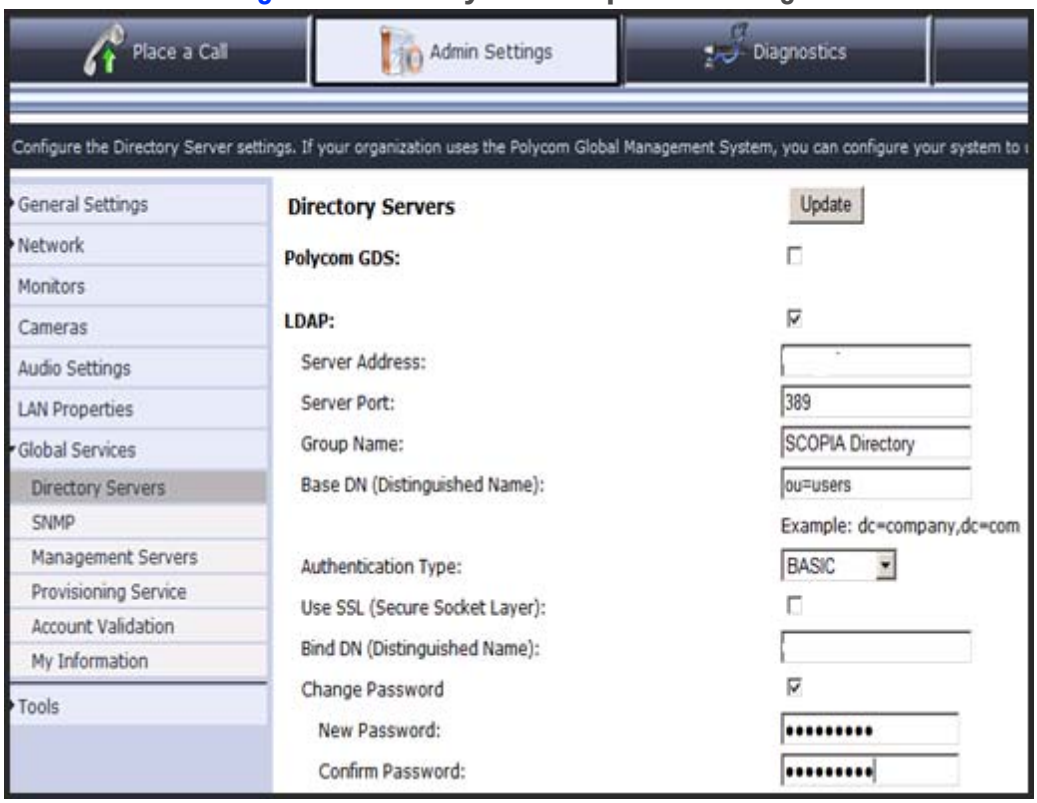
- **Server Address**: set to the iVIEW Management Suite server address.
- **Server Port**: It must be the same as the settings of iVIEW Management Suite. For example: 389.
- **Group Name**: Define a group name.
- **Base DN (Distinguished Name)**: The data input in one of the fields is the suffix of the LDAP Distinguished Name of an entry supplied by the LDAP service. Polycom must use the **ou=users** because Polycom endpoints access via the users to reach the endpoints.

  For example:

  - If iVIEW Management Suite configured the **LDAP Distinguished Name (DN) Suffix** as **None**, in Polycom the **Base DN** should be: **ou=users**.
  - If iVIEW Management Suite configured the **LDAP Distinguished Name (DN) Suffix** as **mycompany** for the Organization Name, in Polycom the Base DN should be **ou=users,o=mycompany**.
  - If iVIEW Management Suite configured the **LDAP Distinguished Name (DN) Suffix** as **mycompany.com** for the Domain Name, in Polycom the Base DN should be: **ou=users,dc=mycompany,dc=com**.
- **Authentication Type**: Define it as **Basic**.

- **Bind DN (Distinguished Name)**: Set it to iVIEW Management Suite's username.
- **Change Password**: set to your user's password.

Figure 3-23 Polycom Endpoint Settings



For Tandberg endpoints, apply these settings (Figure 3-24 on page 69):

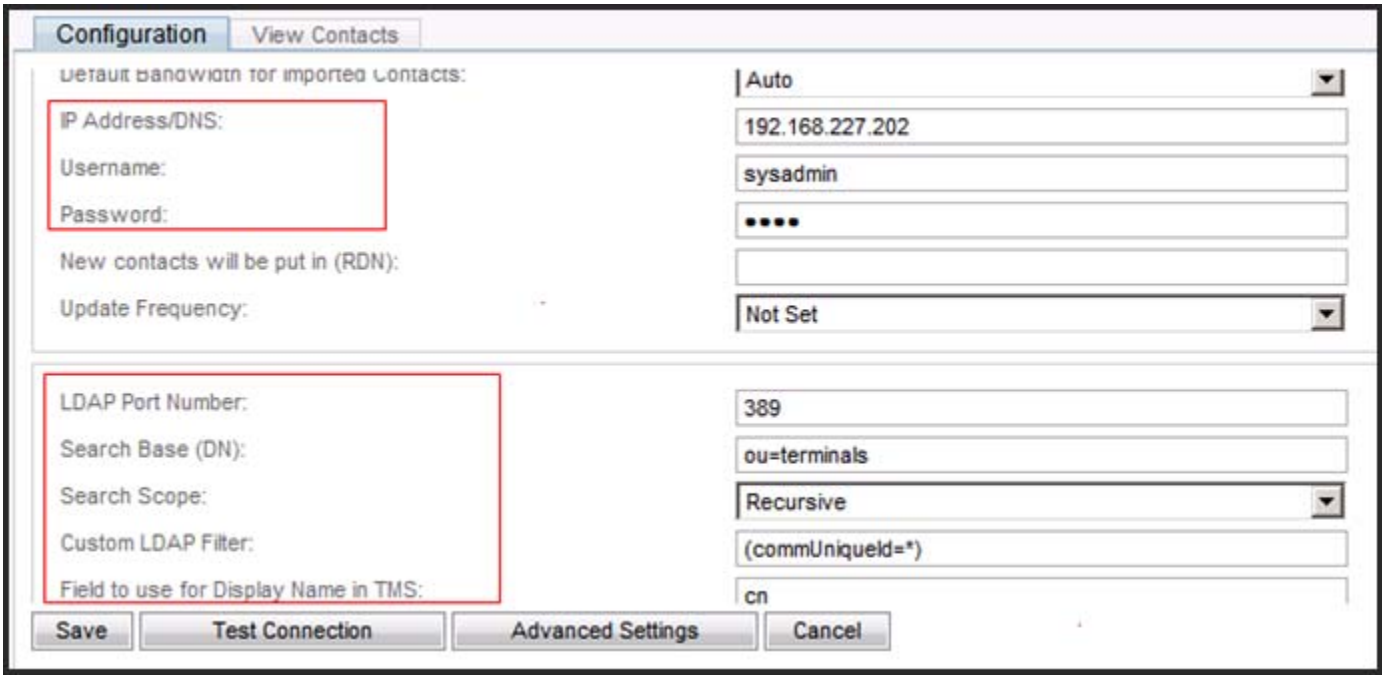
- **IP address/DNS**: Set this field to the iVIEW Management Suite's address.
- **Username**: Set this field to the iVIEW Management Suite's user.
- **Password**: Set to the user's password.
- **LDAP Port Number**: This must be the same as the settings for iVIEW Management Suite. For example, **389**.
- **LDAP Base**: The data input in one of the field will be the suffix of the LDAP Distinguished Name of an entry supplied by the LDAP service. Tandberg's TMS searches terminals by **ou=terminals**.

  For example:

  - If iVIEW Management Suite configured the LDAP Distinguished Name (DN) Suffix as **None**, in TMS the Base DN would be **ou=terminals**.
  - If iVIEW Management Suite configured the LDAP Distinguished Name (DN) Suffix as mycompany for the Organization Name, on the TMS side the Base DN would be **ou=terminals,o=mycompany**.
  - If iVIEW Management Suite configured the LDAP Distinguished Name (DN) Suffix as: mycompany.com, in the TMS the Base DN would be: **ou=terminals,dc=mycompany,dc=com**.

- **Custom LDAP Filter**: Enter the value **(commUniqueId=*)**.
- **Field to use for Display Name in TMS**: Enter the value **cn**.

Figure 3-24 Tandberg Endpoint Settings



Adding Endpoints in iVIEW Management Suite Manually

You can manually add H.323 IP, SIP, SIDN/PSTN H.320, Dual H.320/H.323 endpoints to iVIEW Management Suite. Endpoints must be added to both iVIEW Network Manager and iVIEW Communications Manager.

Procedure

Step 1 Log in to NMS.

Step 2 Select one of the network views (**Network Tree**, **Network Table** or **Network Map**) in the sidebar menu.

Step 3 Select the location in the network view at which you want to add the new element, and do one of the following to create a new element profile:

- Select **Add** > **New** > **New element**.
- Select **Add element** .

Step 4 Select **Endpoint** from the element type list and enter the element name and the management IP address.

Step 5 Select the Endpoint type and the Gatekeeper IP address to which the endpoint will be registered to.

Step 6 (Optional) Select **Set iVIEW-NMS as the default trap server** to use the NMS as the SNMP trap server for endpoint elements.

Step 7 Select **OK** to add the endpoint to NMS.

Step 8 Log in to iVIEW Communications Manager.

To add H.323 IP endpoints, see "Adding H.323 IP Endpoints" on page 70.

To add SIP IP endpoints, see Adding SIP IP Endpoints page 71.

To add ISDN/PSTN H.320 endpoints, see "Adding ISDN/PSTN H.320 Endpoints" on page 72.

To add mobile endpoints, see "Adding Mobile Endpoints" on page 73.
To add dual H.320/H.323 endpoints, see "Adding Dual H.320 and H.323 Endpoints" on page 73.

Adding H.323 IP Endpoints

Define all H.323 endpoints registered to gatekeepers that are configured in iVIEW Communications Manager.

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **Resource Management** in the sidebar menu.

Step 3 Select **Terminals**.

Step 4 Select **Add** to create a new endpoint profile.

Step 5 (Optional) Select **Selected Users** to associate this endpoint as the default endpoint for selected users defined in iVIEW Communications Manager.

Step 6 Select **OK** to apply your selections and to close the **Select Users** window.

Step 7 (Optional) Enter any description text that you may have for this endpoint in the **Description** field.

Step 8 Select **IP(H.323)** from the **Terminal Type** list.

Step 9 Enter the E.164 IP phone number of the endpoint registered on the gatekeeper in the IP Phone Number field as specified in the **Registered to** field.

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

Step 10 Select the office or branch from the **Location** list, to which the endpoint will be part of.

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

Step 11 Define the default bandwidth for the endpoint by selecting bandwidth settings in the **Video Profile** list. iVIEW Communications Manager uses the bandwidth number to reserve resources for this endpoint.

Step 12 (Optional) Select an entry from the Meeting Room field to associate this endpoint with a meeting room defined in iVIEW Management Suite.

Step 13 (Optional) Select **Display in global address book**.

Step 14 (Optional) Select **VIP** to indicate that this is an important endpoint whose video resolution should not be scaled down to below HD quality even when the available effective bandwidth is less than optimal.

This option is only available when the effective available bandwidth is above 1800 Kbps.

Step 15 Select **OK** to save your changes.

Adding SIP IP Endpoints

Define all SIP endpoints registered to gatekeepers that are configured in iVIEW Communications Manager.

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **Resource Management** in the sidebar menu.

Step 3 Select **Terminals**.

Step 4 Select **Add** to create a new endpoint profile.

Step 5 (Optional) Select **Default Users** to associate this endpoint as the default endpoint for selected users defined in iVIEW Communications Manager.

Step 6 Select **OK** to apply your selections and to close the **Select Users** window.

Step 7 (Optional) Enter any description text that you may have for this endpoint in the **Description** field.

Step 8 Select **IP(SIP)** from the **Terminal Type** list.

Step 9 Define the endpoint name or endpoint 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”.

Step 10 Define the default bandwidth for the endpoint by selecting bandwidth settings in the **Video Profile** list. iVIEW Communications Manager uses the bandwidth number to reserve resources for this endpoint.

Step 11 Select a topology setting from the **Location** list.

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

Step 12 (Optional) Select **Display in global address book**.

Step 13 (Optional) Select **VIP** to indicate that this is an important endpoint whose video resolution should not be scaled down to below HD quality even when the available effective bandwidth is less than optimal.

This option is only available when the effective available bandwidth is above 1800 Kbps.

Step 14 Select **OK** to save your changes.

Adding ISDN/PSTN H.320 Endpoints

Define all H.320 endpoints that you want iVIEW Communications Manager to automatically invite to a meeting and manage their availability.

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **Resource Management** in the sidebar menu.

Step 3 Select **Terminals**.

Step 4 Select **Add** to create a new endpoint profile.

Step 5 (Optional) Select **Default Users** to associate this endpoint as the default endpoint for selected users defined in iVIEW Communications Manager.

Step 6 Select **OK** to apply your selections and to close the **Select Users** window.

Step 7 (Optional) Enter any description text that you may have for this endpoint in the **Description** field.

Step 8 Select **ISDN/PSDN(H.320)** from the **Terminal Type** list.

Step 9 Define the default bandwidth for the endpoint in the **Bandwidth** field. iVIEW Communications Manager uses the bandwidth number to reserve resources for this endpoint.

Step 10 Select **Restricted Mode** for a PSTN/ISDN network working in restricted mode.

Step 11 Enter the phone number of the terminal in the Country Code, Area Code and Number fields.

If you do not specify this information, iVIEW Communications Manager cannot find the optimal gateway for the endpoint when scheduling a conference.

Step 12 (Optional) Select **Display in global address book**.

Step 13 Select **OK** to save your changes.

Adding Mobile Endpoints

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

Procedure

Step 1 Log in iVIEW Communications Manager.

Step 2 Select **Resource Management** in the sidebar menu.

Step 3 Select **Terminals**.

Step 4 Select **Add** to create a new terminal profile.

Step 5 (Optional) Select **Default Users** to associate this terminal as the default terminal for selected users defined in iVIEW Communications Manager.

Step 6 Select **OK** to apply your selections and to close the Select Users window.

Step 7 (Optional) Enter any description text that you may have for this terminal in the Description field.

Step 8 Select **Mobile** from the Terminal Type list.

Step 9 Define the default bandwidth for the terminal in the Bandwidth field. iVIEW Communications Manager uses the bandwidth number to reserve resources for this terminal.

Step 10 Enter the phone number of the terminal in the Country Code, Area Code and Number fields.

If you do not specify this information, iVIEW Communications Manager cannot find the optimal gateway for the terminal when scheduling a conference.

Step 11 Select **3G** for 3G terminals.

Step 12 (Optional) Select **Display in global address book**.

Step 13 Select **OK** to save your changes.

Adding Dual H.320 and H.323 Endpoints

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **Resource Management** in the sidebar menu.

Step 3 Select **Terminals**.

Step 4 Select **Add** to create a new endpoint profile.

Step 5 (Optional) Select **Default Users** to associate this endpoint as the default endpoint for selected users defined in iVIEW Communications Manager.

Step 6 Select **OK** to apply your selections and to close the **Select Users** window.

Step 7 (Optional) Enter any description text that you may have for this endpoint in the Description field.

Step 8 Select **Dual (H.320 and H.323)** from the **Terminal Type** list.

Step 9 Enter the E.164 IP phone number of the endpoint registered on the gatekeeper in the IP Phone Number field as specified in the **Registered to** field.

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

Step 10 Define the default bandwidth for the endpoint in the **IP Bandwidth** and **ISDN Bandwidth** fields. iVIEW Communications Manager uses the bandwidth number to reserve resources for this endpoint.

Step 11 Select a topology setting from the **Location** list.

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

Step 12 Select **Restricted Mode** for a PSTN/ISDN network working in restricted mode.

Step 13 Select one of the following resolutions for video displayed on this endpoint in the **Video Profile** list:

- **Auto (According to BW)**: If there is enough bandwidth available, video is displayed in the highest resolution the endpoint is capable of.
- **Standard Definition**: Video is displayed in a resolution of 352p.

Step 14 Enter the phone number of the ISDN endpoint in the **Country Code**, **Area Code** and **Number** fields.

If you do not specify this information, iVIEW Communications Manager cannot find the optimal gateway for the endpoint when scheduling a conference.

Step 15 (Optional) Select **Display in global address book**.

Step 16 (Optional) Select **VIP** to provide enhanced quality video to this endpoint.

Step 17 Select **OK** to save your changes.

Setting the Managed Status of Endpoints

You can configure iVIEW Management Suite to manage all endpoints registered to a gatekeeper, or, you can manually set endpoints to be managed by iVIEW Management Suite. Managed endpoints communicate with iVIEW Management Suite to provide events and alarms management.

Procedure

Step 1 Log in to iVIEW Network Manager.

Step 2 Select **Settings**.

Step 3 Select **Endpoint Management**.

Step 4 Select the endpoint type from the list, and select **Access**.

Step 5 Enter a username and password, and check the **Automatically manage EPs which are registered to a managed GK**.

Step 6 To manually set the status of an endpoint to managed, select the **Network Tree** in the sidebar menu.

Step 7 Click **Endpoints**.

Step 8 Right-click the endpoint you require in the Endpoints tab.

Step 9 Select **Manage**.

Removing Endpoints

Endpoints should be removed from the iVIEW Network Manager only. In iVIEW Communications Manager, endpoints are downloaded from the gatekeeper, or, when your organization synchronizes with an LDAP server, endpoints are downloaded from the LDAP server, therefore, endpoints should be removed from the gatekeeper itself or from the LDAP server.

Procedure

Step 1 Log in to iVIEW Network Manager.

Step 2 Open the network tree from the sidebar.

Step 3 Select **Endpoints**.

Step 4 Select the endpoint entry you want to delete.

Step 5 Select the **Delete** icon  and then **Yes**.
The endpoint profile is deleted from the scheduler and information about the endpoint is removed from the database.

Searching for an Endpoint

You can search for a specific endpoint and modify some settings, such as maximum bandwidth, video profile, location, etc.

Procedure

Step 1 Log in to iCM.

Step 2 Select **Resource Management** in the sidebar menu.

Step 3 Select **Terminals**.

Step 4 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.

Step 5 (Optional) Select **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 indicted by a book icon after the terminal name.

Step 6 (Optional) Select **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 indicted by a book icon after the terminal name.

Step 7 Select **Search**.

Search results are listed.

Step 8 To return to the complete list of meeting rooms, clear the Name and Dialing Info fields, and then select **Search**.

Managing Endpoints Configuration Upload History

This section applies to Polycom, Tandberg, SCOPIA VC240, SCOPIA XT Series and Sony endpoints only. You can view, upload or remove entries from the upload log.

Procedure

Step 1 Log in to iVIEW Network Manager.

Step 2 Click **Settings** in the sidebar menu.

Step 3 Click **Endpoint Management**.

Step 4 Click **Upload Log**.

Step 5 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.

Adding a Lync Server or OCS Profile in iVIEW Management Suite

Microsoft's Lync Server and OCS Server are SIP devices. iVIEW Management Suite 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 iVIEW Communications Manager.

You can view the connection status between iVIEW Management Suite and your Lync Server or OCS by navigating to the **Gatekeeper/SIP server/Presence server** tab, located in **Resource Management**.

To enable iVIEW Management Suite to operate with SIP endpoints, configure iVIEW Communications Manager with an external SIP server to which SIP endpoints are registered.

iVIEW Communications Manager is interoperable with these external SIP servers:

- Microsoft Lync Server 2010
- Microsoft Office Communications Server 2007 R2
- Microsoft Lync Server 2010 Hosting Pack
- Broadsoft IPCentrix

Procedure

Step 1 Log into the iVIEW Communications Manager.

Step 2 Select **Resource Management** in the sidebar.

Step 3 Select **Gatekeeper/SIP server/Presence server**.

The **Gatekeeper/SIP server/Presence server** tab opens.

Step 4 Select **Add** to create a new SIP server profile.

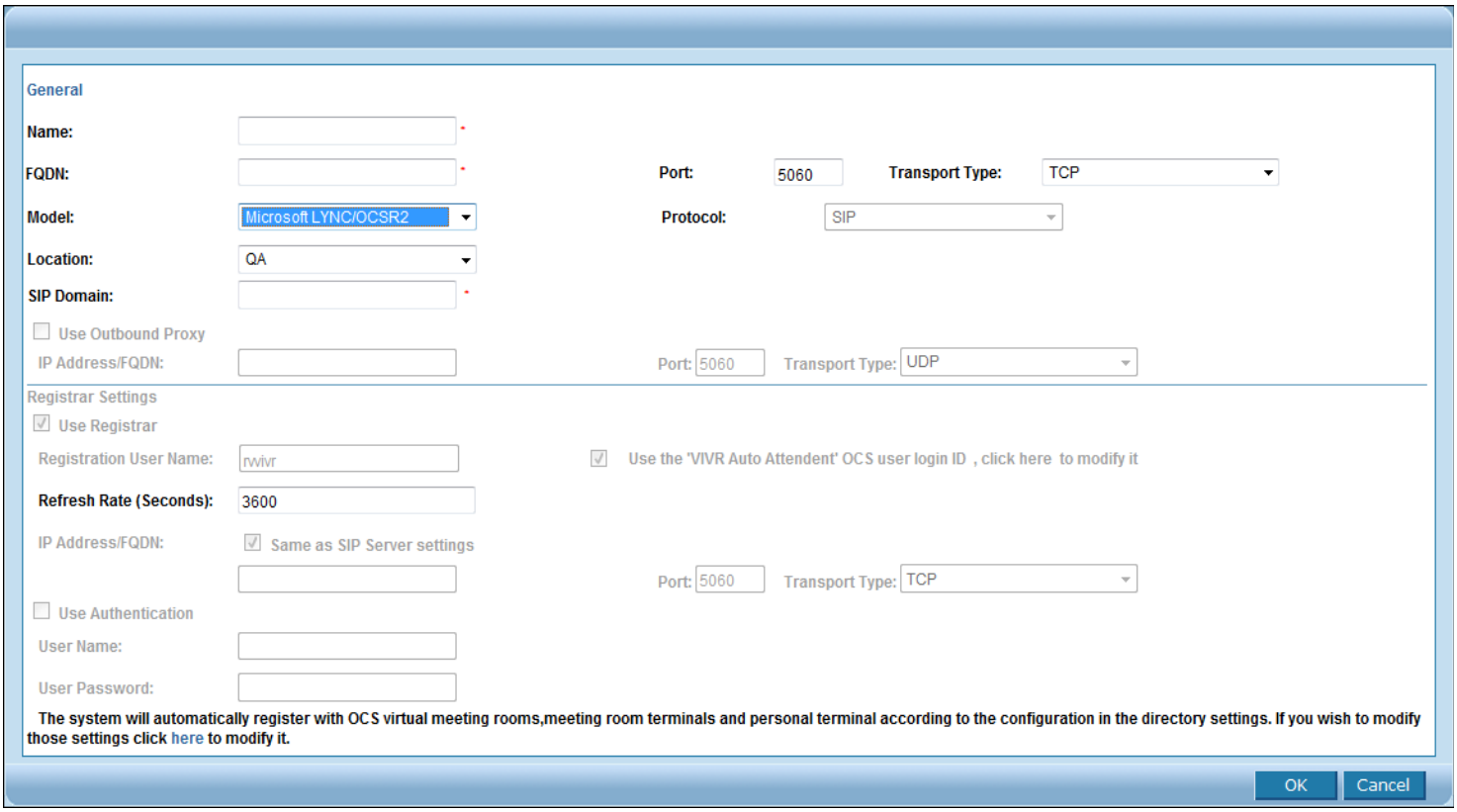
The **New Gatekeeper/SIP server/Presence server** window opens.

Step 5 Configure these settings:

Field	Description
Name	Enter the name of the server. We recommend that you use the IP address as the name unless the selected model is a Microsoft LYNC/OCSR2 server; in this case, used the server FQDN as the name.
Model	Select the relevant model of the SIP server depending on your deployment. If you select **Other**, select SIP in the Protocol list.
FQDN	If you select Microsoft LYNC/OCSR2 in the Model list, enter the Lync Server or OCS FQDN which iVIEW Communications Manager can resolve. Depending on the deployment, you might need to enter the FQDN of the Director Server. See from Step 8 to configure support of the Director Server.
Transport Type	Set this value to **TCP** or **TLS**.
Port	Enter a value for port. The default value is 5060 for a TCP port and 5061 for a TLS port.

Field	Description
Protocol	Select **SIP** from the list if you selected **Other** from the Model list.
Location	In distributed deployments select the office or branch to which the SIP server is registered. Each office or branch can have only one SIP server.
SIP Domain	Enter the Lync Server's default SIP domain.

Figure 3-25 Configuring settings for the Lync Server or OCS



Step 6 (Optional) Enter the name of a preferred and an alternative DNS server in the relevant fields.

Step 7 Select **OK** to save your changes.

Step 8 If you need to configure support for the Director Server per your deployment requirements, stop the iVIEW Management Suite service and the iVIEW Management Suite SIP service.

Step 9 Navigate to C:\Program Files\RADVISION\iVIEW Suite\iCM\jboss\bin.

Step 10 Open the **vcs-core.properties** file in a text editor.

Step 11 Verify that the parameter `vnex.vcms.core.ucgw.check.viaHeaders;` is set to `true`.

Step 12 Save and close the file.

Step 13 Restart the iVIEW Management Suite and iVIEW Management Suite SIP services.

Enabling Remote Access to GUI of Video Network Devices

Only administrators can configure remote access parameters.

You can configure default information for all devices of a specific type, and, you can define remote access information for a specific device. When configuring remote access for a specific device, these information overrides the default parameters configured for all devices of this type.

This section explains how to configure remote access information for network devices configured in the network.

- Configuring Remote Access to Network Devices and Endpoints ..... page 79
- Configuring Remote Access to GUI of SCOPIA PathFinder ..... page 80
- Defining Specific Information for Remote Access of Network Devices ..... page 81

Configuring Remote Access to Network Devices and Endpoints

Default access settings allow connection to a network device (or a network endpoint) for monitoring and configuration without having to first go through the login window for that device or endpoint.

Note: You can override default access settings by defining specific access information for network devices. See "Defining Specific Information for Remote Access of Network Devices" on page 81 for details.

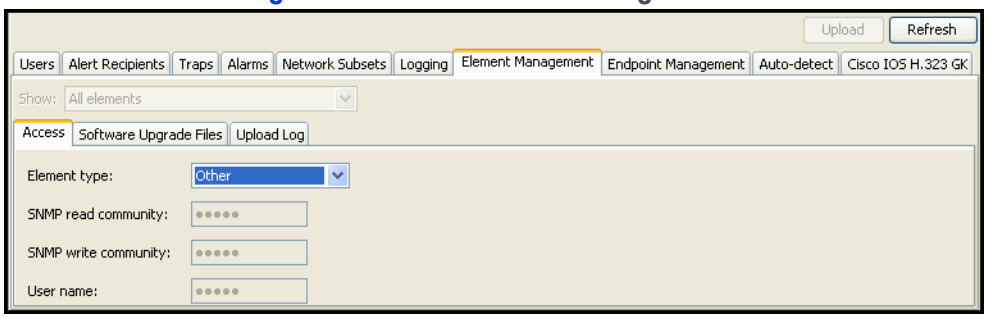
Procedure

Step 1 Log in to NMS.

Step 2 Select **Settings** in the sidebar menu.

Step 3 Select **Element Management** (for managing elements) or **Endpoint Management** (for managing endpoints).

Figure 3-26 Element Management



Step 4 For element management, select the **Access** tab.

-or-

For endpoint management select **Endpoint Type**.

Step 5 For element management, select an **Element Type**.

-or-

For endpoint management, select the **Access** tab.

Step 6 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.

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 SCOPIA iVIEW Network Manager to retrieve information from the element.

Step 7 Select **Upload** to save the information to the SCOPIA iVIEW Network Manager database.

Configuring Remote Access to GUI of SCOPIA PathFinder

Default access settings allow connecting to a SCOPIA PathFinder Server for monitoring and configuration without having to first go through the login window.

Procedure

Step 1 Log in to NMS.

Step 2 Select **Network Tree** in the sidebar menu.

Step 3 Select the required SCOPIA PathFinder Server element.

Step 4 Select **Access**.

Step 5 Enter a collaborator user name and password in the relevant fields.

This is the user account with which iVIEW Network Manager connects to the SCOPIA PathFinder Server. It should match the account details of a user defined on the SCOPIA PathFinder Server with the collaborator user type.

Default values are Collab and balloC respectively.

Step 6 Enter an SFTP user name and password in the relevant fields.

This is the user account with which iVIEW Network Manager connects to the SCOPIA PathFinder Server to download logs.

Default values are uadmin and admin respectively.

Step 7 Enter the SFTP port number.

The default value is 22.

Step 8 Enter an HTTP user name and password in the relevant fields.

This is the user account with which iVIEW Network Manager accesses the SCOPIA PathFinder Server web user interface.

Default values are admin and admin respectively.

Step 9 Enter the web server service port number of the SCOPIA PathFinder Server in the HTTP Port field.

The default value is 8080.

Step 10 Enter an SSH user name and password in the relevant fields.

This is the user account with which iVIEW Network Manager connects to the SCOPIA PathFinder Server platform.

Default values are admin and admin respectively.

Step 11 Select **Upload** to save the information to the SCOPIA iVIEW Network Manager database.

Defining Specific Information for Remote Access of Network Devices

You can define specific access information for network devices. Once these information is defined, all default settings are override with these new settings.

Procedure

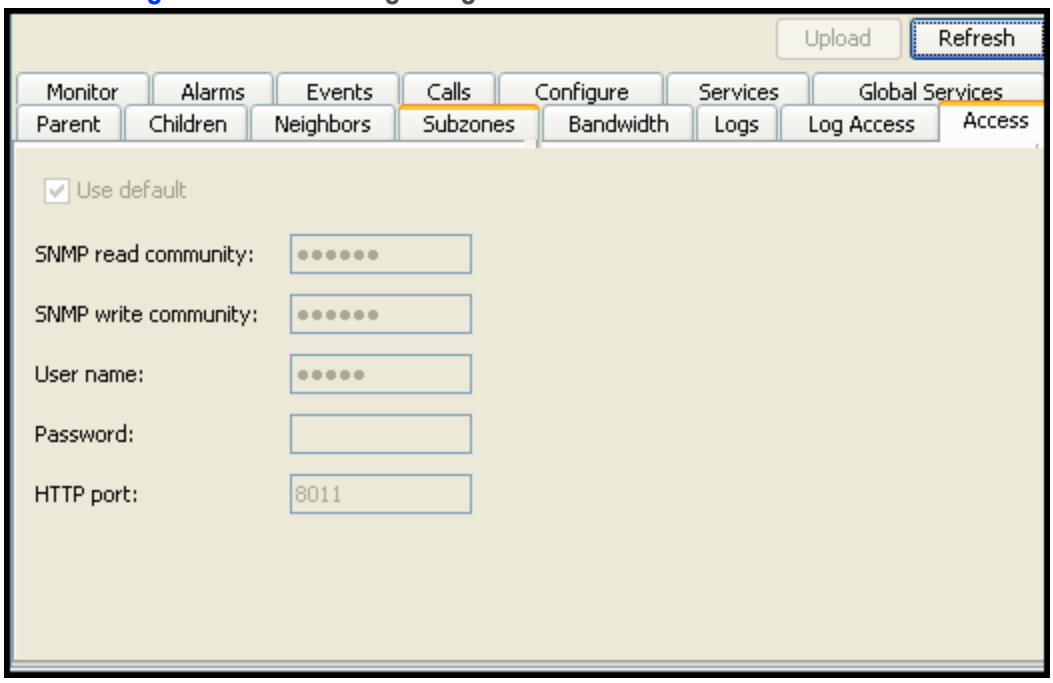
Step 1 Log in to NMS.

Step 2 Select **Network Tree** in the sidebar menu.

Step 3 Select the required network device in the network tree.

Step 4 Select **Access**.

Figure 3-27 Configuring network device remote access



Step 5 Select **Use default** to use the default access settings for the device type.

When deselected, all other parameters are enabled.

Availability of the following access configuration parameters depends on the device type selected.

Step 6 Configure the following parameters:

- SNMP read community
- SNMP write community
- User name
- Password
- HTTP port

SNMP community information must match the settings defined in the selected device to enable SCOPIA iVIEW Network Manager to connect with the device.

Planning and Configuring Telepresence in iVIEW Management Suite

With the new Telepresence Interoperability support, iVIEW Management Suite can establish connections with third party telepresence systems from Cisco, Logitech/LifeSize, Polycom and Tandberg, allowing telepresence users to view all meeting participants in a mulit-party call, including those on traditional videoconferencing systems or telepresence systems from other vendors.

The concepts described in the following sections relate to the different telepresence endpoints as a single unified endpoint.

- Understanding Telepresence Systems ..... page 82
- Managing Telepresence in iVIEW Management Suite ..... page 83
- Configuring Telepresence Endpoints ..... page 83
- Calculating Resources for Telepresence ..... page 85
- Scheduling Telepresence Systems ..... page 85

Understanding Telepresence Systems

The SCOPIA MCU and iVIEW Management Suite support the following telepresence (TP) systemsiVIEW Management Suite:

- SCOPIA XT Telepresence
- Polycom ATX 300
- Polycom RPX 200
- Polycom RPX 400
- Polycom TPX HD 306
- Tandberg T3
- LifeSize Conference

- Cisco Telepresence
- Generic (other telepresence endpoints that have 3 screens)

iVIEW Management Suite does not require any specific license for supporting telepresence but is aware of the SCOPIA MCU telepresence license in order to deliver warning messages to administrators and for display purposes.

The MCU Resource Tab displays a small telepresence icon near the MCU which are licensed for telepresence support.

Managing Telepresence in iVIEW Management Suite

Telepresence is managed by iVIEW Management Suite according to the network deployment:

- In mixed deployments with both telepresence enabled MCUs and telepresence disabled MCUs, iVIEW Management Suite chooses the MCU host according to the end point specifications.
- In centralized deployments with telepresence Meetings, iVIEW Management Suite will choose a telepresence enabled MCU. For centralized deployments with Non telepresence Meetings, iVIEW Management Suite gives preference to a MCU with no telepresence support. If there are no resources on the non telepresence MCU, it will use a telepresence enabled MCU.
- In distributed deployments with telepresence Meetings, iVIEW Management Suite chooses a telepresence enabled MCU according to the best location. For distributed deployments in non telepresence Meetings, iVIEW Management Suite chooses the best MCU according to location even if the MCU is telepresence enabled; Location has higher priority than telepresence preference.

Configuring Telepresence Endpoints

Endpoints can be manually configured to support telepresence or, when using an LDAP server, endpoints can be pre-configured in the LDAP server to support telepresence.

Endpoints that support telepresence are displayed in the Terminal tab with a telepresence icon .

When configuring telepresence, note the following restrictions and guidelines:

- Telepresence will be supported only for IP endpoints.
- Telepresence will be supported only for a bandwidth which is higher than 768Kbps.
- Video profiles will be grayed out and set to auto.
- Personal Terminal support – The telepresence endpoint will not be associated with any specific user. The **Choose Participant** option will be hidden.
- The administrator will not be able to associate the telepresence endpoint with a specific user.
- Administrators will not be able to change a defined endpoint into a telepresence endpoint, and vice versa. To do so, you must delete and redefine the endpoints again.
- The VIP option will unchecked and grayed out for any telepresence endpoints.

- If there is a collision with another defined endpoint, the system will pop up the appropriate error message.
- The telepresence will always be connected to the Master conference since we can only send a single video steam from the master to the slave.

Procedure

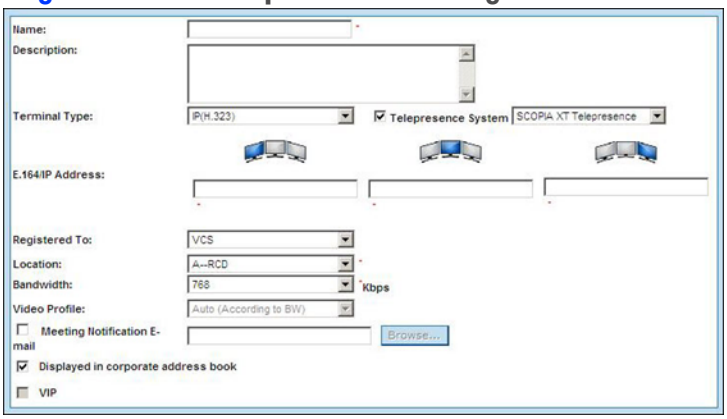
Step 1 Log in to iCM.

Step 2 Select **Resource Management** in the sidebar menu.

Step 3 Select **Terminals**.

Step 4 Select **Add**.

Figure 3-28 Telepresence Configuration Screen



Step 5 Insert a **Name** and **Description** (optional).

Step 6 Select the type of endpoint from the **Terminal Type** list.

Step 7 Select the **Telepresence System** check box.

Step 8 Select the telepresence system from the **Telepresence System** list.

Note: If your telepresence endpoint is not listed and has three screens, select **Generic**.

Step 9 Enter up to four E.164 phone numbers or IP addresses, depending on the system.

Step 10 Select the gatekeeper the telepresence endpoint is registered to in the **Registered to** field.

Step 11 Select the office or branch from the **Location** list, to which the endpoint will be part of.

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

Step 12 Define the default bandwidth for the endpoint in the **Bandwidth** field. iCM uses the bandwidth number to reserve resources for this endpoint.

Step 13 (Optional) To send a telepresence system user an email when the telepresence endpoint joins, leaves, or is disconnected from a meeting, select **Meeting Notification E-mail**, and then browse to the email text you would like to use.

Step 14 (Optional) Select **Display in corporate address book**. The telepresence endpoint will be represented in the address book as a single endpoint. The number which the system displays will be the number assigned to the primary endpoint. This relates to all the interfaces including:

- iVIEW Management Suite
- SCOPIA Desktop
- Lotus Notes Plug-in
- Outlook Plug-in
- Room Systems via H.350

Step 15 Select **OK**.
Once configured, the Terminal Resource tab displays a small icon near the endpoint name, indicating that the endpoint is a telepresence system, as well as dialing info numbers with relevant prefixes.

Calculating Resources for Telepresence

Resources are calculated according to the number of supported screens.

For example: For scheduled telepresence endpoints which have two screens, iVIEW Management Suite calculates 2 HD ports. For scheduled telepresence end points which have four screens, iVIEW Management Suite calculates 4 HD ports.

If a telepresence system is dialing into the system (which can be done from each one of the pre-configured numbers), iVIEW Management Suite attempts to allocate the total number of ports on the master conference, and if managed to do so, it will authorize to connect the call.

Scheduling Telepresence Systems

When scheduling a telepresence system, the following restrictions apply:

- Enabled telepresence MCU must be selected.
- Telepresence must be scheduled to the master conference.
- Pre-positioning the telepresence endpoint in a specific sub frame will not be supported for the telepresence endpoint.

Configuring iVIEW Management Suite redundancy

The iVIEW Management Suite redundant solution is based on two iVIEW Management Suite servers which act as a master/slave hot swap mechanism. The redundant solution supports an internal gatekeeper and an internal database.

- Configuring Redundancy Mode ..... page 86
- Monitoring Redundancy Status ..... page 90
- Disabling Redundancy Mode ..... page 90

Configuring Redundancy Mode

Before You Begin

- For an existing redundant deployment, verify that iVIEW Management Suite is installed on an additional server.
- For a new redundant deployment, verify that iVIEW Management Suite products are installed on two separate servers.
- Verify that two Microsoft SQL databases are installed and configured to work in the Mirror failover mode.
- For servers running Windows Server 2008, install WinPcap version 4.1.2 to enable the network switch update its cache when a failover occurs. To download, see http://www.winpcap.org/install/default.htm.
- Decide which iVIEW Management Suite server will act as a master in the deployment.

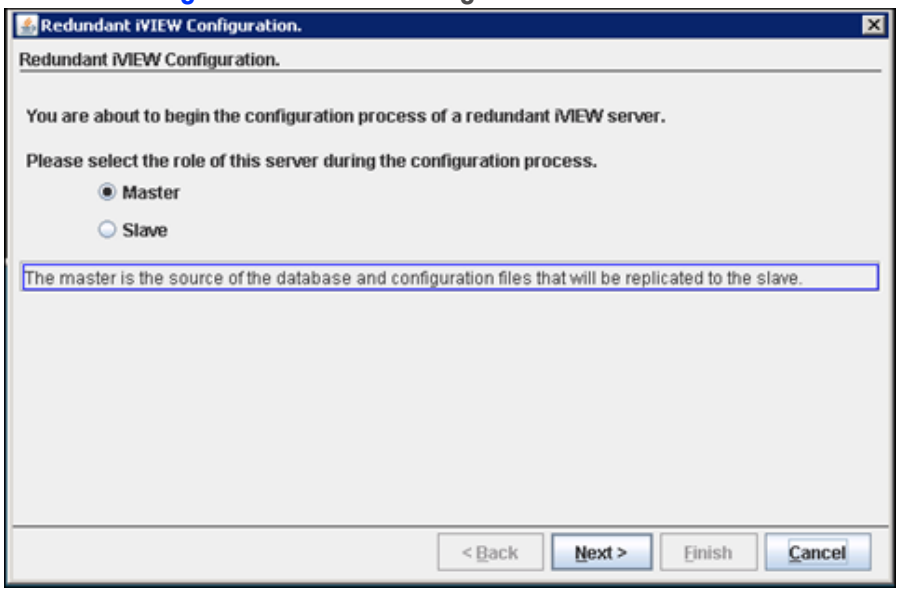
Procedure

Step 1 On the iVIEW Management Suite server designated to be a master select **Start > Programs > RADVISION iVIEW Management Suite > Launch Redundant iVIEW Management Suite Configuration Tool**.

The redundancy tool starts.

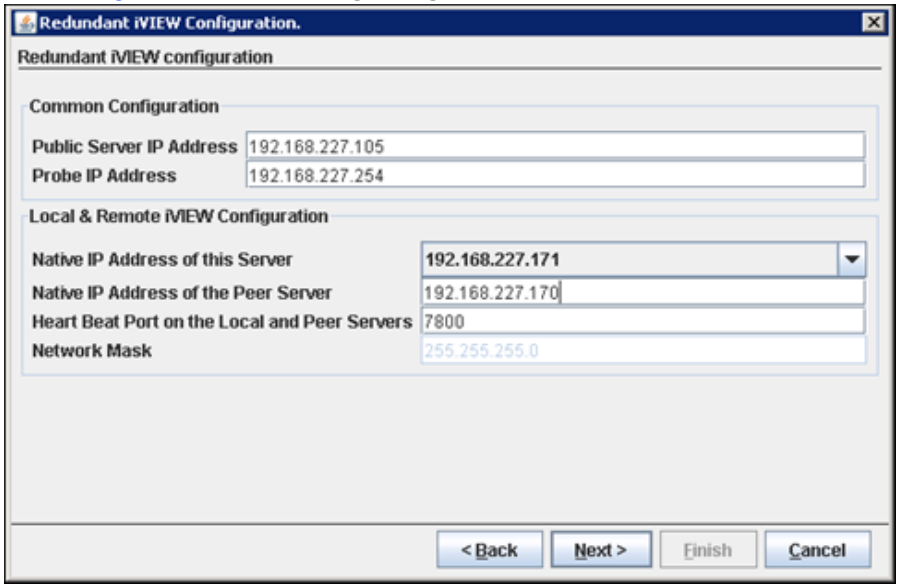
Step 2 Select **Master**, and then select **Next**.

Figure 3-29 Selecting the master server



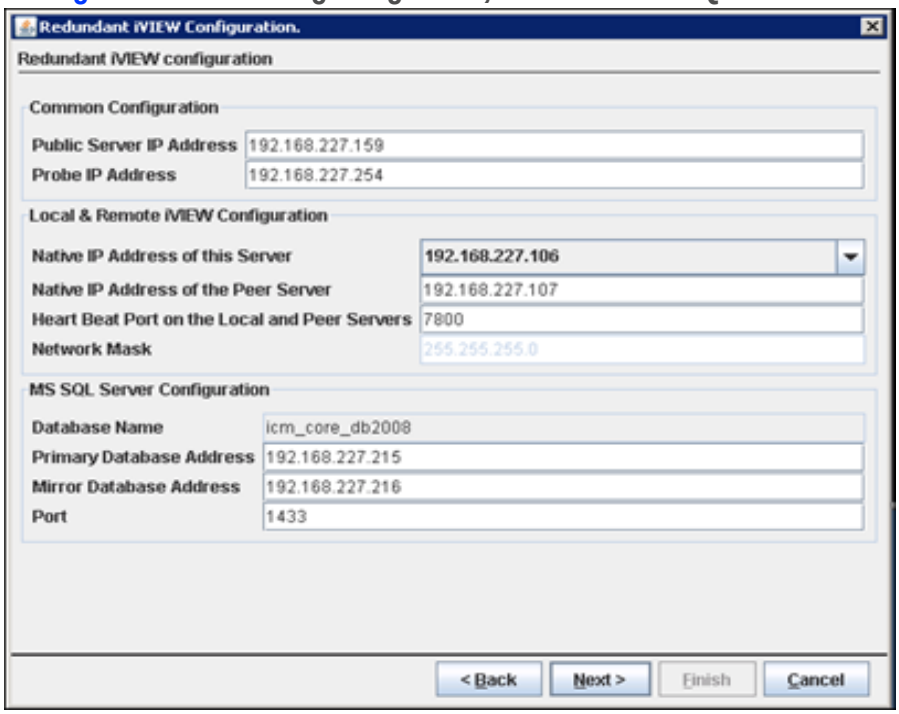
Step 3 If the iVIEW Management Suite server uses an internal database, the following window is displayed. Enter the settings for this server and the remote server. If the MS SQL Database is used, proceed to the next step. specify the database-related settings. Select **Next**.

Figure 3-30 Configuring local and remote servers



Step 4 If the MS SQL Database is used, specify the database-related settings. Select **Next**.

Figure 3-31 Configuring local, remote and SQL servers



Step 5 Select **Next** to start the configuration. At this stage the iVIEW service is stopped.

The configuration process on this service is paused until you run the redundancy tool on the other iVIEW Management Suite server.

Step 6 On the other iVIEW Management Suite server select **Start > Programs > iVIEW Management Suite > Redundant iVIEW Management Suite Configuration.**

The redundancy tool starts.

Step 7 Select **Slave**, and then select **Next**.

Step 8 Select **Next** to start the configuration. At this stage the iVIEW service is stopped.

The redundancy tool on the master server communicates with the redundancy tool on the slave server and configures redundancy. Status of the configuration is displayed on both master and slave servers.

Figure 3-32 Configuration status on the master server

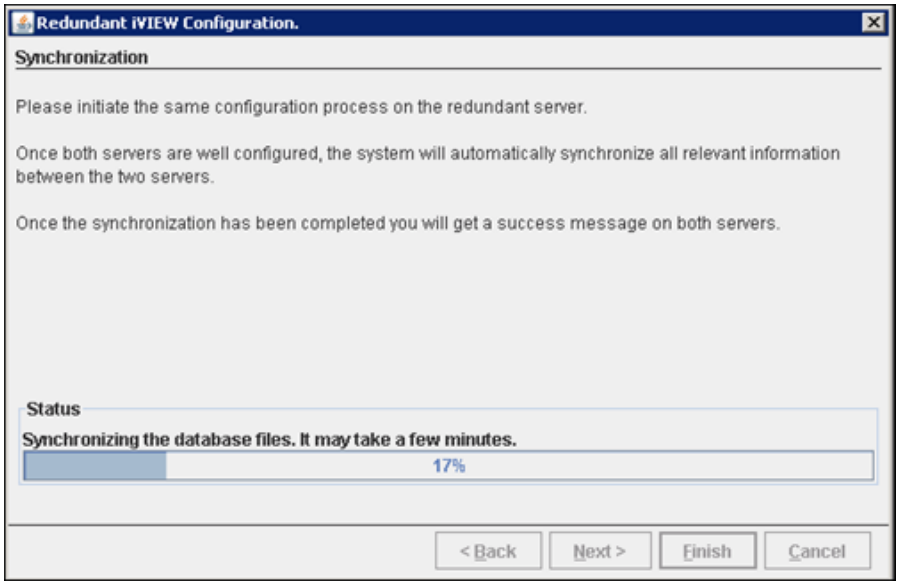
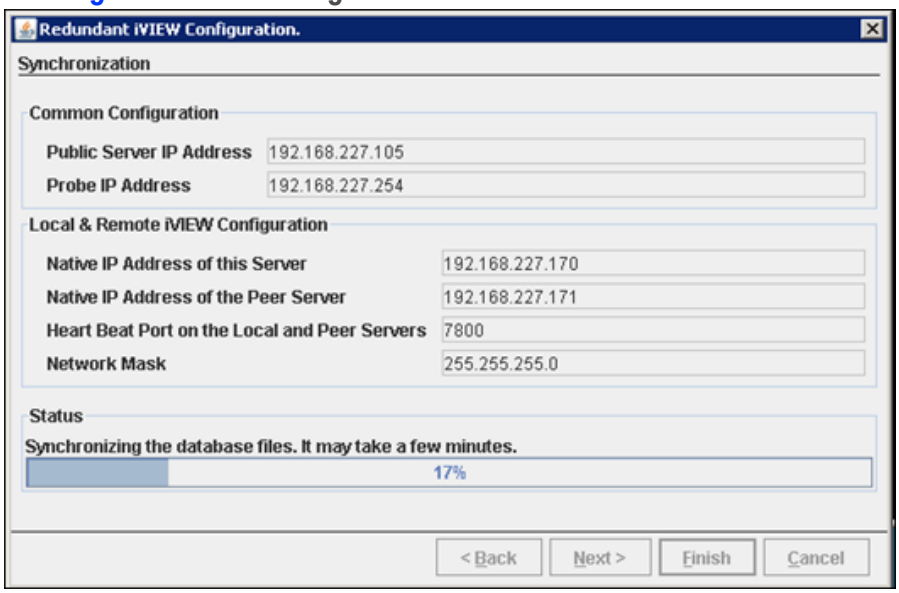


Figure 3-33 Configuration status on the slave server



When the configuration is completed successfully the success message is displayed.

Step 9 In the redundancy tool window on the master iVIEW Management Suite server, select **Finish**.

Step 10 In the redundancy tool window on the slave iVIEW Management Suite server, select **Finish**.

Note: When a standalone iVIEW Management Suite deployment is being converted to a redundant deployment, the recommended approach is use the old IP address of the standalone iVIEW Management Suite as public IP address.

The redundant iVIEW Management Suite deployment needs three IP addresses. Two are private IP address for master and slave, and the third is a public IP address. For instance, for a standalone iVIEW Management Suite deployment with an IP address of 192.168.1.1,

the iVIEW Management Suite has run for a few days and has some data. When you want to upgrade it to a redundant deployment, you need to get two additional IP addresses, e.g. 192.168.1.2 and 192.168.1.3.

The recommended solution is to configure the old iVIEW as master, assign one new IP address to it as private IP (for example 192.168.1.2). Then, install another new iVIEW Management Suite server as a slave with IP 192.168.1.3, and configure the 192.168.1.1 as a public IP. The advantage is that the IP address is not changed from the point of view of other components, which would otherwise need to be re-configured.

Monitoring Redundancy Status

Once the redundancy mode is configured, you can view the redundancy real-time status at any time by clicking the redundant deployment icon on the toolbar .

You can view the following information:

- **Virtual IP**: The virtual IP of the active iVIEW Management Suite server.
- **Probe IP**: The IP address of a router or other device that the iVIEW Management Suite server contacts to check network connectivity.
- **Master Server Native IP**: The static IP address of the original Master iVIEW Management Suite server.
- **Slave Server Native IP**: The static IP address of the original Slave iVIEW Management Suite server.
- **Last Hot Swap**: The time and date of the last repair or replacement of a system component that occurred on the iVIEW Management Suite sever, without shutting down the server.
- **Slave Server Status**: The status of the Slave iVIEW Management Suite server.
- **Database Status**: The database replication status between the master and slave servers. An error indicates that the master and slave databases are out of sync.

Note: System administrators receive email alerts when the CPU on the active iVIEW Management Suite server reaches 100%, and when a switch occurs between the master and slave servers.

Disabling Redundancy Mode

When disabling the redundancy mode, you have to disable both the master and the slave server.

Procedure

Step 1 On the master iVIEW Management Suite server select **Start > Programs > iVIEW Management Suite > Redundant iVIEW Management Suite Configuration**.

The redundancy tool starts.

Step 2 Select **Yes**, and then select **Next**.

The configuration process starts. The system informs you when the redundancy mode has been disabled.

Step 3 Select **Finish**.

Step 4 Repeat this procedure on the slave iVIEW Management Suite server.

4 Defining and Managing Video Users

Users profiles and user groups can be defined within iVIEW Management Suite, or sourced directly from the organization's external users directory, interfacing with Microsoft's Active Directory or IBM's Domino. When an external directory is used, the connection between iVIEW Management Suite and the LDAP server must be configured.

This section explains how service providers create organizations, and how administrators add and manage users within iVIEW Management Suite.

- Adding Organization Profiles to iVIEW Management Suite ..... page 92
- Managing Video Users ..... page 99
- Managing Virtual Rooms..... page 108
- Managing User Groups..... page 114
- Limiting User Access to Types of Meetings ..... page 116
- Managing Your Own User Profile..... page 122
- Configuring Corporate Address Books..... page 126

Adding Organization Profiles to iVIEW Management Suite

This section is for service providers only.

An organization is a company, an enterprise or an individual that is registered with a service provider for video meeting services.

Before you create organizations, make sure you have defined meeting types. See "Modifying Meeting Types" on page 120. Once meeting types are defined, you can assign meeting type groups to the organization. MCUs are responsible for providing meeting types, as services, to iVIEW Management Suite. When an organization is defined with a meeting type group, MCUs that provide these meeting types are assigned to the organization.

When an organization profile is created, iVIEW Management Suite automatically creates the first user as the organization administrator, with permission to log in and provision other users. This organization administrator cannot be deleted from the iVIEW Management Suite.

- Creating a New Organization..... page 93
- Limiting Organization Access to Different Meeting Types..... page 94
- Defining Organization Administrators..... page 95

- Limiting the Number of Concurrent Calls per Organization ..... page 95
- Limiting the Number of SCOPIA Desktop Pro and SCOPIA Mobile Licenses..... page 97
- Dedicating the SCOPIA Video Gateway to an Organization..... page 97
- Removing Inactive Organization Profiles ..... page 97
- Generating an Organization Report ..... page 98
- Branding the User Interface ..... page 99

Creating a New Organization

Organizations are registered with a service provider for videoconferencing services.

Once the videoconferencing network is defined, service providers can define organizations.

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **Organization Management** in the sidebar menu.

Step 3 Select **Active**.

Step 4 Select **Add**.

Step 5 Enter the name of the organization in the **Organization Name** field.

Users in the organization use this name to access the SCOPIA iVIEW Communications Manager web user interface.

Step 6 Enter address information for the organization in the relevant fields.

Step 7 Enter the alias of the organization in the **Alias** field.

The alias is a single word, used as part of the URL of a SCOPIA Desktop virtual room in an organization. For example, http://service_provider.com/:port/scopia/mt/organization_alias. This appears as part of the URL in a SCOPIA Desktop meeting invitation.

The alias can also be used as an H.323 organization alias when dialing endpoints across different organizations. For example, stephen@orgname.

Step 8 Enter contact information for the organization in the relevant fields.

The telephone number appears in the Active and Inactive tabs.

Step 9 Select **Integration with Directory Server** for adding or configuring organizations. Enabling this checkbox is required for a Hosting Pack deployment and optional for any other multi-tenant deployment.

Step 10 Select **OK** to save your changes.

MCUs are assigned to organizations through meeting type groups. This procedure is divided in three steps that should be performed in the below order:

1. Assign meeting types (MCU services) to specific MCU.

   Meeting types can be defined directly in the MCU or via iVIEW Management Suite. For details, see "Modifying Meeting Types" on page 120.
2. Define a group of multiple meeting types that fit the profile of different types of organizations.

   For example, organizations that pay different rates for low bandwidth and high bandwidth calls will be assigned different meeting groups, one that covers low bandwidth services and the other which includes all services. Each meeting type group uses services from specific MCUs.
3. Assign a meeting type group to an organization.

This section explains how to create meeting type groups and how to assign a meeting type group to an organization.

Before You Begin

Make sure meeting types are configured and up-to-date in iVIEW Management Suite and in the relevant MCUs.

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **Meeting Types** in the sidebar menu.

Step 3 Select **Meeting Type Groups**.

Step 4 Select **Add** to create a new meeting type group.

Step 5 Enter a name and, optionally, a description of the group in the appropriate fields.

Step 6 Use the arrows to select the meeting types included in this group.

Step 7 Select **Organization Management** in the sidebar menu.

Step 8 Select **Active**.

Step 9 Select **Add** to add a new organization or select the organization link to edit organization details.

Step 10 Locate the Meeting Type Groups field.

Step 11 Select the **Select Groups** to view a list of available meeting type groups.

Step 12 Use the arrows in the Select Groups window to select meeting type groups to be assigned to the organization.

By default, all users in an organization have access to all meeting types assigned to the organization.

Step 13 Select **OK** to save your changes.

Defining Organization Administrators

Once the organization is defined by the service provider, the organization administrator is automatically created. Service providers then create the login ID, password and email address for this user.

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **Organization Management** in the sidebar menu.

Step 3 Select **Active**.

Step 4 Select **Add**.

Step 5 Locate the System Administrator Information section.

Step 6 Enter a login ID, password, and e-mail address for the system administrator of the organization in the relevant fields.

Step 7 Select a user provisioning option for synchronizing information about users defined in an external directory server.

Step 8 Select **OK** to save your changes.

Limiting the Number of Concurrent Calls per Organization

This procedure defines the maximum number of concurrent calls that can be scheduled on MCUs and gateways for an organization.

In a multi-tenant deployment, the SCOPIA Video Gateway can be used as a resource shared among multiple organizations by limiting the number of simultaneous Lync calls hosted per organization that is part of the deployment.

This configuration can be paired with assigning a SCOPIA Video Gateway to a particular organization in a multi-tenant deployment. The feature is described in "Dedicating the SCOPIA Video Gateway to an Organization" on page 97

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **Organization Management** in the sidebar menu.

Step 3 Select **Active**.

Step 4 Select **Add**.

Step 5 Check **Limit Gateway Use to n Concurrent Calls**, **Limit MCU Use to n Concurrent Calls**, or **Limit SCOPIA Video Gateway 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, SCOPIA iVIEW Communications Manager checks if a newly scheduled meeting exceeds the defined limit.

Step 6 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.

Step 7 Select **OK** to save your changes.

Allowing Calls between Organizations

This section is intended for a service provider who uses the Microsoft Lync Server Multitenant Hosting Pack.

An organization (or tenant) can allow its users to place calls to selected federated organizations, to all the federated organizations, or to outside organizations.

Likewise, an organization can also prevent its users from placing such calls. For more information on this type of configuration, see the Microsoft Lync Hosting Pack Deployment documentation.

Follow this procedure for allowing tenants to place calls.

Procedure

Step 1 On the Lync Server, select the **Start** button.

Step 2 Select **Microsoft Lync Server 2010 > Lync Server Management Shell > Run as Administrator**.

The Lync Server Management Shell window opens.

Step 3 Get the names and IDs of the federated organizations by entering this command:

```
Get-CsTenant | format-table name,tenantid
```

Step 4 If required, review the configuration of a particular organization by entering this command:

```
Get-CSTenantFederationConfiguration -Tenant [TenantID]
```

Step 5 Add one or more domains to an organization's call allow list by entering these commands:

```
$d1 = New-CSEdgeDomainPattern -Domain "vtenant3.com"
$d2 = New-CSEdgeDomainPattern -Domain "vtenant4.com"

$a = New-CSEdgeAllowList -AllowedDomain @{replace=$d1,$d2}
Set-CSTenantFederationConfiguration -Tenant [TenantID]-AllowedDomains $a
```

Limiting the Number of SCOPIA Desktop Pro and SCOPIA Mobile Licenses

Administrators can limit the number of licenses for a specific organization that is part of a multi-tenant deployment.

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **Organization Management** in the sidebar menu.

Step 3 Select **Active**.

Step 4 Select **Add**.

Step 5 Enter the number of users to which you want to assign SCOPIA Desktop Pro or SCOPIA Mobile licenses.

Step 6 Select **OK** to save your changes.

Dedicating the SCOPIA Video Gateway to an Organization

This configuration can be implemented in conjunction with the limitation of concurrent calls per tenant as described in "Limiting the Number of Concurrent Calls per Organization" on page 95.

Procedure

Step 1 In the iVIEW Management Suite server, stop the iVIEW Management Suite services and the iVIEW Management Suite SIP service.

Step 2 Navigate to C:\Program Files\RADVISION\iVIEW Suite\iCM\jboss\bin.

Step 3 Open the **vcs-core.properties** file in a text editor.

Step 4 Verify that the parameter `com.visionnex.vcms.core.ucgw.schedule.rejectCallWhenNoBestUCGW` is set to `true`.

Step 5 Save and close the file.

Step 6 Restart the iVIEW Management Suite and iVIEW Management Suite SIP services.

Removing Inactive Organization Profiles

Only inactive organizations can be removed from iVIEW Management Suite. Service providers can delete organizations that are no longer registered with video conferencing services.

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **Organization Management** in the sidebar menu.

Step 3 On the Active tab, select the check box beside the name of the organization profile you want to deactivate.

Step 4 Select **Deactivate**.

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

Step 5 (Optional) Select **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.

Step 6 On the Inactive tab, select the check box beside the name of the organization profile you want to remove.

Step 7 Select **Delete**.
The organization profile is deleted from the scheduler and information about the organization is removed from the database.

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

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **Organization Management** in the sidebar menu.

Step 3 Select **Generate Reports** on the Active tab.

Information about each organization is included in the report.

Step 4 Select **Save** to save the report.

Step 5 Browse to the location at which you want to save the file, enter the file name and type, and then click **Save**.

Branding the User Interface

Administrators can change the product logo that appears in the top left corner of the user interface.

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **Organization Management** in the sidebar menu.

Step 3 Select **Active**.

Step 4 Select **Add**.

Step 5 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 Management Suite Configuration Tool.

Step 6 Select **OK** to save your changes.

Managing Video Users

You can download user profiles from an LDAP server, or you can manually add users to an iVIEW Management Suite local directory.

- Managing Users from the LDAP Server ..... page 100
- Managing Users with a Local User Directory ..... page 105
- Defining SCOPIA Desktop User Authorization ..... page 108

Managing Users from the LDAP Server

iVIEW Management Suite integrates with Microsoft Active Directory and IBM Lotus Domino for easy user provisioning. When your organization uses an LDAP server, each user defined in this directory is downloaded to iVIEW Management Suite, along with all the information associated to it.

You can configure iVIEW Management Suite to associate individual users or user groups pre-defined in the LDAP server, with iVIEW Management Suite settings, for example, you can select a specific group and define that this group will have administrator permissions. Once users are synchronized with the LDAP server, this group of users will be added to iVIEW Management Suite as administrators. In the same way, you can define which users will be assigned with a virtual room. Endpoints are also defined in the LDAP server as users and can be downloaded and managed by iVIEW Management Suite. See Downloading H.323 Endpoints from the LDAP Server page 54.

Once all users are downloaded to iVIEW Management Suite, iVIEW Management Suite will frequently synchronize with the LDAP server so information is always up-to-date.

Note: Make sure the external directory is customized to use standard schema attributes and class labels, otherwise iCM will not correctly configure the database to synchronize with the directory server.

- Connecting iVIEW Management Suite with the LDAP Server ..... page 100
- iVIEW Management Suite LDAP Information Attributes ..... page 103
- Securing the Connection between iVIEW Management Suite and an LDAP Server. page 103
- Downloading Users from the LDAP Server ..... page 104
- Updating User Profiles from the LDAP Server ..... page 105

Connecting iVIEW Management Suite with the LDAP Server

To allow user provisioning and synchronization of user profiles using an LDAP server, you have to configure the connection between iVIEW Management Suite and the LDAP server.

Before You Begin

Make sure **User Provisioning Using a Directory Server** is selected during the installation process (see I*nstallation Guide for iVIEW Management Suite*). When working with Microsoft Active Directory and the iVIEW Microsoft Outlook Add-on, select **User Provisioning Using a Directory Server with Single Sign-on**.

For a multi-tenant deployment, select **Integration with Directory Server** when adding or configuring organizations (see "Creating a New Organization" on page 93).

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **Advanced Settings** in the sidebar menu.

Step 3 Select **LDAP Configurations**.

Step 4 Select **Add** to add a new LDAP server, or click the required LDAP server entry to modify an existing LDAP server.

Step 5 Select the type of LDAP server in the **Server Type** field. This is the LDAP Server to which you connect iVIEW Communications Manager. For a deployment that includes the SCOPIA Video Gateway, select **Active Directory Server** in the **Server Type** field.

Step 6 Enter the directory server domain or directory server URL in the Domain/URL field.

> Note: For the secure connection between the iVIEW Management Suite and LDAP server use the ldaps:// prefix. For regular connection use the ldap:// prefix.

Step 7 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 iVIEW Communications Manager. This user account does not have to be part of the search base.

Step 8 Select **Configure** to configure the LDAP Search Base field. A tree structure of the **Users Search Base** appears, showing all OUs (Organization Units) defined on the directory server. Figure 4-1 on page 101 and Figure 4-2 on page 102 illustrates the tree structure for an enterprise deployment and a multi-tenant deployment respectively.

Figure 4-1 Tree structure in an enterprise deployment

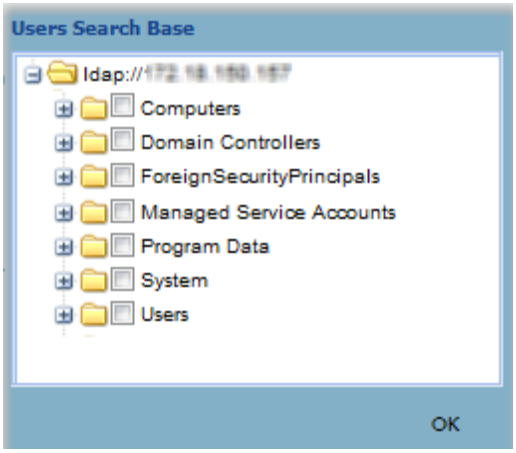
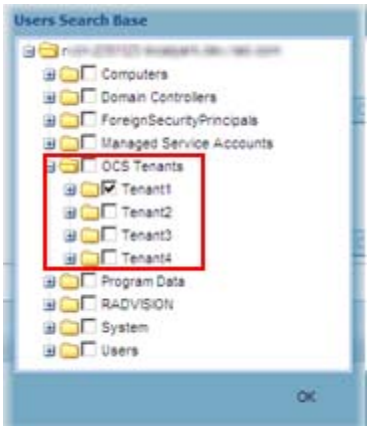


Figure 4-2 Tree structure in a multi-tenant deployment



> **Note:** In the multi-tenant deployment do not check the checkbox of the tenant sub-tree. Rather, click the **+** sign next to it and select the specific tenant you want to download.

Step 9 Select the OUs or tenant OUs whose users you want to download.

Step 10 Select **OK** to close the Users Search Base. The selected OUs are displayed in the **LDAP Search Base** field.

Step 11 To download users from the LDAP server, see "Downloading Users from the LDAP Server" on page 104.

Step 12 To download endpoints, see "Downloading H.323 Endpoints from the LDAP Server" on page 54.

Step 13 To download virtual rooms, see "Managing Virtual Rooms" on page 108"Downloading Virtual Rooms from the LDAP Server" on page 108.

iVIEW Management Suite LDAP Information Attributes

The table below present a list of standard schema attributes and their naming convention used by iVIEW Management Suite to synchronize with the LDAP server.

Table 4-1 iVIEW Communications Manager LDAP Information Attributes

iVIEW Management Suite Name	LDAP Attribute name (Active Directory)	LDAP Attribute name (Domino Directory)
User Login Identifier	userPrincipalName	cn
	sAMAccountName	uid
email	email	email
telephone	telephoneNumber	telephoneNumber
mobile	mobile	mobile
givenName	givenName	givenName
sn	sn	sn
sipUri	msRTCSIP-PrimaryUserAddress	N/A
sipUriEnabled	msRTCSIP-UserEnabled	N/A
Organizational Unit	ou	ou
Role	memberOf	member

Securing the Connection between iVIEW Management Suite and an LDAP Server

For deployments using Microsoft Active Directory, user credentials can be secured in the bind requests sent by the iVIEW Management Suite. In this case, user credentials are encrypted using MD5 algorithm ensuring the highest security level.

For deployments using Microsoft Active Directory or IBM Domino you can secure the entire connection between iVIEW Management Suite and the LDAP server. When defining the LDAP connections, use the ldaps://prefix. See "Connecting iVIEW Management Suite with the LDAP Server" on page 100.

Procedure

Step 1 Open the **Properties** window of your Microsoft Active Directory.

Step 2 Select the **Password never expires** and **Store password using reversible encryption** options. Users who do not use a strong password cannot log in to iVIEW Management Suite.

You can assign an iVIEW Management Suite user type to users and user groups defined in the LDAP server. This way, when users are downloaded from the LDAP server to iVIEW Management Suite, roles and permissions will be automatically assigned. If user types are not defined, a default user type will be assigned to all users.

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Click **Advanced Settings** in the sidebar menu.

Step 3 Click **LDAP Configurations**.

Step 4 Click **Advanced**.

Step 5 Click **Select** next to each user type to assign LDAP user groups to a specific iVIEW Communications Manager user type.

You can assign multiple LDAP user groups to each iVIEW Communications Manager 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.

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

When configuring terminals in a multi-tenant deployment, only select user groups belonging to the tenant that you are currently configuring.

Step 6 (Optional) Set the **Default User Type** field to **Don't download** to instruct iVIEW Communications Manager not to download users that are not assigned to any listed iVIEW Communications Manager user role.

Step 7 Click **OK** to save your changes.

Updating User Profiles from the LDAP Server

Once users are downloaded from the LDAP server and displayed in iVIEW Management Suite User Management tab, you can update certain attributes such as time zone, allowed meeting types, etc., for specific user groups.

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **User Management** in the sidebar menu.

Step 3 Select **Provisioning**.

Step 4 Select the group or groups to be updated.

Step 5 Define the relevant attributes to be updated for the user group.

Step 6 Select **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 iVIEW Communications Manager using a directory server login ID and password.

Managing Users with a Local User Directory

You can add or modify a user profile if iVIEW Management Suite uses its own database for storing user information.

- Creating a User Profile within iVIEW Management Suite ..... page 105
- Searching for a User Profile ..... page 106
- Removing a User Profile..... page 107

Creating a User Profile within iVIEW Management Suite

You can manually add a user profile in iVIEW Management Suite when a local database is used for storing user profiles.

If your organization is synchronized with an LDAP server to provision users, you can only modify the settings stored in iVIEW Management Suite, such as virtual room, default terminals, allowed meeting types, groups, and time zone. See "Managing Users from the LDAP Server" on page 100.

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

Procedure

Step 1 Log in to iCM.

Step 2 Select **User Management** in the sidebar menu.

Step 3 Select **Users**.

Step 4 Select **Add** to create a new user profile.

Step 5 Enter the user ID and last name in the relevant fields.

Step 6 (Optional) Enter the first name, email address and password for the user in the relevant fields, and confirm the password.

Step 7 (Optional) Select **Virtual Room Setting** to add or modify virtual room settings for the user. See

Step 8 Select **Advanced**.

Step 9 Select a user type and enter telephone numbers in the relevant fields.

Step 10 Select **Select Terminal** to assign a default endpoint to this user.

Step 11 Select the **Allowed Meeting Types** to restrict this user to a subset of all available meeting types.

By default, all active meeting types are allowed.

Step 12 Select the group to which this user belongs from the Groups list.

Step 13 Select a default time zone.

Local time zones are used by default at User > My Meetings and User > All Meetings.

Step 14 Select **Enabled** in the Account Status field to activate the user account and allow the user to log in to iVIEW Communications Manager.

Step 15 Select a recording policy option for this user from the Recording Policy list.

Step 16 Select a location preference for this user.

Step 17 Enable the user to log in to SCOPIA Desktop, if required.

Step 18 Select an allowed bandwidth for SCOPIA Desktop calls.

Step 19 Select **OK** to save your changes.
The user profile is saved and iVIEW Communications Manager sends the user a notification e-mail containing login access information.

Searching for a User Profile

You can search the Users list by a specific user name, virtual room number or by groups.

Procedure

Step 1 Log in to iCM.

Step 2 Select **User Management** in the sidebar menu.

Step 3 Select **Users**.

Step 4 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.

Step 5 Select the group in which you want to perform the search.

The default is All Groups.

Step 6 Select **Search**.

Search results are listed.

Step 7 To return to the complete list of users, clear the Name or Virtual Room field, and then select **Search**.

Removing a User Profile

You can only delete users stored on local directory server. When iVIEW Management Suite uses an external directory for users provisioning, users must be deleted from the external directory.

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

Step 1 Log in to iCM.

Step 2 Select **User Management** in the sidebar menu.

Step 3 Select **Users**.

Step 4 Select the user profile you want to delete in the Name column.

Step 5 Select **Delete** and then **OK**.

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

Defining SCOPIA Desktop User Authorization

You can configure user's authorization when accessing SCOPIA Desktop meetings, for example, you can define which users can invite participants to meetings, or record meetings and access the recordings.

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Click **Advanced Settings** in the sidebar menu.

Step 3 Click **Default User Settings**.

Step 4 (Optional) If a single SCOPIA Desktop Server or multiple SCOPIA Desktop Servers are configured to work with enterprise iVIEW Management Suite, select **Enable SCOPIA Desktop user authentication** to instruct the SCOPIA Desktop Server to authenticate and authorize users.

Step 5 Check the options you requite for defining which users can access meetings and webcasts, invite participants to meetings, and record meetings and access the recordings.

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

Managing Virtual Rooms

Virtual meeting rooms are literally virtual rooms that serve as a meeting place for SCOPIA Solution videoconference users.

Virtual rooms can be created manually within iVIEW Management Suite, or downloaded from the LDAP server, when your organization uses an LDAP server for user provisioning.

- Downloading Virtual Rooms from the LDAP Server ..... page 108
- Creating a Virtual Room for an iVIEW Management Suite User ..... page 112
- Enabling Recording for Specified Users Virtual Rooms ..... page 113
- Enabling Streaming for a User Virtual Room ..... page 114

Downloading Virtual Rooms from the LDAP Server

Virtual meeting rooms are literally virtual rooms that serve as a meeting place for your video network users. Virtual meeting rooms can be public, available for any user, and personal, assigned to a specific user, who is the only one allowed to schedule meetings in this room.Virtual meeting rooms appear in the Contact List of Microsoft Lync or Office Communications Video Chat Clients, unlike personal endpoints which are not shown.

Virtual rooms, meeting rooms and endpoints are pre-defined in the LDAP server and downloaded to iVIEW Management Suite during LDAP synchronization.

To download virtual rooms from the LDAP server, the following conditions must be met:

- The value of the LDAP field mapped to the virtual room must be numeric.
- The virtual room number is not editable in the virtual room profile window.
- If the same virtual room number is defined for two users in the LDAP server, the virtual room is created and downloaded to iVIEW Management Suite for only one of the users.

Each virtual room in iVIEW Management Suite is defined by the default settings configured in **Advanced Settings > Default Meeting Settings**.

Virtual rooms are available only in video networks where a RADVISION MCU is deployed.

The virtual meeting rooms comprise an additional contact named “My Virtual Room”. This is a personal meeting place where the user can host meetings. When “My Virtual Room” is enabled in the system, it shows its availability in the Contact List (while the user’s personal virtual room indicates an unknown presence).

Before You Begin

Check the prefixes used for the auto-attendant and for other components within your network, such as RADVISION MCUs, ECS, and SCOPIA Gateway. Prefixes assigned to virtual rooms must be unique.

Choose a SIP URI for the user to whom a virtual room is assigned (for example, “bfmyvr@lync2010.com”).

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **Advanced Settings** in the sidebar.

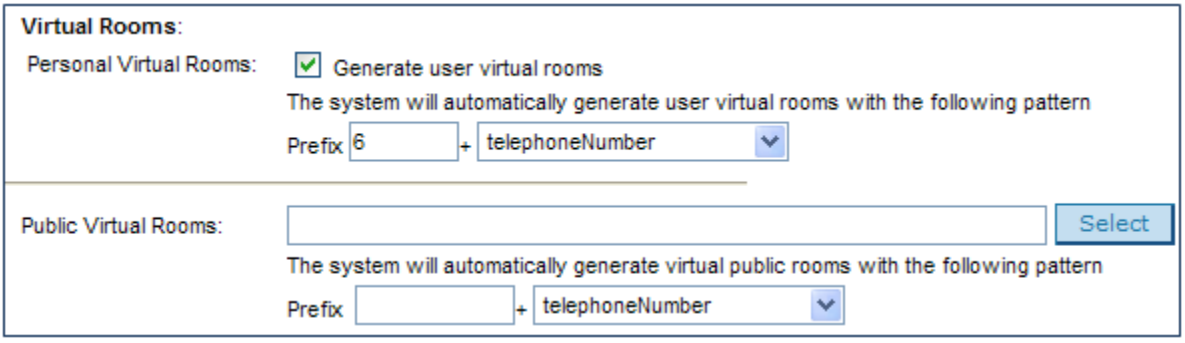
Step 3 Select the **LDAP Configurations** tab.

Step 4 Select the LDAP server to which organization users were added.

Step 5 Select **Advanced**. The Advanced section of the screen is displayed.

Step 6 Navigate to the **Virtual Rooms** section of the tab.

Figure 4-3 Virtual Rooms section of the LDAP Configurations tab



Step 7 Configure public virtual rooms in the Virtual Meeting Rooms area of the Virtual Rooms section as described in Table 4-2.

Table 4-2 Configuring settings for downloading virtual meeting rooms and terminals

Field	Description
The **Select** button	Select the Active Directory user group to which you assigned the public virtual rooms in the Virtual Room field. When configuring terminals in a multi-tenant deployment, only select user groups belonging to the tenant that you are currently configuring.
The **Prefix** field	Enter a number that you want to use for a prefix. Use any number that is shorter than 11 digits and is not used as a prefix for the auto attendant or for other deployment components.
The **telephoneNumber** list	Verify that the telephoneNumber options is selected.

Step 8 Configure personal virtual rooms for all LDAP users as follows:

a. Check **Generate user virtual rooms**.

b. Configure prefix and telephone number as described in Table 4-2.

Step 9 Define how often users and meeting rooms are synchronized with the LDAP server by selecting a value from the **Update Frequency** list.

Step 10 Select **OK**.

Step 11 Select **Synchronize** on the LDAP Configurations tab.

Users from the LDAP server downloaded into iVIEW Management Suite as virtual meeting rooms.

Step 12 Verify that the virtual meeting rooms were downloaded correctly:

a. Select **Users Management** in the sidebar.

b. Select the **Users** tab.

c. Verify that the virtual meeting rooms defined in the LDAP server were downloaded and appear on the Users tab.

Step 13 If new users were added to the Active Directory after you downloaded users' virtual rooms, you can force synchronization between the Active Directory and the Lync Server to update the Lync Contact List immediately:

a. On the Lync Server, select **Start > Microsoft Lync Server 2010 > Lync Server Management Shell > Run as administrator**.

b. Type **Update-CsAddressBook** and press Enter.

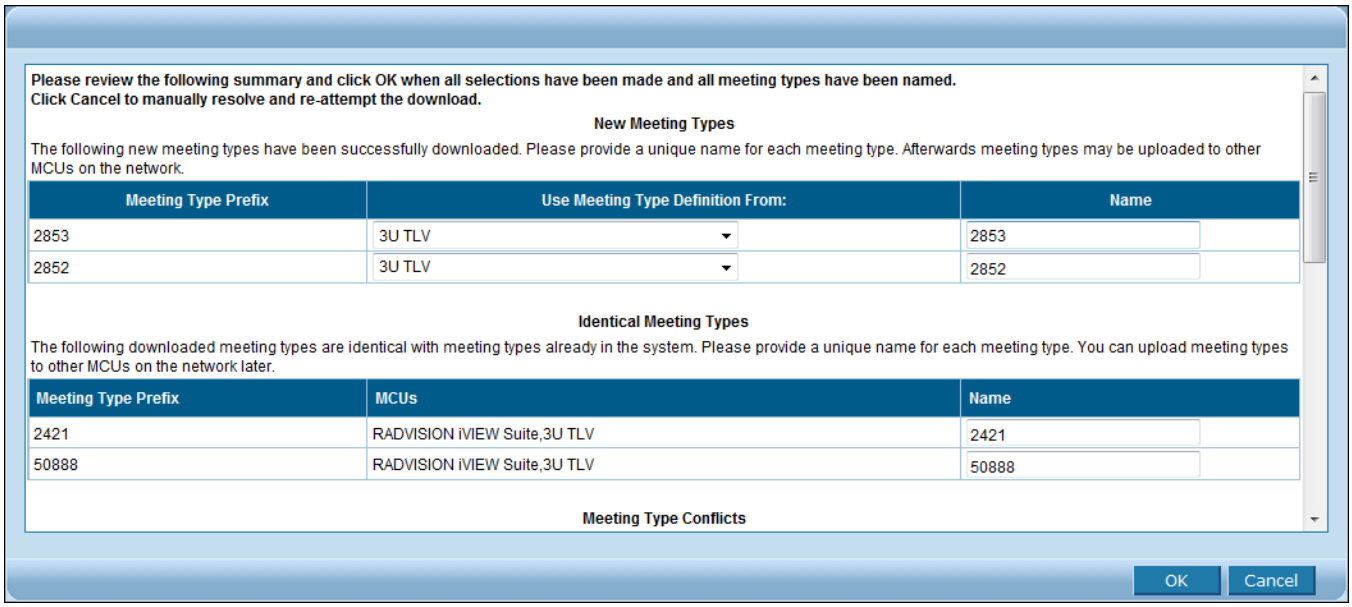
Step 14 Download the meeting types from MCUs.

a. Select **Meeting types** in the sidebar.

b. Select **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 in your deployment.

Figure 4-4 Meeting types downloaded into the iVIEW Management Suite from MCUs



c. Enter a unique name for each meeting type.

d. Select **OK**.

Step 15 Enable the "My Virtual Room" for a specific user:

a. Assign the AD user you configured to a personal virtual room:

a. Select **Advanced Settings** in the sidebar.

b. Select the **Default Meeting Settings** tab.

c. Select **Enable My Virtual Room**.

Figure 4-5 Enabling the personal virtual room



d. Enter the SIP URI of My Virtual Room.

e. Select **OK**.

Creating a Virtual Room for an iVIEW Management Suite User

You can manually create virtual rooms for users within iVIEW Management Suite. If your organization uses an LDAP server for user provisioning, and the Generate user virtual rooms option is not selected, you can manually create virtual rooms for users. If this option is checked, the configuration settings defined manually will be override every time that iVIEW Management Suite is synchronized with the LDAP server.

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

Procedure

Step 1 Log in to iCM.

Step 2 Select **User Management** in the sidebar menu.

Step 3 Select **Users**.

Step 4 Select the link in the Name column for the user you require, or select **Add** to create a new user profile.

Step 5 Enter the user ID and last name in the relevant fields.

Step 6 (Optional) Enter the first name, email address and password for the user in the relevant fields, and confirm the password.

Step 7 (Optional) Select **Virtual Room Setting** to add or modify virtual room settings for the user.

Step 8 Enter a name for the virtual room.

Step 9 Select from the list of **Meeting Types** the meeting type allowed to be scheduled in this virtual room.

Step 10 Enter a number for the virtual room in the **Virtual Room Number** field. Use any number that does not start with the prefix of the auto attendant, auto routing, or other deployment components.

Step 11 (Optional) Check **Secure meeting with a PIN** to enable security. Participants of a meeting will be required to enter this number to access the meeting.

Step 12 (Optional) Enter a Moderator PIN. Once the moderator PIN number is entered, the two options below are enabled:

a. (Optional) Select **Place participants in a "waiting room" until moderator joins the meeting** to create a waiting room.

b. (Optional) Select **Record meeting when meeting starts**.

Step 13 (Optional) Allow streaming for the virtual room, as described in "Enabling Streaming for a User Virtual Room" on page 114.

Step 14 (Optional) Allow ad hoc meetings for the virtual room and define the maximum number of ports per ad hoc meeting.

Step 15 Click **OK** to save the settings for the virtual room.

Enabling Recording for Specified Users Virtual Rooms

You can configure iVIEW Management Suite to automatically record a user virtual room or a scheduled meeting when the meeting begins.

Before You Begin

Make sure recording support is enabled in iVIEW Management Suite. See "Enabling Recording on iVIEW Management Suite" on page 34.

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **User Management** in the sidebar menu.

Step 3 Select **Users**.

Step 4 Select the link in the Name column for the user you require.

Step 5 Select **Virtual Room Setting**.

Step 6 Enter a Moderator PIN.

Step 7 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.

Step 8 Select **OK** to save your changes.

Enabling Streaming for a User Virtual Room

You can configure streaming support for a virtual room, to allow broadcasting the videoconference scheduled in the virtual room to an audience of listeners and viewers who are not active participants in the conference.

Before You Begin

Make sure iVIEW Management Suite is configured to support streaming. See "Enabling Streaming on your Video Network" on page 32.

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **User Management** in the sidebar menu.

Step 3 Select the link in the Name column for the user you require, or select **Add** to create a new user profile.

Step 4 Select **Virtual Room Setting**.

Step 5 Set Streaming to **Enabled**.

Step 6 Select **OK** to save your changes.

Managing User Groups

User groups join together users that share specific settings, allowing you to modify and update configuration on a group level. There are two types of user groups:

- Directory user groups

  Directory groups are user groups defined in the external user directory (Active Directory) and imported to iVIEW Management Suite during user provisioning. Directory groups cannot be edited or deleted from iVIEW Management Suite. Changes to these user groups must be performed in the active directory.

- Local user groups

  Local groups are created within iVIEW Management Suite and are used to join together a group of users sharing a specific setting.

This section explains how to create and manage user groups:

- Creating a User Group ..... page 115
- Modifying a User Group ..... page 115
- Removing a User Group ..... page 116
- Limiting Group Access to Meeting Types ..... page 116

Creating a User Group

You can create groups of users that share specific parameters. User groups are created within iVIEW Management Suite, and are not synchronized with the external active directory, if your organization uses an external directory.

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **User Management** in the sidebar menu.

Step 3 Select **Groups**.

Step 4 Select **Add**.

Step 5 Enter a name for the group in the Name field.

Step 6 Select participants and terminals from the Available Contacts list and select the right-arrow button to move them to the Selected Contacts list.

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

Modifying a User Group

Only user groups created within iVIEW Management Suite can be modified. User groups imported from the external active directory cannot be edited or deleted.

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **User Management** in the sidebar menu.

Step 3 Select **Groups**.

Step 4 Select the link in the Name column for the user group you require.

Step 5 Modify the name of the user group.

Step 6 Select **OK** to save your changes.

Removing a User Group

Only user groups created within iVIEW Management Suite can be deleted. User groups imported from the external active directory cannot be deleted.

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **User Management** in the sidebar menu.

Step 3 Select **Groups**.

Step 4 Select the group you want to delete.

Step 5 Select **Delete** and then **OK**.
The user group is deleted from the scheduler.

Limiting Group Access to Meeting Types

You can update settings on a group level instead of updating individual users. Access to meeting types is one of the settings that is commonly applied to a group of users. You can have a group of users with permission to schedule audio only meetings, and you can have a group of users with permission to schedule high quality videoconferences.

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **User Management** in the sidebar menu.

Step 3 Select **Provisioning**.

Step 4 Select one or any of the groups listed in the Available Groups list and select the right-pointing arrow.

Step 5 Select **Allowed Meeting Types** and select Select.

Step 6 Select the required meeting types and select **OK**.

Step 7 Select **OK** to save your changes.

Limiting User Access to Types of Meetings

Meeting types are defined in the MCUs as services, and downloaded to iVIEW Management Suite, allowing users to schedule and participate on different types of meetings. You can limit the meeting types available for each user by assigning specific type of meeting to each user.

- Downloading Meeting Types to iVIEW Management Suite ..... page 117
- Upload a Meeting Type to Network MCUs ..... page 117
- Resolving Meeting Type Conflicts..... page 118

- Defining a Default Meeting Type ..... page 119
- Configuring Meeting Type Details ..... page 119
- Defining the Meeting Types Available for Users ..... page 120
- Modifying Meeting Types ..... page 120
- Modifying a Meeting Type Group ..... page 121
- Searching for a Meeting Type ..... page 121
- Removing a Meeting Type ..... page 122

Downloading Meeting Types to iVIEW Management Suite

Meeting types are downloaded from all MCUs to the iVIEW Management Suite when new MCUs are added to the network, or when new services are configured in specific MCUs.

Procedure

Step 1 Select **Meeting Types** in the sidebar menu.

Step 2 Select **Download**.

MCU services are downloaded from all network MCUs and displayed in a Download Meeting Type list, according to the following categories:

- New meeting types
- Identical meeting types: meeting types with different prefix number but same meeting definitions.
- Meeting type conflict: meeting types with the same prefix number. To learn how to resolve conflicts, see "Resolving Meeting Type Conflicts" on page 118.

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

Step 3 Enter a unique name for each meeting type. See for details on how to resolve meeting types conflicts.

Step 4 Select **OK**.

Upload a Meeting Type to Network MCUs

You can download a specific meeting type from an MCU and upload this meeting type to all other MCUs in the network. This way specific MCUs or all MCUs can have the same meeting type.

Make sure the MCUs support the meeting types being uploaded, for example, you cannot upload a meeting type defined to supports High Definition Continuous Presence (HD CP) conferences to an MCU that is not enabled for HD CP.

Procedure

Step 1 Log in to iCM.

Step 2 Select **Meeting Types** in the sidebar menu.

Step 3 Select the meeting types you want to upload from iCM on the **Active Meeting types** tab.

Step 4 Select **Upload**.

Step 5 Use the arrows to select the target MCUs.

Only MCUs that support the selected services are displayed.

Step 6 Select **OK**.
Since MCU services are uploaded via SNMP, the process may take some time if there are many MCUs to connect to.

Resolving Meeting Type Conflicts

You can have two types of conflicts when downloading meeting types (services) from MCUs:

- Meeting conflicts between MCUs: when two meeting types with the same prefix number are downloaded from two different MCUs.
- Meeting conflicts between iCM and MCU: when a meeting type downloaded from an MCU has the same prefix number of a meeting type that already exists in iVIEW Communications Manager. In this case, the service stored in iVIEW Communications Manager is selected by default during conflict resolution.

  When an MCU is removed from the network, meeting types that existed only in this MCU are no longer available for meeting scheduling.

Procedure

Step 1 Log in to iCM.

Step 2 Click **Meeting Types** in the sidebar menu.

Step 3 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.

Step 4 Scroll down to the Meeting Type (Service) Conflicts section on the Download Meeting Types (Services) screen.

Step 5 Select the entry that you want to keep in the **Use Meeting Type Definition From** column for each service prefix listed.

iVIEW Communications Manager 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 iVIEW Communications Manager 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.

Step 6 Enter a unique name for each meeting type.

Step 7 Click **OK**.

Defining a Default Meeting Type

When a new meeting is scheduled, default settings configured in the default meeting type configured in the Default Meeting Settings tab is displayed in the Meeting Scheduling window. A fallback meeting type is defined so iVIEW Management Suite uses it when the system fails to create a meeting of the default type due to the lack of resources. The fallback mechanism is relevant only for ad hoc meeting creation and scheduled meeting upon creation.

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Click **Advanced Settings** in the sidebar menu.

Step 3 Click **Default Meeting Settings**.

Step 4 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.

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

Configuring Meeting Type Details

You can modify some parameters of an existing meeting type, according to the video services that you want to provide. Once meeting types are defined, upload them to the relevant MCUs.

Procedure

Step 1 Log in to iCM.

Step 2 Select **Meeting Types** in the sidebar menu.

Step 3 Select the link in the Name column for the meeting type you require on the Active Meeting Types.

Step 4 (Optional) Enter a new name for the meeting type.

Step 5 (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.

Step 6 (Optional) If the meeting type supports lecture mode, select **Lecture Mode Support** to enable this support.

Step 7 (Optional) Select **Auto Attendant Support** to specify this meeting type as the Auto Attendant meeting type.

Step 8 Select **OK** to save your changes.

Defining the Meeting Types Available for Users

You can limit the meeting types available for users or user groups. This way, a user that has permissions to schedule and participate on audio only meetings, will not be able to schedule video meeting.

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **User Management** in the sidebar menu.

Step 3 Select **Users**.

Step 4 Select the link in the Name column for the user you require, or select **Add** to create a new user profile.

Step 5 Select **Advanced**.

Step 6 Select **Select** next to the Allowed Meeting Types field.

Step 7 Select the required meeting types and select **OK**.

Step 8 Select **OK** to save your changes.

Modifying Meeting Types

After meeting types are downloaded from all MCUs defined in the network, some parameters can be modified, such as the name of the meeting type, the default connection rate and the auto attendant support. Once meeting types are modified and ready, you can upload them to other MCUs.

Procedure

Step 1 Log in to iCM.

Step 2 Select **Meeting Types** in the sidebar menu.

Step 3 Select the link in the Name column for the meeting type you require on the Active Meeting Types.

Step 4 (Optional) Enter a new name for the meeting type.

Step 5 (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.

Step 6 (Optional) If the meeting type supports lecture mode, select **Lecture Mode Support** to enable this support.

Step 7 (Optional) Select **Auto Attendant Support** to specify this meeting type as the Auto Attendant meeting type.

Step 8 Select **OK** to save your changes.

Modifying a Meeting Type Group

Only service providers and administrators of a distributed deployment can create and modify meeting type groups. Each meeting type groups is comprised of multiple meeting types. A meeting type group can then be assigned to an organization, that will have permission to use only these meeting types.

Procedure

Step 1 Log in to iCM.

Step 2 Select **Meeting Types** in the sidebar menu.

Step 3 Select **Meeting Type Groups**.

Step 4 Select the link in the Group Name column for the group you require, or select **Add** to create a new meeting type group.

Step 5 Enter a name and, optionally, a description of the group in the appropriate fields.

Step 6 Use the arrows to select the meeting types included in this group.

Step 7 Select **OK** to save your changes.

Searching for a Meeting Type

You can search for a specific meeting type, to modify some parameters, or to view details about the meeting type.

Procedure

Step 1 Log in to iCM.

Step 2 Select **Meeting Types** in the sidebar menu.

Step 3 Enter the partial or complete name of the meeting type in the Name field.

Step 4 Select **Search**.

Search results are listed.

Step 5 To return to the complete list of meeting types, clear the Name field, and then select **Search**.

Removing a Meeting Type

You must deactivate a 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 iVIEW Communications Manager, 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

Step 1 Log in to iCM.

Step 2 Select **Meeting Types** in the sidebar menu.

Step 3 Select the meeting type you want to delete.

Step 4 Select **Deactivate** and then **OK**.
The meeting type is removed from the Active Meeting Types tab and placed on the Inactive Meeting Types tab.

Managing Your Own User Profile

Based on your user type, the iVIEW Management Suite interface displays a different user interface. This section explains how to change profile information for Operators, Organizers, and Regular Users.

- Modifying Administrators Log in Information ..... page 123
- Modifying Your Time Zone ..... page 124
- Defining Your Meeting Display Preferences ..... page 124
- Modifying a Service Provider Profile ..... page 125

Note: Meeting organizers, operators and regular users can modify their time zone and meeting display preferences. Administrators can modify their log in information only.

Modifying Administrators Log in Information

Only administrators can change their log in information and password. Other users cannot modify these information.

Procedure

Step 1 Log in to iCM.

Step 2 Select Users in the side bar menu.

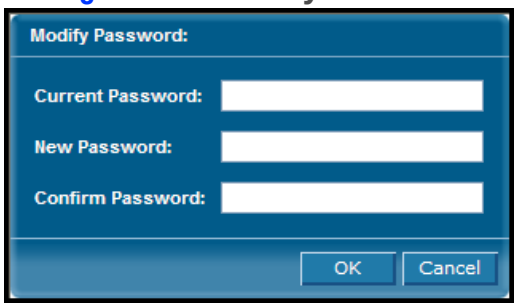
Step 3 Select the **My Profile** icon in the sidebar menu.

Figure 4-6 My Profile



Step 4 To change the password, select **Modify Password**.

Figure 4-7 Modify Password



Step 5 Complete the information as required and Select **OK** to save your changes.

Step 6 To change the format of the information displayed, select the **My Preferences** tab.

Modifying Your Time Zone

Operators, meeting organizers, and regular users can modify their time zone to comply with their current location.

Procedure

Step 1 Log in to iCM.

Step 2 Select **My Profile** in the sidebar menu.

Step 3 Select **My Info**.

Step 4 Select **Advanced**.

Step 5 Select the required time zone.

Step 6 Select **OK** to save your changes.

Defining Your Meeting Display Preferences

When logging in as an operator, a meeting organizer or a regular user, you can define a number of meeting preferences.

Procedure

Step 1 Log in to iCM.

Step 2 Select **My Profile** in the sidebar menu.

Step 3 Select **My Preferences**.

Step 4 Select a default virtual room from the drop-down list.

The default virtual room is automatically selected when you schedule a meeting from the SCOPIA iVIEW Management Suite Web interface.

For LDAP users, the virtual rooms created during LDAP synchronization are automatically set as the default virtual room.

Step 5 Select **Don't include me in the meeting** if you do not want to be automatically included in the **Selected Participants** list on the Invite tab when you schedule a new meeting.

Step 6 Enter a value in **Delete meeting history items older than n days** to delete meetings from My Meetings > History after the specified number of days.

Step 7 Select **Use Full Screen Display** to display meetings without a menu or title bar in your browser.

Deselect to display meetings using default browser settings.

Step 8 Select an option from the **Name Display Format** list to change the way your name is displayed in meeting-related information and in the meeting video display.

Step 9 Select **Last name** or **First name** from the **Sort by** list to change the sort order for participant name columns.

Step 10 Select an option from the **Date Display Format** list to change the way dates are displayed.

Step 11 Select **OK** to save your changes.

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 SCOPIA iVIEW Management Suite.

Procedure

Step 1 Log in as the service provider administrator, and then go to **My Profile**.

Step 2 Modify the login ID in the **User ID** field.

Step 3 Select **Modify Password** to modify the service provider administrator password.

Step 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

Step 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.

Step 6 Select **OK** to save and apply changes.

Configuring Corporate Address Books

The corporate address book feature synchronizes the organization directory (local directory or LDAP server) to all endpoints. The organization directory will be available for endpoints as the corporate address book. Administrators can define the endpoints to be displayed in the address book, and those to be private numbers.

The following endpoints are supported to use this feature:

- Life-Size: Passport, Express, Team, Room, Conference
- Polycom: HDX Series, VSX Series
- SCOPIA XT Series
- Tandberg via TMS: All

Note: To secure the LDAP connection and avoid sending the password in clear text over the network, iVIEW Management Suite supports LDAP over TLS/SSL.

This section includes the following topics for configuring corporate address books.

- Enabling a Corporate Address Book ..... page 126
- Configuring Endpoints to be Displayed in the Corporate Address Book ..... page 128

Enabling a Corporate Address Book

By default, this service is disabled. You must enable it to allow iVIEW Management Suite to synchronize the organization directory and distribute this information as a corporate address book to endpoints.

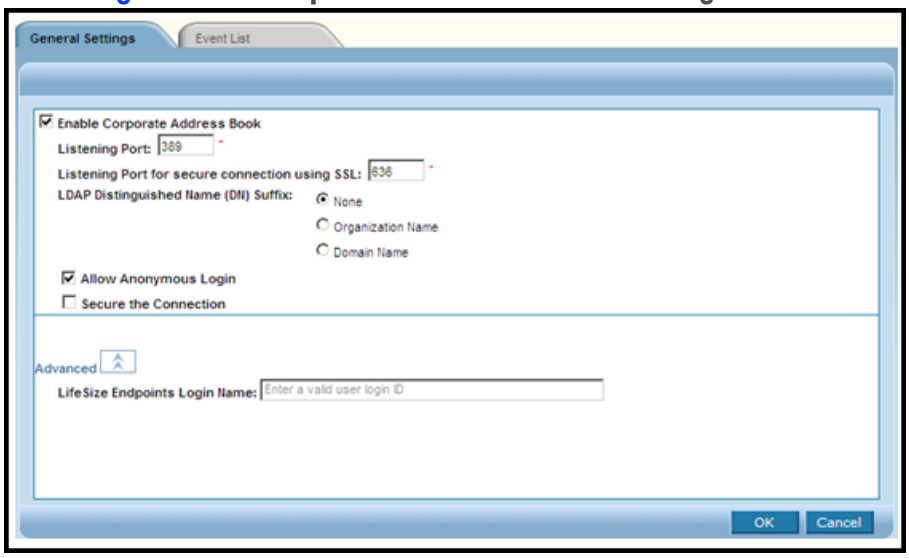
Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **Corporate Address Book** icon in the sidebar.

Step 3 Select **General Settings**.

Figure 4-8 Corporate Address Book Configuration



Step 4 Select **Enable Corporate Address Book** for remote systems.

If your organization uses an LDAP server as the organization directory for provisioning users, proceed to the next steps. Otherwise, refer to step 9.

Step 5 Insert the Listening Port: the port that the service receives the LDAP request.

Step 6 (Optional) Select the LDAP Distinguished Name (DN) Suffix.

The data input in one of the fields will be the suffix of the distinguished name of an entry supplied by the LDAP service. If the Organization Name field is filled with, for example, “Westco”, the DN suffix will be “o=westco”; if the domain name field is filled with, for example, “westco.com”, the DN suffix will be “dc=westco,dc=com”.

When configuring the search base of the LDAP configuration on the endpoints, you should append the suffix accordingly:

- If the suffix is not filled, the search base for users will be "ou=users", o=westco” if the organization name field is filled, or “ou=users,dc=westco,dc=com” if the domain name field is filled.
- The search base for terminals will be "ou=terminals" if no suffix is filled.The search base for terminals will be “ou=terminals,o=westco” if the organization name is filled, or “ou=terminals,dc=westco,dc=com” if the domain name is filled.

Step 7 (Optional) Select the **Allow Anonymous Login** box. If this box is checked, the end point can search the data in the LDAP service without the needs of an account.

Step 8 (Optional) Select **Secure the Connection**. If this box is checked, only SSL connections are allowed.

Step 9 Select **OK** to save your change.

Configuring Endpoints to be Displayed in the Corporate Address Book

You can define if an endpoint is displayed in the corporate address book, or if it is a private number and other endpoints should not have access to this information.

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **Resource Management** in the sidebar menu.

Step 3 Select **Terminals**.

Step 4 Select the endpoint you want to configure.

Step 5 (Optional) Select **Display in global address book** to allow this endpoint information to be displayed in the corporate address book, or de-select **Display in global address book** to make this endpoint information private.

Step 6 Select **OK** to save your changes.

5 Securing your Video Network

You can secure your video network in the SCOPIA Solution by configuring the network's components to communicate via the secured standard of the Transport Layer Security (TLS) protocol, and you can secure your browser access to iVIEW Management Suite using the secure HTTPS protocol.

- Securing Web Access to iVIEW Management Suite Using HTTPS..... page 129
- Securing Your Video Network Using TLS..... page 134

Securing Web Access to iVIEW Management Suite Using HTTPS

HTTPS is a method used for encrypting communications between a server and a web browser, in this case between iVIEW Management Suite and anyone logging in to manage it using a web browser. HTTPS employs powerful well-known algorithms to secure communications using encryption keys which are held in a certificate.

The iVIEW Management Suite is shipped with a pre-created and pre-installed certificate, but it contain non-unique encryption keys. For full encryption, you must first install certificates with unique keys on the application server, and then configure the application server to use HTTPS. After performing these configurations, access iVIEW Management Suite using HTTPS.

Once iVIEW Management Suite's computer (application server) installs the full (private key) certificate, its communications will be encrypted, and only browsers with a corresponding matching (public key) certificates will be able to understand the communication. A private key certificate and its public key certificate are created as a matching pair.

Typically you request a trusted third party certification authority (CA) to issue a certificate which contains the encryption keys to be used for secure communications. A trusted CA signs all the certificates they issue. A trusted signature ensures that iVIEW Management Suite is who it claims to be, and not an imposter. Popular web browsers are preconfigured to trust certificates that are signed by well-known CAs.

But in your deployment it may be good enough for you to issue your own certificates as an administrator if you are solely responsible for both the server's installation (iVIEW Management Suite) and the client side (the browser). Certificates that you issue are self-signed. Most web browsers will issue an alert when communicating with servers whose certificate is not signed by a well-known CA, questioning the trustworthiness of the server.

There are three stages to this configuration:

- Installing Certificates with Unique Keys on the Application Server ..... page 130
- Configuring the Application Server to Use HTTPS ..... page 132
- Accessing iVIEW Management Suite Using HTTPS ..... page 134

Installing Certificates with Unique Keys on the Application Server

The iVIEW Management Suite is shipped with a pre-created and pre-installed certificate, but it contain non-unique encryption keys.

To create a certificate with unique keys for true authentication, you must generate and install a new unique certificate, and then replace the pre-installed certificate held in `keytool`'s `.keystore` file.

This solution was tested on the Java-enabled JBoss application server. While secured iVIEW Management Suite communications may also function on other middleware application servers supporting Java, we recommend using JBoss for this configuration.

The certificate workflow uses a command line Java utility called `keytool`. It accesses the keystore, a file containing your keys and certificates, which is protected with a password.

Note: The iVIEW Management Suite server has Java 1.6 (Java 6) and JBoss pre-installed.

The `keytool` utility contains many more commands and parameters than are mentioned in this procedure. For more information, see the Java Development Kit (JDK) documentation: http://java.sun.com/j2se/1.4.2/search.html.

Procedure

Step 1 Stop the **RADVISION iVIEW Management Suite** service.

Step 2 Copy the `icmservice.keystore` file located in <iVIEW_install_dir>\iCM\jboss\server\default\conf\icmservice.keystore to a temporary working folder, for example, *C:\cert*.

The keystore file holds the certificates on each server. Currently they hold the default non-unique certificates.

Step 3 Open a command line window. Use the `keytool` utility, located in <iVIEW_install_dir>\iCM\jre_rt\bin, to perform the following steps.

Step 4 Create a key pair to be stored in the keystore file using the genkey parameter, as follows:

```
keytool -genkey -keyalg RSA -dname "cn= <iVIEW FQDN>" -alias scheduler
-keystore icmservice.keystore -storepass radvision
```

Where:

- Determine the algorithm used to sign the certificate using the `-keyalg` command. The default is DSA, which is not supported by all versions of browsers. We recommend using RSA.
- `<iVIEW FQDN>` is the computer name of iVIEW Management Suite.The `-dname` parameter can also include information about the organizational unit (OU), organization (O), location, country, and more.
- The alias of the pre-installed key pair is `scheduler`.
- The `icmservice.keystore` refers to the path of the `.keystore` file that is saved in the temporary working folder.
- The password on the `.keystore` file is `radvision`.

Step 5 Press **Enter** at the `Enter key password for <scheduler>` prompt.

Step 6 Create a certificate signing request (CSR) file to be sent to the CA using the `certreq` parameter, as follows:

```
keytool -certreq -v -alias scheduler -file filename.csr -keystore
icmservice.keystore -storepass radvision
```

The certification signing request file (CSR) is stored in the file <filename.csr>.

Step 7 Send the <filename.csr> file to your selected CA for signing.

The CA sends back the newly issued certificate (the CA signed certificate) and the CA trusted root certificate.

Step 8 When you receive the two certificates back from the CA, save them to the local bin directory. In the following examples, **caroot.cer** refers to the CA trusted root certificate, and **icm.cer** refers to the CA signed certificate.

Step 9 Import the **CA trusted root certificate** into the keystore using the `-import` parameter, as follows:

```
keytool -import -trustcacerts -alias caroot -file caroot.cer -keystore
icmservice.keystore -storepass radvision
```

Where:

`caroot` is the alias of the CA trusted root certificate file that you received from the CA.

The system confirms the certificate was added to the keystore.

Step 10 Import the **CA signed certificate** into the keystore file using the same alias name that was first given to the certificate key pair, as follows:

```
keytool -import -trustcacerts -alias scheduler -file icm.cer -keystore
icmservice.keystore -storepass radvision
```

The system confirms the certificate was added to the keystore. You have now created a keystore file that stores a valid certificate for use.

Step 11 Copy the `.keystore` file back to its original location.

Step 12 Restart the **RADVISION iVIEW Management Suite** service.

Step 13 Configure the JBoss application server to use HTTPS (SSL), as described in "Configuring the Application Server to Use HTTPS" on page 132.

This procedure details how to configure the JBoss application server to use HTTPS (SSL).

This solution was tested on the JBoss application server which supports Java. While secured iVIEW Management Suite communications may also function on other middleware application servers supporting Java, we recommend using JBoss for this configuration.

Before You Begin

Generate and install a certificate with unique keys, as described in "Installing Certificates with Unique Keys on the Application Server" on page 130.

Procedure

Step 1 Copy the icmservice.keystore file to:

<iVIEW Communications Manager installation directory>\jboss\server\default\conf

Step 2 Open the server.xml file, located in jboss\server\default\deploy\jbossweb.sar:

Figure 5-1 server.xml file

```
<!-- SSL/TLS Connector configuration using the admin devl guide keystore
<Connector protocol="HTTP/1.1" SSLEnabled="true"
     port="8443" address="${jboss.bind.address}"
     maxThreads="100" strategy="ms" maxHttpHeaderSize="8192"
     emptySessionPath="true"
     scheme="https" secure="true" clientAuth="false"
     keystoreFile="${jboss.server.home.dir}/conf/chap8.keystore"
     keystorePass="rmi+ssl" sslProtocol = "TLS" />
-->
<Connector port="8443" address="${jboss.bind.address}"
           maxThreads="100" minSpareThreads="5" maxSpareThreads="15"
           scheme="https" secure="true" clientAuth="false"
           keystoreFile="${jboss.server.home.dir}/conf/icmservice.keystore"
           keystorePass="radvision" keyAlias="icmservice"
           truststoreFile="${jboss.server.home.dir}/conf/icmservice.keystore"
           truststorePass="radvision"
     sslProtocol = "TLS" />
```

Step 3 Comment out the following line by adding a comment indicator at the end:

```
<!-- SSL/TLS Connector configuration using the admin devl guide keystore
```

Step 4 Locate the section beginning with this line and perform the steps below:

```
<Connector Protocol="HTTP/1.1" SSLEnabled="true"
```

a. Uncomment out this section by removing the comment indicator located after the line:

```
keystorePass="rmi+ssl" sslProtocol = "TLS" />
```

b. Change the keystore file from **chap8.keystore** to **icmservice.keystore**.

c. Change the keystorePass from rmi+ssl to `radvision`, which is the password set in "Installing Certificates with Unique Keys on the Application Server" on page 130.

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 iVIEW Communications Manager. Like port 80, port 443 is a known HTTPS port.

Step 5 Comment out the section beginning with this line by doing the following:

`<Connector port=”8443” address=”${jboss.bind.address}”`

a. Add the comment indicator before this line:

`<Connector port=”8443” address=”${jboss.bind.address}”`

b. Add the indicator marking the end of the comment after this line:

`truststorePass=“radvision” sslProtocol = “TLS” />`

The modified text should appear as follows:

Figure 5-2 Modified server.xml file

```
      <!-- SSL/TLS Connector configuration using the admin devl guide keystore     -->
      <Connector protocol="HTTP/1.1" SSLEnabled="true"
           port="8443" address="${jboss.bind.address}"
           maxThreads="100" strategy="ms" maxHttpHeaderSize="8192"
           emptySessionPath="true"
           scheme="https" secure="true" clientAuth="false"
           keystoreFile="${jboss.server.home.dir}/conf/scheduler.keystore"
           keystorePass="111111" sslProtocol = "TLS" />
<!--
      <Connector port="8443" address="${jboss.bind.address}"
                 maxThreads="100" minSpareThreads="5" maxSpareThreads="15"
                 scheme="https" secure="true" clientAuth="false"
                 keystoreFile="${jboss.server.home.dir}/conf/icmservice.keystore"
                 keystorePass="radvision" keyAlias="icmservice"
                 truststoreFile="${jboss.server.home.dir}/conf/icmservice.keystore"
                 truststorePass="radvision"
           sslProtocol = "TLS" />
-->
```

Step 6 Restart the iVIEW Management Suite service. You can now access iVIEW Management Suite from your web browser using HTTPS, as described in “Accessing iVIEW Management Suite Using HTTPS” on page 134.

Accessing iVIEW Management Suite Using HTTPS

This procedure details how to access iVIEW Management Suite from your web browser using the HTTPS protocol.

Procedure

Step 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.

Step 2 Click **Yes** to access iVIEW Communications Manager.

Step 3 Click **View Certificate** to avoid this message in future logins.

Step 4 Click **Install Certificate**.
After the certificate is installed, the user will not see the security alert on subsequent logins.

Securing Your Video Network Using TLS

You can configure your SCOPIA Solution to support Transport Layer Security (TLS) for the SIP signaling protocol.

The TLS protocol is based on a public and private keys for authorization and encryption, exchanged between iVIEW Management Suite and different components to allow an authenticated and secure connection. The public and private keys are contained in a certificate signed by a certification authority (CA) known as a CA signed certificate.

As you configure your deployment for TLS, you need to generate a certificate signed request for every component that uses TLS in your deployment and send it to your network administrator for creating a CA signed certificate. A CA has its own certificate—the CA root certificate. When the CA signed certificate is ready, you upload it into the component for which it was created, together with the CA root certificate.

In some cases, when the CA signing the certificate is not a known trusted source, you must obtain an additional certificate vouching for the trustworthiness of the CA. These certificates are known as intermediary certificates, and must be signed by a trusted CA.

Some third party components of your deployment may have pre-installed certificates. For example, you do not need to generate certificates for the Microsoft Lync Server and the Microsoft Office Communications Server.

Each time a TLS connection is established, a deployment component that starts the TLS communication session requests another component to produce its signed certificate together with the CA root certificate if not already available. After the second component verifies its identity with these certificates, a secure connection can be established. Exchanging certificates between components is part of the TLS protocol; it happens in the background and is transparent to a user.

TLS is used to secure the connection between iVIEW Management Suite and the following solution components:

- SCOPIA Video Gateway
- SCOPIA Desktop
- RADVISION SIP Gateway
- Microsoft Office Communications Server or Lync Server
- SIP endpoints

The following set of procedures create a basis for the secure connection between iVIEW Management Suite and the solution components listed above. Perform these tasks in the order listed below:

- Planning the Required Certificates for TLS ..... page 135
- Generating the Certificate Signing Request for iVIEW Management Suite..... page 141

- Generating certificate signed requests (CSR) for other deployment components, which is done via the device. For details about generating CSRs for SCOPIA Solution products, see the product's Administrator Guide.

  Skip this step for the Microsoft Lync Server and the Microsoft Office Communications Server.
- Ensuring that you have the root certificate of the certificate authority your organization uses.

  This root certificate is used for importing signed certificates into iVIEW Management Suite and other components.

- Uploading iVIEW Management Suite Certificates into iVIEW Management Suite... page 144
- Uploading Certificates for Other Devices into iVIEW Management Suite ..... page 146
- Enabling the TLS Connection in iVIEW Management Suite..... page 149

Planning the Required Certificates for TLS

When a device establishes a secure TLS connection with another component, it sends a signed certificate verifying its identity. The signature on the certificate must be from a known (trusted) certification authority (CA).

There are several types of TLS connections:

- Standard TLS, where all certificates are signed by the same CA.
- Unique CAs, where each certificate is signed by a different CA.
- Unknown gateway CA, where the gateway's certificate is signed by an unknown (untrusted) CA.
- Unknown iVIEW Management Suite CA, where iVIEW Management Suite's certificate is signed by an unknown (untrusted) CA.
- Mutually unknown CAs, where both components carry certificates signed by CAs that are unknown to each other.

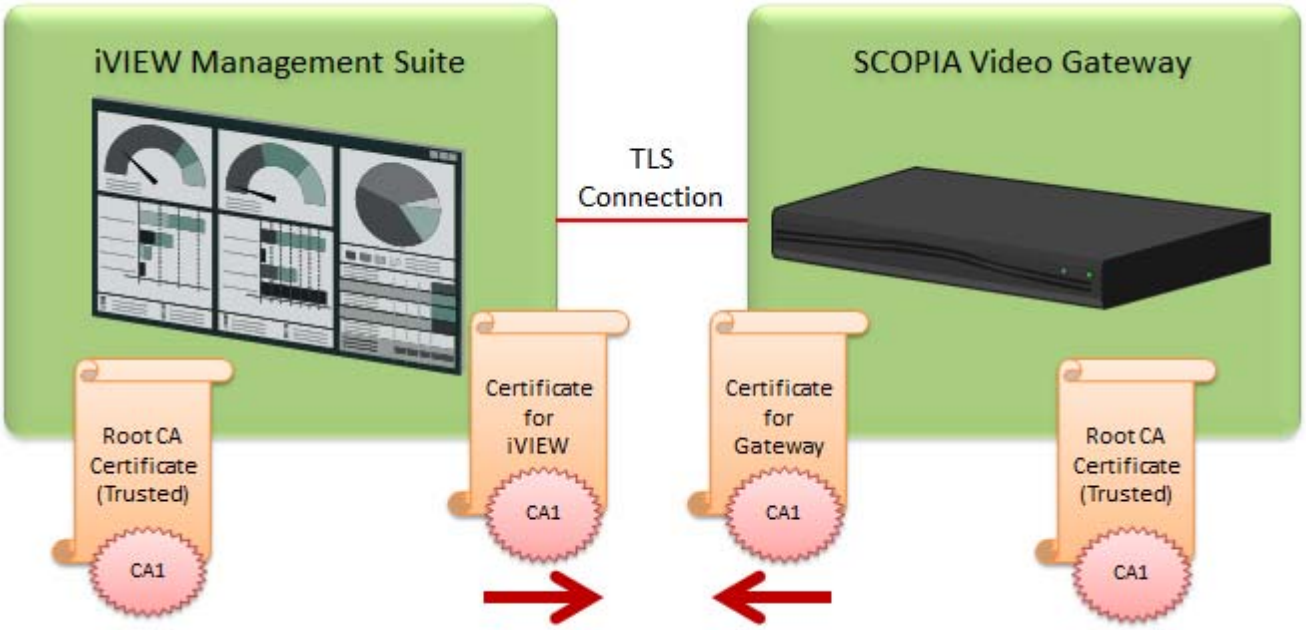
Each situation requires a different set of certificates to be uploaded to each of the components.

A CA's signature is always verified by its root certificate, which identifies the CA and is self-signed by that CA. When a device receives a certificate as part of TLS negotiations, it must verify that the CA signing the certificate is trusted, so it must have the CA's root certificate uploaded.

- **Standard TLS**

  These connections use the same CA for signing all certificates on both sides. In this case, you need to upload two certificates to iVIEW Management Suite and two for the gateway (Figure 5-3 on page 136).

Figure 5-3 Standard TLS: Component Certificates and a CA Root Certificate



Upload the following certificates to the iVIEW Management Suite:

- A certificate identifying iVIEW Management Suite, signed by the CA. This is sent to the gateway as part of the TLS negotiation.
- A root certificate verifying the CA's identity, self-signed by that CA. This is used by iVIEW Management Suite to verify the certificate sent by the gateway.

On the gateway side, upload the following certificates (Figure 5-3 on page 136):

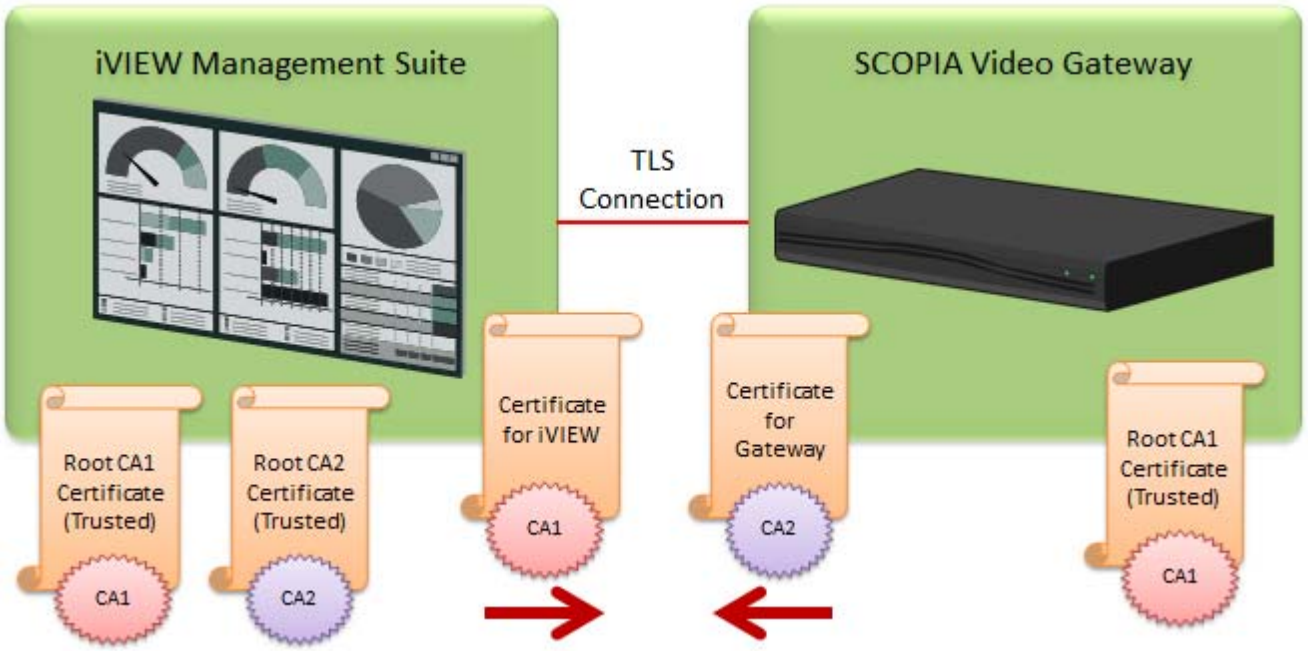
- A certificate identifying the gateway, signed by the same CA. This is sent to iVIEW Management Suite as part of the TLS negotiation.
- A copy of the root certificate verifying the CA's identity, self-signed by the CA. This is used by the gateway to verify the certificate sent by iVIEW Management Suite.

- **Unique CAs**

  When certificates are signed by different CAs, each CA requires its own root certificate to be uploaded for authentication.

  For example, in Figure 5-4 on page 137, the certificate identifying iVIEW Management Suite is signed by CA1, while the gateway's certificate is signed by CA2. This requires three certificates to be uploaded to iVIEW Management Suite and two for the gateway (Figure 5-4 on page 137).

Figure 5-4 TLS connection using certificates signed by different CAs



When each certificate is signed by a different CA (Figure 5-4 on page 137), upload the following certificates to the iVIEW Management Suite:

- A certificate identifying iVIEW Management Suite, signed by trusted CA1. This is sent to the gateway as part of the TLS negotiation.
- A root certificate from the trusted CA1 verifying CA1's identity, self-signed by CA1. This is used by iVIEW Management Suite to authenticate its certificate.
- A root certificate from the trusted CA2 verifying CA2's identity, self-signed by CA2. This is used by iVIEW Management Suite to authenticate the certificate sent by the gateway, which is signed by CA2.

On the gateway side, upload the following certificates (Figure 5-4 on page 137):

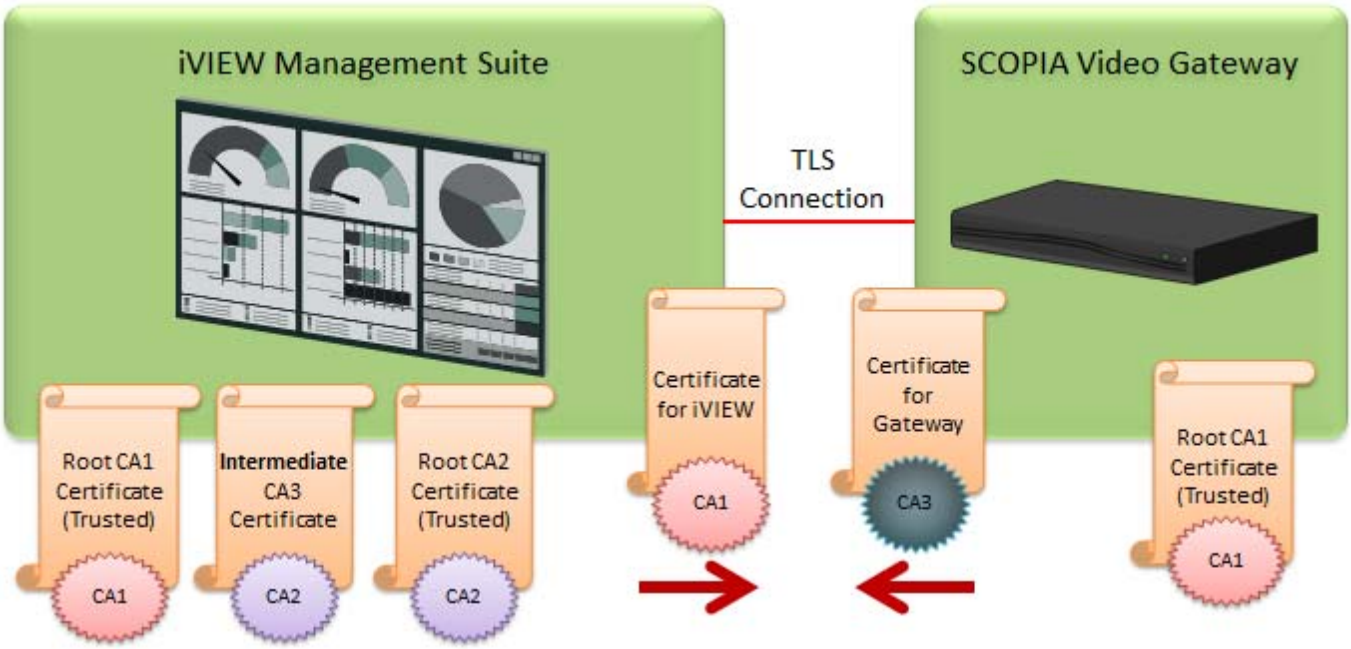
- A certificate identifying the gateway, signed by trusted CA2. This is sent to iVIEW Management Suite as part of the TLS negotiation.
- A root certificate verifying CA1's identity, self-signed by trusted CA1. This is used by the gateway to verify the certificate sent by iVIEW Management Suite, which is signed by CA1.

- **Unknown gateway CA**

  If the CA of the gateway's certificate is unknown, it cannot be trusted unless it comes with an intermediate certificate, which vouches for the trustworthiness of the unknown CA. Intermediate certificates must be signed by a trusted CA.

  For example, in Figure 5-5 on page 138, the certificate identifying the gateway is signed by CA3, which may be known and trusted by those who installed the gateway, but in this scenario CA3 is not trusted by iVIEW Management Suite. Meanwhile iVIEW Management Suite's certificate is signed by CA1, a trusted CA. This scenario requires four certificates to be uploaded to iVIEW Management Suite and two for the gateway (Figure 5-5 on page 138).

Figure 5-5 Signature of Gateway Certificate from Unknown CA



When CA3 is untrusted (Figure 5-5 on page 138), the certificates to upload to the iVIEW Management Suite are:

- A certificate identifying iVIEW Management Suite, signed by trusted CA1. This is sent to the gateway as part of the TLS negotiation.
- A root certificate from CA1 verifying CA1's identity, self-signed by trusted CA1. This is used by iVIEW Management Suite to authenticate its certificate.
- An intermediate certificate vouching for the trustworthiness of CA3, signed by trusted CA2. This is used to trust the certificate sent by the gateway, which is signed by CA3.
- A root certificate from CA2 verifying CA2's identity, self-signed by trusted CA2. This is used by iVIEW Management Suite to authenticate the intermediate certificate, which is signed by CA2.

On the gateway side, the certificates to be uploaded are (Figure 5-5 on page 138):

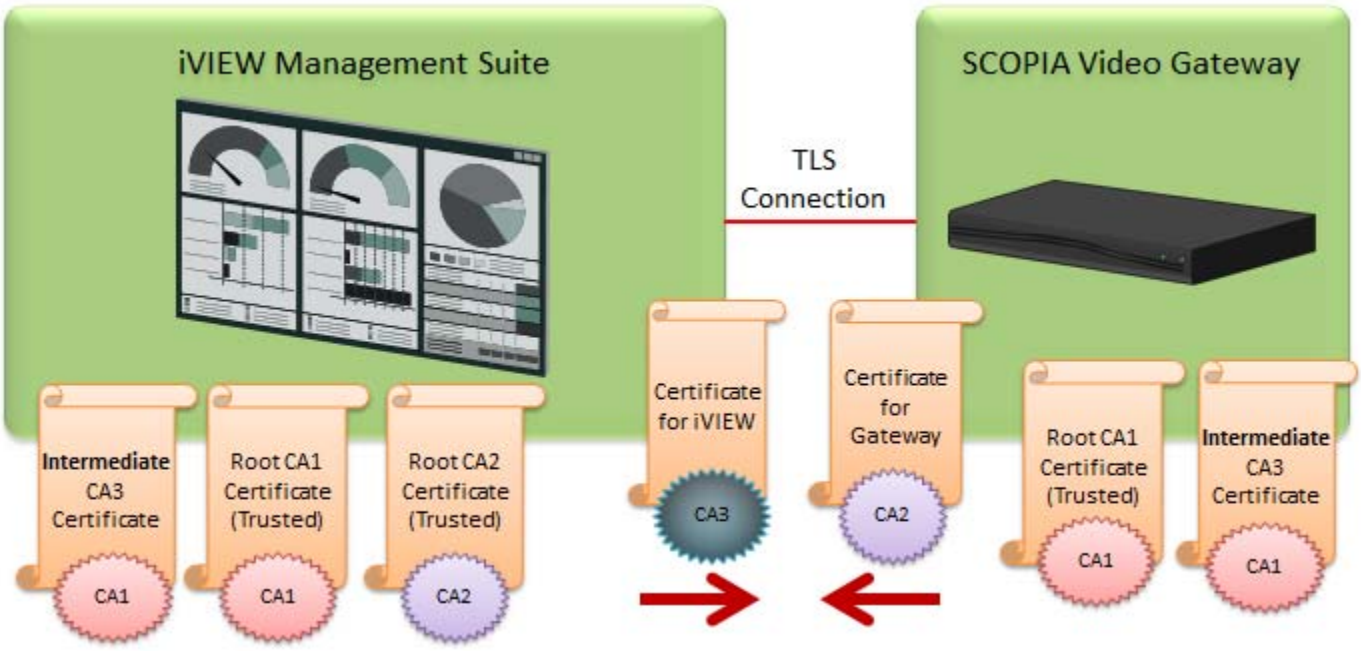
- A certificate identifying the gateway, signed by CA3, an unknown CA. This certificate is sent to iVIEW Management Suite as part of the TLS negotiation.
- A root certificate from CA1 verifying CA1's identity, self-signed by trusted CA1. This is used by the gateway to verify the certificate sent by iVIEW Management Suite, which is signed by CA1.

- **Unknown iVIEW Management Suite CA**

  When iVIEW Management Suite's certificate is signed by a CA unknown to the gateway, you must upload an intermediate certificate for the untrusted CA signed by a trusted CA to vouch for its authenticity.

  In the example of Figure 5-6 on page 139, iVIEW Management Suite's certificate is signed by CA3, an unknown CA, while the gateway's certificate is signed by CA2, a trusted CA. This requires four certificates to be uploaded to iVIEW Management Suite and three for the gateway (Figure 5-6 on page 139).

Figure 5-6 Signature of iVIEW Management Suite Certificate from Unknown CA



When CA3 is untrusted by the gateway (Figure 5-6 on page 139), the certificates to upload to the iVIEW Management Suite are:

- A certificate identifying iVIEW Management Suite, signed by CA3, a CA unknown to the gateway. This is sent to the gateway as part of the TLS negotiation.
- An intermediate certificate vouching for the trustworthiness of CA3, signed by trusted CA1. This is used to trust iVIEW Management Suite's identity certificate, which is signed by CA3.
- A root certificate from CA1 verifying CA1's identity, self-signed by trusted CA1. This is used by iVIEW Management Suite to authenticate the intermediate certificate, which was signed by CA1.
- A root certificate from CA2 verifying CA2's identity, self-signed by trusted CA2. This is used by iVIEW Management Suite to authenticate the gateway's certificate, which is signed by CA2.

On the gateway side, the certificates to be uploaded are (Figure 5-6 on page 139):

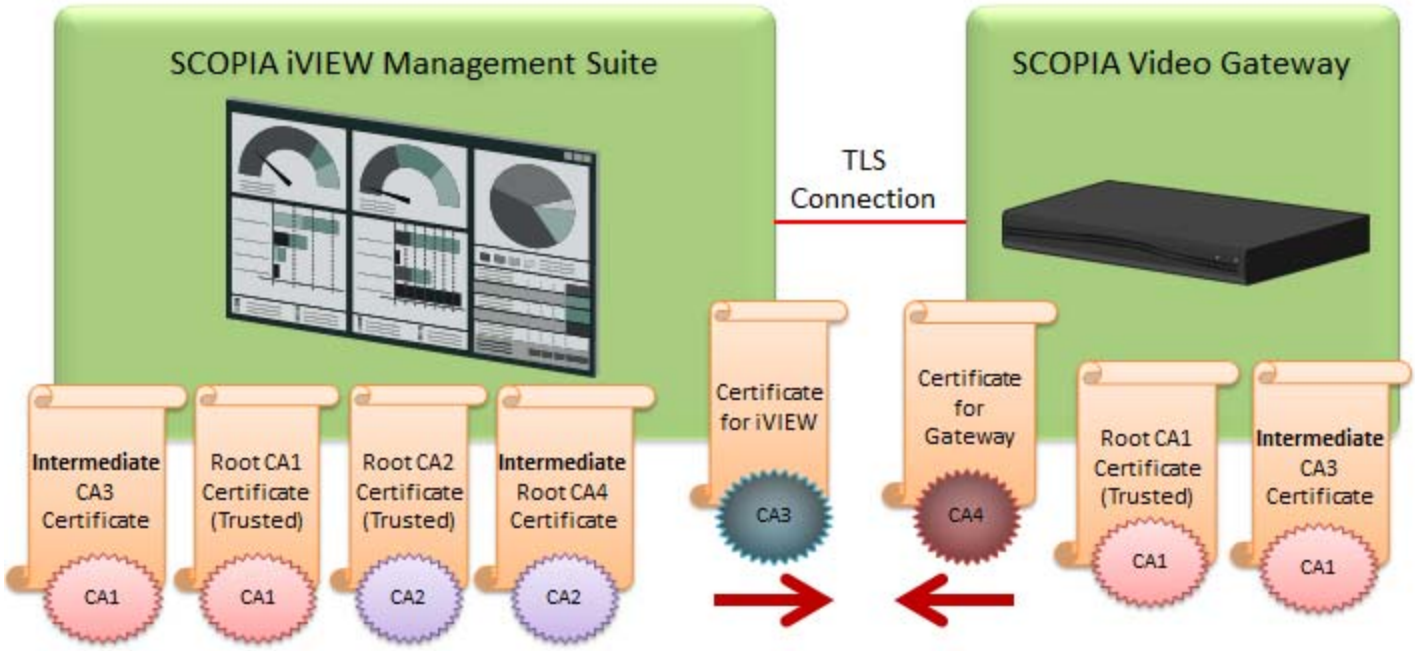
- A certificate identifying the gateway, signed by trusted CA2. This certificate is sent to iVIEW Management Suite as part of the TLS negotiation.
- An intermediate certificate vouching for the trustworthiness of CA3, signed by trusted CA1. This is used to trust iVIEW Management Suite's identity certificate, which is signed by CA3.
- A root certificate from CA1 verifying CA1's identity, self-signed by trusted CA1. This is used by the gateway to verify the intermediate certificate, which is signed by CA1.

- **Mutually unknown CAs**

  In the final scenario, both components use certificates signed by CA's which are not recognized by each other. In this case, there needs to be two intermediate certificates, one for each of the untrusted CAs, to vouch for their authenticity.

  For example, in Figure 5-7 on page 140, the certificate identifying the gateway is signed by CA4, an unknown CA, while iVIEW Management Suite's certificate is signed by CA3, also untrusted. This would require five certificates to be uploaded to iVIEW Management Suite and three for the gateway (Figure 5-7 on page 140).

Figure 5-7 Signature of Both Certificates are from Untrusted CAs



When CA3 is untrusted by the gateway and CA4 is untrusted by iVIEW Management Suite(Figure 5-6 on page 139), the certificates to upload to the iVIEW Management Suite are:

- A certificate identifying iVIEW Management Suite, signed by CA3, a CA unknown to the gateway. This is sent to the gateway as part of the TLS negotiation.
- An intermediate certificate vouching for the trustworthiness of CA3, signed by trusted CA1. This is used to trust iVIEW Management Suite's identity certificate, which is signed by CA3.

- A root certificate from CA1 verifying CA1's identity, self-signed by trusted CA1. This is used by iVIEW Management Suite to authenticate CA3's intermediate certificate, which was signed by CA1.
- A root certificate from CA2 verifying CA2's identity, self-signed by trusted CA2. This is used by iVIEW Management Suite to authenticate CA4's intermediate certificate, which is signed by CA2.
- An intermediate certificate vouching for the trustworthiness of CA4, signed by trusted CA2. This is used to trust the gateway's identity certificate, which is signed by CA4.

On the gateway side, the certificates to be uploaded are (Figure 5-6 on page 139):

- A certificate identifying the gateway, signed by CA4, a CA unknown to iVIEW Management Suite. This is sent to iVIEW Management Suite as part of the TLS negotiation.
- An intermediate certificate vouching for the trustworthiness of CA3, signed by trusted CA1. This is used to trust iVIEW Management Suite's identity certificate, which is signed by CA3.
- A root certificate from CA1 verifying CA1's identity, self-signed by trusted CA1. This is used by the gateway to verify the intermediate certificate, which is signed by CA1.

For more information on uploading certificates to the gateway and to iVIEW Management Suite, see "Securing Your Video Network Using TLS" on page 134.

Generating the Certificate Signing Request for iVIEW Management Suite

This section details how to generate a certificate signing request for iVIEW Management Suite, that must be signed by a CA using a certificate authority (CA) application.

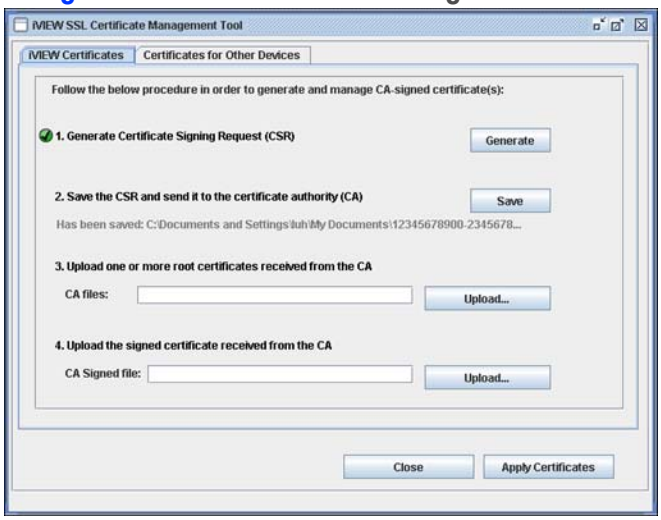
Once properly signed, the certificate would confirm the identity of iVIEW Management Suite to other components in the network, and can also facilitate encrypted communications with other components.

Procedure

Step 1 Navigate to **Start > All Programs > RADVISION iVIEW Management Suite > Certificates Management**. The Certificate Management Tool is displayed.

Step 2 Select the **iVIEW Certificates** tab.

Figure 5-8 Certificate Management Tool



Step 3 Select **Generate**. The Generate CSR window is displayed.

Figure 5-9 Certificate Signing Request

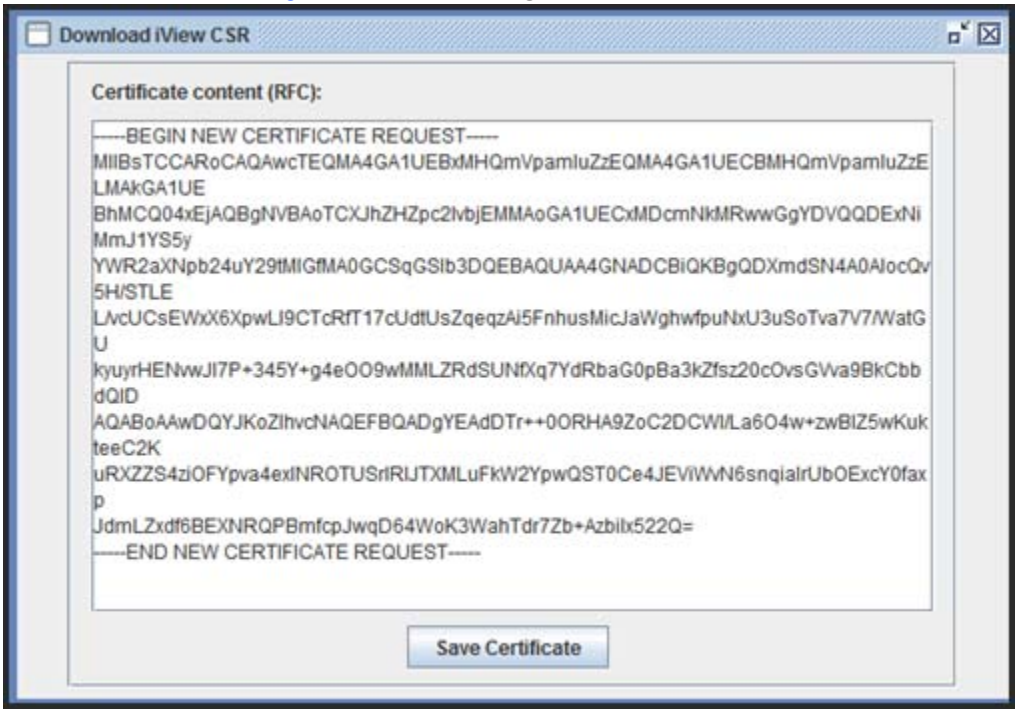


Step 4 Enter details as required. The **Common Name** must be FQDN of iVIEW Manager Server/SIP server: rvcn-iview-7201.radvision.com. For a redundancy deployment, the common name must be the public virtual FQDN. The **Country code** must include two characters.

Step 5 Select **Generate Certificate Signing Request (CSR)**.

Step 6 Select **Save** to view the certificate content. The certificate content is displayed in the Download iView CSR window.

Figure 5-10 Saving the Certificate



Step 7 Select **Save Certificate**. Choose an appropriate folder and file name when saving the certificate. The certificate is saved as a text file compatible with Base-64 ASCII code.

Step 8 Send the text file containing the certificate for signing as a certificate compatible with Base-64 ASCII code. We recommend to use the same CA for both the CSR and the Lync Server certificate.

Note: It is very important that the certificate is signed as a certificate compatible with Base-64 ASCII code.

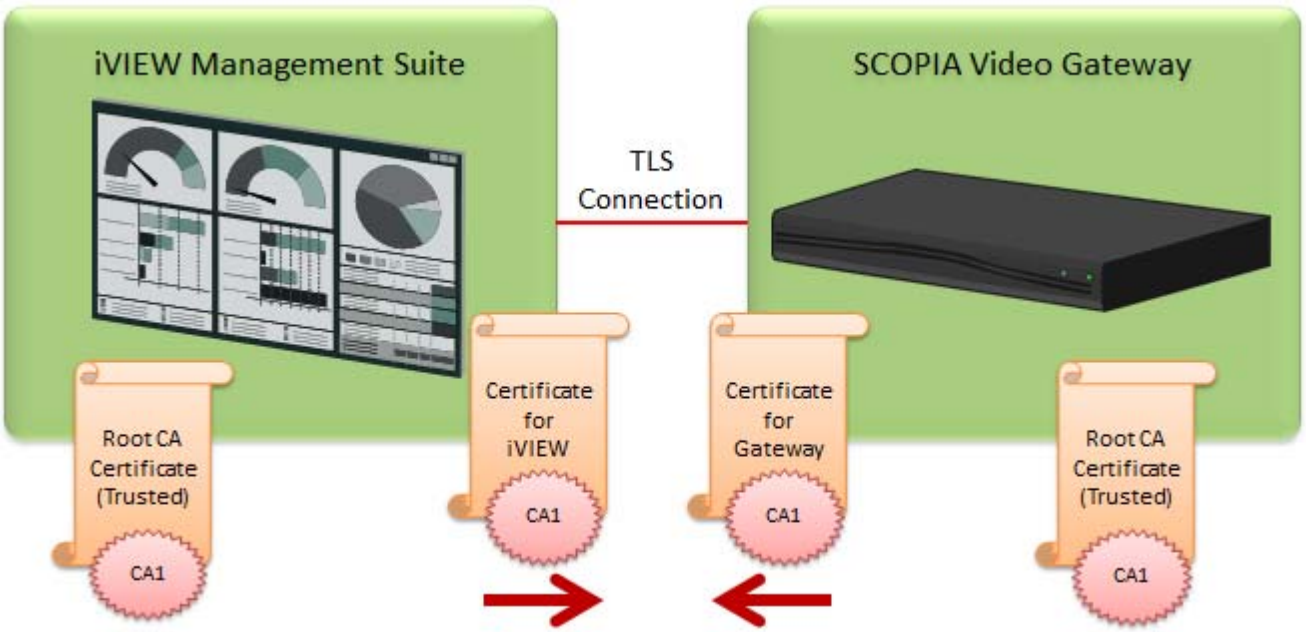
If other components communicating with iVIEW Management Suite also have their own certificates, we recommend using a common CA for all certificates for a more efficient implementation.

Select **Web Server** as the certificate template when submitting a certificate request or renewal request.

This procedure describes how to upload certificates that confirm the identity of iVIEW Management Suite. To upload certificates that confirm the identity of other SCOPIA Solution and third-party devices, see "Uploading Certificates for Other Devices into iVIEW Management Suite" on page 146.

In most TLS connections, iVIEW Management Suite requires two certificates to be uploaded: a signed certificate identifying iVIEW Management Suite signed by a certification authority (CA) and that CA's root certificate (Figure 5-11 on page 144). Each time a deployment component tries to establish a new TLS session with iVIEW Management Suite, it sends its identity certificate to the component to establish a secure connection (Figure 5-11 on page 144).

Figure 5-11 Typical TLS communication with a gateway



However, if the component certificates are signed by a different CA than iVIEW Management Suite's certificate, you may need to upload more certificates to establish authenticity. For more information, see "Planning the Required Certificates for TLS" on page 135.

You need to perform this procedure after you have the signed certificate from the CA for iVIEW Management Suite.

Before You Begin

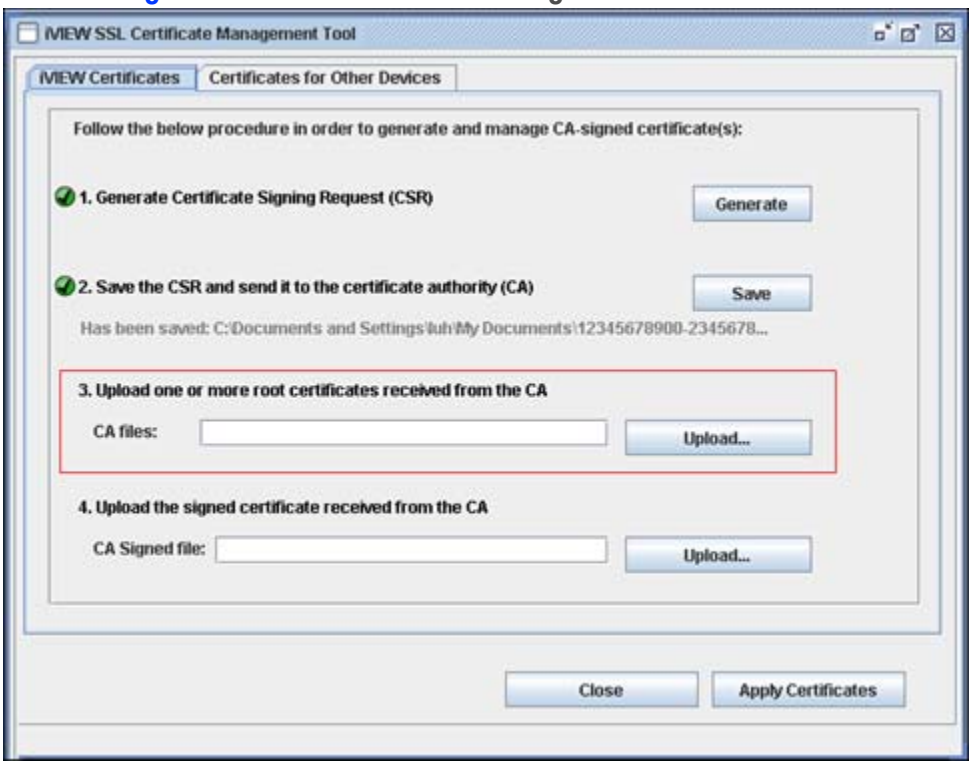
1. Ensure that you have the root certificate for the certificate authority that your organization uses. The root certificate must be compatible with the Base-64 ASCII code.
2. Ensure that you have the signed certificate for the iVIEW Management Suite.

Procedure

Step 1 Copy the CA root certificate and the CA signed certificate that confirm the identity of iVIEW Management Suite into the iVIEW Management Suite server.

Step 2 Open the iVIEW Management Suite Certificates Management tool.

Figure 5-12 Certificate Management Tool window

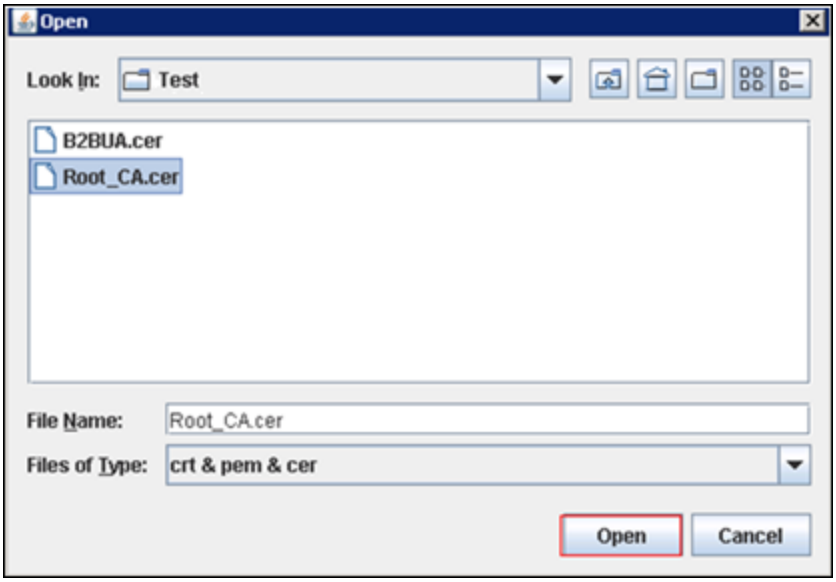


Step 3 Upload the CA root certificate, including intermediate certificates, into iVIEW Management Suite:

a. Select **Upload** next to the CA files.

The Open window is displayed.

Figure 5-13 Open window



b. Browse and select the CA root and intermediate certificates. You can select multiple certificates by holding the **Ctrl** key as you select.

c. Select **Open**. Verify that the upload success message is displayed.

The CA root and intermediate certificates are uploaded into iVIEW Management Suite.

Step 4 Upload the CA signed certificate into iVIEW Management Suite:

a. Select **Upload** next to the CA Signed file.

The Open window is displayed. See Figure 5-13 on page 146.

b. Browse and select the CA signed certificate.

c. Select **Open**. Verify that the upload success message is displayed.

The CA signed certificate is uploaded into iVIEW Management Suite.

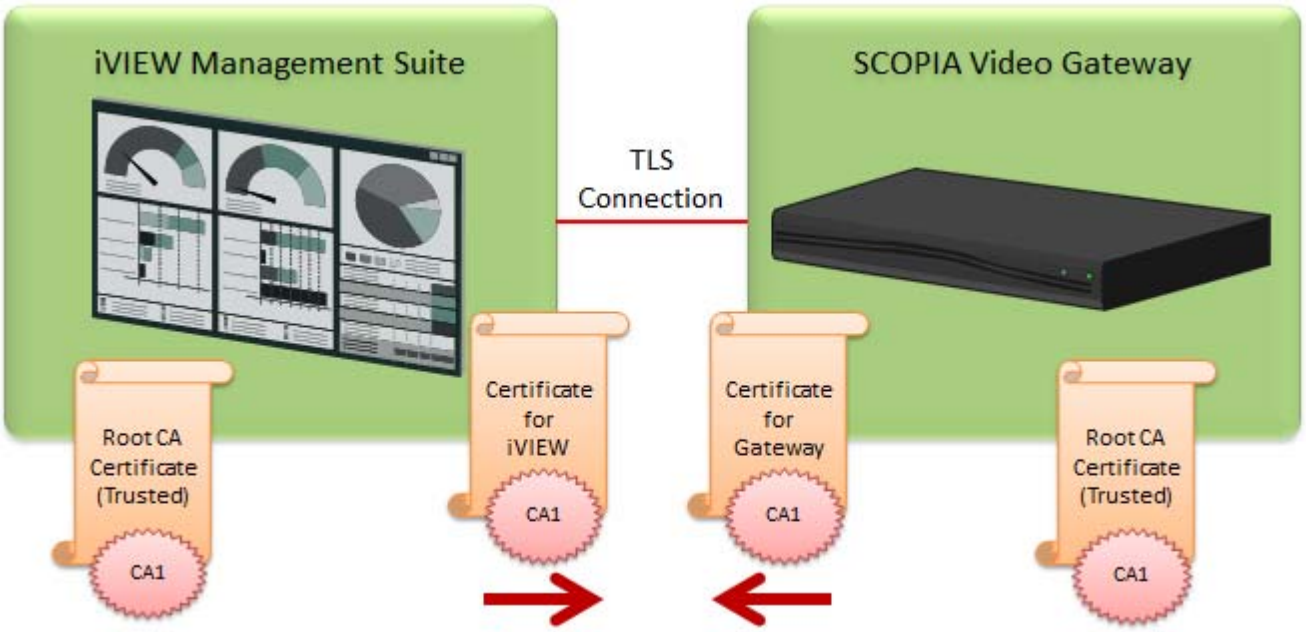
Step 5 Select **Apply Certificates**.
The iVIEW Management Suite service is automatically restarted.

Uploading Certificates for Other Devices into iVIEW Management Suite

This procedure describes how to upload certificates to iVIEW Management Suite for all devices in your deployment, except for the certificates which confirm the identity of iVIEW Management Suite itself. To upload certificates which identify iVIEW Management Suite itself, see "Uploading iVIEW Management Suite Certificates into iVIEW Management Suite" on page 144.

For most TLS connections, you need to upload the device's CA root certificate (Figure 5-14). Each time a deployment component tries to establish a new TLS session with iVIEW Management Suite, it sends its identity certificate to the component to establish a secure connection (Figure 5-14).

Figure 5-14 Typical TLS communication with a gateway



However, if the component certificates are signed by a different CA than iVIEW Management Suite's certificate, you may need to upload more certificates to establish authenticity. For more information, see "Planning the Required Certificates for TLS" on page 135.

You need to perform this procedure after you generate the CSR for the deployment component, which is done via the device. For details about generating CSRs for SCOPIA Solution products, see the product's Administrator Guide.

Before You Begin

Ensure that you have the root certificate, including all intermediate certificates, for the certificate authority that your organization uses to identify the device. The root certificate must be compatible with the Base-64 ASCII code.

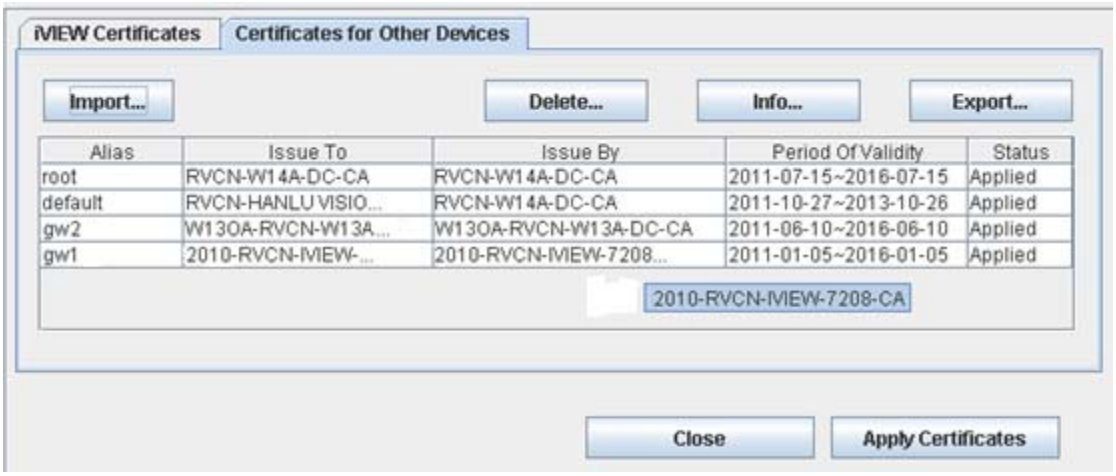
Procedure

Step 1 Copy the CA root (and intermediate, if relevant) certificate that confirms the identity of the device into the iVIEW Management Suite server.

Step 2 Open the iVIEW Management Suite Certificates Management tool.

Step 3 Select the **Certificates for Other Devices** tab (Figure 5-15 on page 148).

Figure 5-15 Certificates for Other Devices tab

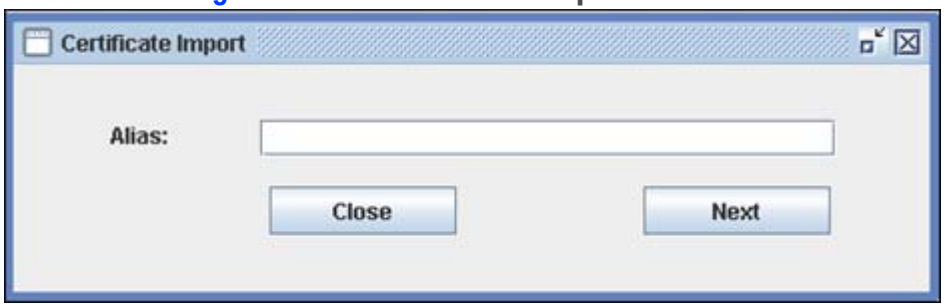


Step 4 Upload the CA root certificates, including intermediate certificates, into iVIEW Management Suite:

a. Select **Import**.

The Certificate Import window is displayed (Figure 5-16 on page 148).

Figure 5-16 Certificate Import window



b. Type an internal name for the certificate (for easy identification) in the **Alias** field.

c. Select **Next** and browse to the CA root certificate.

d. Select **Open**.

e. Repeat steps a--d for other CA root and intermediate certificates, if relevant.

f. Select **Apply Certificates**.

g. Select **OK** in the success message.
The CA root and intermediate certificates are uploaded into iVIEW Management Suite. The iVIEW Management Suite service is automatically restarted.

You can configure your iVIEW Management Suite to use the TLS connection by modifying the configuration of the B2BUA component of the iVIEW Management Suite.

Perform this procedure only if you want to secure your video network using TLS.

Procedure

Step 1 If the TLS connection is with the SCOPIA Video Gateway, configure the device to TLS signaling as explained in "Adding and Configuring a SCOPIA Video Gateway in iVIEW Management Suite" on page 40.

> **Note:** Each SCOPIA Video Gateway in the video network has its own configuration that is saved in iVIEW Management Suite.

Step 2 If the TLS connection is with the RADVISION SIP Gateway, configure the SIP Gateway to TLS signaling as explained in "Adding and Configuring SIP Gateway in iVIEW Management Suite" on page 44.

> **Note:** Each SIP Gateway in the video network has its own configuration that is saved in iVIEW Management Suite.

Step 3 Navigate to *C:\Program Files\RADVISION\iVIEW Suite\iCM\sipserver\conf*.

Step 4 Open the *UpdatedSIPConfig.xml* file in a text editor.

Step 5 Configure FQDN of the B2BUA component by setting the value the <B2bFQDN> element as shown in Figure 5-17. In a redundancy environment, add the FQDN of the public virtual IP address. In a standalone environment, this is automatically added.

Figure 5-17 Adding the B2bFQDN element

```
<SipServerConfiguration>
     <SIPStack>
          <Network>
          <LocalTcpAddressList>127.0.0.1:5060</LocalTcpAddressList>
          <LocalUdpAddressList>127.0.0.1:5060</LocalUdpAddressList>
          <LocalTlsAddressList>127.0.0.1:5061</LocalTlsAddressList>
          <B2bFQDN>rvcndev.radvision.com</B2bFQDN>
          </Network>
          <Stack>
```

Step 6 Configure the DNS of the B2BUA component by setting values in the entire <DNSServerList> element as shown in Figure 5-18:

Figure 5-18 Adding the <DNSServerList> element

```
        <Stack>
                <StackTcpEnabled>true</StackTcpEnabled>
                <StackSendReceiveBufferSize>10000</StackSendReceiveBufferSize>
                <StackTLSEnabled>true</StackTLSEnabled>
                <StackNumOfTlsEngines>2</StackNumOfTlsEngines>
                <StackMaxTlsSessions>1000</StackMaxTlsSessions>
                <TLSMethod>TLS_V1</TLSMethod>
        </Stack>
        <DNSServerList>
                <DNSServerIP>192.168.227.233</DNSServerIP>
                <DNSServerIP>192.168.227.253</DNSServerIP>
                <DNSServerIP>192.168.225.1</DNSServerIP>
        </DNSServerList>
</SIPStack>
```

Step 7 Save and close the file.

Step 8 Start the iVIEW Management Suite service and the iVIEW Management Suite SIP service.

6 Real-time Monitoring

You can monitor and manage the bandwidth used by video communications across the entire network. You can configure iVIEW Management Suite to generate and forward alerts when bandwidth usage exceeds a given threshold.

- Managing iVIEW Management Suite Traps ..... page 151
- Monitoring Network Devices ..... page 156
- Monitoring Device Usage and Utilization ..... page 162
- Monitoring Meetings, Calls and Conferences ..... page 165

Managing iVIEW Management Suite Traps

iVIEW Management Suite can be configured to receive traps from managed devices, and to forward this traps to external servers.

- Configuring iVIEW Management Suite to Receive Traps from Network Devices ... page 151
- How to Configure iVIEW to Forward Traps to a Specific Address ..... page 152
- How to Send Alerts to a Specific User ..... page 154

Configuring iVIEW Management Suite to Receive Traps from Network Devices

You can configure iVIEW Management Suite to get traps from managed devices, and provide events and alarms management.

Procedure

Step 1 Log in to iVIEW Network Manager.

Step 2 Select **Settings** in the sidebar menu.

Step 3 Select **Traps**.

Step 4 Select **Receive traps from elements**.

Step 5 Select **Upload** to save your changes.

How to Configure iVIEW to Forward Traps to a Specific Address

Once iVIEW Management Suite is configured to get traps from managed devices, you can configure forwarding rules so iVIEW Management Suite will forward traps from specific devices to an external server, for monitoring reasons.

- Creating or Modifying a Trap Forwarding Rule ..... page 152
- Disabling a Trap Forwarding Rule..... page 153
- Removing a Trap Forwarding Rule..... page 154

Creating or Modifying a Trap Forwarding Rule

You can instruct iVIEW Management Suite to forward traps received from managed devices to an address specified by a trap forwarding rule.

You can also enable SNMP version 3 support to add privacy, authentication and access control to SNMP traps before forwarding them to the trap server.

Procedure

Step 1 Log in to iVIEW Network Manager.

Step 2 Select **Settings** in the sidebar menu.

Step 3 Select **Traps**.

Step 4 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 select **Edit**.
- Right-click the trap rule you require and select **Edit**.

Step 5 Do one of the following to create a new trap forwarding rule:

- Select **Add**.
- Right-click any trap rule and select **Add**.

Step 6 Enter a description in the **Description** field.

Step 7 Specify the IP address and port number for iVIEW Network Manager to forward traps received from managed elements.

Step 8 Select **Enable trap forwarding**.

Step 9 (Optional) Select **Enable SNMP v3** to add security attributes to SNMP traps, and select a security level.

Note: You can select this option only after selecting the **Enable trap forwarding** option.

- Low—No Authentication or Privacy
- Medium—Authentication without Privacy
- High—Authentication with Privacy

Step 10 (For Medium or High security only) Enter a user name and password for authentication of SNMP trap messages.

Step 11 (For Medium or High security only) Select a protocol for authentication of SNMP trap messages.

The default protocol is MD5.

Step 12 (For High security only) Enter a privacy password for encryption of SNMP trap messages.

Step 13 (For High security only) Select a privacy protocol for encryption of SNMP trap messages.

The default protocol is DES (56-bit).

Step 14 Select **OK** to save your changes.

Disabling a Trap Forwarding Rule

You can disable rules that are temporarily not in use. These rules will remain in the database and can be enabled at any time.

Procedure

Step 1 Log in to iVIEW Network Manager.

Step 2 Select **Settings** in the sidebar menu.

Step 3 Select **Traps**.

Step 4 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 select **Edit**.
- Right-click the trap rule you require and select **Edit**.

Step 5 Deselect **Enable trap forwarding**.

Step 6 Select **OK** to save your changes.
The trap forwarding rule is disabled but remains in the database.

Removing a Trap Forwarding Rule

You can delete rules that are no longer in use. Deleted rules are removed from the database.

Procedure

Step 1 Log in to iVIEW Network Manager.

Step 2 Select **Settings** in the sidebar menu.

Step 3 Select **Traps**.

Step 4 Do one of the following:

- Select the trap rule you require and select **Delete**.
- Right-select the trap rule you require and select **Delete**.

Step 5 Select **OK** to save your changes.
The trap forwarding rule is removed from the database.

How to Send Alerts to a Specific User

You can configure iVIEW Management Suite to send emails to specific users, with notifications of alarms and events registered by the system. You can define a network subset that comprises some of the network devices, for example, you can have a network subset comprised of all MCUs defined in the network. iVIEW Management Suite will then send notifications in an email format with these network subset traps. You can also define the minimum severity level, for example, you can define that notifications are sent only for critical alarms and events.

- Creating or Modifying an Alert Recipient Profile ..... page 154
- Defining Network Subsets ..... page 155
- Removing an Alert Recipient Profile ..... page 156

Creating or Modifying an Alert Recipient Profile

You can define a recipient for email notifications sent by iVIEW Management Suite regarding traps from a specified network subset.

Procedure

Step 1 Log in to iVIEW Network Manager.

Step 2 Select **Settings** in the sidebar menu.

Step 3 Select **Alert Recipients**.

Step 4 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 select **Edit**.
- Right-click the alert recipient you require in the Recipient Name column and select **Edit**.

Step 5 Do one of the following to create a new alert recipient profile:

- Select **Add**.
- Right-click any link in the Recipient Name column and select **Add**.

Step 6 Enter the name and email of the alert recipient in the relevant fields.

Step 7 Select the 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.

Step 8 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.

Step 9 (Optional) Select **Notify on alarms clearing** to enable the alarm recipient to receive an error report via email when the alarms have been cleared.

Step 10 (Optional) Select **Use custom subject line** to include a custom subject line in the email and enter a string for the custom subject line.

Step 11 (Optional) Select **Include element info** to include details of the elements reported in the alerts in the custom subject line.

Step 12 Select **Enable alert** to activate the recipient.

Step 13 Select **OK** to save your changes.

Defining Network Subsets

You can define subsets of the network and restrict users with specific profiles to control and monitor certain network areas. The administrator can define network subsets by creating criteria to include or exclude certain offices or branches, and network devices.

Procedure

Step 1 Log in to iVIEW Network Manager.

Step 2 Select **Settings** in the sidebar menu.

Step 3 Select the **Network Subsets** tab.

Step 4 Select **Add** or right-click an existing network subset and select **Add**.

Step 5 Enter a name for the network subset.

A subset contains all devices which match at least one include criterion but do not match any exclude criterion.

Step 6 Select **Add** to create a new include or exclude criterion.

Step 7 Select a zone (office or branch) and a network device in the relevant fields, and indicate whether or not child zones of the specified zone are contained in the criterion.

Step 8 Select **OK** to add the criterion to the relevant list in the Add Network Subset window.

Step 9 Select **OK** to save your changes.

Removing an Alert Recipient Profile

You can remove a recipient defined to receive notifications about traps.

Procedure

Step 1 Log in to iVIEW Network Manager.

Step 2 Select **Settings** in the sidebar menu.

Step 3 Select **Alert Recipients**.

Step 4 Do one of the following:

- Select the alert recipient you require and select **Delete**.
- Right-select the alert recipient you require in the Recipient Name column and select **Delete**.

Step 5 Select **OK** to save your changes.
The alert recipient profile is removed from the database.

Monitoring Network Devices

You can use the iVIEW Network Manager to monitor the functionality of devices, alarms and events, within your network, and you can use the iVIEW Communications Manager to monitor bandwidth usage and port availability for the videoconferencing network resources.

- About Management Status of Network Devices ..... page 157
- About iVIEW Management Suite Monitoring Views ..... page 158
- Creating your own Monitoring View ..... page 160
- Monitoring Network Events ..... page 160
- Monitoring Network Alarms ..... page 161
- Changing the Severity Level of Alarms ..... page 162

About Management Status of Network Devices

The SCOPIA 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 SCOPIA iVIEW Network Manager database.

Table 6-1Describes the different types of network devices management status.

Table 6-1 Network Devices Management Status

Element Status	Description
Managed	The element exists in the SCOPIA iVIEW Network Manager database and provides monitoring information and access to configuration settings.
Inferred	The element does not exist in the SCOPIA iVIEW Network Manager database, but it might appear as an inferred element because a managed element refers to that element. For example, a gatekeeper is inferred when a managed element is registered to that gatekeeper zone, but the gatekeeper is not managed by the SCOPIA iVIEW Network Manager.
Unmanaged	The element exists in the SCOPIA iVIEW Network Manager database but has no open communication channels with the SCOPIA iVIEW Network Manager and provides no monitoring information or access to configuration settings. An element might be unmanaged when the SCOPIA iVIEW Network Manager license limitations have been exceeded or when the user manually sets the element as unmanaged.

About iVIEW Management Suite Monitoring Views

iVIEW Management Suite provides monitoring of network devices in three different ways:

- Network Tree

  The Network Tree allows you to monitor network devices on a network level, on a location level or on a device level, according to the selected element from the tree. Information available for each level is organized in tabs.

  Any element listed in the Network 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 it. 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.

- Network Table

  The Network Table view allows you to monitor the status of network devices. The following information is displayed in the table:

  - Element status, indicated by an icon, as follows:

    Online

    Unmanaged

    Offline

    Faulty

    Warning

    Information

- Element type (MCU, gatekeeper and so on)
- Element name (acts as a link to its element manager)
- Management IP address
- Version number
- Location (office or branch)
- Traffic usage versus capacity

- Network Map

  The Network Map provides a graphical illustration of the network, with a snapshot of the following parameters:

  - 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

  Each square displayed in the Network Map represents either the network root, a zone (or user-defined folder) or a single element. Inter-zone bandwidth information appears above the zones when relevant.

Procedure

Step 1 Log in to NMS.

Step 2 Select **Network Tree**, **Network Table** or **Network Map** in the sidebar menu.

Creating your own Monitoring View

You can create and monitor your own tree structure according to criteria you define, such as the physical location or other customer-specific criteria. Once you have your customized network tree, you can monitor the devices on a network level.

Procedure

Step 1 Select **Network Tree** in the sidebar menu.

Step 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**.

Step 3 Enter a name for the new tree view and select **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.

Step 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**.

Step 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-select the tree view. To rename or remove folders, right-select the folder and select the relevant option.

Monitoring Network Events

You can monitor events reported by the system for the entire network and for specific network devices. You can sort the list of events according to severity, event time, event message and element, and filter traps by severity and time interval.

Procedure

Step 1 Log in to iVIEW Network Manager.

Step 2 To monitor events on a network level, do one of the following:

- Select **Alarms** from the sidebar menu.
- Select **Network Tree**, and select the Network icon from the tree view.

Step 3 To monitor events of a specific network device, select **Network Tree**, and select the network device you want to monitor events.

Step 4 Select the **Events** tab.

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.

Step 5 Select the column headings in the alarms table to sort the information displayed.

Step 6 (Optional) To filter the events displayed by date and severity level, do one of the following:

- Select **View** > **Filter events**.
- Select the **Current filter** link above the table.

Monitoring Network Alarms

The Alarms tab enables you to view and sort the alarms generated by the devices in the network according to alarm status, alarm message, date and time or element. Alarms can be viewed per network device, network zone (office or branch) or the entire network.

Procedure

Step 1 Log in to iVIEW Network Manager.

Step 2 To view alarms on a network level, do one of the following:

- Select **Alarms** from the sidebar menu.
- Select **Network Tree**, and select the Network icon from the tree view.

Step 3 To view alarms of a specific network device, select **Network Tree**, and select the network device you want to monitor alarms.

Step 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

Step 5 Double-select any network device in the table to display the relevant device manager for that device.

Changing the Severity Level of Alarms

You can modify the severity level of alarms generated by the system, and create events for a specific alarm.

Procedure

Step 1 Log in to iVIEW Network Manager.

Step 2 Select **Settings** in the sidebar menu.

Step 3 Select **Alarms**.

Step 4 Do one of the following to modify an alarm generated by the managed devices in the network:

- Double-select the alarm you require.
- Select the alarm you require and select **Edit**.
- Right-select the alarm you require and select **Edit**.

Step 5 Modify the severity level, and enable or disable the alarm in the relevant fields.

Step 6 Select **Create event for this alarm** to instruct iVIEW Network Manager to create a report at **Alarms** > **Events** every time this alarm occurs.

Step 7 Use the **Apply to all users** option to indicate whether the alarm properties apply only to the current user or to all users.

Step 8 Select **OK** to save your changes.

Monitoring Device Usage and Utilization

This section if for service providers only.

Service providers can manage resources by monitoring devices performance and ports availability of for different meeting types.

- Monitoring Device Usage and Failure by Time Interval ..... page 162
- Monitoring Device Usage and Failure Statistics ..... page 163
- Monitoring MCU Availability for a Meeting Type ..... page 164

Monitoring Device Usage and Failure by Time Interval

This section is available for service providers only.

You can view device usage by monitoring the total number of meetings scheduled, and the number of failed meetings for all MCUs and gatekeepers configured in iVIEW Management Suite during a designated time period (the default time interval is one hour).

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **Device Monitoring** in the sidebar menu.

Step 3 Select **Performance Monitor**.

Table 6-2 describes the information displayed on the Performance Monitor tab.

Table 6-2 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 iVIEW Communications Manager.
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 iVIEW Communications Manager.
% 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 iVIEW Communications Manager.
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 iVIEW Communications Manager.
% Failed Connections	Displays the number of failed connections divided by the total number of connections.

Step 4 To create a new report, select the period of time to be displayed in the report.

Step 5 Select **Display** to view the report, or **Generate Report**, to view the report in an Excel format.

Monitoring Device Usage and Failure Statistics

This report is available for service providers only.

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

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **Device Monitoring** in the sidebar menu.

Step 3 Select **Statistics**.

Table 6-3 describes the information displayed on the Statistics tab.

Table 6-3 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 iVIEW Communications Manager. 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 iVIEW Communications Manager. 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 iVIEW Communications Manager. 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 iVIEW Communications Manager. Gatekeeper information is not displayed.

Step 4 To create a new report, select the period of time to be displayed in the report.

Step 5 Select **Display** to view the report, or **Generate Report**, to view the report in an Excel format.

Monitoring MCU Availability for a Meeting Type

This report is available for service providers only.

You can view MCU availability for a specific meeting type during a designated time period.

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **Device Monitoring** in the sidebar menu.

Step 3 Select **Resource Availability**.

Step 4 Select a meeting type and a starting date.

Step 5 Select **Previous** or **Next** to move between start times.

Step 6 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.

Monitoring Meetings, Calls and Conferences

You can monitor ongoing meetings and upcoming meetings scheduled in your videoconferencing network. In addition, you can monitor system utilization status.

- Monitoring Ongoing Meetings or Calls ..... page 165
- Monitoring Bandwidth and Port Utilization ..... page 166
- Checking the Status of Meetings ..... page 166
- Managing Ongoing Calls ..... page 167
- Managing Ongoing Calls per Network Device ..... page 168
- Disconnecting Calls ..... page 168
- Managing Ongoing Conferences ..... page 168
- Monitoring Ongoing Conferences per Network Item ..... page 169

Monitoring Ongoing Meetings or Calls

You can view and monitor all meetings and calls scheduled in the system. In addition, you can monitor bandwidth and port utilization to make sure values do not exceed the limits set for the videoconference.

You can view meeting details by clicking the meeting link. When necessary, you can terminate meetings. In addition, you can become a moderator. For more details about moderators, refer to *User Guide for SCOPIA iVIEW Management Suite*.

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **Meeting Monitoring** in the sidebar menu.

Step 3 Select **Ongoing Meetings**, **Ongoing Point-to-Point Calls** or **Upcoming Meetings**.

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

All Gateways are listed in the **Gateway** column.

Step 4 Select the link in the **Subject** field for the meeting or call you want to monitor.

Step 5 Enter the moderator PIN if one is used for this meeting or call.

Step 6 Select the Become Moderator icon .
The In-meeting Control interface is not available for meetings or calls in which you are not a participant or the organizer.

Monitoring Bandwidth and Port Utilization

You can monitor port and bandwidth utilization for MCUs, SCOPIA Gateways and SCOPIA Desktops configured in the system to make sure that video traffic does not exceed the maximum utilization defined for the devices.

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **Meeting Monitoring** in the sidebar menu.

Step 3 Select **Overall Status**.

Step 4 Locate the System Utilization Status section.
A graphic representation of port and bandwidth utilization is displayed.

Checking the Status of Meetings

Ongoing and upcoming meeting status is displayed by three icons: creation status, participant status and termination status. You can monitor the status of the meetings, and view the reason of a failure status.

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **Meeting Monitoring** in the sidebar menu.

Step 3 Select **Ongoing Meetings** to see all meetings that are currently in progress.

Step 4 Select **Ongoing Point-to-Point Calls** to see all point-to-point calls that are currently in progress.

Step 5 Select **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, iVIEW Communications Manager 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/endpoint status.

  If the second status indicator is red, a participant/endpoint is not connected.

  If the second status indicator is orange, a participant/endpoint is disconnecting from the meeting.
- Third (right) status icon—Indicates meeting termination status.

Step 6 To view the Reason Failed error message, select the red status indicator, and then select **Retry** to resend the meeting information to the MCU.

> **Note:** If an endpoint is disconnected correctly via the In-meeting Control interface, there is no red status indicator.

Managing Ongoing Calls

You can monitor calls that are currently taking place on a network device.

Procedure

Step 1 Log in to iVIEW Network Manager.

Step 2 Select **Calls** or **Conferences** in the sidebar menu.

Step 3 Select **Calls**.

Step 4 To display extended details per call, click on the table row and click **Show call details**.

Managing Ongoing Calls per Network Device

You can view the current status of all calls currently being hosted on the network, on a specific office or on a selected MCU.

Procedure

Step 1 Log in to iVIEW Network Manager.

Step 2 Click **Network Tree** in the sidebar menu.

Step 3 Click **Network** or a relevant custom view.

Step 4 Select the network item you require.

Step 5 Click **Calls**.

Step 6 To display extended details per call, click on the table row and click **Show call details**.

Disconnecting Calls

You can disconnect ongoing calls when a threshold exceeds, for example, when the duration of the call exceeds the limits, or when the bandwidth used for that call exceeds the maximum bandwidth set for it.

Procedure

Step 1 Select **Calls** in the sidebar menu and then select **Calls**

–or–

Select **Network Tree** in the sidebar menu, select the network item you require, and then select **Calls**.

Step 2 Do one of the following:

- Select the call(s) you want to disconnect and click **Disconnect selected call**.
- Select **Disconnect all calls**.

Managing Ongoing Conferences

The Conferences tab provides a table for monitoring the current status of all conferences being hosted on the network, office or selected MCU. You can access the MCU Conference Control interface to manage and take control of the conference by selecting the MCU link.

Procedure

Step 1 Select **Calls** in the sidebar menu.

Step 2 Select **Conferences**.

Table 6-4 describes the information displayed on the Conferences tab.

Table 6-4 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.
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.

Step 3 (Optional) Double-click the link in the MCU column to display the element manager for that element.

Monitoring Ongoing Conferences per Network Item

You can view the current status of all conferences currently being hosted on the network, office or selected MCU. You can access the MCU Conference Control interface to manage and take control of the conference by selecting the MCU link.

Procedure

Step 1 Log in to iVIEW Network Manager.

Step 2 Select **Network Tree** in the sidebar menu.

Step 3 Select **Network** or a relevant custom view.

Step 4 Select the network item you require.

Step 5 Select **Conferences**.

Step 6 Table 6-4 on page 169 describes the information displayed on the Conferences tab.
(Optional) Double-click the link in the MCU column to display the element manager for that element.

7 Maintaining your Videoconferencing Network

This section details to the ongoing administrator tasks required to maintain your video network, including backing up, restoring, and reflecting changes in the devices and topology of your video network.

- Upgrading, Backing up and Restoring iVIEW Management Suite Data ..... page 170
- Upgrading Network Device Software..... page 173
- Maintaining Gateways ..... page 183
- Daily Maintenance of your Video Network ..... page 183
- Maintaining Scheduled Meetings..... page 188
- Uninstalling SCOPIA iVIEW Management Suite..... page 191
- Customizing your iVIEW Management Suite..... page 191

Upgrading, Backing up and Restoring iVIEW Management Suite Data

You can restore the SCOPIA iVIEW Management Suite database and configuration files from a backup copy. You should back up your database and configuration files on a regular basis.

There are many reasons for performing system backups on a regular basis, such as:

- Hardware failure
- Software failure
- Data corruption
- User errors
- Before a software upgrade

The upgrade procedure may vary depending on the release number and the size of the jump from the current installation to the new release. For more information, see "Upgrading iVIEW Management Suite" on page 172.

Note: Do not attempt to restore the database and configuration files from an old iVIEW Management Suite version. You can only backup and restore database and configuration files within the same iVIEW Management Suite release number.

To restore iVIEW Management Suite data, stop the iVIEW Management Suite service before restoring the database, configuration files, branding and sound files. Then restart the service after completing the restore. Use the iVIEW Management Suite Backup and Restore tool.

- Backing Up iVIEW Management Suite ..... page 171
- Restoring an iVIEW Management Suite Backup ..... page 172
- Upgrading iVIEW Management Suite ..... page 172

Backing Up iVIEW Management Suite

The backup procedure saves the iVIEW Management Suite database containing configuration and scheduling information, and also saves settings stored in local text files, known as property files.

The property files which are backed up are: authentication.properties, ivrslidemsg.properties, vcs-advanced.properties, vcs-core.properties, vnex.properties, aivr-call-state-machine.xml, ha.xml, mdap-context.xml, pre-start-call-state-machine.xml, trap-config.xml, vcs-cdr-conf.xml, vcs-config.xml, vcs-config-dest.xml, vivr-call-state-machine.xml, jndi.properties, log4j.xml, login-config.xml and mysql-ds.xml. The files associated with the back-to-back user agent that are backed up are: service.ini, SIPConfig.xml, and UpdatedSIPConfig.xml.

There are two database files that are backed up in MySQL format: internal and external. Both are required as part of the essential iVIEW Management Suite configuration and scheduling information.

To backup the iVIEW Management Suite:

Procedure

Step 1 Select **Start > Programs > RADVISION iVIEW Management Suite > Launch Backup and Restore Tool**.

Step 2 Select **Backup Configuration**, and then select **Next**.

Step 3 Select the type of files you want to back up.

Step 4 Specify the path to the location where you want to save the backup file. If necessary, modify the backup file name.

By default the file name format is Backup_Database_Props. After the backup process is completed, the current date (YYYYMMDD) and time (1421) stamps are automatically added to the file name. For example, Backup_Database_Props_20091215_1421.zip.

Step 5 Select **Next**.

Step 6 Select **Start**.

The backup process begins. Upon completion the success message is displayed.

Step 7 For the MS SQL database backup, share a folder on the MS SQL server so that it is accessible with read permission.

The share name and the actual name of this folder must be the same. Then click the link to verify that the folder is accessible.

Step 8 Select **OK** to complete the backup procedure.

Restoring an iVIEW Management Suite Backup

The iVIEW Management Suite Backup and Restore Tool offers the safest and most reliable method to restore the database, by creating a new temporary database with the restored data. Upon successful completion, the tool renames the currently active database, and then renames the restored database to take its place. This way, the pre-restore database is still available if needed.

Procedure

Step 1 Select **Start > Programs > RADVISION iVIEW Management Suite > Launch Backup and Restore Tool**.

Step 2 Select **Restore Configuration**, then select **Next**.

Step 3 Select the backup file which you want to use, and then select **Next**.

Step 4 Select **Start**.

The restore process begins. Upon completion the success message is displayed.

Step 5 For the MS SQL database restore:

a. Enter the admin username and password.

b. Share a folder on the MS SQL server so that it is accessible with write permission.

Step 6 Select **OK**.

Step 7 Start the iVIEW Management Suite service.

Upgrading iVIEW Management Suite

The upgrade procedure may vary depending on the release number and the size of the jump from the current installation to the new release.

Back up your iVIEW Management Suite configuration files before performing the upgrade.

Note: Do not attempt to restore the database and configuration files from an old iVIEW Management Suite version. You can only backup and restore database and configuration files within the same iVIEW Management Suite release number.

For more information on the upgrade procedure, see the *Release Notes for SCOPIA iVIEW Management Suite* for the relevant version.

Upgrading Network Device Software

iVIEW Management Suite enables you to manage software upgrades for MCUs and gateways, as well as RADVISION and third party endpoints. Upgrades are managed by applying an upgrade file to chosen devices in SCOPIA iVIEW Management Suite.

To backup a SCOPIA Gateway or a SCOPIA MCU, use iVIEW Management Suite to remotely access the device's menus from the web browser and export the configuration settings directly from there.

- Remotely Upgrading Endpoints and Other Devices from iVIEW Management Suite page 173
- Removing a Software Upgrade File ..... page 175
- Backing Up and Duplicating an Endpoint's Configuration ..... page 176
- Backing Up MCU Configuration Settings ..... page 177
- Restoring MCU Configuration Settings ..... page 177
- Updating the SCOPIA MCU License Keys ..... page 178
- Upgrading the SCOPIA Video Gateway or RADVISION SIP Gateway ..... page 179
- Restoring a Previous Software Version for the SCOPIA Video Gateway or RADVISION SIP Gateway page 181

Remotely Upgrading Endpoints and Other Devices from iVIEW Management Suite

You can quickly and easily perform remote software upgrades of video devices from SCOPIA iVIEW Management Suite by selecting the device and applying an upgrade file. Upgrade files are supplied by the vendor of the device.

You can use this method to remotely upgrade devices such as the SCOPIA Elite MCU, SCOPIA Gateway, room systems such as the SCOPIA XT1000, and endpoints like the SCOPIA VC240 or third party endpoints from Sony or Polycom.

This procedure details how to first upload an upgrade file into iVIEW Management Suite, then how to apply it to a selected device.

Note: Before upgrading an endpoint's software, backup its configuration by retrieving its configuration file. For more information on remote endpoint backups, see "Backing Up and Duplicating an Endpoint's Configuration" on page 176.

Procedure

Step 1 Log in to iVIEW Network Manager.

Step 2 Select **Settings** in the sidebar menu.

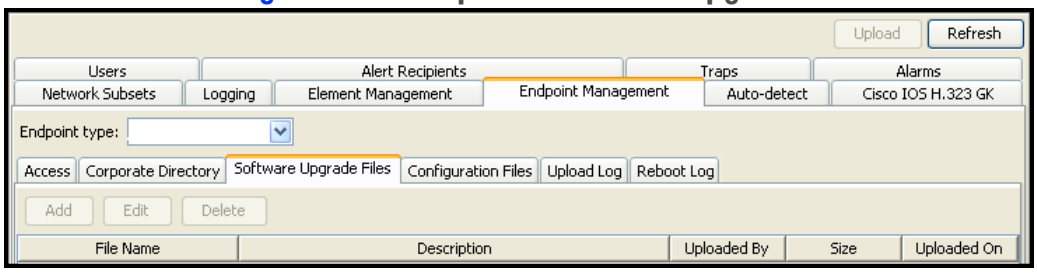
Step 3 Select **Endpoint Management** or **Element Management**.

Step 4 To upgrade an endpoint:

a. Select the specific endpoint type.

b. Select **Software Upgrade Files**.

Figure 7-1 Endpoint Software Upgrade

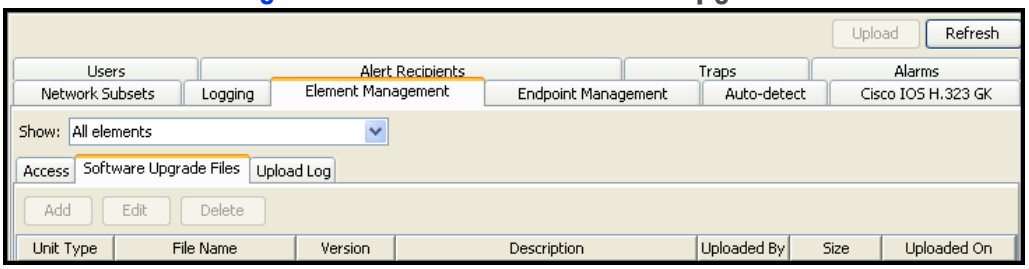


Step 5 To manage elements:

a. Select **Software Upgrade Files**.

b. Select the type of element you require in the **Show** field.

Figure 7-2 Element Software Upgrade



Step 6 Select **Add**. To edit the name of an existing upgrade file, select **Edit**.

Step 7 Enter the full path of the software upgrade file to be added to the SCOPIA iVIEW Network Manager database, or browse to the file.

The SCOPIA VC240 and SCOPIA XT1000 upgrade files are also validated. If the validation process fails, select another package file to upload.

Step 8 Enter a name and description for the upgrade file in the relevant fields.

Step 9 (Polycom endpoints only) Enter a related version number for the upgrade file.

Step 10 Select **OK** to save the upgrade file and its information in iVIEW Management Suite.

Step 11 To apply the upgrade file to one or more video network devices, select the devices to be upgraded.

a. Select **Network Tree** on the left.

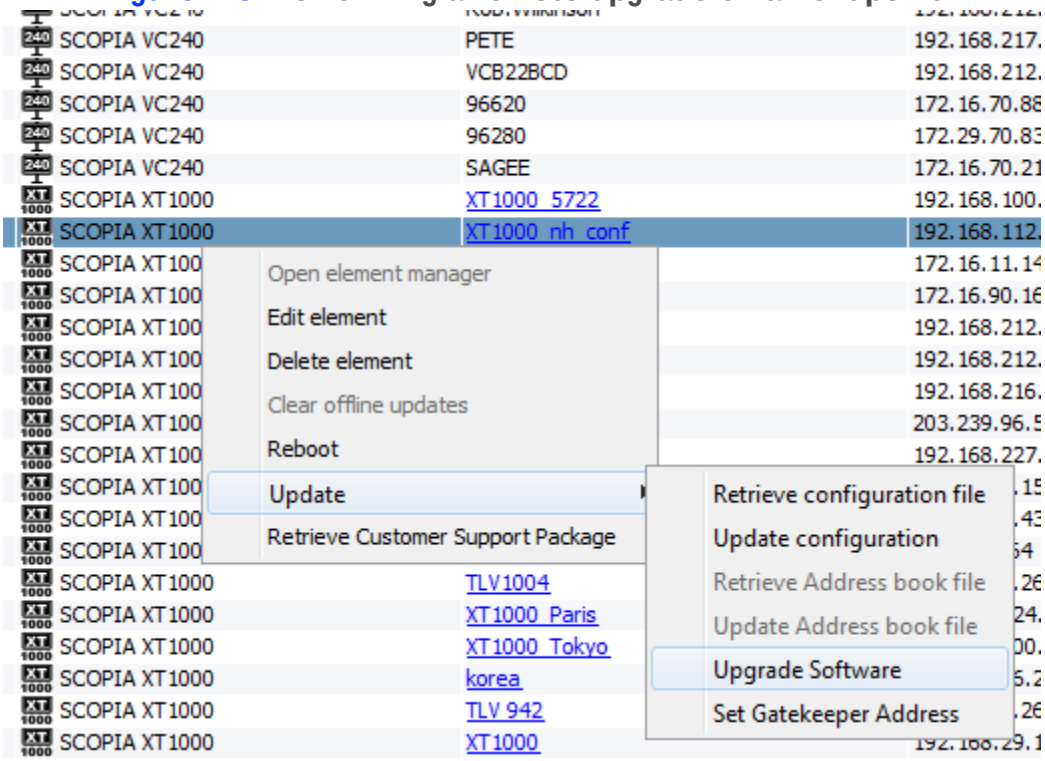
b. Select one or more network devices to be upgraded.

You can optionally sort the list according to **Element Type** to group all devices of the same type.

For example, to apply an upgrade file to all SCOPIA XT1000 units in the organization, sort by Element Type and scroll down to the devices of type SCOPIA XT1000.

Step 12 Right-click the selected devices, select **Update > Upgrade Software**.

Figure 7-3 Performing a remote upgrade on an endpoint



Step 13 Select the upgrade file to be applied to the devices.

Step 14 Select **OK**.
The system displays a warning that the endpoint will shut down for several minutes, and then notifies you when the upgrade has been completed.

Removing a Software Upgrade File

You can quickly and easily perform remote software upgrades of video devices from SCOPIA iVIEW Management Suite by selecting the device and applying an upgrade file. Upgrade files are supplied by the vendor of the device.

You can use this method to remotely upgrade devices such as the SCOPIA Elite MCU, SCOPIA Gateway, room systems such as the SCOPIA XT Series, and endpoints like the SCOPIA VC240 or third party endpoints from Sony or Polycom.

This section describes how to remove the software upgrade file if it is no longer required in iVIEW Management Suite's list of upgrade files.

Procedure

Step 1 Log in to iVIEW Network Manager.

Step 2 Select **Settings** in the sidebar menu.

Step 3 Select **Endpoint Management** or **Element Management**.

Step 4 For element management, select **Software Upgrade Files**. For endpoint management, select a specific endpoint type.

Step 5 For element management, select the type of endpoint you require in the **Show** field. For endpoint management, select **Software Upgrade Files**.

Step 6 Do one of the following:

- Select the software upgrade file you require and select **Delete**.
- Right-select the software upgrade file you require and select **Delete**.

Step 7 Select **OK** to save your changes.
The software upgrade file is removed from the database.

Backing Up and Duplicating an Endpoint's Configuration

SCOPIA iVIEW Management Suite can remotely retrieve and backup the configuration parameters of any listed endpoint, including the SCOPIA VC240, SCOPIA XT Series and third party endpoints from Polycom, Sony and Tandberg.

You can also apply those configuration settings across multiple endpoints in your organization. The retrieved settings are only generic, therefore settings such as the endpoint's IP address are not stored.

This procedure describes how to retrieve the configuration file and store it in iVIEW Management Suite, and how to apply the settings on other endpoints.

You can access an endpoint configuration file by selecting **Settings** in the sidebar and then selecting **Endpoint Management > Configuration Files**.

Procedure

Step 1 Login to SCOPIA iVIEW Network Manager.

Step 2 Select **Network Tree** in the sidebar.

Step 3 Right-click the endpoint and select **Update > Retrieve configuration file**.

The Retrieve Configuration File window shows a list of the configuration files that were previously retrieved.

Step 4 Enter the filename and a description of the new configuration file.

Step 5 Select **OK** to save the file in the iVIEW Management Suite database.

You can access an endpoint configuration file by selecting **Settings** in the sidebar and then selecting **Endpoint Management > Configuration Files**.

Step 6 To apply this configuration file to other endpoints, select the endpoints you want to update.

Step 7 Right-click and select **Update > Update configuration**.

The Update Configuration window shows a list of the configuration files that were previously retrieved, and are associated with the selected endpoint types.

Step 8 Select the file with which to update the selected endpoints.

Step 9 Click OK to start updating the endpoint configuration.

Backing Up MCU Configuration Settings

Backing up the configuration settings of a SCOPIA Elite MCU can be done from within the SCOPIA iVIEW Management Suite.

Procedure

Step 1 Log in to iVIEW Network Manager.

Step 2 Select **Network Tree** in the sidebar menu.

Step 3 Select the MCU you require in the tree.

Step 4 Select **Backup & Restore**.

If **Backup & Restore** does not appear as a tab on the screen, access the device directly by selecting its IP address displayed in the window to perform the backup directly on the device.

For more information on exporting configuration files on a SCOPIA MCU, see the product's User Guide.

Step 5 Select **Backup**.

Step 6 Enter a description of the MCU configuration file in the Retrieve Configuration File window and select **OK**.

Step 7 Select **OK** in the **Configuration file backup successful** message window to complete the backup procedure.

Restoring MCU Configuration Settings

You can restore the configuration settings of a SCOPIA Elite MCU from within the SCOPIA iVIEW Management Suite.

Procedure

Step 1 Log in to iVIEW Network Manager.

Step 2 Select **Network Tree** in the sidebar menu.

Step 3 Select the MCU you require in the tree.

Step 4 Select **Backup & Restore**.

If **Backup & Restore** does not appear as a tab on the screen, access the device directly by selecting its IP address displayed in the window to perform the backup directly on the device.

For more information on exporting configuration files on a SCOPIA MCU, see the product's User Guide.

Step 5 Select a configuration file from the list.

Step 6 Select **Restore**.

Step 7 Select **Yes** at the prompt.

Updating the SCOPIA MCU License Keys

Network administrators can update an MCU license key from the iVIEW Management Suite.

Procedure

Step 1 Login to the iVIEW Network Manager.

Step 2 Select the **Network Tree** icon on the left and explore the tree by expanding network zones to find an MCU.

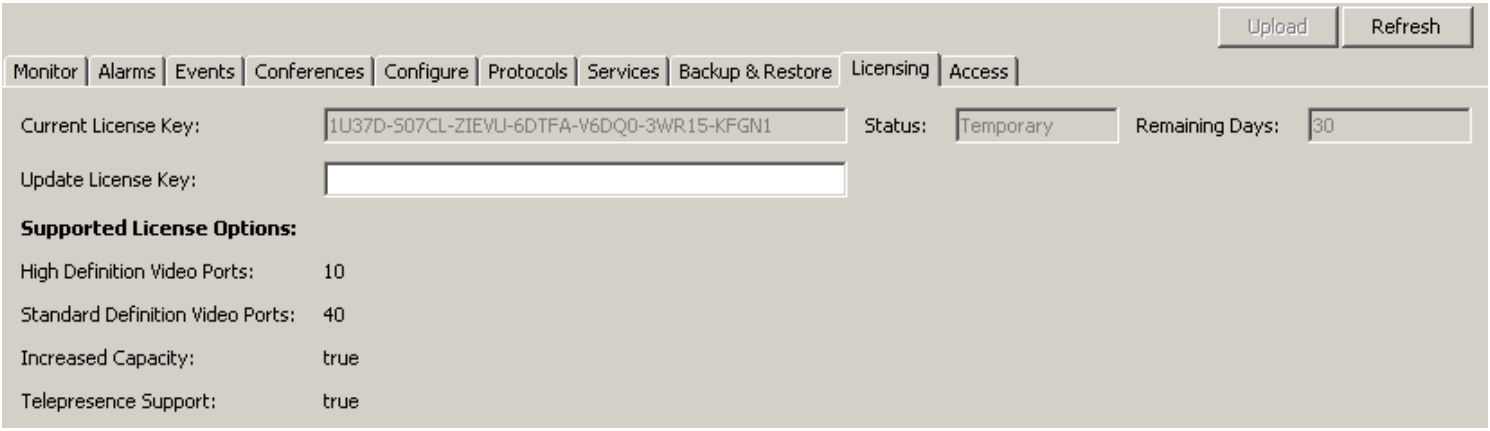
Alternatively, select the **Network Table** icon on the left, and search the Element Type column for one of the SCOPIA Elite MCU models. Double-click on that element.

> **Note:** Ensure it is a SCOPIA Elite MCU. The remote license update functionality is only available for the SCOPIA Elite MCU.

Step 3 Select the **Licensing** tab (Figure 7-4 on page 178). This tab is only visible for a SCOPIA Elite MCU.

If the license is temporary, the **Remaining Days** field will display the number of days before the license expires.

Figure 7-4 Remote update of the SCOPIA Elite MCU license



Step 4 Enter the new license key in the **Update License Key** field.

Step 5 Select the **Upload** button.
The system confirms the license has been updated. If there are any problems with this process, verify the license key is accurate and that the system can properly access the MCU.

Upgrading the SCOPIA Video Gateway or RADVISION SIP Gateway

The upgrade procedure is different when upgrading to a major new version compared with smaller incremental upgrades.

Note: You perform the upgrade remotely using the iVIEW Management Suite. You cannot upgrade the firmware of the gateway directly on the device.

Depending on your support contract, you can upgrade to:

- The next major version.

  Upgrading a major version requires a new license.

  This kind of upgrade changes one of the first two digits in a version number. For example, upgrading from version 7.6 to version 7.7 requires a new license.

- An incremental version.

  Upgrading an incremental version does not require a new license.

  This kind of upgrade changes the third, fourth and fifth digits in the version number. For example, upgrading from 7.6.1.0.1 to 7.6.1.0.2 or to 7.6.2.0.0 does not require a new license.

Upgrades may require first applying the major upgrade and then the incremental upgrade within that major version. For example, to upgrade from 7.6.0.5.0 to 7.7.1.2.0, first apply the major upgrade to 7.7.0.0.0, and then the incremental upgrade to 7.7.1.2.0.

The procedure in this section applies to both types of upgrades.

Note: To upgrade via HTTPS, enable HTTPS in the iVIEW Network Manager. Select the device you are upgrading from the network tree, select the **Configure** tab, and select the **Secure connection using HTTPS** check box.

Before You Begin

Go to http://licensing.radvision.com/ to apply for and download your upgrade package.

If you upgrade to a major version, ensure you have a new license key.

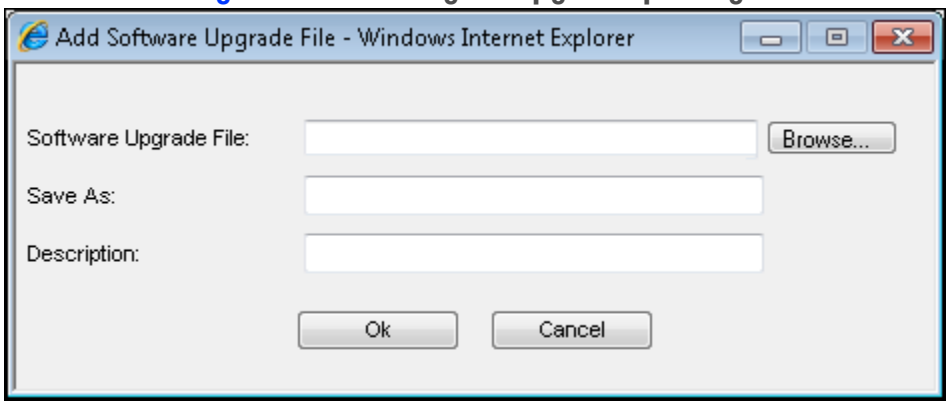
Procedure

Step 1 Access the iVIEW Network Manager.

Step 2 To upload a new upgrade package into iVIEW Management Suite for the gateway, navigate to **Settings > Element Management > Software Upgrade Files**.

Step 3 Select **Add**.

Figure 7-5 Adding an upgrade package



Step 4 Select the upgrade package:

a. Select **Browse** and navigate to the upgrade package.

b. Enter the package name in the **Save As** field which would appear in the table of the **Upgrade Software** dialog box (Figure 7-6 on page 181).

c. Enter a free text description of the upgrade package.

d. Select **Ok.**

Step 5 To apply the new upgrade package to a specific gateway, locate the device in the network tree.

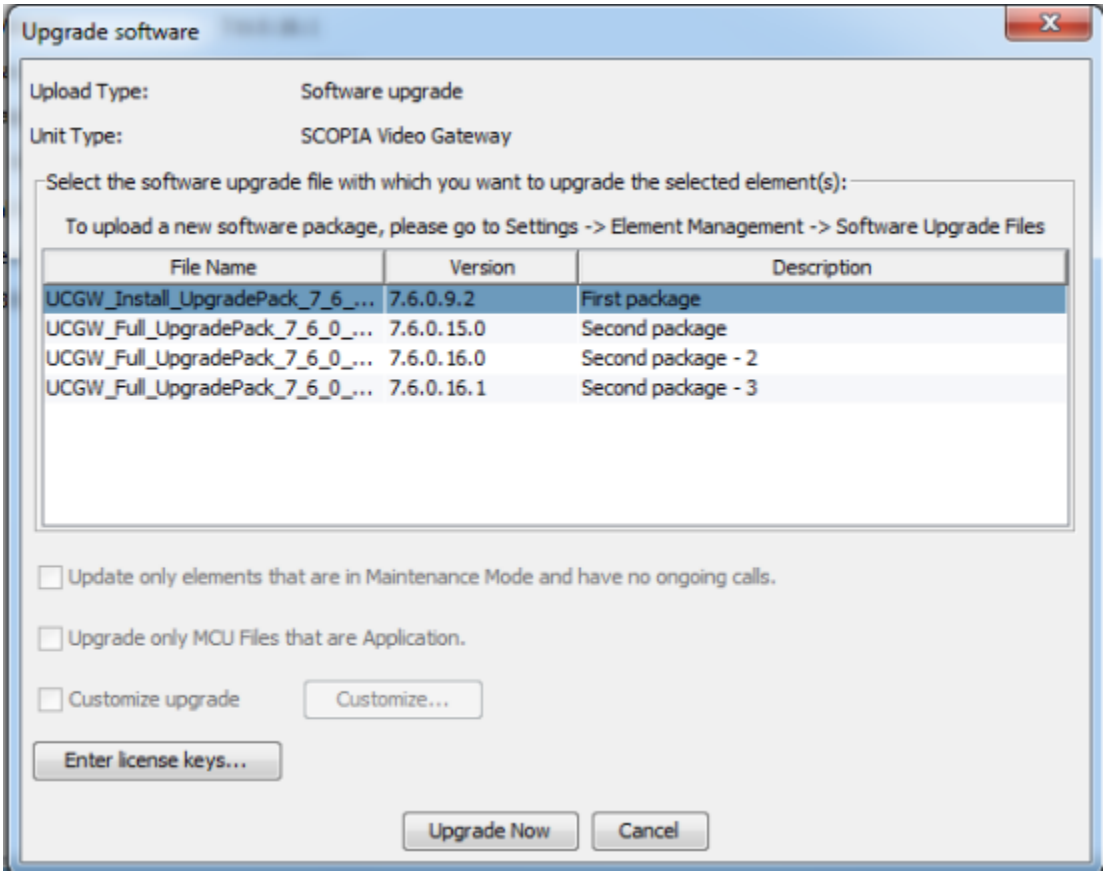
Step 6 Right-click the gateway device and select **Update > Upgrade Software**.

The confirmation message opens informing you that all active calls on the gateway will be disconnected when you begin the upgrade process.

Step 7 Select **Yes** in the confirmation message.

The **Upgrade software** window opens (Figure 7-6).

Figure 7-6 Upgrade software dialog box



Step 8 Select the package you added.

Step 9 If you are upgrading for a major version, enter the license key:

a. Select **Enter license keys**.

b. Enter the license key in the field.

c. Select **OK**.

Step 10 Select **Upgrade now**.

Step 11 Select **OK**.

The Upload Log window opens showing the upgrade progress.
The upgrade process typically takes 10 minutes with optimal network conditions where the iVIEW Management Suite is located in the same network zone as the gateway. The upgrade process may require more time if network connections are less than optimal.

Restoring a Previous Software Version for the SCOPIA Video Gateway or RADVISION SIP Gateway

The procedure in this section explains how to restore a previous software version after you upgrade your gateway. You can restore the same software version only once.

During this procedure the gateway shuts down for a few minutes causing all active calls to be disconnected.

Please notice that some parameters are not backed up and cannot be restored:

- IP address
- IP mask
- Default router
- MTU
- DNS suffix
- DNS primary address
- DNS secondary address

Note: To restore a previous version via HTTPS, enable HTTPS in the iVIEW Network Manager. Select the device you are upgrading from the network tree, select the **Configure** tab, and select the **Secure connection using HTTPS** check box.

Only versions SCOPIA Video Gateway 7.7 and later support HTTPS. If you are restoring an earlier version of SCOPIA Video Gateway, do not enable HTTPS.

Before You Begin

Make sure no active calls are running on the gateway.

Procedure

Step 1 Access the iVIEW Network Manager.

Step 2 Navigate to the required SCOPIA Video Gateway or SIP Gateway in the tree structure.

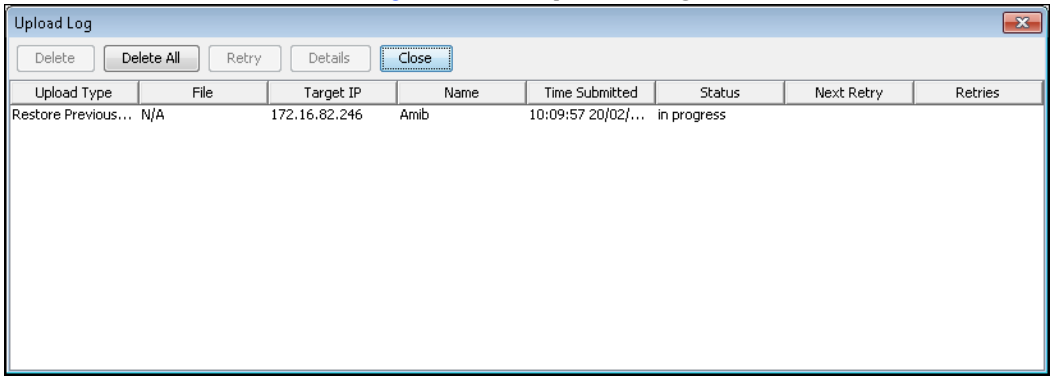
Step 3 Right-click the gateway to be restored and select **Update > Restore Previous Version**.

The confirmation message opens informing you that all active calls on device will be disconnected when you begin the process.

Step 4 Select **Yes** in the confirmation message.

The Upload Log window opens showing the task progress.

Figure 7-7 Upload Log



Maintaining Gateways

There are a number of maintenance tasks, including backing up gateways, changing a gateway's services, registering a gateway with a gatekeeper and removing a gateway.

- Adding a Gateway and its Services in iVIEW Management Suite ..... page 36
- Adding or Editing a Service to an Existing Gateway ..... page 39
- Registering a Gateway with a Gatekeeper ..... page 40
- Backing Up MCU Configuration Settings ..... page 177
- Removing a Network Device from iVIEW Management Suite ..... page 185
- Upgrading the SCOPIA Video Gateway or RADVISION SIP Gateway ..... page 179
- Restoring a Previous Software Version for the SCOPIA Video Gateway or RADVISION SIP Gateway page 181
- Downgrading your SCOPIA Video Gateway or RADVISION SIP Gateway ..... page 183

Downgrading your SCOPIA Video Gateway or RADVISION SIP Gateway

If necessary, you can downgrade your gateway in one of the following ways:

- To downgrade one version back after you upgraded your gateway, perform the procedure in Restoring a Previous Software Version for the SCOPIA Video Gateway or RADVISION SIP Gateway page 181.
- To downgrade to a version earlier than the previous version, see "Upgrading the SCOPIA Video Gateway or RADVISION SIP Gateway" on page 179.

Daily Maintenance of your Video Network

This section provides daily procedures for maintaining your network devices, meeting types, meeting groups and scheduled meetings.

- Searching for Network Devices ..... page 184
- Modifying a Network Device Profile ..... page 184
- Removing a Network Device from iVIEW Management Suite ..... page 185
- Cancelling Pending Offline Configuration Settings ..... page 187
- Modifying Network Devices Hierarchy ..... page 188
- Limiting User Access to Types of Meetings ..... page 116
- Managing Bandwidth in your Network ..... page 188

Searching for Network Devices

You can search for a network device in the iVIEW Network Manager and in the iVIEW Communications Manager. Both procedures are described below, use the relevant procedure.

Procedure

Step 1 To search for a network device in the iVIEW Network Manager, log in to iVIEW Network Manager.

Step 2 Select one of the network views (**Network Tree**, **Network Table** or **Network Map**) in the sidebar menu.

Step 3 Do one of the following to search for an element profile:

- Select **Edit** > **Find** > **Find element**.
- Select **Find element** .

Step 4 Enter the IP address of the element or select the element type.

Step 5 Select **Find**.

The required element is highlighted in the Network Tree, Network Table or Network Map view.

Step 6 To search for a network device in the iVIEW Communications Manager, log in to iVIEW Communications Manager.

Step 7 Select Resource Management in the sidebar menu.

Step 8 Select the tab that represents the type of device you want to search for.

Step 9 Enter the name of the device you want to find and select **Search**.

Modifying a Network Device Profile

You can modify a network device profile in iVIEW Management Suite so the device will comply with your video network requirements. This procedure explains how to modify a device profile in the iVIEW Network Manager and in the iVIEW Communications Manager. Since devices parameters are different in each of these iVIEW Management Suite applications, perform the relevant steps, as follows:

- To modify a network profile in the iVIEW Network Manager, perform steps 1 to 9.
- To modify a network profile in the iVIEW Communications Manager, perform steps 10 to 15.

Procedure

Step 1 Log in to iVIEW Network Manager.

Step 2 Select one of the network views (**Network Tree**, **Network Table** or **Network Map**) in the sidebar menu.

Step 3 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 select **Edit element** .

Step 4 Enter the element name and IP address in the relevant fields.

Step 5 Select the required element type.

The element type cannot be modified.

Step 6 (Optional) Select **Managed element** to enable SCOPIA iVIEW Network Manager to manage the element.

This option is not available for endpoint elements.

Step 7 (Optional) Select **Allow offline configuration** to allow offline configuration of the element.

This option is not available for SCOPIA Elite MCU, RADVISION SIP Gateway, SCOPIA Video Gateway for Microsoft Lync, SCOPIA PathFinder or endpoint elements.

The SCOPIA 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.

Step 8 (For endpoints only) 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**.

Step 9 (Optional for endpoints only) Select **Set iVIEW NMS as the default trap server** to use iVIEW Network Manager as the SNMP trap server for endpoint elements.

Step 10 Select **OK** to save your changes.

Step 11 Log in to iVIEW Communications Manager.

Step 12 Select **Resource Management** in the sidebar menu.

Step 13 Select the tab that represents the type of device you want to change.

Step 14 Select the network device you want to modify. The Modify window is displayed.

Step 15 Modify the device profile, and select **OK**.

Removing a Network Device from iVIEW Management Suite

Deleted elements are not added to the iVIEW Management Suite 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.

In the case of a SCOPIA MCU or gateway, you must take the network device offline before you can remove it from the iVIEW Management Suite database. See "Taking a SCOPIA MCU or Gateway Offline" on page 187.

Procedure

Step 1 Log in to NMS.

Step 2 Select one of the network views (**Network Tree**, **Network Table** or **Network Map**) in the sidebar menu.

Step 3 Do one of the following to remove an existing element profile:

- Right-select 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 select **Delete element** .

Step 4 Select **Yes**.

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

Step 5 Log in to iCM.

Step 6 Select **Resource Management** in the sidebar menu.

Step 7 Select the network device to be removed.

Step 8 Select **Delete** and then **OK**.

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

Step 9 Log in to iVIEW Communications Manager.

Step 10 Select **Resource Management** in the sidebar menu.

Step 11 Select the network device tab that represents the network device you want to delete.

Only service providers or administrators of a distributed environment can delete gatekeepers.

Step 12 Select the network device you want to delete. The Modify window is displayed.

Step 13 Select **Delete** and then **OK**.

Taking a SCOPIA MCU or Gateway Offline

This procedure is relevant for SCOPIA MCUs and Gateways only. These are the only network devices that can be taken offline. An offline network device is still part of the network, and can be taken online at any time. However this is usually a prelude to removing the device from iVIEW Management Suite (see "Removing a Network Device from iVIEW Management Suite" on page 185).

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **Resource Management** in the sidebar menu.

Step 3 Select an MCU or a gateway.

Step 4 Select the link in the Name column for the MCU you require.

Step 5 To take the MCU offline temporarily, select **Take this MCU/gateway offline and reschedule all meetings on this MCU/gateway up to this date** and set the date to bring the MCU/gateway online again.

Step 6 To take the MCU/gateway offline permanently, select **Take this MCU/gateway offline and reschedule all meetings currently on this MCU/gateway**.

Step 7 Select **OK** to save your changes.

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

- iVIEW Communications Manager cannot schedule meetings for the offline MCU.
- All meetings currently in progress are terminated. iVIEW Communications Manager attempts to reschedule upcoming meetings for the offline MCU on other MCUs/gateways 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, iVIEW Communications Manager 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, iVIEW Communications Manager attempts to reschedule all future meetings scheduled to this MCU.

Cancelling Pending Offline Configuration Settings

You can cancel any configuration update that was performed in a device while it was offline.

Procedure

Step 1 Log in to iVIEW Network Manager.

Step 2 Select **Network Tree** in the sidebar menu.

Step 3 Right-click an offline element.

Step 4 Select **Clear offline updates**.

The element configuration settings which existed before the offline modifications are restored.

Modifying Network Devices 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, SCOPIA Gateway and 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

Step 1 Log in to iVIEW Network Manager

Step 2 Select **Network Tree** in the sidebar menu.

Step 3 Select an element in the network tree.

Step 4 Drag and drop the element to the required location in the hierarchy.

Step 5 Deselect the element.

Managing Bandwidth in your Network

Bandwidth for in-zone, cross-zone and pro-to-pro calls are managed within iVIEW Management Suite. The following topics describe how to configure bandwidth thresholds.

- Defining Bandwidth Limits for the new Office or Branch ..... page 13
- Defining Bandwidth for SCOPIA Desktop Pro to Pro Calls ..... page 32

Maintaining Scheduled Meetings

This section explains how to maintain scheduled meetings.

- Searching for a Meeting ..... page 189
- Modifying Upcoming Meetings ..... page 190

Searching for a Meeting

You can search for a specific meeting, to monitor or terminate the meeting. You can also access meeting information by selecting the meeting subject link.

Procedure

Step 1 Log in to iCM.

Step 2 Select **Meeting Monitoring** in the sidebar menu.

Step 3 Select **Ongoing Meetings**, **Ongoing Point-to-Point Calls** or **Upcoming**, as required.

Step 4 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.
- Select 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.
- Select 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.

Step 5 Select **Search**.

Search results are listed.

Step 6 To return to the complete list of meetings, clear each of the fields.

Step 7 Select **Search**.

Modifying Upcoming Meetings

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

Procedure

Step 1 Log in to iCM.

Step 2 Select **Meeting Monitoring** in the sidebar menu.

Step 3 Select **Upcoming**.

Step 4 Select the subject of the meeting you want to modify.

Step 5 Enter the required information in the Meeting Detail page.

Uninstalling SCOPIA iVIEW Management Suite

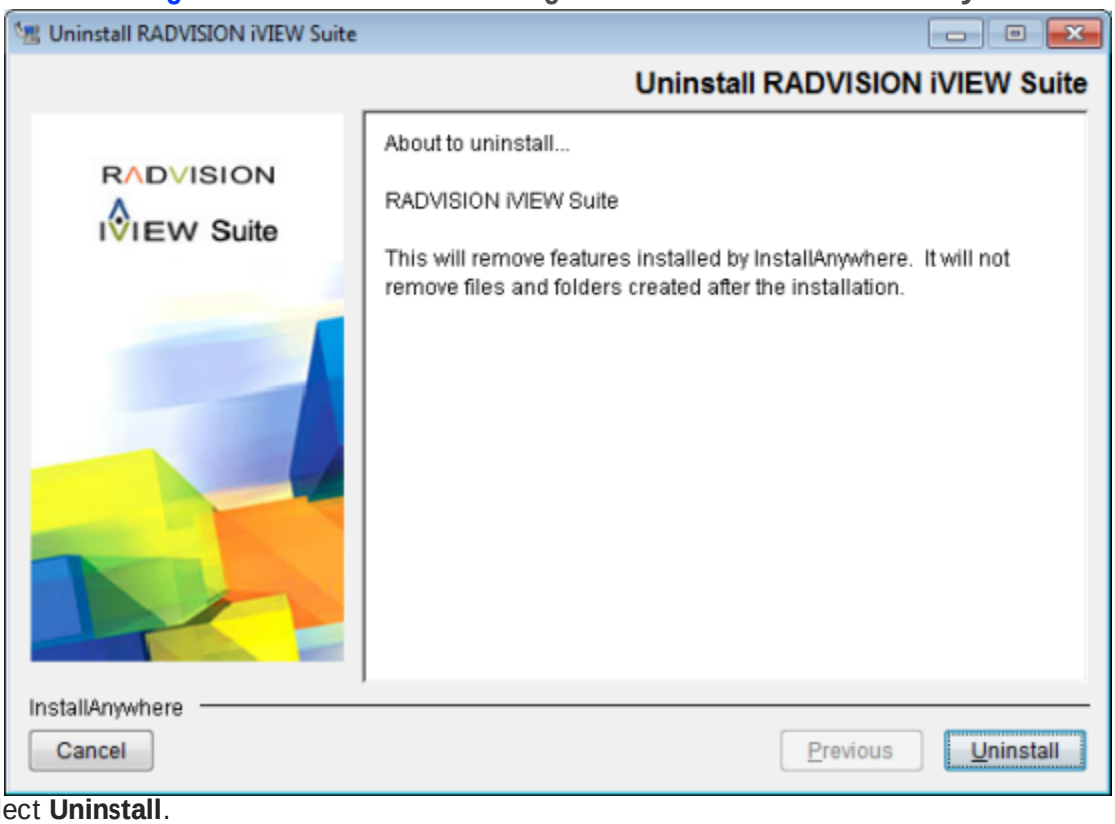
Uninstalling iVIEW Management Suite has been made simple with an uninstall utility, which can be accessed in the Start menu in the same folder as the application itself.

Procedure

Step 1 Select **Start > All Programs > RADVISION iVIEW Management Suite**.

Step 2 Launch **Uninstall RADVISION iVIEW Management Suite**.

Figure 7-8 The iVIEW Management Suite Uninstall Utility



Step 3 Select **Uninstall**.

Customizing your iVIEW Management Suite

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

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

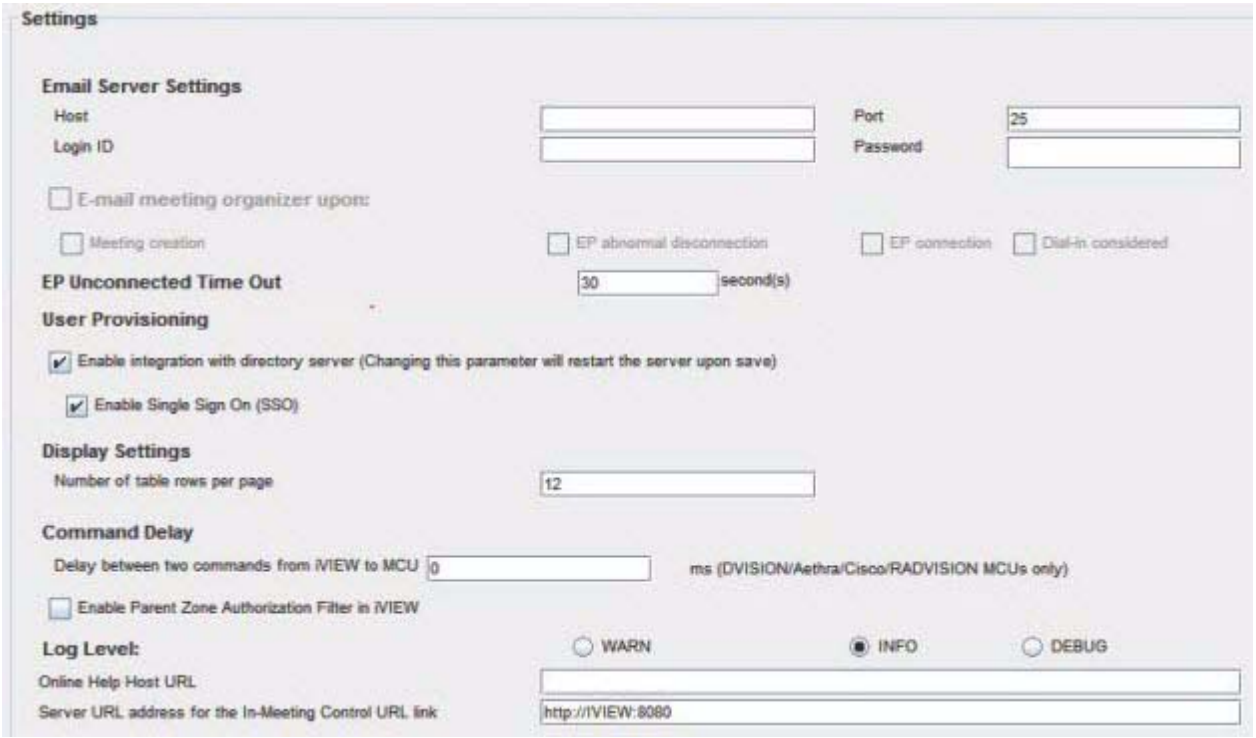
- Defining General Settings for iVIEW Management Suite ..... page 192
- Defining the iVIEW Management Suite Web Interface..... page 198
- Defining Meeting Scheduling Settings..... page 194
- Defining Custom Time Zones ..... page 199
- Defining Custom Branding for Vendors ..... page 200
- Defining Database Server Settings..... page 201
- Configuring SNMP Trap Server Profiles and Utilization Thresholds..... page 202
- Defining Security Settings..... page 202
- Defining Call Data Record (CDR)..... page 203
- Customizing Meeting Invitation E-mails ..... page 204

Defining General Settings for iVIEW Management Suite

The iVIEW Management Suite Configuration Tool allows you to change settings configured during iVIEW Management Suite installation.

The following general parameters can be configured using the iVIEW Management Suite Configuration Tool:

Figure 7-9 Configuring General Parameters



- **Email server settings**

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

- **Endpoint unconnected time out**

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

- **User Provisioning**

  You can integrate iVIEW Management Suite's user list with the network's Active Directory, and enable single sign on with these settings.

- **Display settings**

  You can define the number of rows per page displayed in iVIEW Management Suite tables.

- **Command delay**

  You can define the interval that iVIEW Management Suite waits when sending sequential internal messages to the MCU.

- **Log level**

  You can select from three levels (warn, info or debug) of details for a log file. The more details a log file has, the larger the log file.

- **Parent zone authorization filter**

  This setting is only applicable when working with an Gatekeeper. 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 to determine the dial-out string when an endpoint is invited to a meeting.

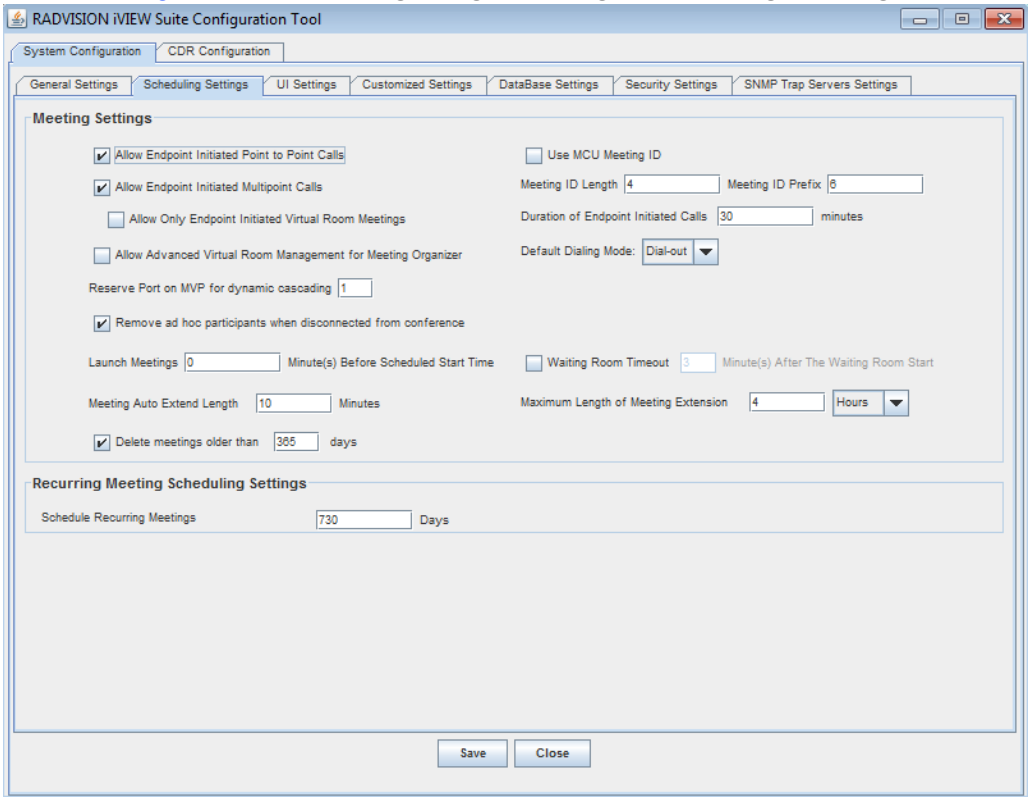
- **Online help host URL**

  If you have a local or remote copy of the online help files, you can define the URL from which the files can be accessed.

- **Server URL address for the In-Meeting control URL link**

  You can define the URL address used to access the meeting control user interface during the meeting. This URL address appears as a link in the meeting invitation.

Figure 7-10 Configuring Meeting Scheduling Settings



- Call authorization

  When iVIEW Management Suite and a SCOPIA Enhanced Communication Server are working in authorization mode, iVIEW Management Suite can restrict endpoint-initiated conferences by configuring these settings to prevent uncontrolled and unmanaged access in a videoconference network.

  - **Allow Endpoint Initiated Point to Point Calls**
  - **Allow Endpoint Initiated Multipoint Calls**

- **Allow Only Endpoint Initiated Virtual Room Meetings**

  This option is enabled only when the **Allow Endpoint Initiated Multipoint Calls** is selected. It ensures that endpoint-initiated MCU calls must use a defined virtual room.

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

- **Allow Advanced Virtual Room Management for Meeting Organizer**

  This option enables Meeting Organizers to have multiple virtual rooms. When selected, a meeting organizer can have multiple virtual rooms under his 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.

- Dynamically cascading multiple MVPs for a single conference

  Enter a positive number in the **Reserve Port on MVP for dynamic cascading** field to allow an existing endpoint-initiated ad hoc meeting to grow beyond the size of a single MVP. You can instruct iVIEW Management Suite 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, iVIEW Management Suite creates a new meeting on another MVP when a new call joins the meeting. iVIEW Management Suite 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.

- Default meeting settings

  - **Use MCU Meeting ID**

    Select this option to work with the MCU conference ID instead of the iVIEW Communications Manager conference ID.

    This option is meant to work when iVIEW Management Suite and ECS are not working in authorization mode, and all meetings dial out to their meeting participants.

- **Meeting ID Length**

  The number of digits included in the Meeting ID.

- **Meeting ID Prefix**

  The prefix of the meeting ID. You can use any number that is not used as a prefix for the auto attendant, auto routing, or for other deployment components.

  The prefix must be shorter than the number specified in the Meeting ID Length field.

- **Duration of Endpoint Initiated Calls**

  The default value is 30 minutes. iVIEW Management Suite uses this value in resource allocation and meeting creation.

- **Default Dialing Mode**

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

  If you select Dial-out, the iVIEW Communications Manager system dials out to meeting participants.

- **Remove ad hoc participants when disconnected from conference**

  Select this option 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 iVIEW Communications Manager 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.

- **Launch Meetings <n> Minutes before scheduled start**

  Specify the amount of time prior to the scheduled start of a meeting that the meeting actually begins. If the early start attempt fails, iVIEW Management Suite attempts to create this meeting again at the regular scheduled start time.

- Delete meetings older than

- **Meeting Auto Extend Length**

  Define the length of time that a meeting can be extended after the scheduled end of the meeting.

- Waiting Room Timeout

  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.

- Maximum Length of Meeting Extension

  Specify the maximum length of time that you want to allow for extending a meeting.

  The maximum values that iVIEW Management Suite allows are 10 days, 240 hours and 14400 minutes.

- Default recurring meeting settings

- **Use MCU meeting ID**

  This option is relevant when iVIEW Management Suite and ECS are not working in authorization mode, and all meetings dial out to their meeting participants.

- **Meeting ID Length**

  The number of digits included in the Meeting ID.

- **Meeting ID Prefix**

  The prefix of the meeting ID. You can use any number that is not used as a prefix for the auto attendant, auto routing, or for other deployment components.

  The prefix must be shorter than the number specified in the Meeting ID Length field.

- **Duration of Endpoint Initiated Calls**

  The default value is 30 minutes. iVIEW Management Suite uses this value in resource allocation and meeting creation.

- **Default Dialing Mode**

  If you select Dial-in, meeting participants enter a meeting by dialing into the meeting, and if you select Dial-out, the iVIEW Management Suite system dials out to meeting participants.

- Remove ad hoc participants when disconnected from conference

  This is useful for endpoint initiated ad-hoc conferences where a meeting operator can manually remove a disconnected participant from the conference list. When a disconnected participant remains in the In-Meeting Control participant list, such participant still use MCU ports even though they are no longer connected.

- **Launch Meetings <n> Minutes before scheduled start**

  If the early start attempt fails, iVIEW Management Suite attempts to create this meeting again at the regular scheduled start time.

- Delete meetings older than

- **Meeting Auto Extend Length**

  Define the length of time that a meeting can be extended after the scheduled end of the meeting.

- Waiting Room Timeout

  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.

- **Maximum Length of Meeting Extension**

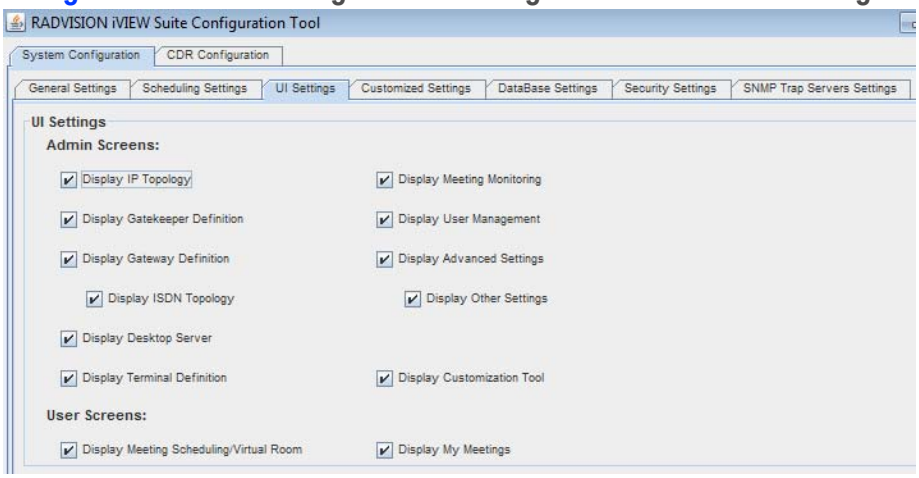
  The maximum values that iVIEW Management Suite allows are 10 days, 240 hours and 14400 minutes.

- **Recurring Meeting Scheduling Settings**

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

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

Figure 7-11 Defining iVIEW Management Suite UI Settings



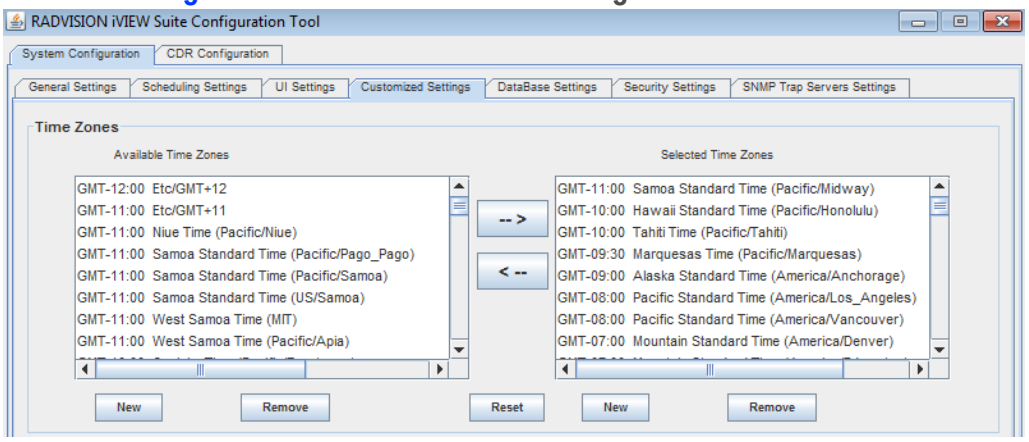
- **Display IP Topology**: enables the IP Topology tab in Admin > Network Management.
- **Display Gatekeeper Definition**: enables the Gatekeeper/SIP server/Presence server tab in Admin > Resource Management > Gatekeeper/SIP server/Presence server.
- **Display Gateway Definition**: enables the Gateway tab in Admin > Resource Management.
- **Display ISDN Topology**: enables the ISDN Topology tab in Admin > Network Management. The ISDN Topology tab is only displayed when the gateway is enabled.
- **Display Desktop Server**: enables the Desktop server tab in Admin > Resource Management.
- **Display Terminal Definition**: enables the Terminal tab in Admin > Resource Management.
- **Display Meeting Monitoring**: enables the Meeting Monitoring section accessible via the Admin sidebar menu.
- **Display User Management**: enables the User Management section accessible via the Admin sidebar menu.
- **Display Advanced Settings**: enables the Advanced section accessible via the Admin sidebar menu.
- **Display Other Settings**: enables the Other Settings tab in the Scheduling a New Meeting and in Meeting Details windows.
- **Display Customization Tool**: enables the Customization button on upper-right of the application window that provides access to the Customization Tool window in which you can customize terminology in the iVIEW Communications Manager web interface.
- **Display Meeting Scheduling and Virtual Room**: enables the Meeting Scheduling and Virtual Room sections accessible via the User sidebar menu.
- **Display My Meetings**: enables the My Meetings section accessible via the User sidebar menu.

The Customized Time Zone(s) area lists Java standard time zones, as well as custom defined time zones.

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. In addition, you can create new time zone, delete existing time zones, add daylight saving to a time zone, and revert settings of a customized time zone to its default settings. When modifying time zones, consider the following:

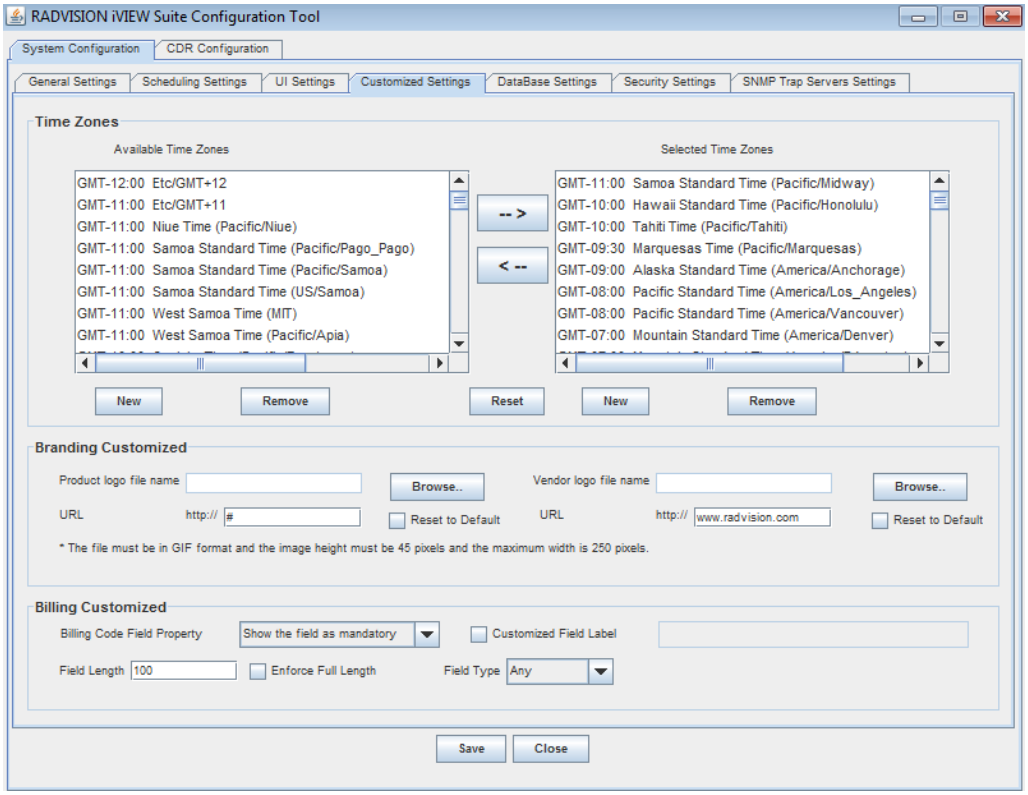
- Once a new time zone is defined and saved, its name cannot be changes.
- If you create a custom time zone that has the same name as the key string in a default Java time zone, the new custom time zone overrides the rules of the default Java time zone.
- When modifying daylight saving time on existing time zones, you have to create a new time zone, specify daylight saving time and save it with the same name as the Java time zone that you want to modify. This happens because the start time for daylight saving time in the USA is scheduled to change in the year of 2007.

Figure 7-12 Customized Settings for Time Zones



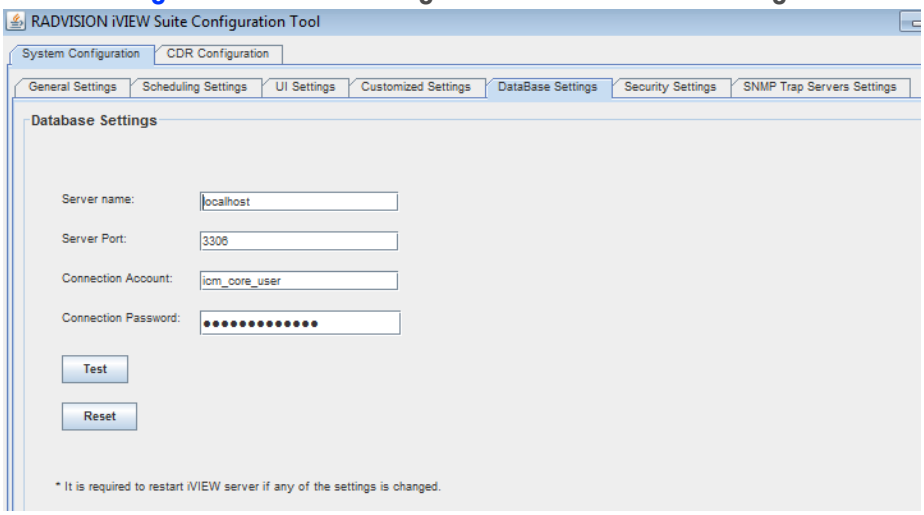
Administrators change the iVIEW Management Suite product logo via iVIEW Communications Manager > Advanced Settings > Look and Feel. Use the iVIEW Management Suite Configuration Tool to define the location of the .gif file with the vendor's logo.

Figure 7-13 Defining Branding for Vendors



The iVIEW Management Suite internal database can be defined using the Configuration Tool.

Figure 7-14 Defining database server settings



Procedure

Step 1 Select **System Configuration > Database Settings** in the iVIEW Management Suite Configuration Tool.

Step 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.

Step 3 Enter the account name used by iVIEW Communications Manager to connect to the database in the Connection Account field. "Root" appears by default.

Step 4 Enter a password in the Connection Password field for use by iVIEW Communications Manager when a connection to the database server is established.

Step 5 Select **Test** to verify that the database configuration is correct.

A message window shows the test results.

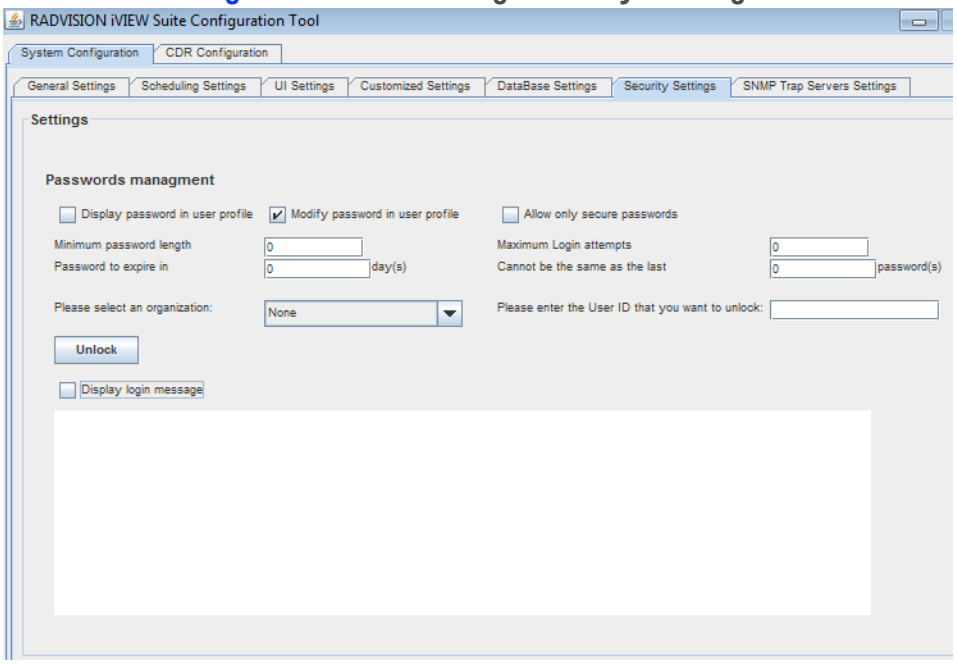
Step 6 Select **Reset** to revise your configured database server settings and select Save.

Step 7 Restart iVIEW Communications Manager to apply your changes.

Defining Security Settings

You can define password settings, login message, and unlock policy for user accounts.

Figure 7-15 Defining security settings

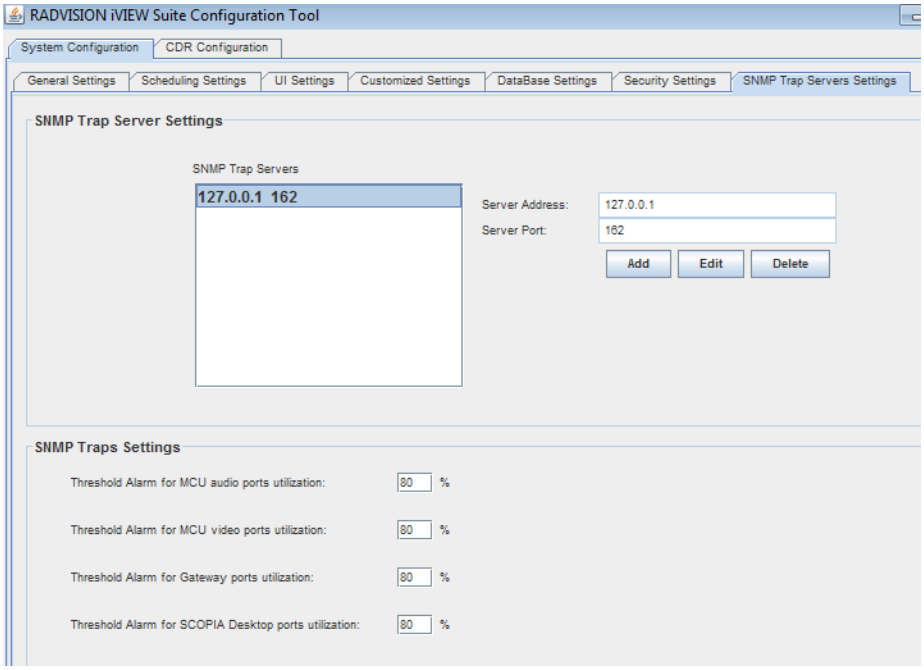


Configuring SNMP Trap Server Profiles and Utilization Thresholds

You can add a new SNMP trap server, modify an existing profile or remove unused profiles, and define one of the following threshold limits:

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

Figure 7-16 Defining SNMP Trap server settings



Defining Call Data Record (CDR)

iVIEW Management Suite creates and stores Call Data Records (CDR) 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. The following actions can be performed using the Configuration Tool:

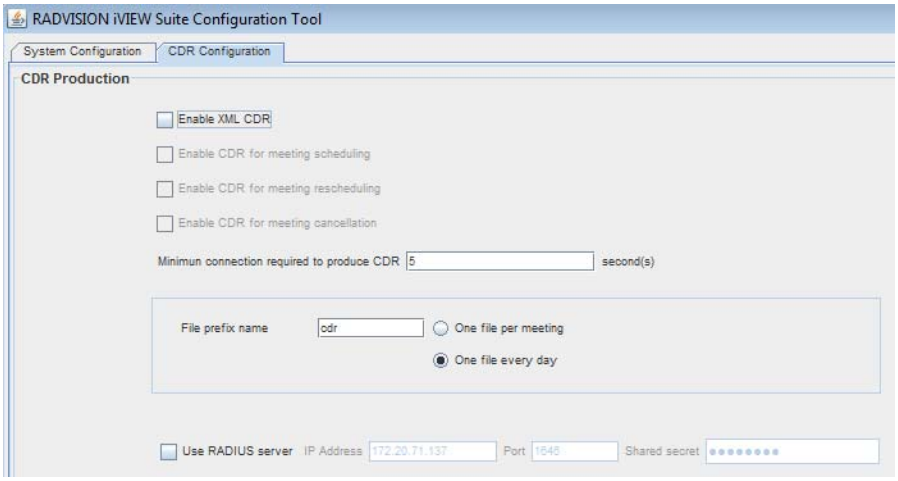
- Creating CDR information in XML format, by checking the **Enable XML CDR** field.
- Defining required terminal connection duration
- Defining an CDR file prefix

  A standard iVIEW Communications Manager installation creates a directory called iCM in the Program Files directory. For example, C:\Program Files\iVIEW Management Suite\iCM. CDR files are stored in a default sub-directory called cdrdata. For example, C:\Program Files\iVIEW Management Suite\iCM\cdrdata\cdrfilename.xml
- Defining how often CDRs are produced; one file per meeting or one file per day

  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

  Select Use RADIUS server to enable streaming. iVIEW Communications Manager and the RADIUS server exclusively use the shared secret password as part of the security system.

Figure 7-17 Defining CDRs



For a complete description of the XML tags used in the CDRs, see the *Reference Guide for iVIEW Management Suite CDR Files*.

Customizing Meeting Invitation E-mails

You can customize the content of the invitation e-mail that participants receive when a meeting is scheduled, modified or cancelled through iVIEW Management Suite or through iVIEW Management Suite Outlook plug-in.

When using iVIEW Management Suite or iVIEW Management Suite Outlook plug-in to schedule meetings, you check the participants availability in terms of their calendar, and the most important feature, you check iVIEW Management Suite resources availability for services and ports.

Note: Service providers should ensure that the URL used to access the SCOPIA Desktop virtual room in an organization should feature the organization's alias name.

Procedure

Step 1 Log in to iVIEW Communications Manager module of the iVIEW Management Suite.

Step 2 Click **Advanced Settings** in the sidebar menu.

Step 3 Click **Default Meeting Settings**.

Step 4 (Optional) Select **Customize the 'meeting invitation' introduction message** and then enter your text to override the introduction message in the initial meeting invitation e-mail.

Step 5 (Optional) Select **Customize the 'meeting update' introduction message** and enter your text to override the introduction message in the meeting update e-mail.

Step 6 (Optional) Select **Customize the 'meeting cancellation' introduction message** and enter your text to override the introduction message in the meeting cancellation e-mail.

Step 7 (Optional) Select **Override IP Terminal Access Information** and enter your text to override default access information for IP terminals.

Step 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 SCOPIA Gateways configured in iVIEW Communications Manager.

Step 9 (Optional) Select **Add LYNC/OCSR2 client access information** to include a link to a meeting in the Lync client or Office Communicator client.

Step 10 (Optional) Select **Hide the Attendees list** to hide the attendees section in the invitation e-mail.

Step 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 e-mail.

Step 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.

Step 13 Click **OK** to save your changes.

8 Generating Reports for Statistics and Analysis

You can generate reports for usage, utilization, statistics and history or call and meetings scheduled in the system.

- Generating Reports of Upcoming Meetings ..... page 206
- Generating a Call Information Report ..... page 208
- Generating a Port Usage Report ..... page 208
- Generating a Resource Usage Report ..... page 209
- Generating Statistic Report for Meetings ..... page 210
- Generating Reports for Finished Meetings ..... page 210
- Generating Bandwidth Utilization Reports ..... page 213
- Generating a Report of Network Device Performance and Availability ..... page 214

Generating Reports of Upcoming Meetings

On the Upcoming tab, 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.

Procedure

Step 1 Log in to iCM.

Step 2 Select **Meeting Monitoring** in the sidebar menu.

Step 3 Select **Upcoming**.

Step 4 Select the calendar icon in the From and To fields to choose a start and end date for information in the generated report.

Step 5 Select **Report**.

Table 8-1 describes the information categories that are included in a generated report.

Table 8-1 Generated Report Information Categories

Category	Description
Virtual Meeting ID	A meeting ID that can be dialed, used 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.
SCOPIA iVIEW Management Suite Meeting ID	Internal database ID for the meeting.
Meeting Subject/Party Name	Corresponds to Subject field in Meeting Scheduling.
Meeting Description	Corresponds to the Meeting Description field in Meeting Scheduling.
Location	Corresponds to the Location Preference 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.
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.

Step 6 Select **Save** to save the report to a location of your choice.

Generating 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

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

Step 1 Log in to iCM.

Step 2 Select **Reports and Statistics** in the sidebar menu.

Step 3 Select **Usage**.

Step 4 Select **Create New Report**.

Step 5 Select an option from the Report Type field.

Step 6 Select the time period to be covered by the report in the Graph X-Axis field.

Step 7 Select a start and end time for the report in the relevant fields.

Step 8 Select **Total Number** or **Total Duration (Minutes)** in the Graph Y-Axis field.

Step 9 Select a week range and hour range where relevant.

Step 10 (Optional) Select **Recent Report** to see the last call report generated.

Step 11 Select **Generate**.

The report appears on the in the Usage tab.

Step 12 (Optional) Select **Generate PDF Report** to print your report to a PDF file.

Generating a Port Usage Report

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

- MCU
- Gateway
- SCOPIA Desktop

The reports provide this information:

- System utilization peaks
- Terminal utilization
- Virtual room utilization

Procedure

Step 1 Log in to iCM.

Step 2 Select **Reports and Statistics** in the sidebar menu.

Step 3 Select **Utilization**.

Step 4 Select **Create New Report**.

Step 5 Select an option from the Report Type field.

Step 6 Select the time period to be covered by the report in the Graph X-Axis field.

Step 7 Select a start and end time for the report in the relevant fields.

Step 8 Select a week range and hour range where relevant.

Step 9 (Optional) Select **Recent Report** to see the last port utilization report generated.

Step 10 Select **Generate**.

The report appears on the in the Utilization tab.

Step 11 (Optional) Select **Generate PDF Report** to print your report to a PDF file.

Generating 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

Step 1 Log in to iCM.

Step 2 Select **Reports and Statistics** in the sidebar menu.

Step 3 Select **Utilization**.

Step 4 Select **Create New Report**.

Step 5 Select **Terminals Utilization** or **Virtual Room Utilization** from the Report Type field.

Step 6 Select up to 3 terminals or virtual rooms from the pop-up list and select **OK**.

Step 7 Select the time period to be covered by the report in the Graph X-Axis field.

Step 8 Select the start and end points for the report in the relevant fields.

Step 9 (Optional) Select **Recent Report** to see the last port utilization report generated.

Step 10 Select **Generate**.

The report appears on the in the Utilization tab.

Step 11 (Optional) Select **Generate PDF Report** to print your report to a PDF file.

Step 12 (Optional) Select **Generate Excel Report** to print your report to an Excel file.

Generating Statistic Report for Meetings

Statistic reports show the following information:

- The percentage of ad hoc meetings X scheduled meetings
- The percentage of each type of meeting including ad hoc and scheduled meetings
- The percentage of video calls X audio calls
- The percentage of SCOPIA Desktop calls X non-SCOPIA Desktop calls
- The percentage of meetings duration and size according to the number of participants

Procedure

Step 1 Log in to iVIEW Communications Manager.

Step 2 Select **Reports and Statistics** in the side bar.

Step 3 Select **Create New Report**.

Step 4 Select from the **Report Type** field one of the following options:

- General Meeting Statistics to view the percentage of your network meetings that are ad hoc and the percentage that are scheduled.
- Average Meeting Size to view a chart with your network meetings divided according to the number of participants.
- Average meeting Duration to view a chart with your network meetings divided according to the duration (in minutes) of the meeting.

Step 5 Set the period of time the report will cover.

Step 6 (Optional) Select **Recent Report** to display the last generated statistic report.

Step 7 Select **Generate**. The charts are displayed.

Step 8 (Optional) Select **Generate PDF Report** to convert the report to a pdf file.

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 Management 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.

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.

Procedure

Step 1 Log in to iCM.

Step 2 Select **Reports and Statistics** in the sidebar menu.

Step 3 Select **History**.

Step 4 To search for a specific meeting, do one of the following and select **Search**:

- Enter the partial or complete subject of the meeting in the Subject field. If any part of the meeting subject matches it, the meeting record is displayed.
- Enter the E.164 number of an attending terminal in the E.164 field.
- Select the calendar icon in the From or To field, and select a date and time in the window that opens. Meetings scheduled after or 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.

Step 5 Select the calendar icon in the From and To fields to choose a start and end date for information in the generated report.

Step 6 Select **Report**.

Table 8-1 describes the information categories that are included in a generated report.

Table 8-2 Generated Report Information Categories

Category	Description
Meeting ID/Party Number	A meeting ID which can be dialed 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.
SCOPIA iVIEW Management Suite Meeting ID	Internal database ID for the meeting.
Meeting Subject/Party Name	Corresponds to Subject field in Meeting Scheduling.
Meeting Description	Corresponds to the Meeting Description field in Meeting Scheduling.
Location	Corresponds to the Location 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.
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.

Step 7 Select **Save** to save the report to a location of your choice.

In order to improve Administrator visibility, real time information about bandwidth usage is available by generating a Bandwidth Usage report.

The guidelines and restrictions for generating the Bandwidth Utilization report include:

- The Utilization Tab will only be displayed if there is one or more zones and at least one of them has a configured bandwidth limit.
- If there is no limit for the bandwidth, the utilization will always be set to zero.
- Once a report is created, a Summary link is available to present data in a text format.

Procedure

Step 1 Log in to iCM.

Step 2 Select **Reports and Statistics** icon in the sidebar menu.

Step 3 Select **Utilization**.

Step 4 Select **Create New Report**.

Step 5 Select **Bandwidth Utilization** from the Report Type field.

Step 6 Select the time period to be covered by the report in the Graph X-Axis field.

Step 7 Select a start and end time for the report in the relevant fields.

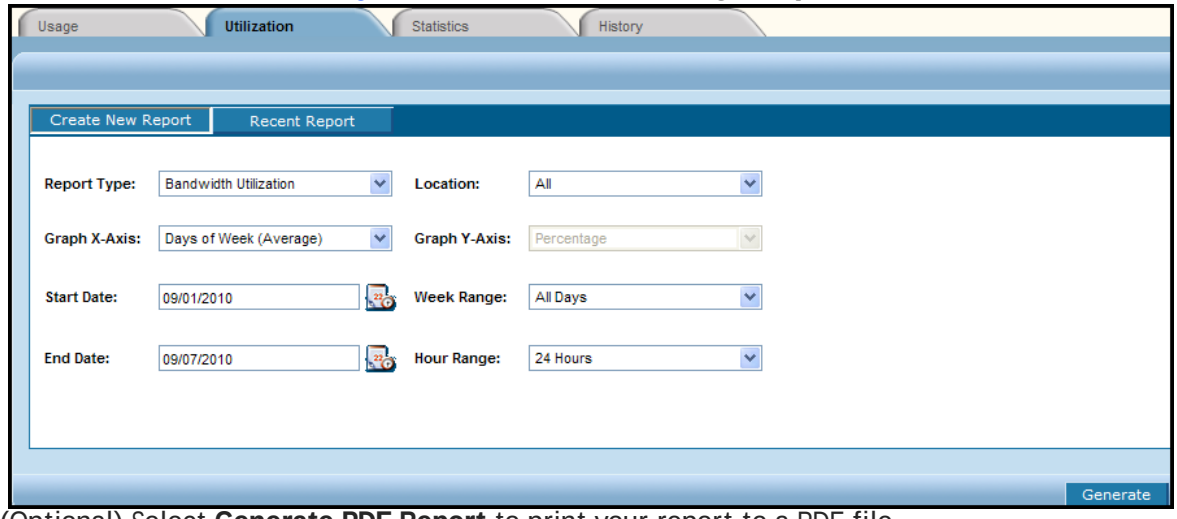
Step 8 Select a week range and hour range where relevant.

Step 9 (Optional) Select **Recent Report** to see the last port utilization report generated.

Step 10 Select **Generate**.

The report appears on the in the Utilization tab.

Figure 8-1 Bandwidth Usage Report



Step 11 (Optional) Select **Generate PDF Report** to print your report to a PDF file.

Generating a Report of Network Device Performance and Availability

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

Step 1 Log in to iCM.

Step 2 Select **Device Monitoring** in the sidebar menu.

Step 3 Select **Resource Availability** or **Statistics**.

Step 4 Select the calendar icons by the From and To fields to select a start and end period within which to generate the report.

Step 5 Select **Generate Report**.

Information about each device is included in the report.

Step 6 Select **Save** to save the report.

Step 7 Browse to the location in which you want to save the file, enter the file name and type, and then select **Save**.



About RADVISION

RADVISION (NASDAQ: RVSN) is the industry's leading provider of market-proven products and technologies for unified visual communications over IP, 3G and IMS networks. With its complete set of standards-based video communications solutions 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 IMS networks. To gain additional insights into our products, technology and opinions, visit blog.radvision.com. For more information about RADVISION, visit www.radvision.com

USA/Americas
T +1 201 689 6300
F +1 201 689 6301
infoUSA@radvision.com

EMEA
T +44 20 3178 8685
F +44 20 3178 5717
infoUK@radvision.com

APAC
T +852 3472 4388
F +852 2801 4071
infoAPAC@radvision.com

This document is not part of a contract of license as may be expressly agreed RADVISION is registered trademarks of RADVISION, Ltd. All trademarks recognized. All rights reserved © 2010 RADVISION, Ltd.

RADVISION®
Delivering the Visual Experience®