InformaCast Virtual Appliance Basic Paging®

Version 11.0.2

Installation and User Guide for a Cisco® Unified Communications Manager Environment

June 29, 2015

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2015 Cisco Systems, Inc. All rights reserved.

© 2015 Singlewire. All rights reserved.

InformaCast is a trademark of Singlewire Software.

All other referenced trademarks are trademarks of their respective owners and our reference to them does not imply or indicate any approval, endorsement, sponsorship or affiliation with such owners unless such approval, endorsement, sponsorship or affiliation is expressly indicated.

Last Updated: June 29, 2015

CONTENTS

InformaCast Virtual Appliance Basic Paging Overview 1-1
- Intended Audience 1-1
- User Guide Standards 1-1
- Prerequisites 1-2
- Hardware Requirements 1-2
- Port Configuration 1-3
- DSCP Quality of Service Policies 1-4
- Licensing Information 1-5
- InformaCast Illustrations 1-6
- Virtual Appliance Interface Orientation 1-6
- Troubleshooting 1-11
- Getting Help 1-11
- Technical Support 1-12

Install InformaCast 2-1
- Prepare Your Multicast Environment 2-1
- Install InformaCast Virtual Appliance 2-6
- Access InformaCast Virtual Appliance 2-21
- Update JTAPI 2-22
- Set the System Time 2-27
- Integrate CUCM 2-30
- Manage Installation Administration 2-70

Access InformaCast 3-1
- Log into InformaCast for the First Time 3-2
- Change the Administrator's Password 3-6
- View Your License Key 3-7

Configure Recipients 4-1
- Manage InformaCast's Telephony 4-2
- Manage Recipient Groups 4-11
- Manage Recipient Administration 4-37

Configure Messages and Broadcasts 5-1
- Manage Messages 5-1
- Manage SIP Functionality 5-4
- Manage DialCasts 5-40
- Send a DialCast/Broadcast 5-45
- Cancel a DialCast/Broadcast 5-46

Maintain InformaCast 6-1
Manage InformaCast Backups 6-2
Manage Phone Updates 6-12
Configure SNMP Monitoring 6-14
Configure Session Timeout 6-15
Upgrade InformaCast from Basic to Advanced 7-1
Note the Differences 7-2
Upgrade InformaCast 7-3
Enter Your New License Key 7-9
Frequently Asked Questions (FAQ) 8-1
Troubleshooting 9-1
Server Hardening 9-1
Multicast 9-1
Log Files 9-1
Resolve EULA Error 9-2
Log into InformaCast Virtual Appliance's Interfaces 9-2
Start/Stop/Restart InformaCast and its Server 9-3
VMware Tools 9-3
Authentication 9-3
Phone Discovery 9-4
Broadcasts 9-5
Upgrading InformaCast 9-7
Upgrading from Basic to Advanced InformaCast 9-7
Manage InformaCast Virtual Appliance 10-1
Log into InformaCast Virtual Appliance's Interfaces 10-1
Manage Virtual Appliance Actions 10-10
Change the InformaCast Virtual Appliance's Password 10-17
Change InformaCast Virtual Appliance's IP Address 10-20
Upgrade your VMware Tools 10-24
Upgrade InformaCast Virtual Appliance 10-25
Release Notes 11-1
InformaCast 11.0.2 11-1
InformaCast 11.0.1.a 11-2
InformaCast 11.0.1 11-2
InformaCast 9.1.1 11-3
InformaCast 9.0.2 11-4
InformaCast 9.0.1 11-5
InformaCast 8.5.1 11-7
InformaCast 8.4.a 11-8

InformaCast 8.3.a 11-9
InformaCast 8.3 11-10
Glossary 12-1
Acknowledgments 13-1
Index 14-1

InformaCast Virtual Appliance Basic Paging Overview

InformaCast Virtual Appliance Basic Paging is Singlewire's bundled package for virtualized environments. It contains a virtual machine (the Virtual Appliance) and InformaCast Basic Paging (InformaCast or Basic InformaCast), Singlewire Software's IP telephony broadcast application that allows you to send a live audio stream to Cisco IP phones. InformaCast is designed to get messages quickly to large groups of people; when these messages are sent through InformaCast, they are called *broadcasts*.

In addition, InformaCast exposes its powerful representational state transfer (REST) application programming interface (API) that allows you to combine your existing technology with a notification component. If you're interested in using InformaCast's REST API, please see http://www.singlewire.com/help/InformaCastAPI/ for more information.

Intended Audience

This guide is intended for the users and administrators of InformaCast Virtual appliance and will walk you through the installation, configuration, and administration of both the application and the virtual machine.

There are three versions of this guide: one for installations using Basic Paging, one for installations using Advanced Notification in conjunction with Cisco's Unified Communications Manager (CUCM), and one for installations using Advanced Notification in conjunction with a Hybrid Runtime Environment (HRE). Please make sure you have the right version by looking at the cover page, or by looking at the environment type printed at the bottom of every page.

The versions are both separate and overlapping. Where versions overlap, *InformaCast* will be used. Where versions differ, *Advanced InformaCast* or *Basic InformaCast* will be used.

User Guide Standards

Specific fonts are used to represent specific kinds of information in this guide. The fonts and their meaning are listed here:

- **Bold fonts** indicate the name of a button, text field, or other element with which you interact and any text that you must enter.
- *Italic fonts* indicate the name of an area or section on one of the applications' pages.
- Angled brackets enclose text that varies with your specific environment, i.e. http://<Your IP Address> means that you would enter your specific IP address instead of the brackets and what they enclose.
- Blue, underlined text indicates a hyperlink.

- Underlined text indicates a tooltip in the user interface. Hover your mouse over the tooltip to see an explanation of the underlined text.

There are several kinds of notification boxes used in this guide:

- **Tip.** These offer advice or "best practices."
- **Note.** These contain additional information, usually relevant in special cases.
- **Caution.** These contain information about a procedure that may reduce the performance of your system.
- **Warning.** These contain information about a procedure that can impair or disable your system.

Prerequisites

InformaCast has the following prerequisites:

- Compliance with the hardware requirements as defined in this user guide (see "Hardware Requirements" on page 1-2)
- Use of supported phones if you intend to use them as broadcast recipients (go to http://www.singlewire.com/compatibility-matrix.html and click the **Cisco IP Phones** link)
- Use of one of the following supported browsers: Firefox 38, Chrome 43, or Internet Explorer 11
- Multicast routing enabled and configured for all network segments between InformaCast and its phones
- A static IP address configured on the InformaCast Virtual Appliance
- A Cisco Unified Communications Manager (CUCM) server (including Business Edition 6000); the following versions are supported: 8.5.1, 8.6.2, 9.0.1, 9.1.2, 10.0.1, 10.5.2, and 11.0.1
- Web access enabled on any Cisco IP phones working with InformaCast
- SNMP enabled on all servers in a CUCM cluster
- The AXL service running on at least one server in the CUCM cluster
- The CTIManager service running on at least one node that's also running the CallManager service. The CTIManager service can run on up to eight nodes in a cluster, and you should use more than one node with this service for redundancy.

You must also know how to obtain access to the command-line interface (bash prompt) of InformaCast, perform basic UNIX commands, and use nano for editing files.

Tip Singlewire recommends a screen resolution of at least 1024x768.

Hardware Requirements

You should deploy InformaCast Virtual Appliance on hardware supported by VMware ESXi because it provides the lowest overhead of the VMware products (other VMware products such as VMware Player, VMware Workstation, or VMware Server will work for lab or demonstration purposes). VMware ESXi is available free of charge from vmware.com. If VMware is new to you, you may find these resources useful:

- Learn more about what benefits VMware can provide your organization
- How to install VMware ESXi

If you are unsure whether your server hardware supports VMware, check the VMware ESXi compatibility list.

For a list of Singlewire-supported VMware ESXi versions, go to http://www.singlewire.com/compatibility-matrix.html and click the **InformaCast Platform** link.

InformaCast Virtual Appliance requires:

- 4Gb of memory
- A dedicated virtual CPU (vCPU); the operating system and application are 32-bit, and may run on 32- or 64-bit CPUs. For IP phone deployments, InformaCast does not have a minimum CPU speed requirement; regardless of the number of phones, InformaCast will scale to meet the need. In general, faster CPU means faster phone activation time.
- A single virtual NIC configured for bridging, not NAT; InformaCast Virtual Appliance will not work through NAT'd network connections
- 80Gb disk, which can be either local disk or SAN-attached disk (the SAN may be of any type supported by VMware)

As a virtual machine (VM), InformaCast Virtual Appliance may be run co-resident with other Cisco UC virtual machines on a VMware ESX host (a solution that is supported by Cisco's TAC), as long as you don't modify the InformaCast OVA configuration or oversubscribe the host CPU or memory. It is possible to run more virtual machines than the VMware host physically supports (i.e. oversubscription), but this will adversely affect audio quality and phone activation performance. In order to avoid oversubscribing your VMware host, please make sure the following is true:

- The sum of all vCPUs does not exceed the number of cores on the VMware host
- The sum of memory needed by all VMs does not exceed the amount of physical RAM on the VMware host
- The InformaCast Virtual Appliance is run in thick disk mode

Port Configuration

When configuring your firewall for compatibility with InformaCast Virtual Appliance, use the following tables, which depend on the direction of your traffic.

Note This list of ports applies only to the Virtual Appliance side (i.e. server side). It does not include those for clients' workstations.

Table 1: Inbound Traffic

Port	Protocol	Application and/or Purpose
22	TCP	Secure shell (SSH) for server management
80	TCP	Singlewire Start page's non-secure web interface
123	UDP	Network Time Protocol (NTP)
427	TCP and UDP	InformaCast SLP

Table 1: Inbound Traffic

Port	Protocol	Application and/or Purpose
443	TCP	Singlewire Start page's secure web interface
1161	UDP	InformaCast SNMP
8081	TCP	InformaCast's non-secure web interface
8101	TCP	Control Center's non-secure web interface
8444	TCP	InformaCast's secure web interface
8463	TCP	Control Center's secure web interface
10000	TCP	Webmin interface
32068-32468	UDP	InformaCast's inbound RTP streams (inbound calls to CTI ports and inbound SIP)
5060-1	TCP	InformaCast's SIP

Table 2: Outbound Traffic

Port	Protocol	Application and/or Purpose
80	TCP	InformaCast's outbound connections to IP phones
161	UDP	CUCM SNMP phone data
427	UDP and TCP	InformaCast SLP
443	TCP	Secure web interface for: • webservices.singlewire.com • CUCM AXL web services
2748	TCP	CUCM's CTI ports/route points
20480-21080	UDP	Default multicast ports to which InformaCast sends audio
32068-32468	UDP	InformaCast's outbound RTP streams (outbound calls to CTI ports and outbound SIP)

DSCP Quality of Service Policies

InformaCast puts real-time audio traffic on the network. To ensure that your time-sensitive network traffic reaches its destination, you can prioritize network traffic to provide certain levels of Quality of Service (QoS). Using the Differentiated Services Code Point (DSCP) field in the IP Header of a packet, you can mark, or "color," traffic to denote the type of packet and priority or place in the queue. InformaCast has no direct requirements, but will color its traffic to fit into the standard and recommended queues outlined by Cisco's Solution Reference Network Design (SRND) guide (see http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book/QoSIntro.html).

The DSCP values in the following table will be applied to their respective types of traffic.

Table 3: DSCP QoS Policies

DSCP	Traffic Type Leaving Server
EF	Voice Media Real-time Transport Protocol (RTP)
CS3	Call control for Session Initiation Protocol (SIP) and Computer Telephony Integration (CTI)
0	All other traffic leaving the server

These values cannot be modified within the InformaCast application. If you must make modifications to the defaults, you will have to change them on the network itself. See http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book/QoSIntro.html for more information.

Licensing Information

InformaCast's Virtual Appliance functionality is based on its license, and depending on the license you have, you will be able to access all of InformaCast's functionality or only parts of it. *InformaCast Basic Paging* functionality includes the ability to send live audio broadcasts to up to 50 phones by dialing a number on your Cisco IP phone. Among other features, *InformaCast Advanced Notification* functionality includes the ability to:

- Send a number of different types of broadcasts (e.g. live audio, pre-recorded audio, pre-recorded audio and text, etc.) using your Cisco IP phone's interface and/or InformaCast's web interface
- Interact with InformaCast's plugins (e.g. conduct conference calls, trigger contact closures, post to Twitter, send broadcasts to email addresses, etc.)
- Customize scripts that can be attached to broadcasts
- Receive confirmation when broadcasts are sent
- Configure resiliency

Note Upgrading from Basic to Advanced InformaCast is easily accomplished through the **Try** or **Buy** icons or by contacting Singlewire to obtain a license for a switch in functionality. Downgrading from Advanced InformaCast back to Basic is accomplished by clicking the **Stop Advanced Notification Trial** button on InformaCast's Manage License Key page (**Admin** | **Manage License Key**). This will cause InformaCast to reboot, as will any future change in InformaCast functionality or license type.

In addition to Basic and Advanced functionality, InformaCast can also be obtained with a basic, trial, demonstration, subscription, or perpetual license. The basic license applies only to Basic InformaCast functionality, is embedded within the application, and exists in perpetuity. The rest of the licenses apply only to Advanced InformaCast and can be obtained through Singlewire Software.

The *trial license* is included with your initial copy of InformaCast and allows you to try Advanced InformaCast for free for 60 days. If you downgrade to Basic InformaCast before your trial period ends, you can elect to resume your trial for the remaining period (e.g. obtain Basic InformaCast, upgrade to Advanced InformaCast through the trial, use Advanced InformaCast for 30 days, downgrade to Basic

InformaCast, and upgrade to Advanced InformaCast through the trial for the remainder of the 60 days). When your trial period ends, you can elect to go back to Basic InformaCast or you can contact Singlewire to obtain a demonstration, subscription, or perpetual license.

The *demonstration license* allows you to try Advanced InformaCast for a set period of time. Because it ends on a certain date, you cannot downgrade to Basic InformaCast and then resume Advanced InformaCast on the demo license past its expiration date (e.g. you cannot obtain Basic InformaCast, upgrade to Advanced InformaCast through the trial, obtain a demonstration license of Advanced InformaCast that is valid for two weeks, downgrade to Basic InformaCast after one week, and resume using Advanced InformaCast three weeks later).

The *subscription license* allows you to purchase Advanced InformaCast without the hassle of a long-term contract; however, you must install InformaCast on an Internet-accessible server.

The *perpetual license* allows you to purchase Advanced InformaCast and own it outright for a one-time, upfront fee with no expiration date. Both subscription and perpetual licenses come with access to Singlewire's Support team and free software upgrades.

Caution If you upgrade from Basic to Advanced InformaCast through either the trial, demonstration, subscription or perpetual licenses and you decide to return to Basic functionality, all additional information entered during your Advanced phase will not be saved (e.g. when you revert to Basic from Advanced, any information you entered after you upgraded initially—dialing configurations, users, recipient groups, etc.—will not be available once you downgrade to Basic InformaCast). If you choose to upgrade back to Advanced InformaCast, that information will reappear; however, any new information you entered after you reverted to Basic functionality will be unavailable.

Warning **If you are moving from Basic InformaCast to Advanced InformaCast (and you have previously had Advanced InformaCast), InformaCast will be restarted with the installation of this new license. Please plan your upgrades accordingly.**

InformaCast Illustrations

The web-based administrative interface to InformaCast is dynamic; it changes with the kind of environment (Basic or Advanced) as well as the permitted capabilities of the person logged into the administrative webpages. Therefore, the screenshots displayed in this guide may not exactly match what you see on your system. However, as specific points are covered in the instructions, the salient interface elements will be shown.

Virtual Appliance Interface Orientation

If you have a specific task in mind, peruse the "Contents" on page i-iii to locate the instructions for that task. Additionally, the index that starts on page IN-1 can help you locate desired information.

InformaCast has multiple user interfaces:

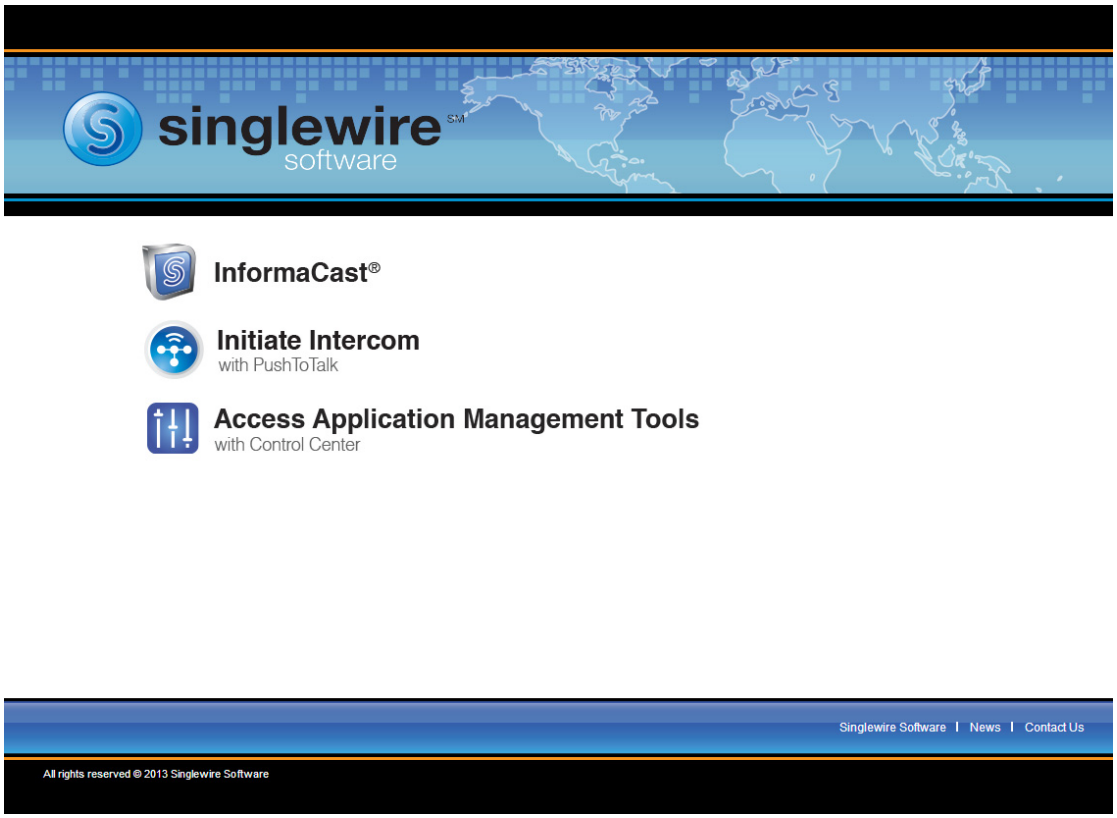
- Singlewire Start page
- InformaCast web interface
- Control Center

- Virtual machine administrative web interface (Webmin)
- Command line interface (CLI)

Note The initial login credentials for all interfaces are **admin** (login) and **changeMe** (password).

Singlewire Start Page

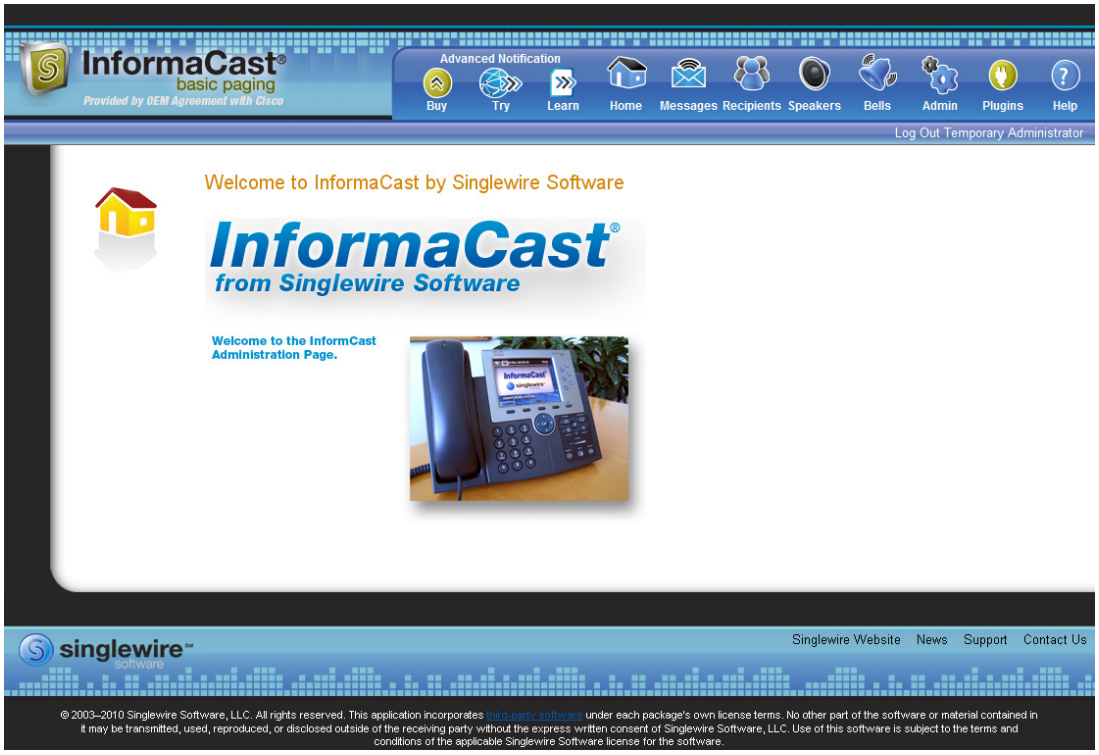
The Singlewire Start page is accessible through a web browser addressed with the IP address of your Virtual Appliance, and it contains links to InformaCast and the Control Center.



Though you see a link for PushToTalk you cannot access this application with Basic InformaCast.

InformaCast Web Interface

The webpages you'll use to administer InformaCast are comprised of navigational icons at the top, which also house dropdown menus, and an administration pane whose contents change with what you're doing. The icons and their options also change with the access permissions you have in InformaCast.



Depending on your access level, you'll have access to:

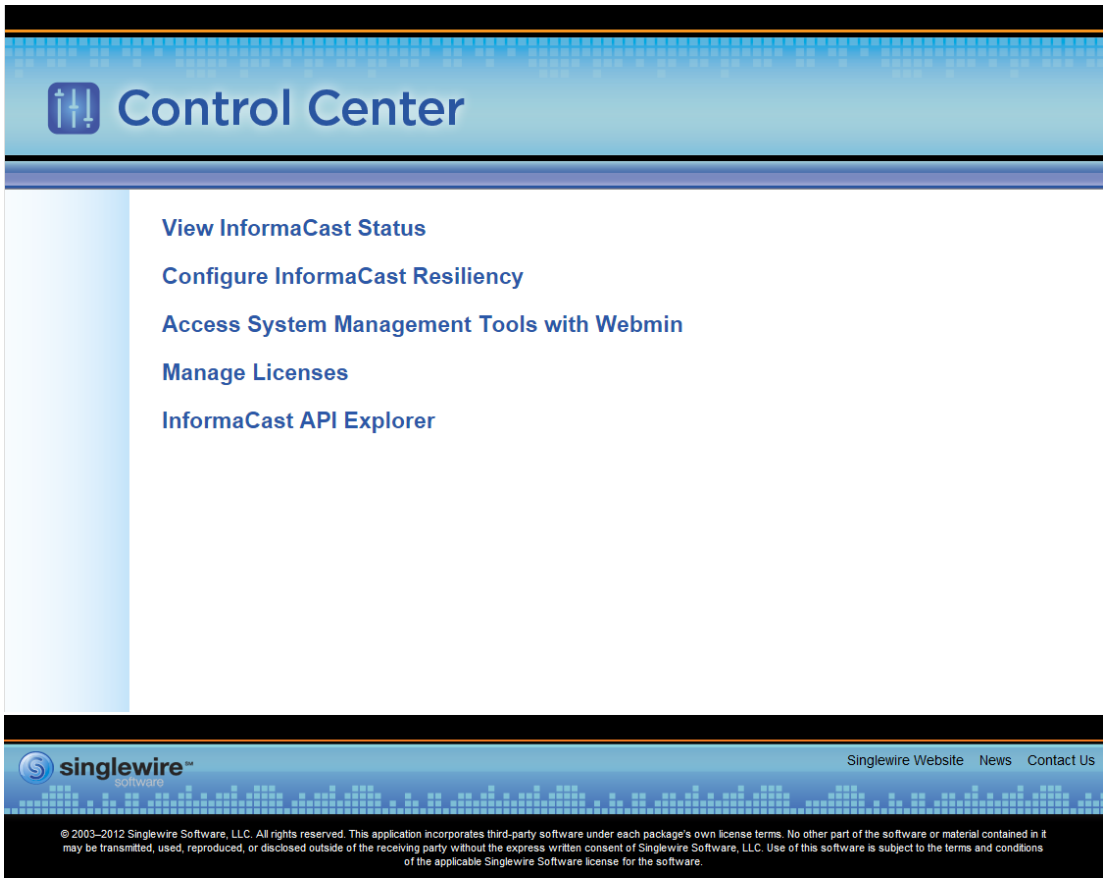
- **Home.** InformaCast's homepage, complete with RSS news feed.
- **Messages.** The message administration page.
- **Recipients.** The recipient group administration page, allowing you to create and manage recipient groups.
- **Admin.** The configuration overview page, allowing you to view scheduled updates and backups; manage the license key; and set up the system, network, and broadcast parameters, along with DialCasts.
- **Help.** InformaCast's help pages, allowing you access to various aspects of the online help system.

Three additional icons (**Try**, **Buy**, and **Learn**) allow you to try Advanced InformaCast through a 60-day free trial, upgrade to Advanced InformaCast through a perpetual or subscription license, or learn more about the features of Advanced InformaCast.

Note While in Basic InformaCast, you will see a number of menu items that are grayed out, and you will not be able to access them. These menu items are only available when you have Advanced InformaCast.

Control Center

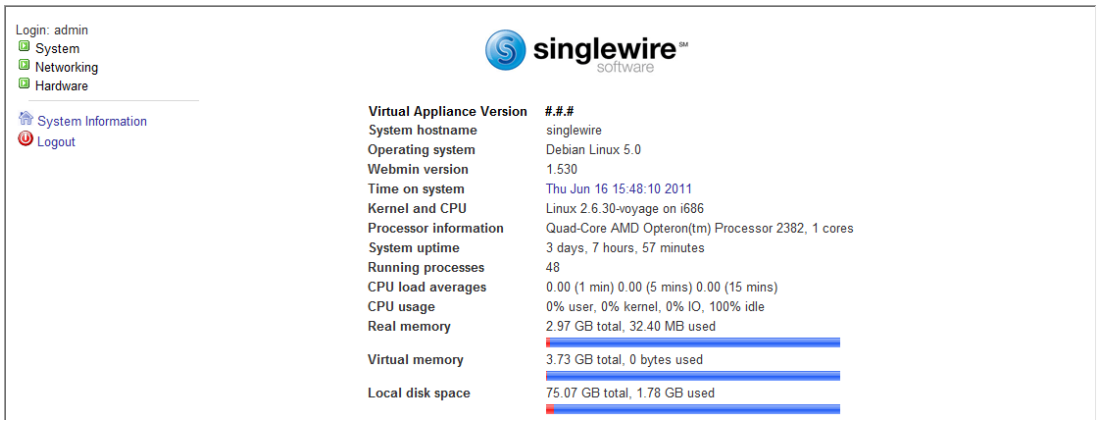
Control Center is designed to be an inclusive destination for application- and system-level accessories. Here, you can view InformaCast's status (e.g. running time, JTAPI version, etc.) or access the License Manager to update your Basic license with an Advanced version (see "Upload a New License" on page 10-31). Through the Control Center, you can also access Webmin, the administrative web interface used for administering the underlying operating system of the Virtual Appliance (e.g. configuring the network interface, stopping and starting applications, and shutting down the virtual machine). Lastly, if you're interested in InformaCast's API, the InformaCast API Explorer is your window to viewing the operations and resources that the InformaCast API has to offer, crafting API requests, and reviewing the information the API will provide based on your requests. See http://www.singlewire.com/help/InformaCastAPI/ for more information.



Note The **Configure InformaCast Resiliency** link is dependent upon your license containing resiliency functionality; if your license doesn't include resiliency, you won't see the link.

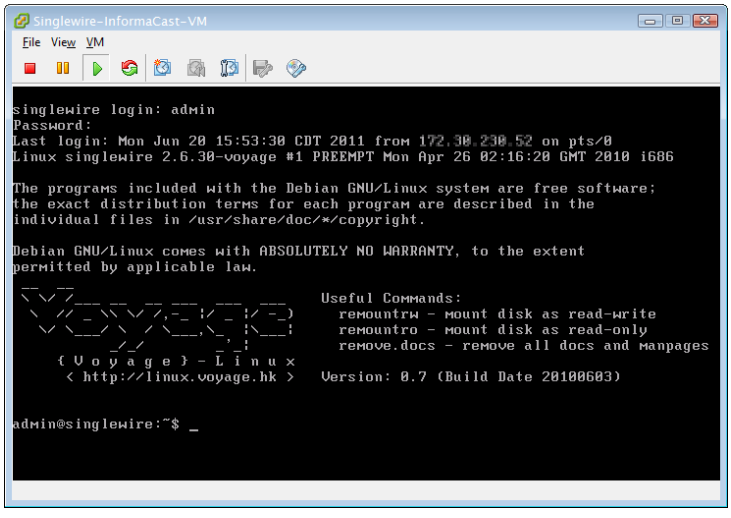
Virtual Appliance Administrative Web Interface (Webmin)

The Virtual Appliance administrative web interface (accessed through the Control Center) is used for administering the underlying operating system of the virtual machine, e.g. configuring the network interface, stopping and starting InformaCast and shutting down the virtual machine.



Command Line Interface

Outside of the Singlewire Start page, the command line interface is a text-based interface used for support issues and some configuration procedures (e.g. those that require manual editing of files or the running of scripts). The command line interface uses the bash command line shell, and can be accessed via a virtual machine console window or over the network through the use of an SSH (Secure Shell) client.



Note Rudimentary knowledge of bash is required to use the command line interface. If files are to be edited on the virtual machine itself, knowledge of the nano text editor is also required. If you are not familiar with the nano editor, you can optionally transfer files that need to be modified to another machine, edit them there, and then transfer the modified file back to the InformaCast virtual machine. The transfer

process can be achieved via an SCP (Secure Copy) client, such as PSCP on Windows. PuTTY, available as a free download (http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html), contains all the necessary tools for transferring files.

Troubleshooting

If you've followed the instructions in this guide and are still having trouble getting InformaCast to work, "Frequently Asked Questions (FAQ)" on page 8-1 may help you figure out what's wrong. You may also find a useful answer in "Troubleshooting" on page 9-1.

Getting Help

Your first line of support is the **Help** icon. Clicking it takes you to the online help system. Accessing its dropdown menu allows you to access:

- The online help system
- Its FAQ section
- Its Troubleshooting section
- InformaCast's Support page

Note If you do not have an active network connection to the Internet, not all of the content on InformaCast's Support page or homepage will be available.

InformaCast's Support page (**Help** | **Support**) is where you can access all of the previously listed online help links as well as the Calling Terminal Diagnostics page, InformaCast's Performance, Summary, and SIP logs, and the log collection tool.

Technical Support

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Install InformaCast

Many of the concepts involved in installing InformaCast Virtual Appliance require familiarity with VMware ESXi and CUCM.

The general steps to install InformaCast are:

- "Prepare Your Multicast Environment" on page 2-1
- "Install InformaCast Virtual Appliance" on page 2-6
- "Access InformaCast Virtual Appliance" on page 2-21
- "Update JTAPI" on page 2-22
- "Set the System Time" on page 2-27
- "Integrate CUCM" on page 2-30
- "Manage Installation Administration" on page 2-70

Prepare Your Multicast Environment

You must enable multicast across your network in order for your recipients to receive the audio portion of InformaCast broadcasts.

Caution Just because music on hold works on your phones does not mean that it is using multicast. Music on hold can be used with either unicast or multicast.

Plan for a Multicast Environment

Multicast is communication between a single sender and multiple receivers on a network. InformaCast has no special requirements for how multicast is enabled, and you should use your network vendor's best practices and design considerations. Multicast is typically routed with Protocol Independent Multicast (PIM) that is deployed in either sparse or dense mode. InformaCast will work with either mode.

For WAN links where your circuit provider will not route your multicast, you can configure GRE tunnels, which carry your multicast traffic from the location where the InformaCast server is located to its recipients. The only traffic that needs to traverse these GRE tunnels is the multicast traffic you might want to route. The tunnels do not need to create a full mesh between sites; they only need to be configured from the hub location to the spoke location(s). Please see the following link for details: http://www.cisco.com/en/US/tech/tk828/technologies_configuration_example09186a00801a5aa2.shtml

For recipients to receive the audio portion of InformaCast broadcasts, they make requests using Internet Group Management Protocol (IGMP). While most networks default to IGMPv2, newer recipients may use IGMPv3. If newer recipients are being deployed, be sure to enable the newer protocol version on network devices.

Network design and multicast configuration is outside the scope for which Singlewire can provide support. It is recommended that you work with your network vendor or partner. The following table provides guides and resources for more information on configuring multicast on your network.

Resource	Description
Quick Start Guide	Cisco IP Multicast Quick Start Configuration that provides concise configuration examples
Design Guides	Cisco Design Zone for IP Multicast for access to the AVVID SRND for Multicast Design
Multicast Troubleshooting	Cisco IP Multicast Troubleshooting Guide
IGMP Snooping	Cisco CGMP and IGMP Snooping documentation
GRE Tunnels	Cisco Multicast over a GRE Tunnel (for when a WAN carrier will not route multicast)
Testing Tool	Singlewire tool to send and receive multicast traffic, which can be used to verify and troubleshoot multicast routing
Protocol Analyzer	Wireshark download link, which can be used to view network traffic for troubleshooting

If you have a Cisco network, you can work with the Cisco TAC or locate a local Cisco Partner. The following table provides Cisco resources for configuration help.

Resource	Description
Support Home	Cisco Troubleshooting Homepage
Phone or Email	Cisco TAC Telephone Numbers
Open Case Online	Cisco TAC Case Creation Tool
Partner Locator	Locate a Cisco Partner to contract for network consulting

Test Your Multicast Environment

Once you've configured multicast across your network, it's important to test that configuration to ensure that all of your recipients receive the audio portion of InformaCast's broadcasts. Singlewire offers a Multicast Testing Tool to help troubleshoot and isolate multicast routing issues. It can be downloaded from the Singlewire Support website at http://info.singlewire.com/singlewire-networking-support-tools/.

There are three options available to you with the Multicast Testing Tool:

- Option 1 has the tool working as a multicast server and transmitting packets to the network
- Option 2 has the tool working as a multicast client and receiving packets

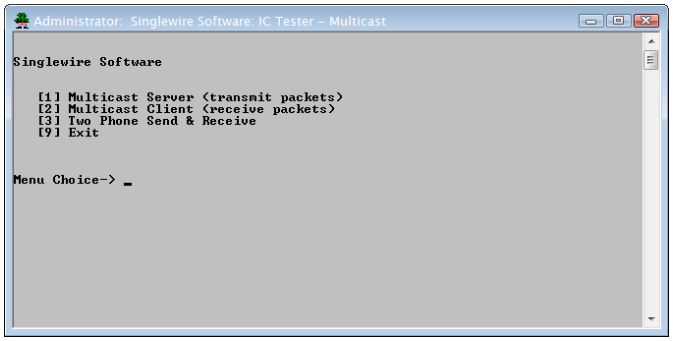
Note Typically, you will want to run Options 1 and 2 in tandem: Option 1 on a Windows machine on the same subnet as InformaCast and Option 2 on the location of your recipients (i.e. a PC on the same VLAN as your recipients).

- Option 3 allows the tool to "hijack" two phones: one to receive packets and the other to transmit them

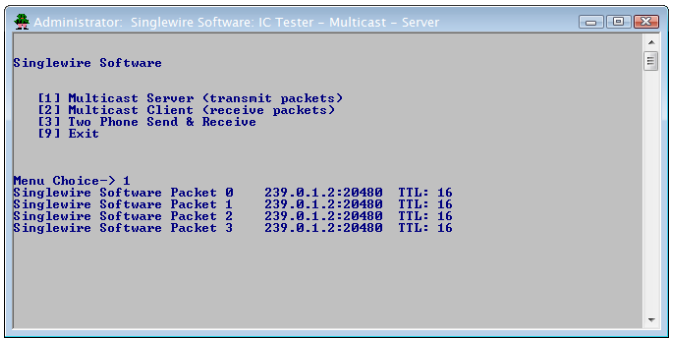
Use Options 1 and 2

Use the following steps to have the Multicast Testing Tool act as a multicast server and transmit packets to the network from one location, and act as a multicast client and receive packets from a different location.

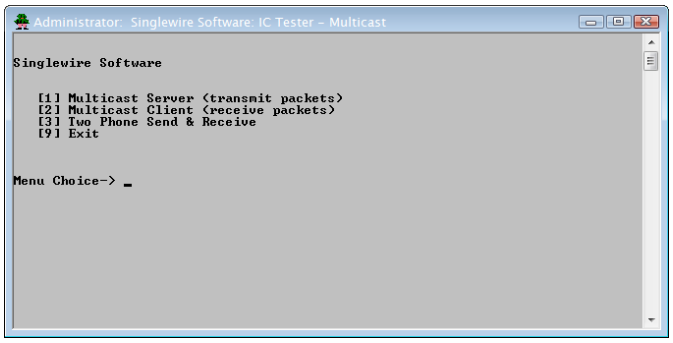
Step 1 Open the **IC_Tester_Mcast.exe** file on a Windows machine on the same subnet as the Virtual Appliance. The IC Tester - Multicast window appears.



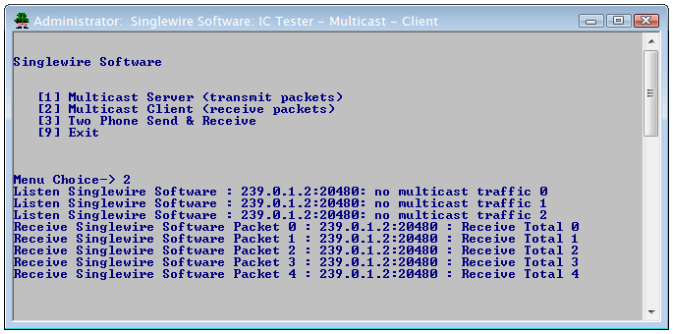
Step 2 Enter **1** at the **Menu Choice** prompt and press the **Enter** key. The IC Tester - Multicast window refreshes, showing multicast packets being sent across your network.



Step 3 Open the **IC_Tester_Mcast.exe** file at the location of your recipients. The IC Tester - Multicast window appears.



Step 4 Enter **2** at the **Menu Choice** prompt and press the **Enter** key. The IC Tester - Multicast window refreshes, showing it initially failed to find multicast, but then detects it.



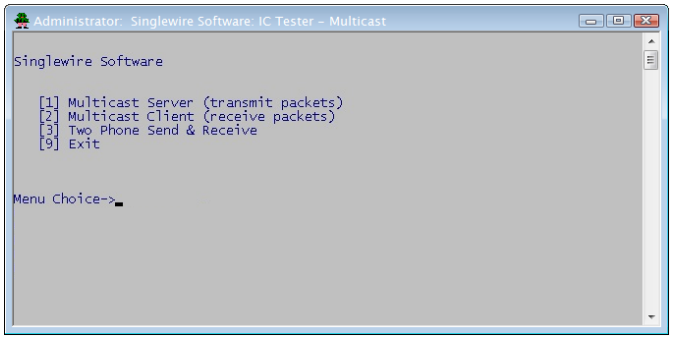
If you receive a "no multicast traffic" result, you can try Option 3, follow the recommendations in "Review Multicast Configuration" on page 2-70, or see "Multicast" on page 9-1.

Use Option 3

Use the following steps to have the Multicast Testing Tool "hijack" two phones: one to receive packets and the other to transmit them.

Note You will need the IP addresses of two phones on your network and the username and password of the application user associated with both of those phones. Work with your CUCM administrator if you don't have this information on hand.

Step 1 Open the **IC_Tester_Mcast.exe** file on the same network as your phones. The IC Tester - Multicast window appears.



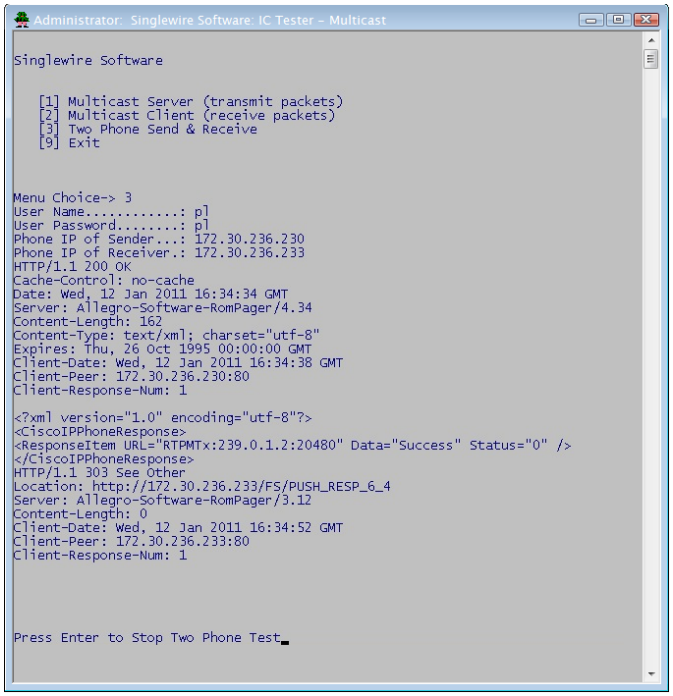
Step 2 Enter **3** at the **Menu Choice** prompt and press the **Enter** key.

Step 3 Enter the username of the application user associated with your phones at the **User Name** prompt and press the **Enter** key.

Step 4 Enter the password of the application user associated with your phones at the **User Password** prompt and press the **Enter** key.

Step 5 Enter the IP address of the phone that will source the multicast packets at the **Phone IP of Sender** prompt and press the **Enter** key.

Step 6 Enter the IP address of the phone that will receive the multicast packets at the **Phone IP of Receiver** prompt and press the **Enter** key. The IC Tester - Multicast window shows the phones' reply to the commands sent by the Multicast Testing Tool.



Step 7 Pick up the receiver of the source phone and speak into it. Your voice should be heard coming from the receiving phone.

If you can't hear any audio, follow the recommendations in "Review Multicast Configuration" on page 2-70 or see "Multicast" on page 9-1.

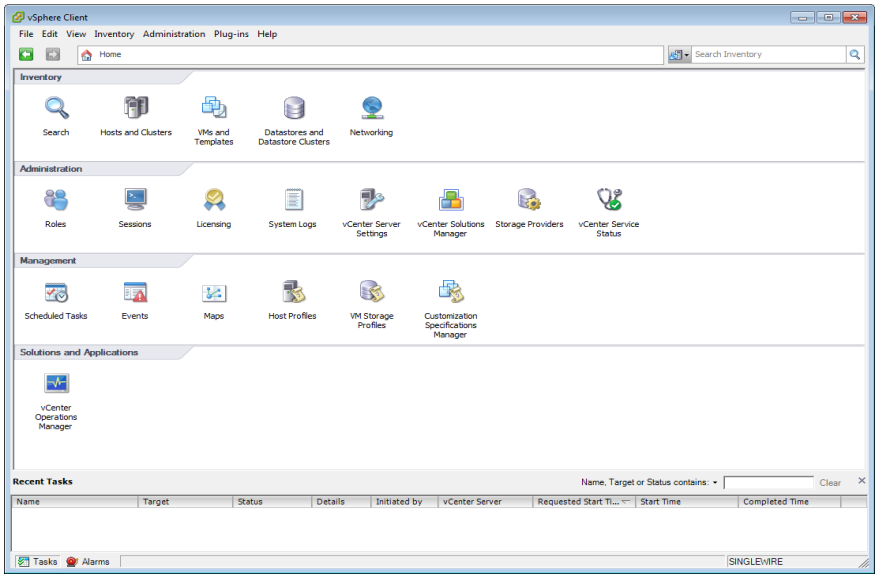
Install InformaCast Virtual Appliance

Singlewire supports InformaCast Virtual Appliance on the VMware ESXi platform, which is managed through the vSphere client. This section describes how to import InformaCast Virtual Appliance using the vSphere client. Your client can be downloaded from your VMware server.

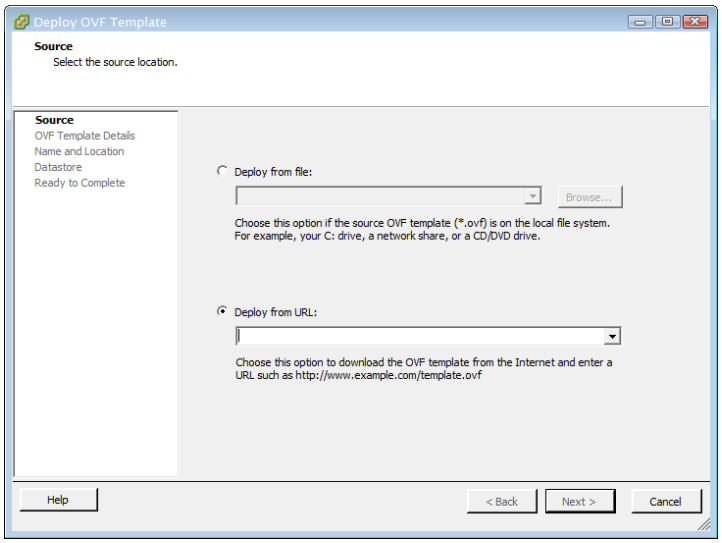
Step 1 Download the OVA file from Cisco's website.

Note If you are using InformaCast on the CUCM Business Edition 6000, you will be supplied with a DVD in a package with an OVA on it (physical media).

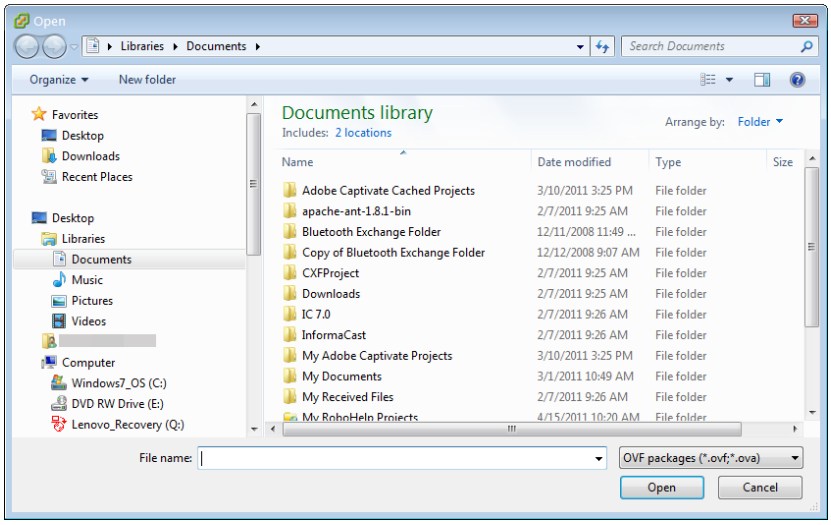
Step 2 Open and log into the vSphere client. The vSphere Client window appears.



Step 3 Go to **File** | **Deploy OVF Template**. The Deploy OVF Template dialog box appears.

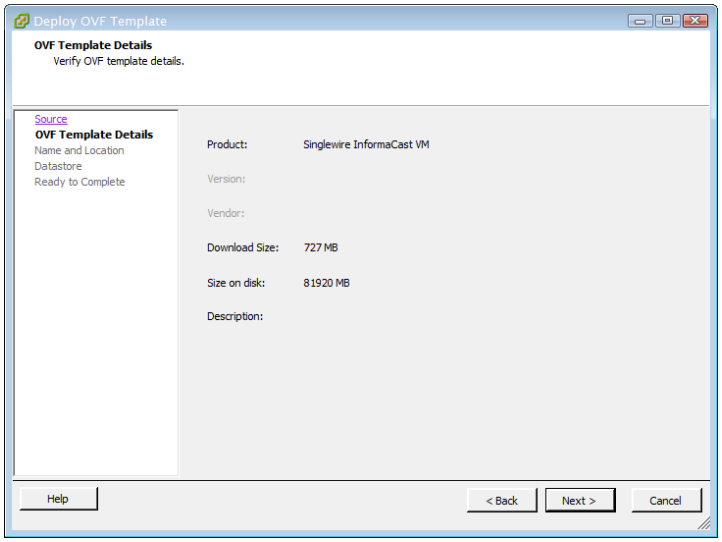


Step 4 Click the **Deploy from File** radio button and click its **Browse** button. The Open dialog box appears.

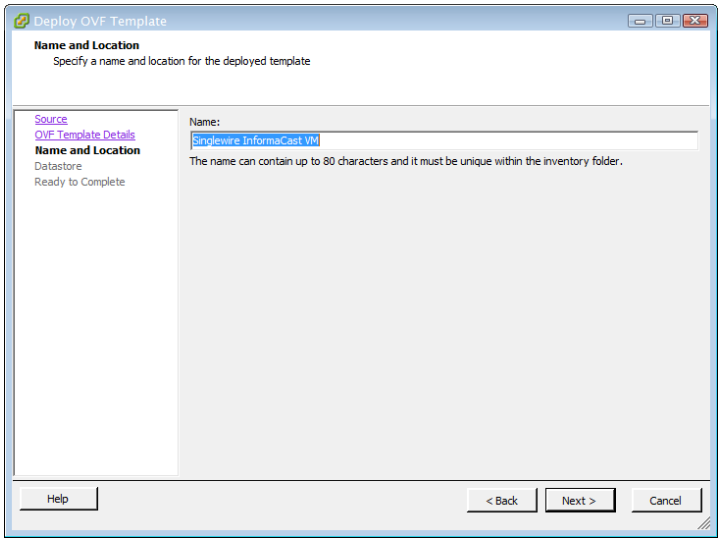


Step 5 Navigate to where you saved the OVA file (or to the OVA file on the supplied DVD), select it, and click the **Open** button.

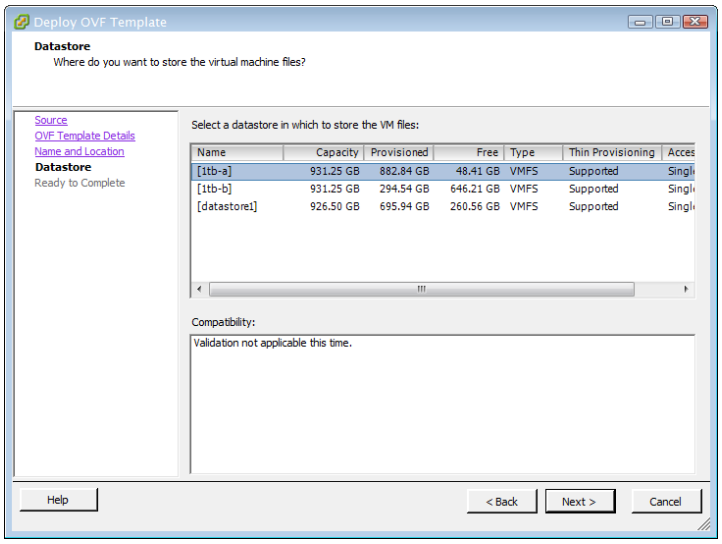
Step 6 Click the **Next** button. The Deploy OVF Template dialog box refreshes.



Step 7 Click the **Next** button. The Deploy OVF Template dialog box refreshes.



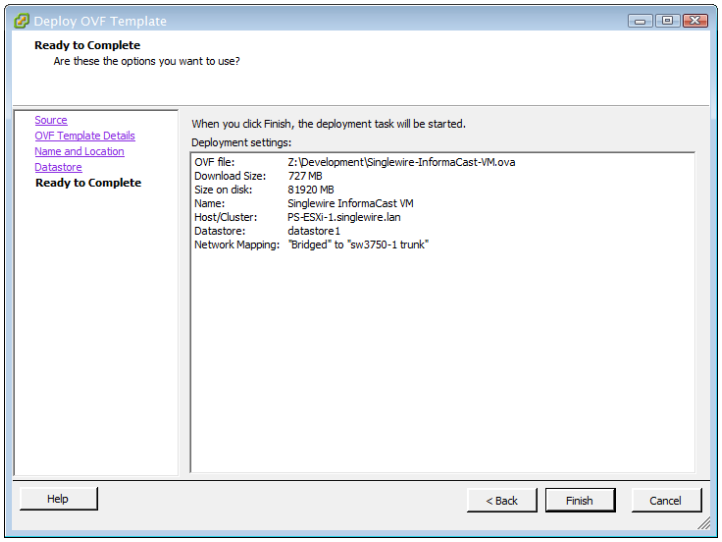
Step 8 Click the **Next** button. The Deploy OVF Template dialog box refreshes.



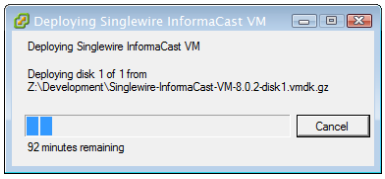
Step 9 Select the network on which the new virtual machine will reside and click the **Next** button.

Tip It is good practice to place the Virtual Appliance on the same VLAN as your CUCM.

The Deploy OVF template dialog box refreshes.

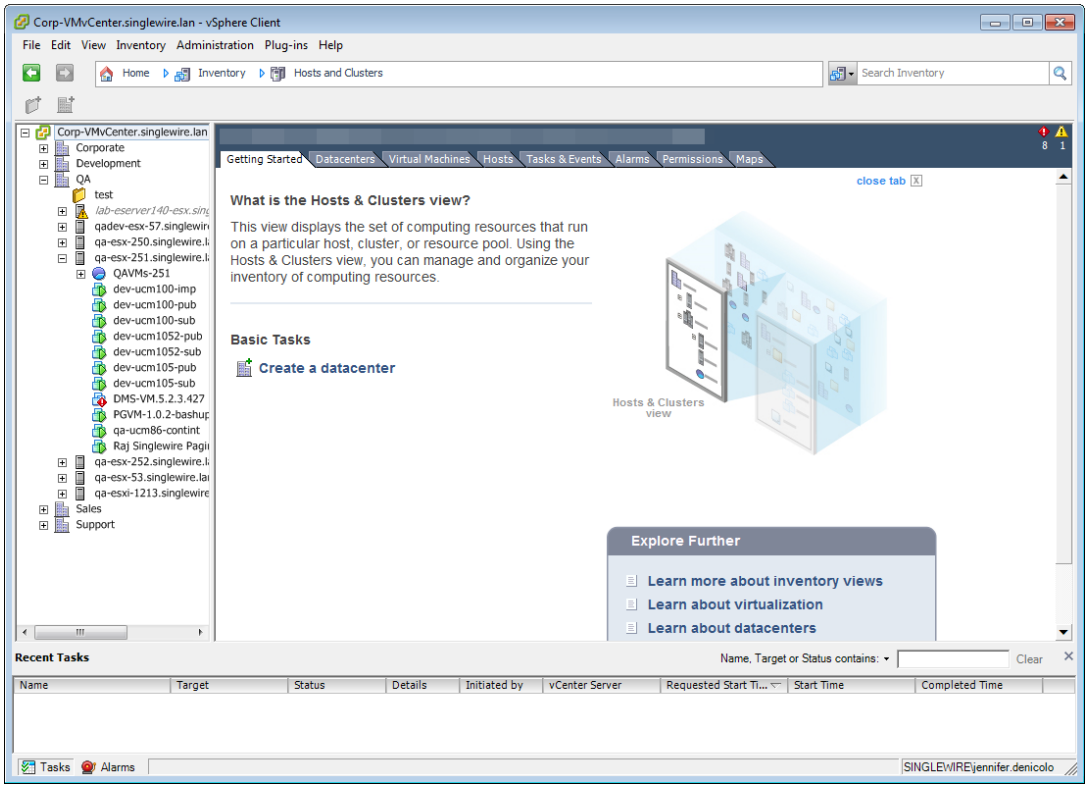


Step 10 Click the **Finish** button. InformaCast Virtual Appliance will begin importing.

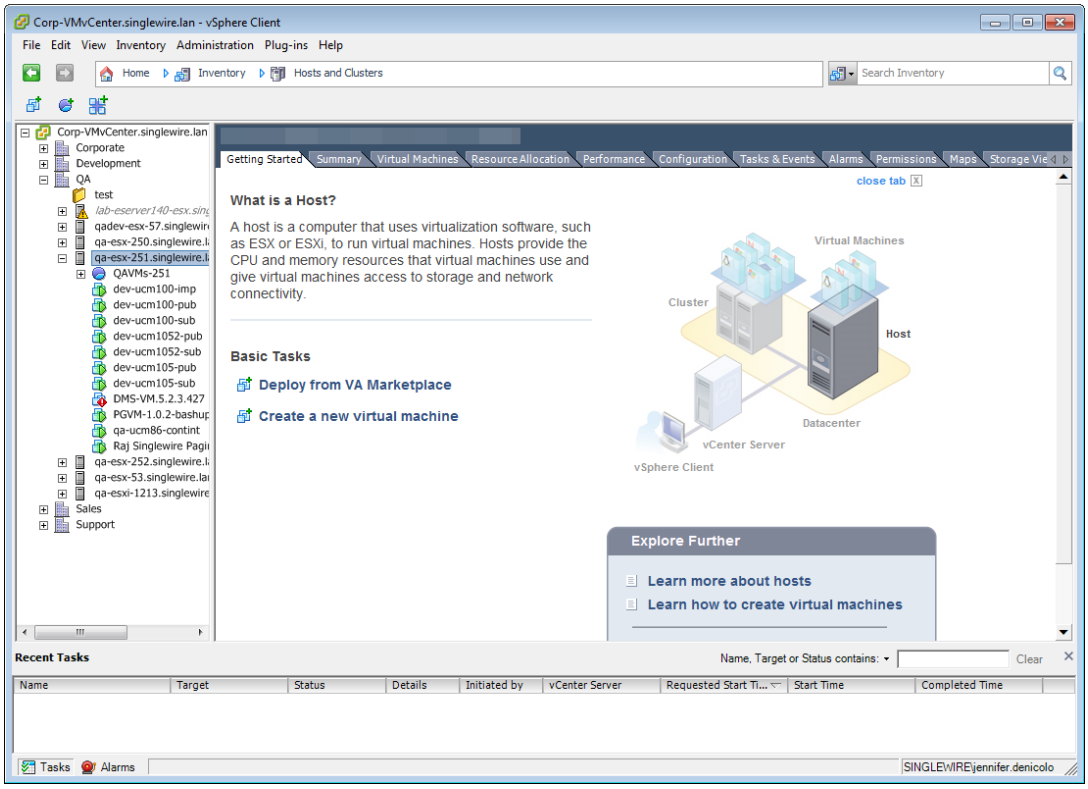


When it's finished, click the **Close** button.

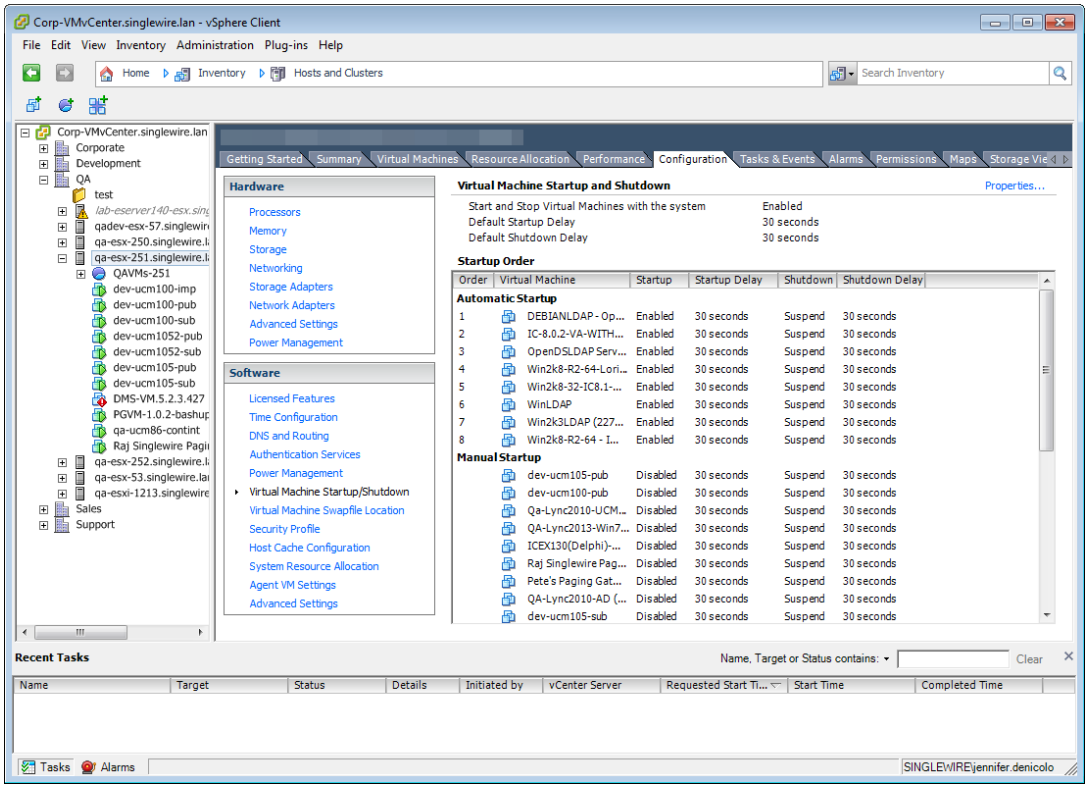
Step 11 Go back to your vSphere Client window and click the **Hosts and Clusters** icon ( ). The vSphere Client window refreshes.



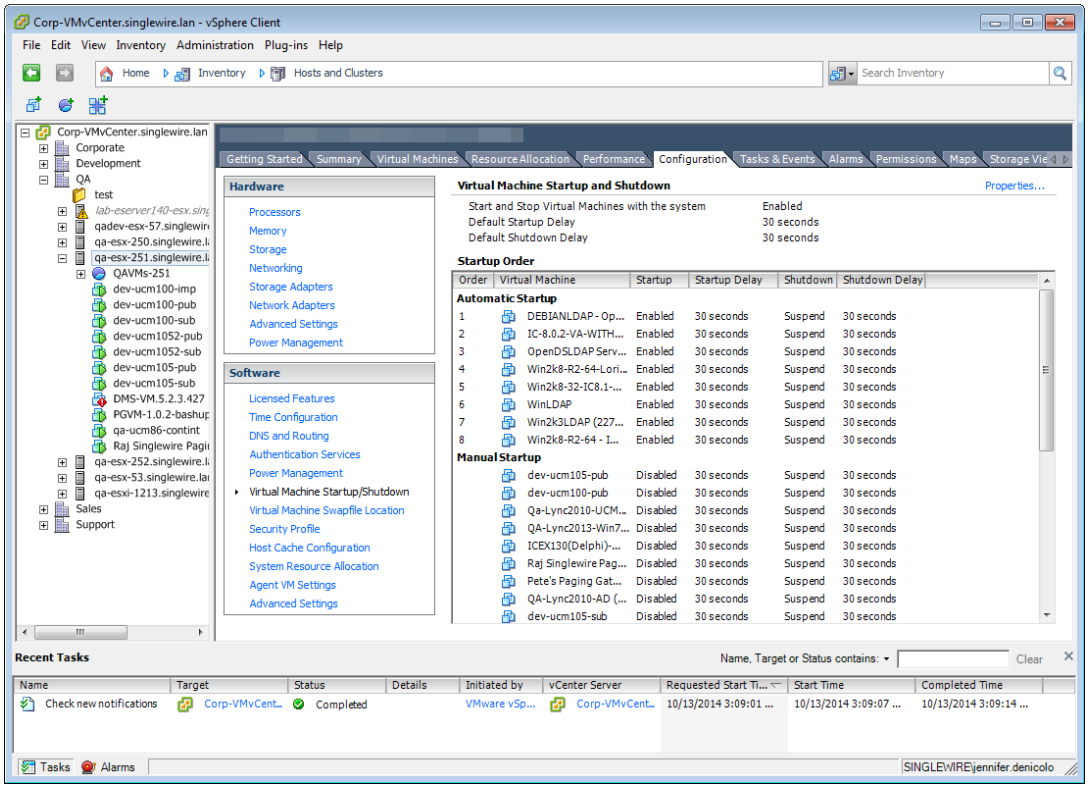
Step 12 Select your host server. The vSphere Client window refreshes.



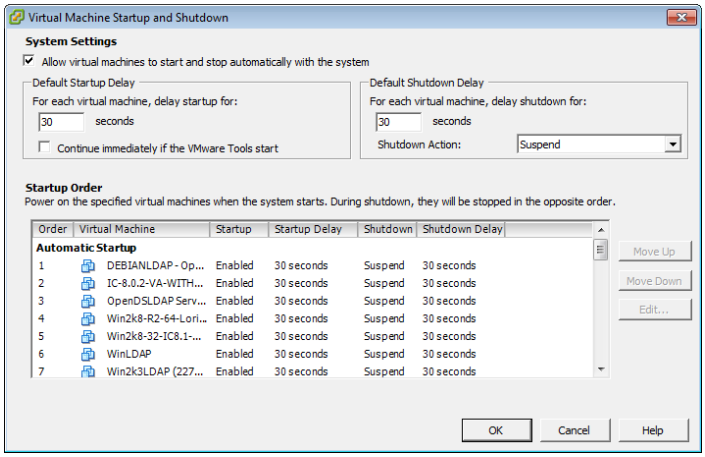
Step 13 Click the **Configuration** tab. The vSphere Client window refreshes.



Step 14 Click the **Virtual Machine Startup/Shutdown** link in the *Software* area. The vSphere Client window refreshes.



Step 15 Click the **Properties** link in the upper right corner. The Virtual Machine Startup and Shutdown dialog box appears.

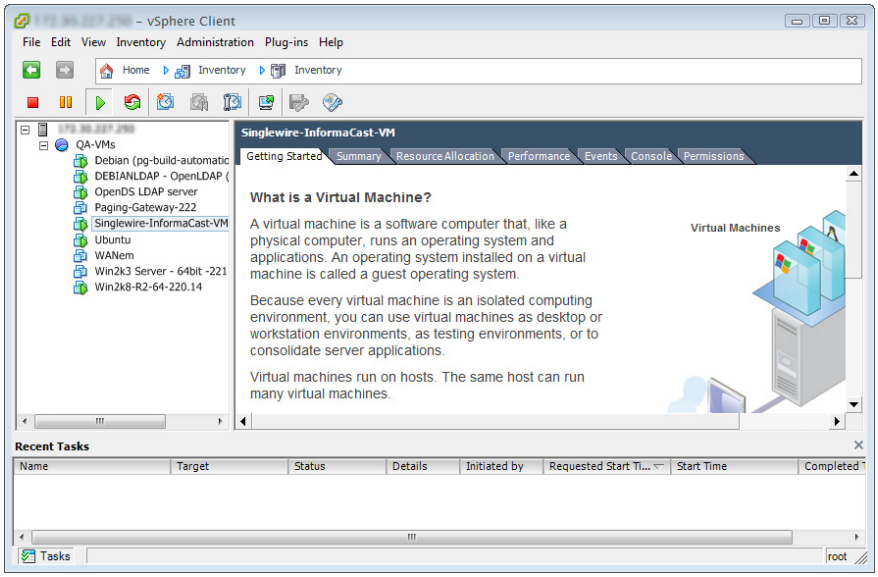


Step 16 Select the **Allow virtual machines to start and stop automatically with the system** checkbox in the *System Settings* area.

Step 17 Scroll to the **Manual Startup** section of the **Startup Order** field, select your virtual machine (by default, this is Singlewire InformaCast VM), and move it from the **Manual Startup** section to the **Automatic Startup** section using the **Move Up** button.

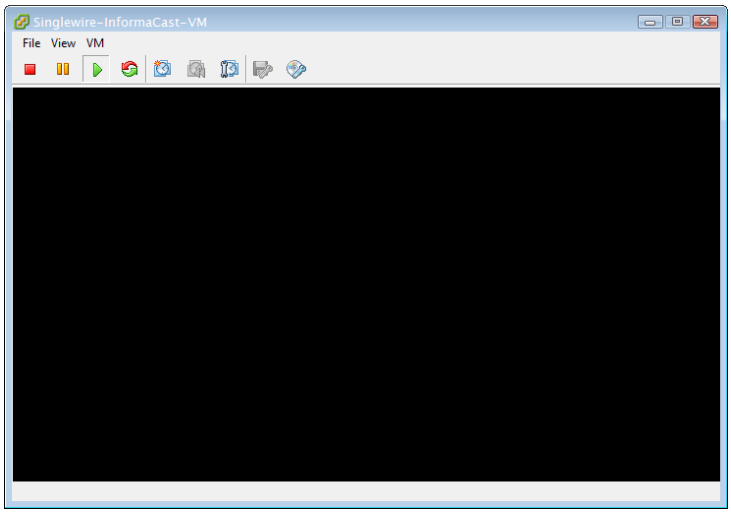
Step 18 Click the **OK** button. The InformaCast Virtual Appliance will now start and stop automatically with the server on which it's housed. Now you will turn on InformaCast's virtual machine and set its network configuration.

Step 19 Go to **View** | **Inventory** | **VMs and Templates**. The vSphere Client window refreshes.

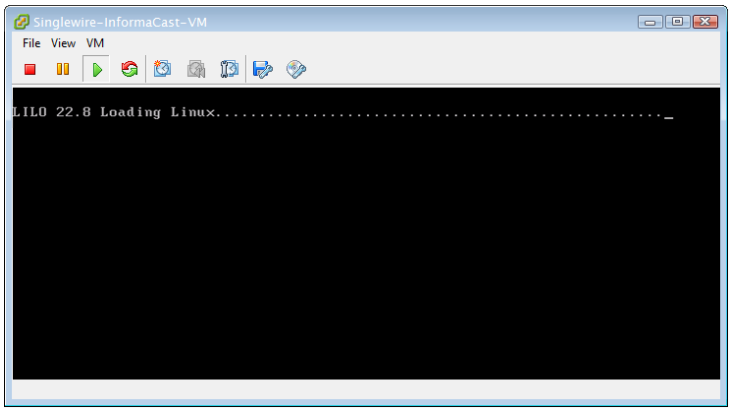


Step 20 Select your virtual machine.

Step 21 Go to **Inventory** | **Virtual Machine** | **Open Console**. The Singlewire InformaCast VM console window appears.

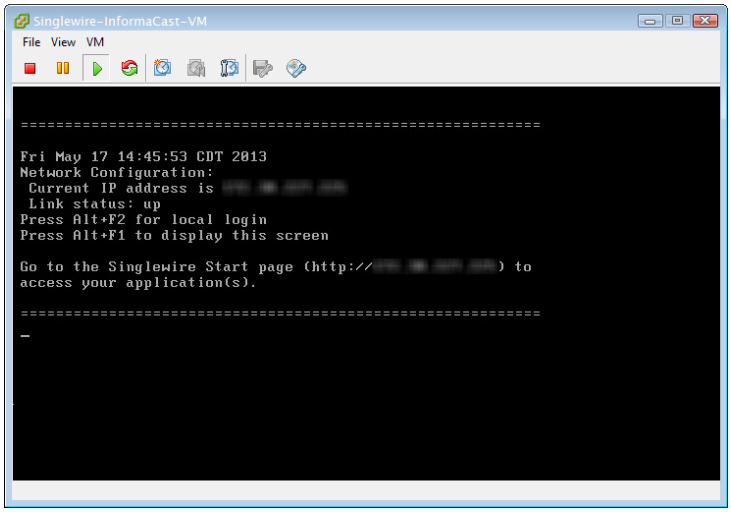


Step 22 Click the green arrow button ( ) to turn on the virtual machine. The Singlewire InformaCast VM console window begins booting the virtual machine.



Note Depending on the hardware resources available to InformaCast Virtual Appliance, it will likely boot in less than a minute.

When InformaCast Virtual Appliance is done booting, it will acquire an IP address using DHCP (if there is a DHCP server available). The acquired DHCP address can be seen in the console.



Note Singlewire recommends that you configure a static IP address for InformaCast Virtual Appliance. For specifics on IP addresses and packet routing, please see your network administrator.

SwiftStart will then start automatically, and you will see the End User License Agreement (EULA) page.

Note SwiftStart will only automatically start on the initial boot of InformaCast Virtual Appliance.

Step 23 Click the **I Agree** button to accept the EULA.

Note If you do not accept the End User License Agreement, InformaCast will not be started and you will not be able to progress to further installation and configuration steps in this guide.

If you have DHCP enabled on your network, you will see the following picture:

If you do not have DHCP enabled on your network, you will see the following picture:

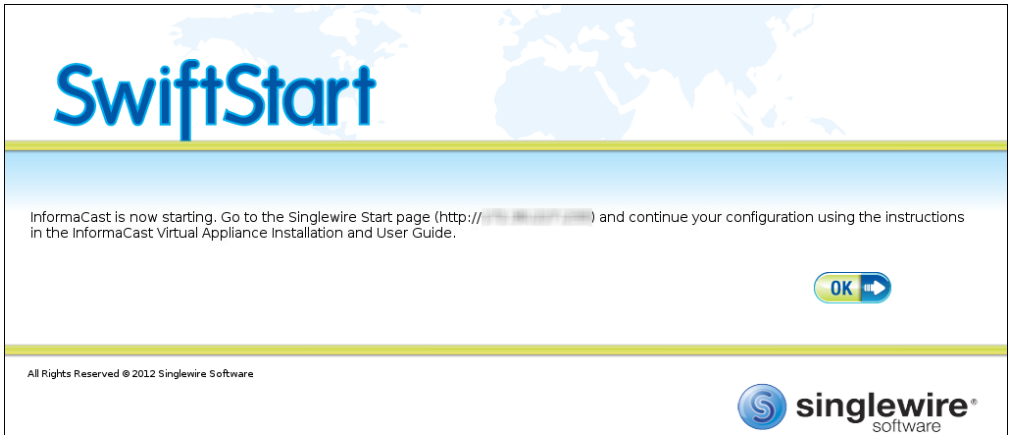
Step 24 Determine if you will use DHCP or manual entry to set the static IP address of InformaCast:

- Selecting the **Use DHCP Parameters** radio button will allow SwiftStart to make static the IP address it has detected, pull the relevant network configuration information from this IP address, and configure your network to work with InformaCast.
- Selecting the **Enter Manually** radio button will allow you to enter a routable IP address on your network that's not currently in use, a valid netmask for that IP address, its default gateway, the IP address(es) of a DNS server(s) on your network.

Step 25 Click the **Submit** button. SwiftStart will make the IP address you've configured/entered static and configure your network to work with InformaCast.

When your network configuration is successful, the Network Configuration page will refresh with a statement confirming the success.

Step 26 Click the **Finish** button. The SwiftStart window appears with a note about starting InformaCast.



Step 27 Click the **OK** button and close your open console window.

Access InformaCast Virtual Appliance

If you completed all of the SwiftStart steps in "Install InformaCast Virtual Appliance" on page 2-6, the InformaCast Virtual Appliance should be running and you can access the Singlewire Start page, which houses the links to the Virtual Appliance's user interfaces.

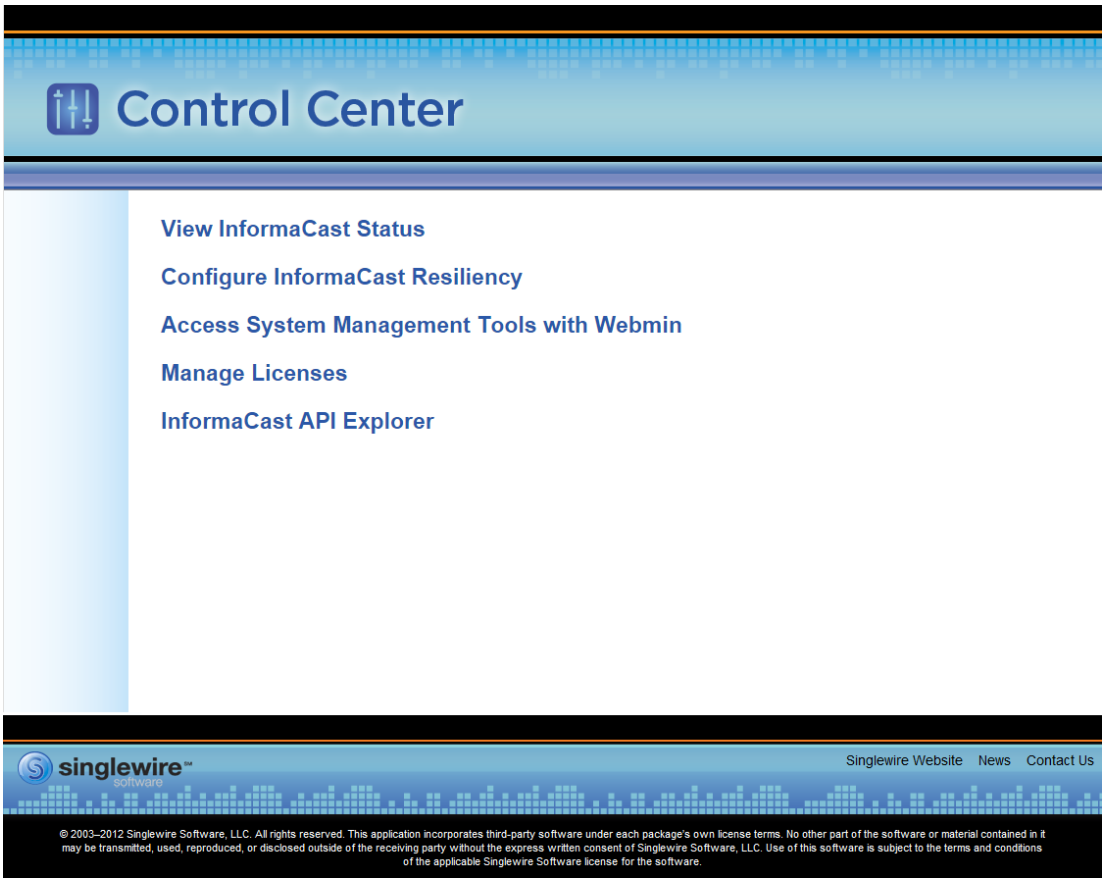
Open a web browser, enter the IP address of the InformaCast Virtual Appliance (which you set in Step 24 on page 2-19), and press the **Enter** key. The Singlewire Start page appears.

Tip The Singlewire Start page allows you to easily access all of your Virtual Appliance user interfaces along with application- and system-level management tools. You may find it helpful to both keep this tab/window open during the time that you're working with the Virtual Appliance and bookmark it for future use.

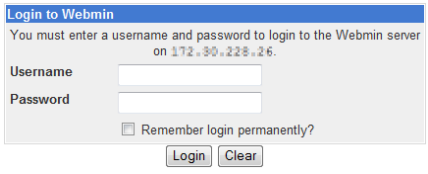
Update JTAPI

When you initially install InformaCast Virtual Appliance or whenever you change versions of CUCM, you need to update the JTAPI library used by InformaCast Virtual Appliance to the same version used by your CUCM server.

Step 1 Click the **Access Application Management Tools with Control Center** link on the Singlewire Start page. A separate tab/window opens to the Control Center menu page.

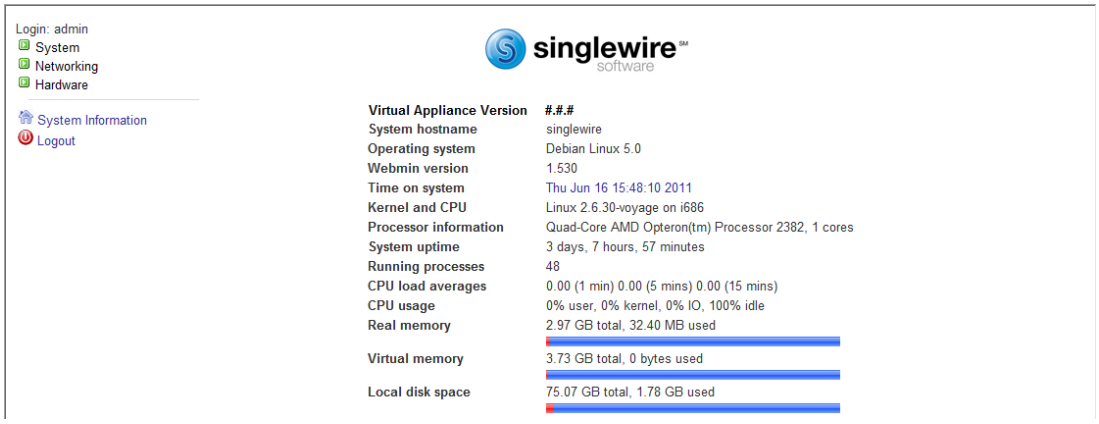


Step 2 Click the **Access System Management Tools with Webmin** link. The Login to Webmin page appears.

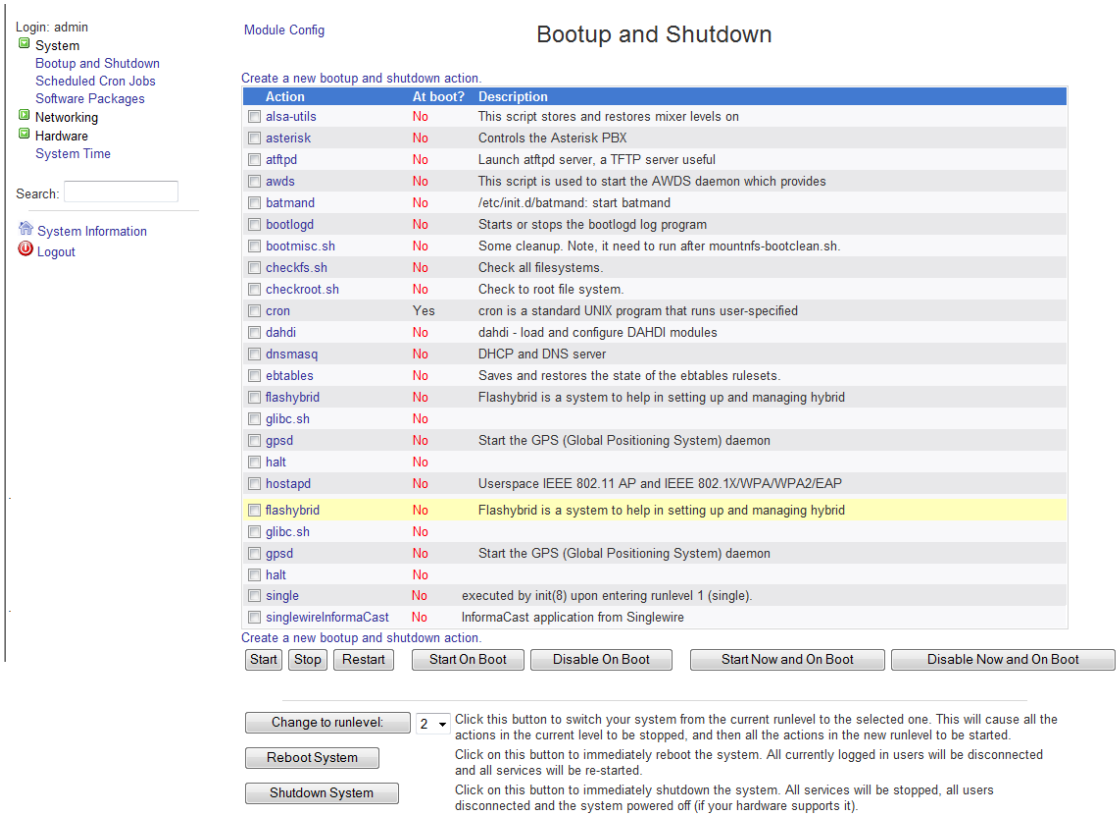


Note You may have to accept a warning from your web browser about the security of this page's content.

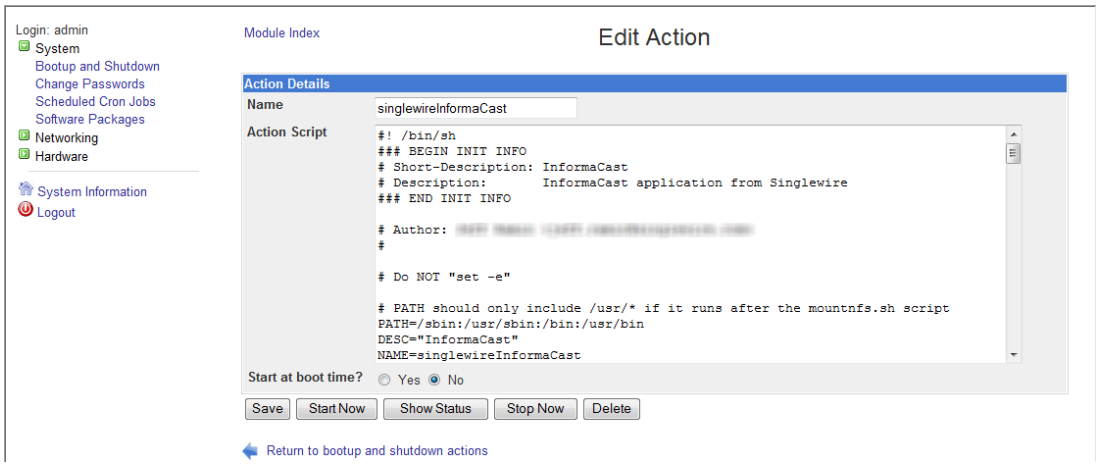
Step 3 Enter your login credentials and click the **Login** button. By default, your username is **admin** and your password is **changeMe**. The Webmin homepage appears.



Step 4 Go to **System** | **Bootup and Shutdown**. The Bootup and Shutdown page appears.



Step 5 Scroll down the list of actions until you come to **singlewireInformaCast**. Click its link. The Edit Action page appears.

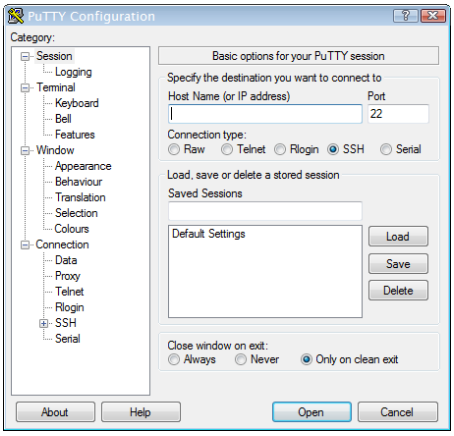


Step 6 Click the **Stop Now** button. It will take a minute or so for InformaCast to stop.

Note Leave this window open. You will come back to it.

Step 7 Use an SSH client (e.g. PuTTY: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html) to access InformaCast's command line interface.

Step 8 Open PuTTY. The PuTTY Configuration window appears.

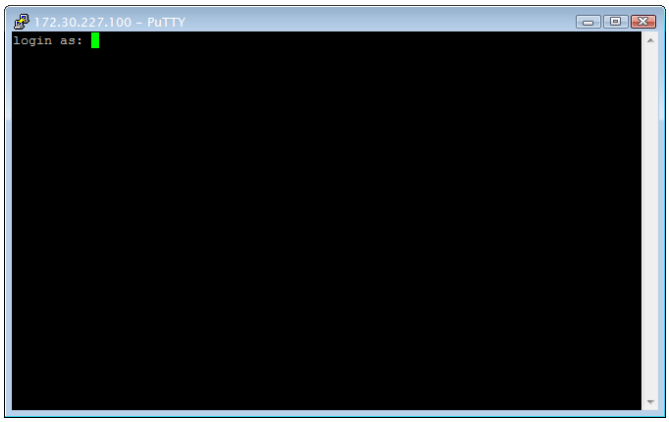


Step 9 Enter InformaCast's IP address in the **Host Name (or IP address)** field.

Step 10 Leave the **Port** field at its default of 22.

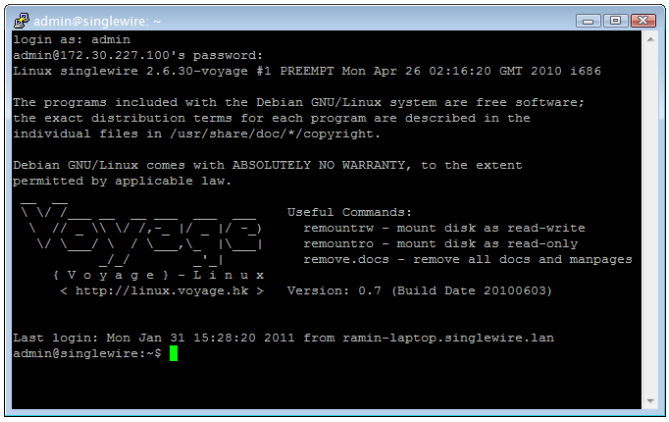
Step 11 Click the **SSH** radio button.

Step 12 Click the **Open** button. The command-line interface for InformaCast appears.



Step 13 Enter **admin** at the prompt and press the **Enter** key.

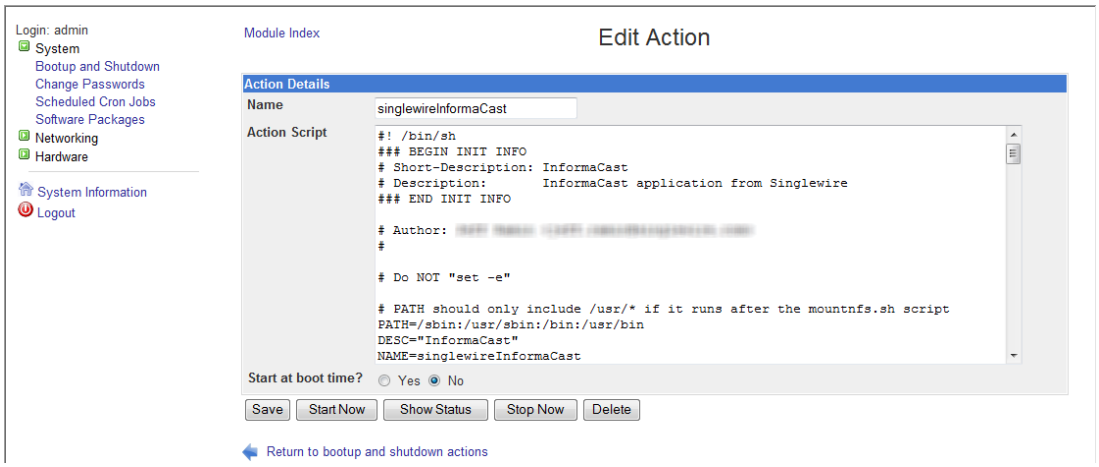
Step 14 Enter **changeMe** at the prompt and press the **Enter** key. The command-line interface refreshes, showing you that you're logged in.



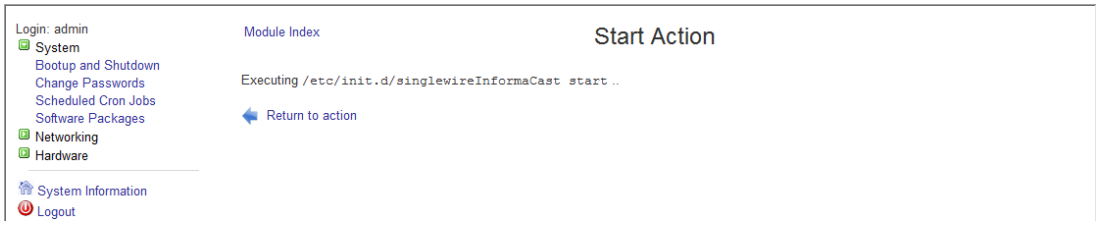
Step 15 Enter **updateJTAPI <CUCM IP Address>**, where <CUCM IP Address> is replaced by the IP address of your CUCM, at the prompt and press the **Enter** key.

Step 16 Enter **exit** at the prompt and press the **Enter** key.

Step 17 Go back to your Stop Action page and click the **Return to action** link. The Edit Action page appears.



Step 18 Click the **Start Now** button. It will take a minute or so for InformaCast to start.

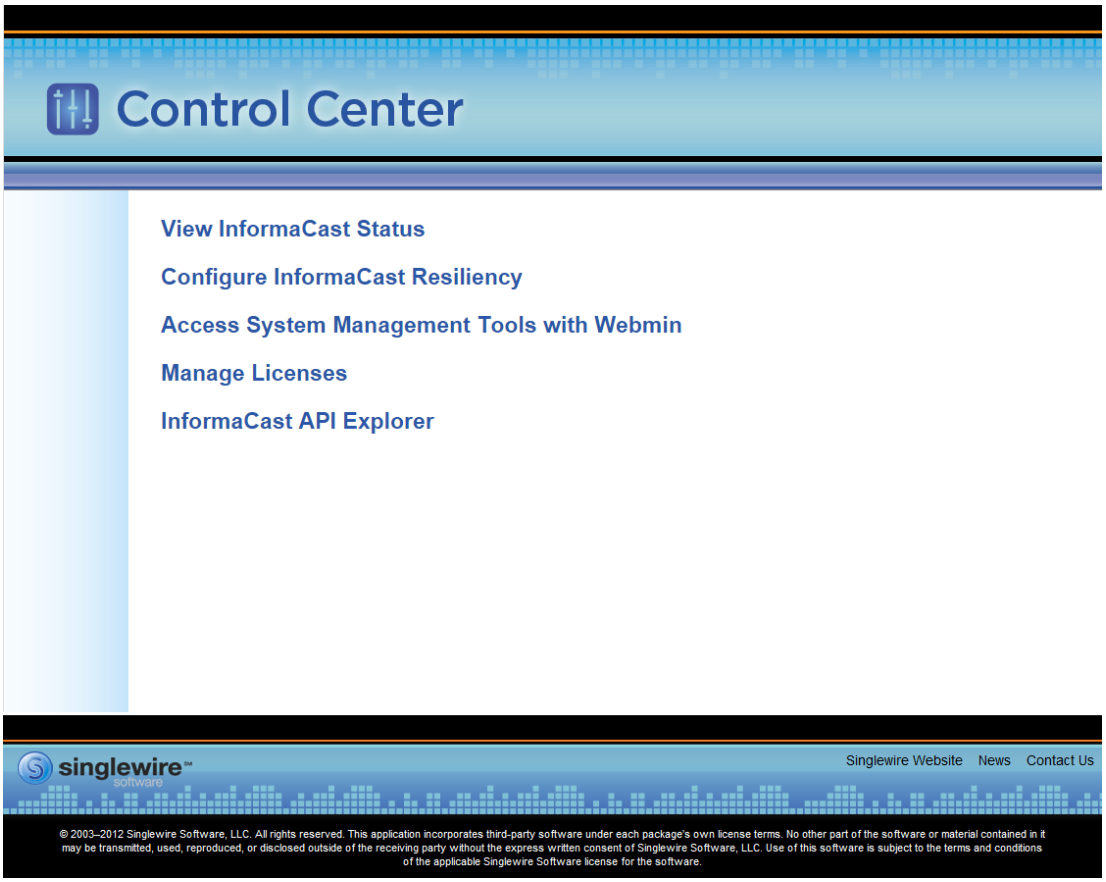


Set the System Time

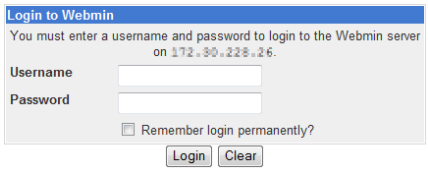
Note You can skip this section if your Virtual Appliance has Internet access and using the default NTP server is acceptable.

The InformaCast Virtual Appliance's system time is automatically set for you using the pool.ntp.org server, but if your Virtual Appliance does not have Internet access or if you want to use your own NTP server, you can do so.

Step 1 Click the **Access Application Management Tools with Control Center** link on the Singlewire Start page. A separate tab/window opens to the Control Center menu page.

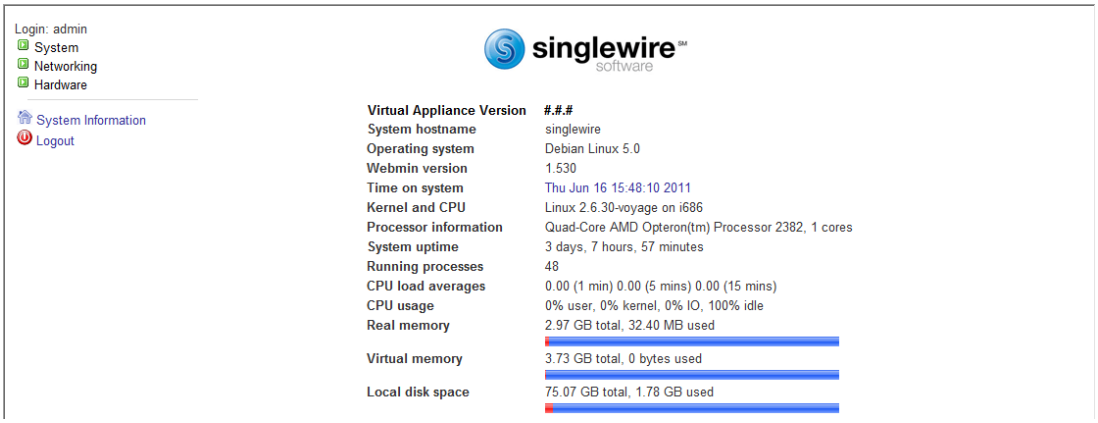


Step 2 Click the **Access System Management Tools with Webmin** link. The Login to Webmin page appears.

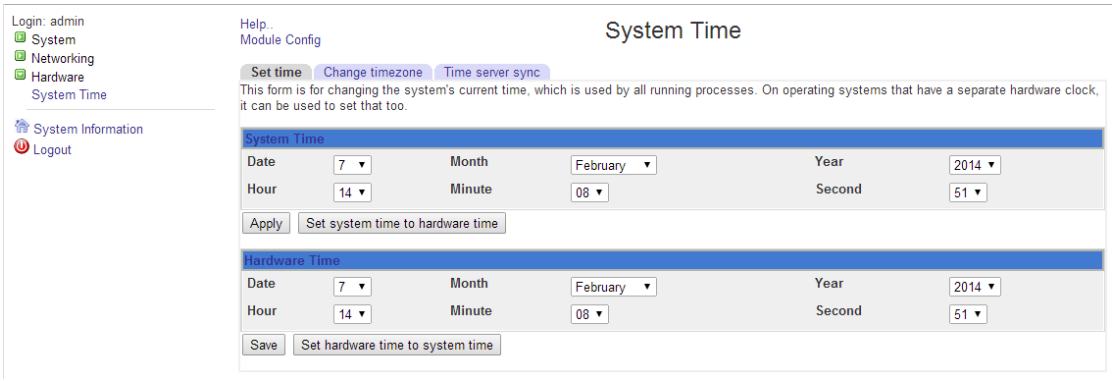


Note You may have to accept a warning from your web browser about the security of this page's content.

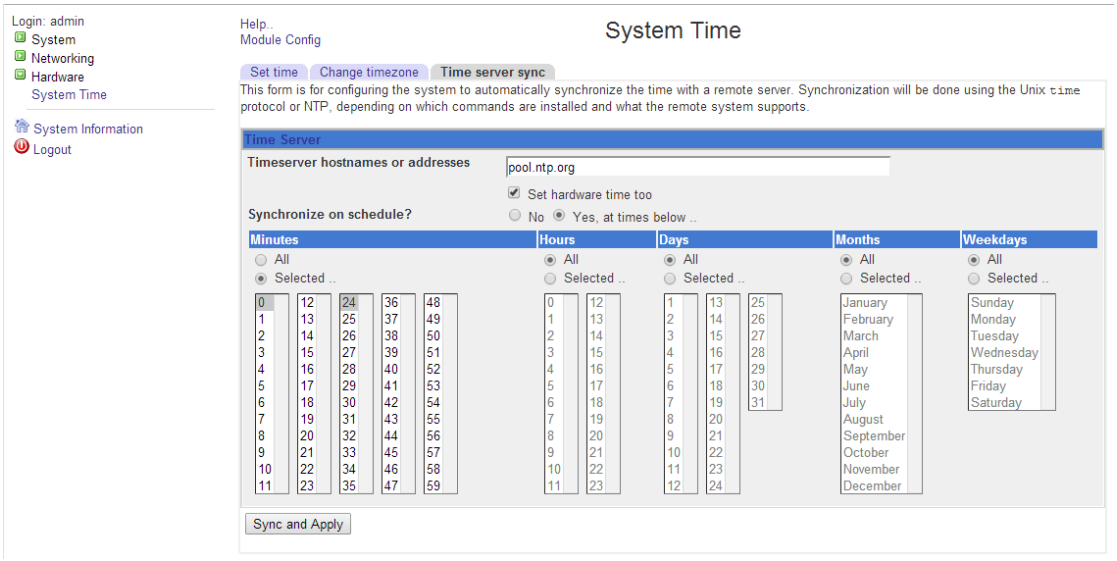
Step 3 Enter your login credentials and click the **Login** button. By default, your username is **admin** and your password is **changeMe**. The Webmin homepage appears.



Step 4 Go to **Hardware** | **System Time**. The System Time page appears.



Step 5 Click the **Time server sync** tab. The System Time page refreshes with the contents of the **Time server sync** tab.

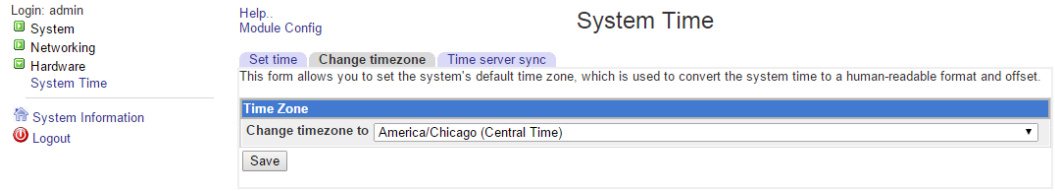


Step 6 Enter the hostname or IP address of the NTP server you want to use in the **Timeserver hostnames or addresses** field.

Tip You can also change the time at which the Virtual Appliance checks with the NTP server by modifying the fields and radio buttons in the *Minutes*, *Hours*, *Days*, *Months*, and *Weekdays* areas.

Step 7 Click the **Sync and Apply** button to save your changes.

Step 8 Click the **Change Timezone** tab. The System Time page refreshes with the contents of the **Change Timezone** tab.



Step 9 Select the time zone in which your Virtual Appliance resides from the **Change timezone** to dropdown menu.

Step 10 Click the **Save** button.

Integrate CUCM

Before you can begin using InformaCast in a telephony environment, you must configure your version of CUCM. Perform all of the steps in the following sections:

- "Configure CUCM SNMP" on page 2-31
- "Set the Default Codec to G.711" on page 2-36
- "Create a Device Pool" on page 2-40
- "Create a Route Partition" on page 2-42
- "Create a Calling Search Space" on page 2-43
- "Create CTI Ports" on page 2-44
- "Create an AXL User Group/Access Control Group" on page 2-49
- "Create an Application User" on page 2-53
- "Enable Web Access for Cisco IP Phones" on page 2-56
- "Set Your Authentication URL" on page 2-64
- "Reboot Your Phones" on page 2-65
- "Test Your Phones" on page 2-67

Tip When naming your CUCM components, it is recommended to use a standardized name or abbreviation so that the components will display together. For example, this documentation will use the abbreviation of ICVA for InformaCast Virtual Appliance.

In the past, CTI route points were recommended for use with DialCast functionality, which allows you to trigger an InformaCast broadcast by calling a route point that is configured to send a specific message to predetermined recipient groups (see "Manage DialCasts" on page 5-40 for more information). For easier troubleshooting, it is now recommended that DialCast functionality be used in conjunction with SIP instead (see "Manage SIP Functionality" on page 5-4 for more information). CTI route points are no longer recommended for DialCast configurations; this section has been removed from the documentation. You should update your DialCast configurations accordingly.

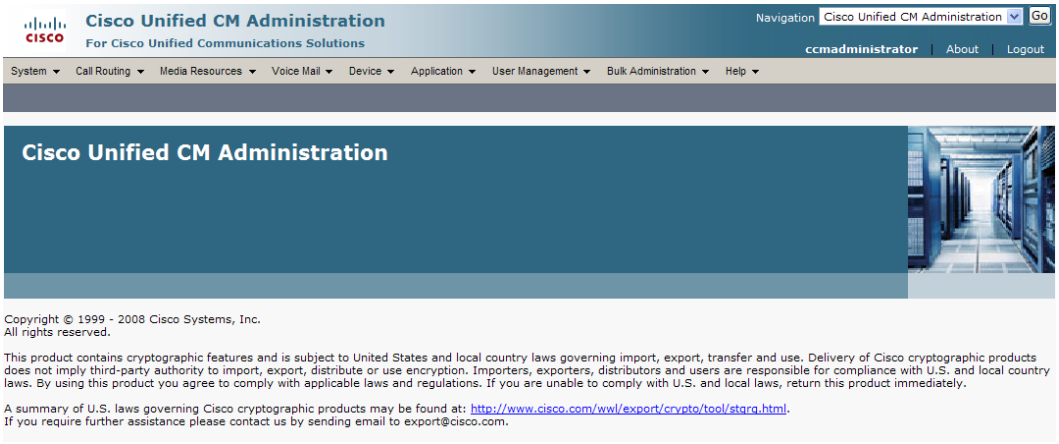
Configure CUCM SNMP

InformaCast uses SNMP to gather phone information from CUCM.

Enable SNMP on CUCM Cluster Nodes

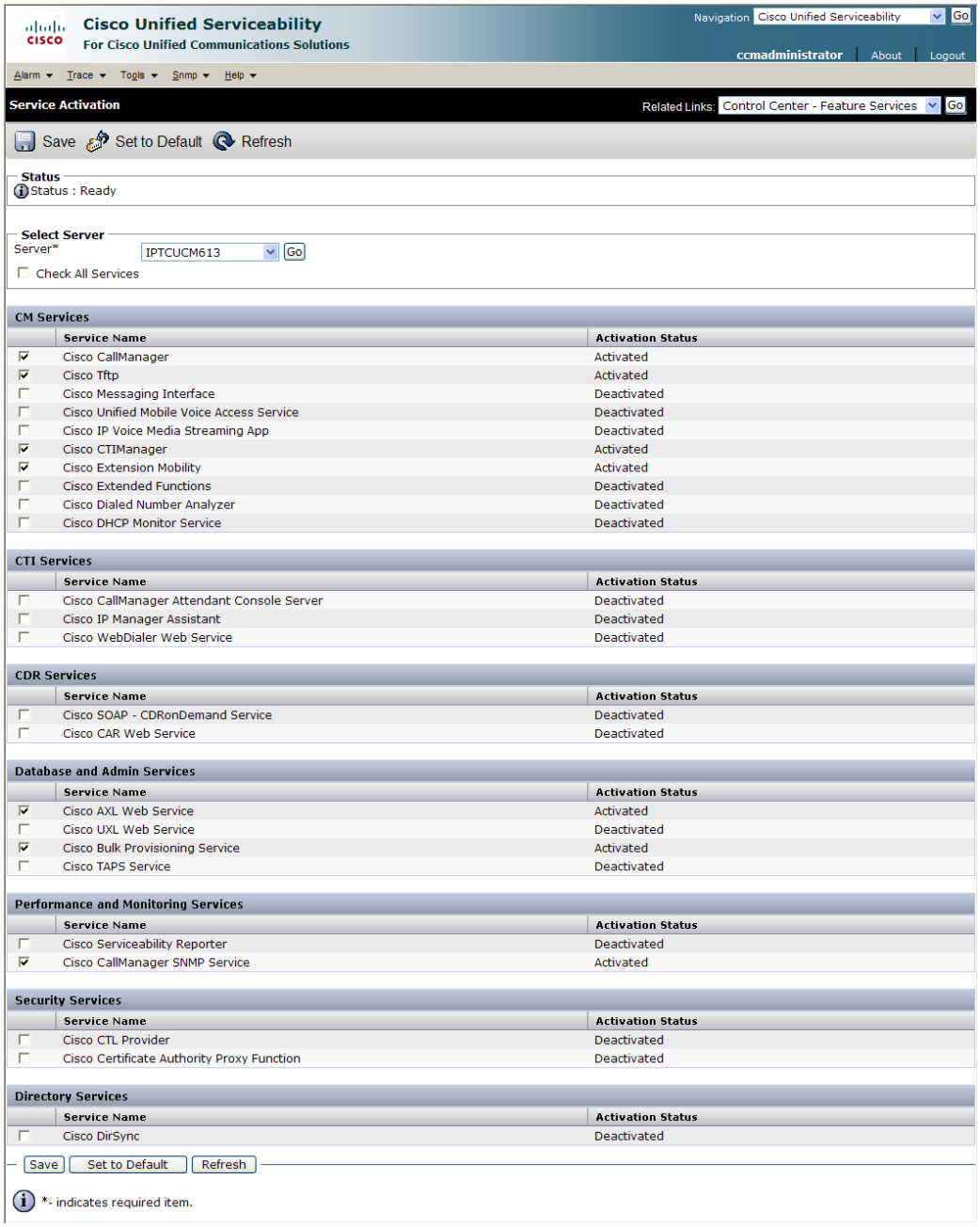
You must enable SNMP on CUCM cluster nodes that will function with InformaCast.

Step 1 Open a web browser and log into the administration interface of the CUCM server (the address will be similar to https://<CUCM IP Address>/ccmadmin). The Cisco Unified CM Administration page appears.



Step 2 Select **Cisco Unified Serviceability** from the **Navigation** dropdown menu and click the **Go** button. The Cisco Unified Serviceability page appears.

Step 3 Go to **Tools | Service Activation**. The Service Activation page appears.

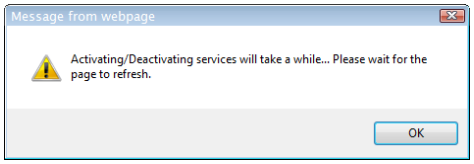


Note If you have more than one server, you'll have to select your server from the **Server** dropdown menu and click the **Go** button. The Service Activation page for that server will then appear.

Step 4 Ensure the following services' checkboxes are selected: **Cisco CallManager**, **Cisco CTIManager**, **Cisco AXL Web Service**, and **Cisco CallManager SNMP Service**.

Step 5 Click the **Save** button to save your changes.

Step 6 Click the **OK** button if you receive a message about activating/deactivating services.

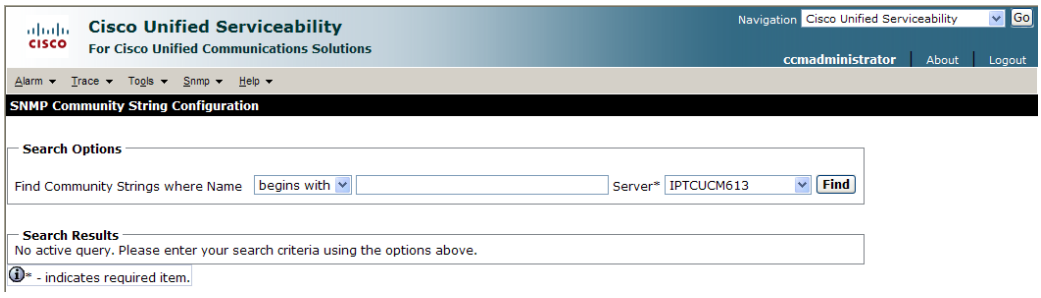


Step 7 Verify your services are running by going to **Tools | Control Center - Feature Services**. **Cisco CallManager**, C**isco CTIManager**, **Cisco AXL Web Service**, and **Cisco CallManager SNMP Service** should say they are **Activated**. If not, click the green arrow in the top left hand corner to start the services.

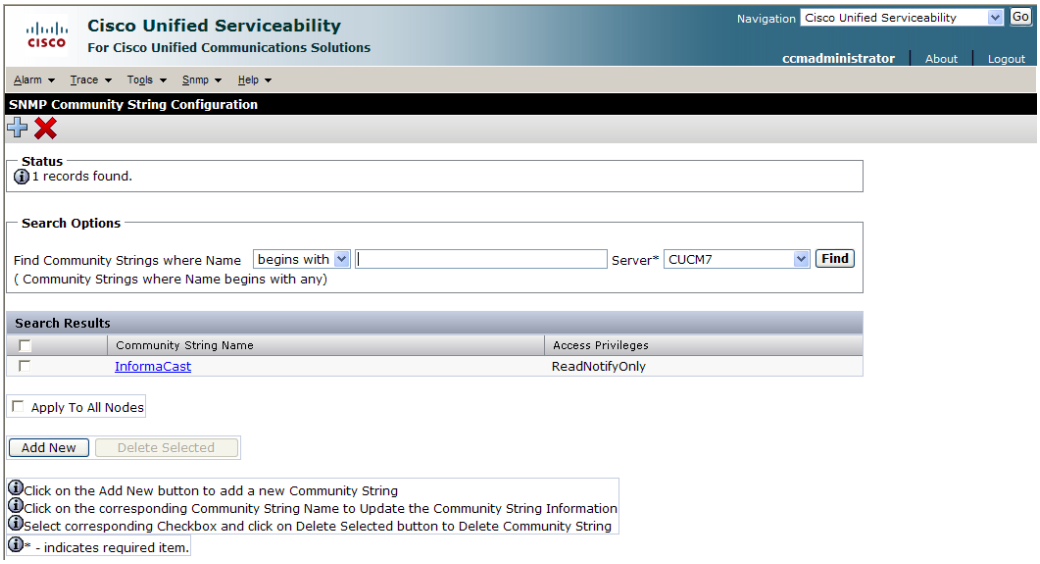
Create an InformaCast SNMP Community String

Follow these steps to create an InformaCast SNMP community string.

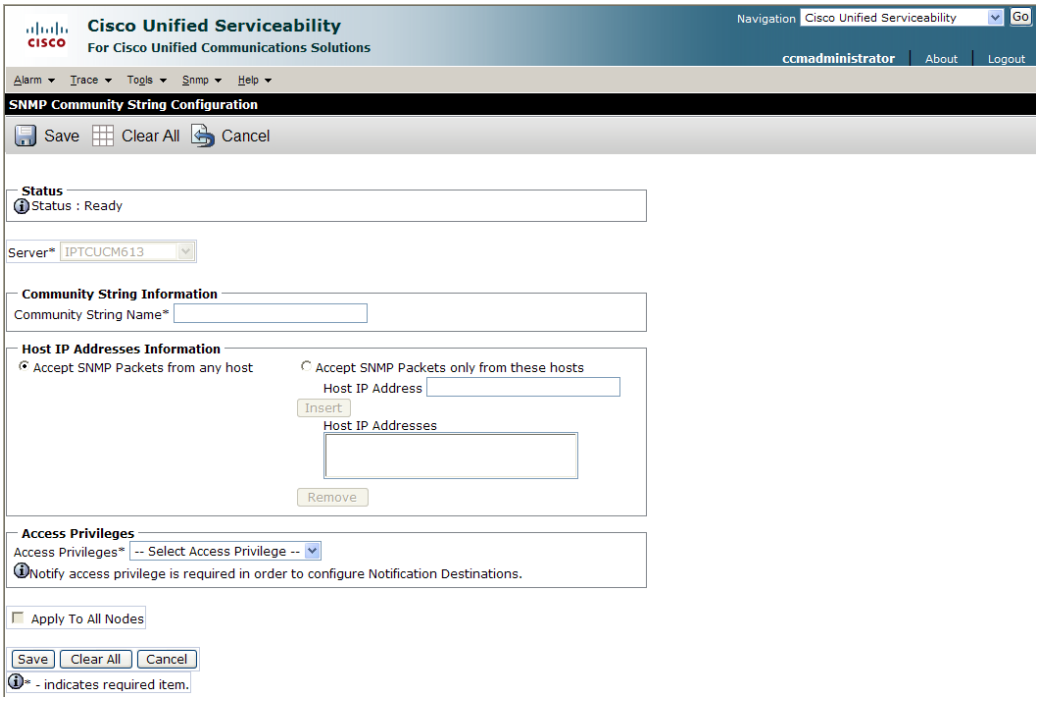
Step 1 Go to **SNMP | V1/V2c | Community String**. The SNMP Community String Configuration page appears.



Step 2 Select your server from the **Server** dropdown menu and click the **Find** button. The SNMP Community String Configuration page refreshes.



Step 3 Click the **Add New** button to create a new community string. The SNMP Community String Configuration page refreshes again.



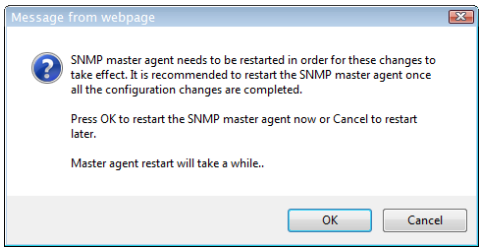
Step 4 Enter **ICVA** into the **Community String Name** field. You will need to remember this name when you edit InformaCast's SNMP configuration in "Configure Your Default CUCM Cluster" on page 4-2.

Note For additional security, click the **Accept SNMP packets only from these hosts** radio button and enter the Virtual Appliance's IP address in the **Host IP Address** field.

Step 5 Select **ReadOnly** from the **Access Privileges** dropdown menu.

Step 6 Select the **Apply to All Nodes** checkbox, if possible.

Step 7 Click the **Save** button. If you are prompted to restart the SNMP service, click the **OK** button.



Set the Default Codec to G.711

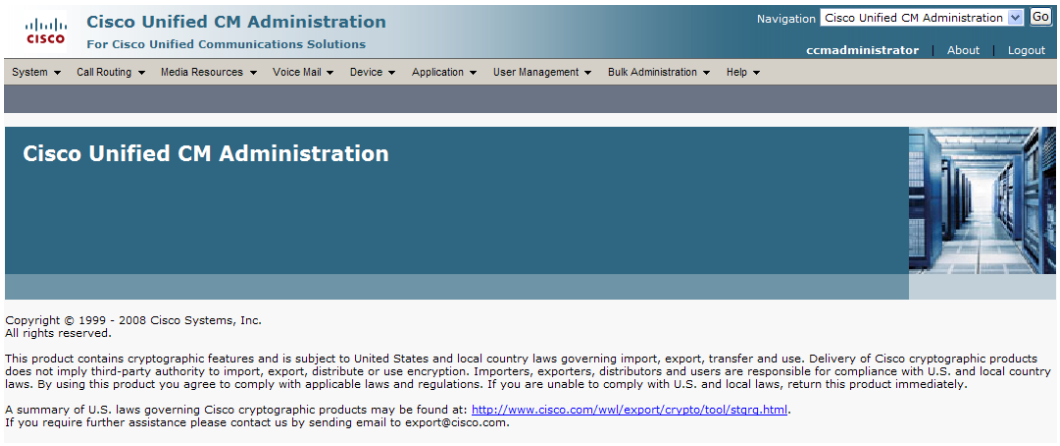
The Virtual Appliance requires that audio streams be in G.711 μLaw format. Because most CUCM deployments use G.729 across the WAN, you need to create a region for the Virtual Appliance that will always use G.711 for all calls to all other regions.

The steps for this section depend on your version of CUCM. If you are using a version of CUCM prior to 9.x, proceed with the following section. If you are using CUCM 9.x or later, skip to "Set the Default Codec to G.711 for Versions of CUCM 9.x or Later" on page 2-38.

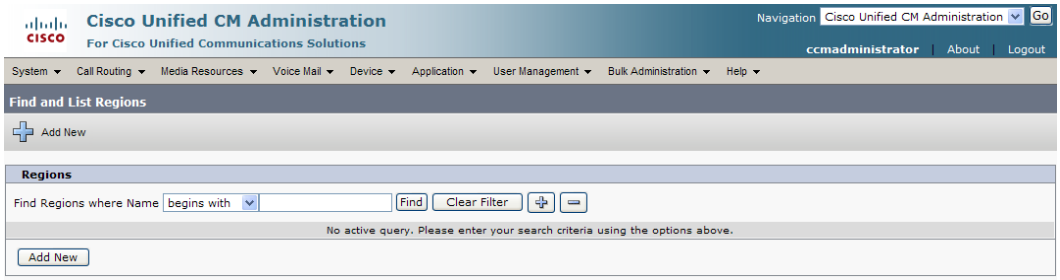
Set the Default Codec to G.711 for Versions of CUCM Prior to 9.x

If you are using a version of CUCM prior to 9.x, use the following steps to create a region that uses the G.711 codec.

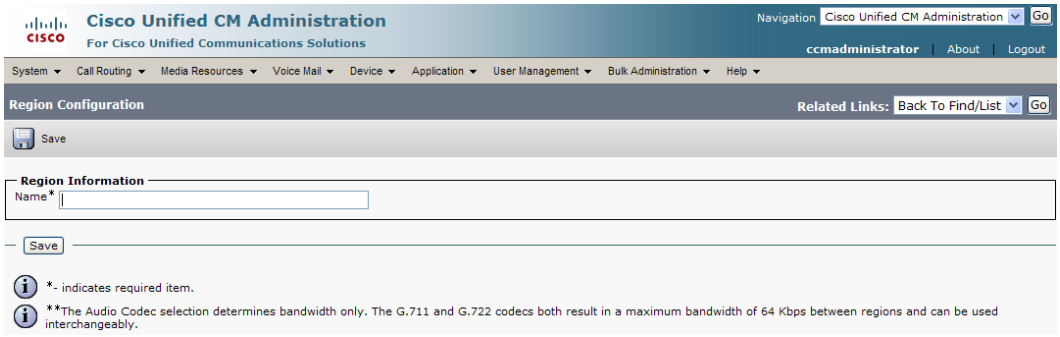
Step 1 Select **Cisco Unified CM Administration** from the **Navigation** dropdown menu and click the **Go** button. The Cisco Unified CM Administration page appears.



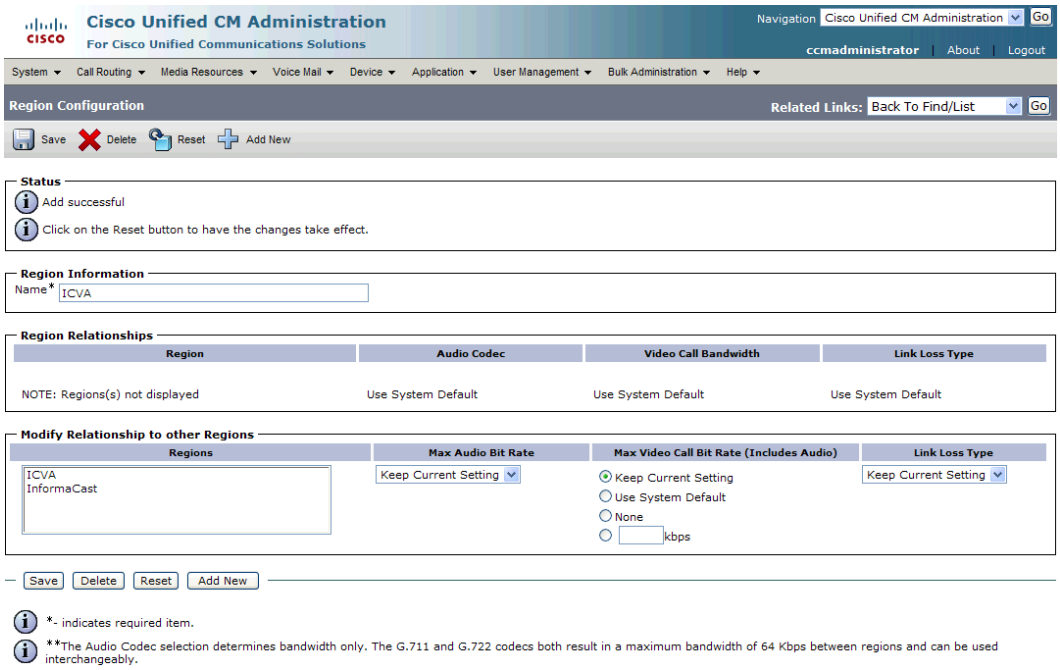
Step 2 Go to **System** | **Region**. The Find and List Regions page appears.



Step 3 Click the **Add New** button. The Region Configuration page appears.



Step 4 Enter **ICVA** in the **Name** field and click the **Save** button. The Region Configuration page refreshes.



Step 5 Press **Ctrl** + click to select all of your regions in the *Regions* area.

Step 6 Select **64 kbps (G.722, G.711)** from the **Max Audio Bit Rate** dropdown menu.

Step 7 Select the **None** radio button in the *Max Video Call Bit Rate (Includes Audio)* area.

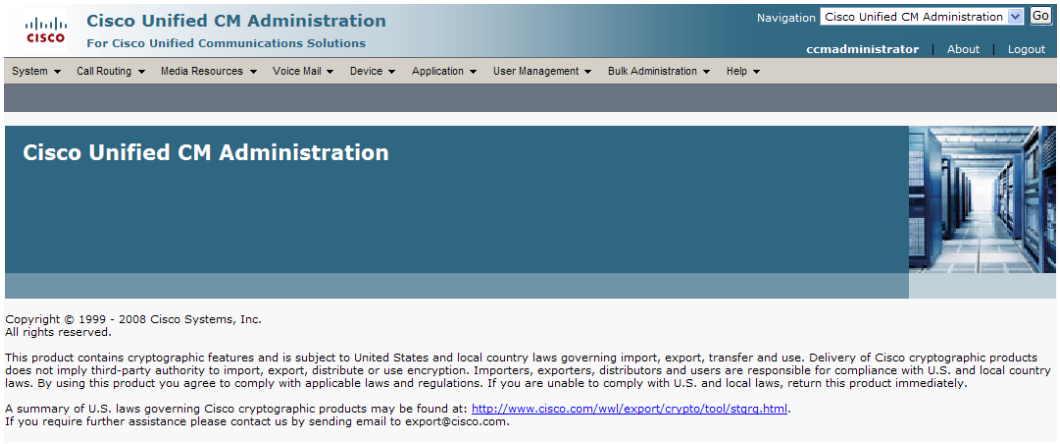
Step 8 Click the **Save** button.

Note Once changes have been saved, verify that all phone regions are associated to the ICVA region and using the G.711 audio codec. This will ensure that the Virtual Appliance can communicate with the phones in these regions.

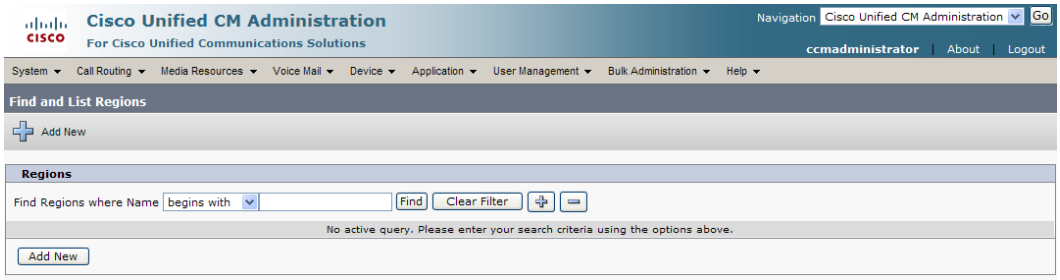
Set the Default Codec to G.711 for Versions of CUCM 9.x or Later

If you are using a 9.x or later version of CUCM, use the following steps to create a region that uses the G.711 codec.

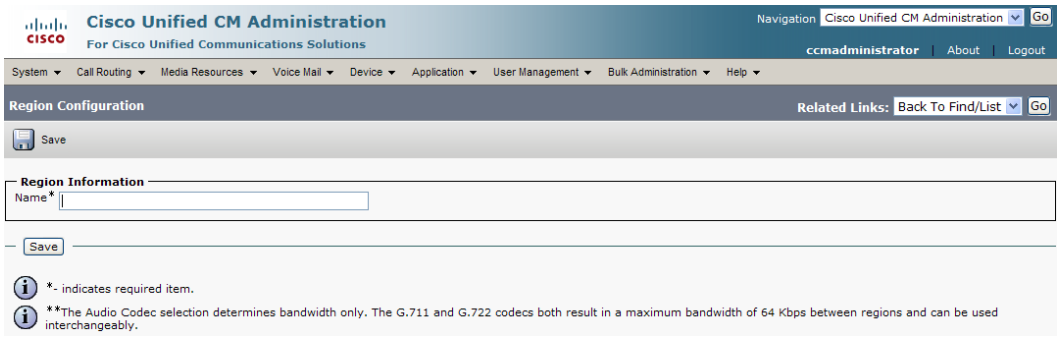
Step 1 Ensure you are in Cisco Unified CM Administration or select **Cisco Unified CM Administration** from the **Navigation** dropdown menu and click the **Go** button. The Cisco Unified CM Administration page appears.



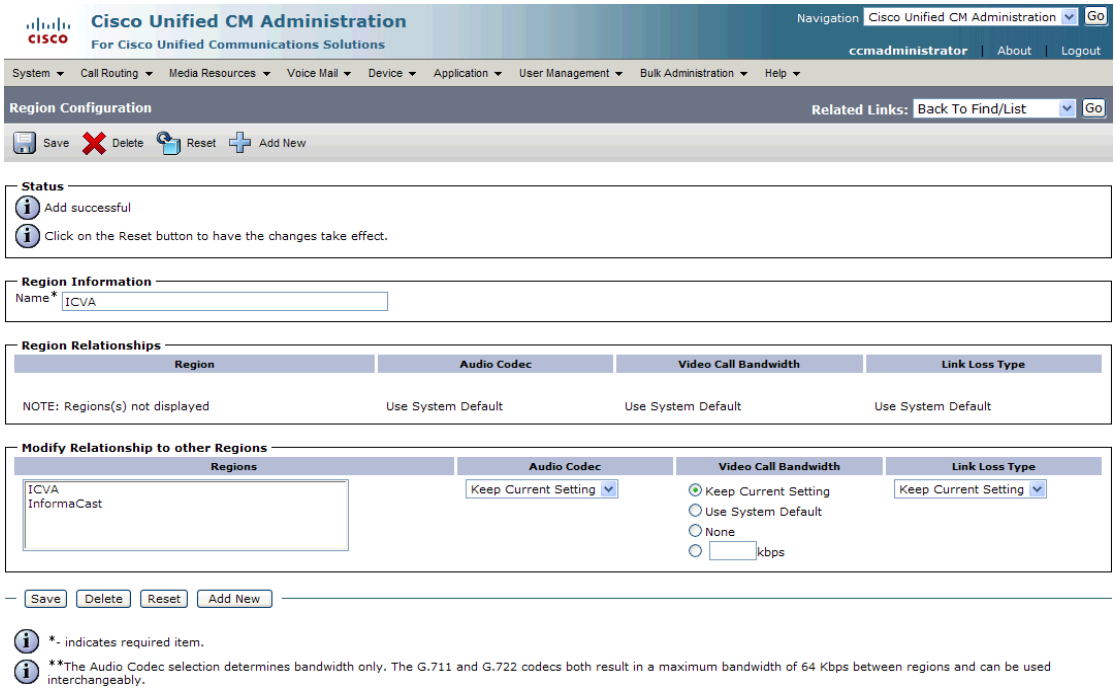
Step 2 Go to **System** | **Region Information** | **Region**. The Find and List Regions page appears.



Step 3 Click the **Add New** button. The Region Configuration page appears.



Step 4 Enter **ICVA** in the **Name** field and click the **Save** button. The Region Configuration page refreshes.



Step 5 Press **Ctrl** + click to select all of your regions in the *Regions* area.

Step 6 Select **64kbps (G.722, G.711)** from the **Maximum Audio Bit Rate** dropdown menu.

Step 7 Select the **None** radio button in the *Maximum Session Bit Rate for Video Calls* area.

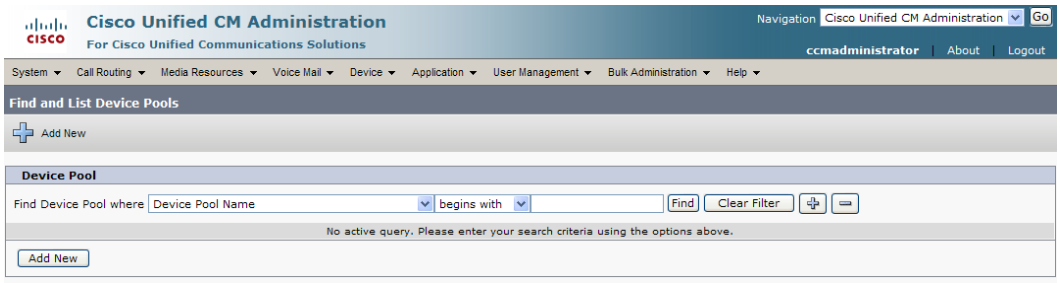
Step 8 Click the **Save** button.

Note Once changes have been saved, verify that all phone regions are associated to the ICVA region and using the G.711 audio codec. This will ensure that the Virtual Appliance can communicate with the phones in these regions.

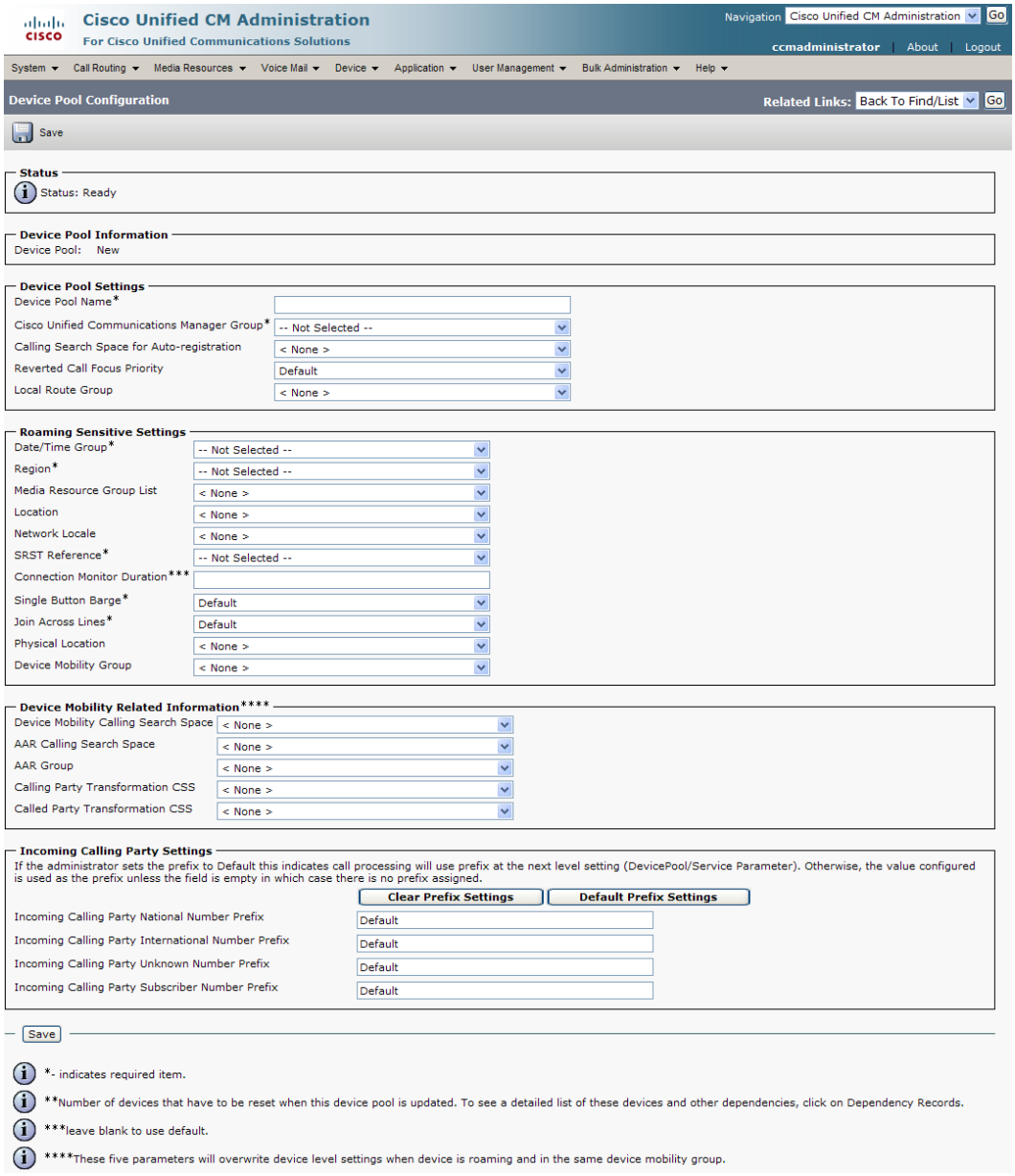
Create a Device Pool

Subsequent sections will walk you through creating devices, CTI ports, and application users on CUCM. In order to have those components use the newly created G.711 μLaw region, you must first create a device pool.

Step 1 Go to **System** | **Device Pool**. The Find and List Device Pools page appears.



Step 2 Click the **Add New** button. The Device Pool Configuration page appears.



Step 3 Select a CUCM group from the **Cisco Unified Communications Manager Group** dropdown menu.

Tip Make sure that the CUCM group you choose contains the CUCM with which the Virtual Appliance will communicate.

Step 4 Select a date/time group from the **Date/Time Group** dropdown menu.

Tip Select **CMLocal** unless you are performing dialing restrictions/re-routing by time of day.

Step 5 Select **ICVA** from the **Region** dropdown menu. This refers to the region you created in "Set the Default Codec to G.711" on page 2-36.

Step 6 Select **Disable** from the **SRST Reference** dropdown menu.

Step 7 Select **On** from the **Join Across Lines** dropdown menu.

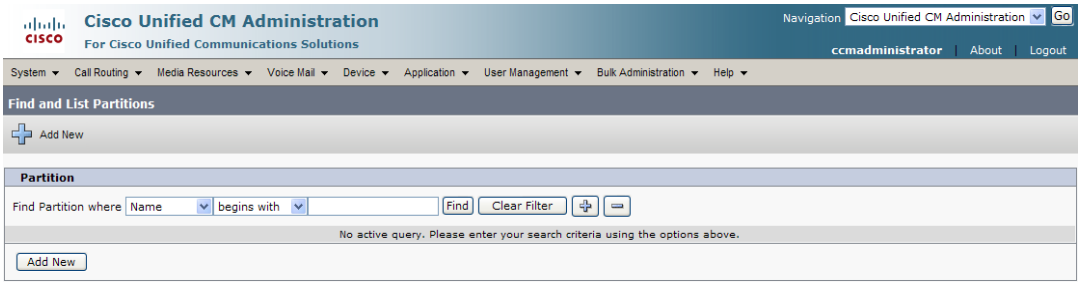
Step 8 Select/enter appropriate values for any required fields, which are marked with asterisks (*).

Step 9 Click the **Save** button.

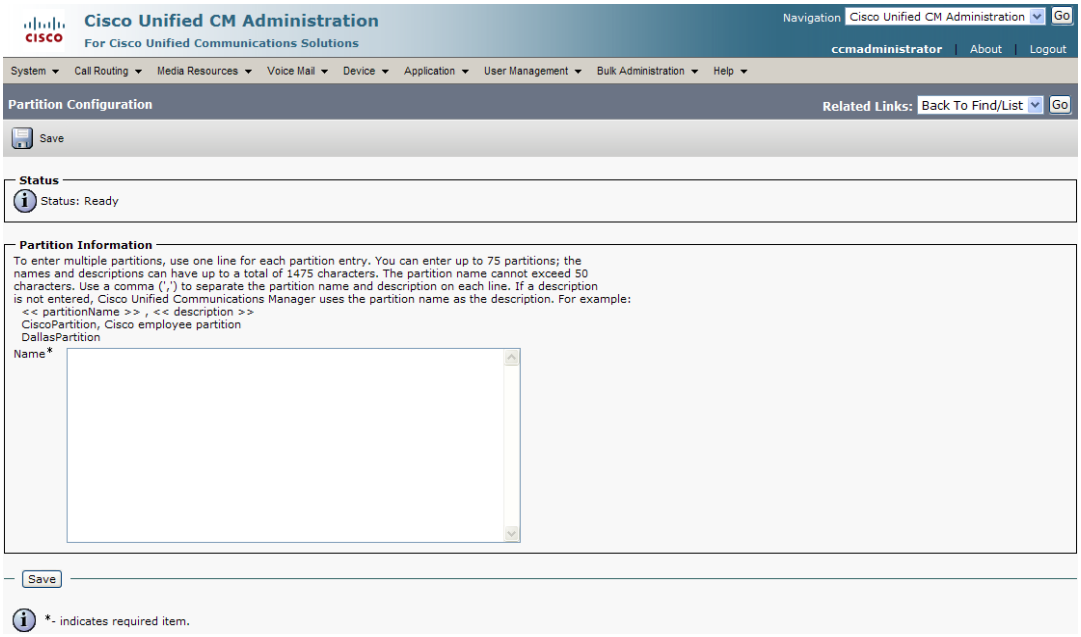
Create a Route Partition

Partitions can be seen as a collection of directory numbers, allowing you to assign and group route points for easier administration of the services that certain phones can reach.

Step 1 Go to **Call Routing** | **Class of Control** | **Partition**. The Find and List Partitions page appears.



Step 2 Click the **Add New** button. The Partition Configuration page appears.



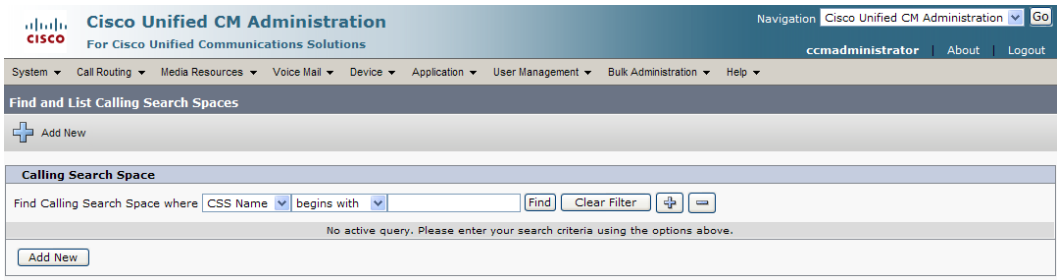
Step 3 Enter **ICVA-CTIOutbound,ICVA-Do not add to any phone CSS** in the **Name** field.

Step 4 Click the **Save** button.

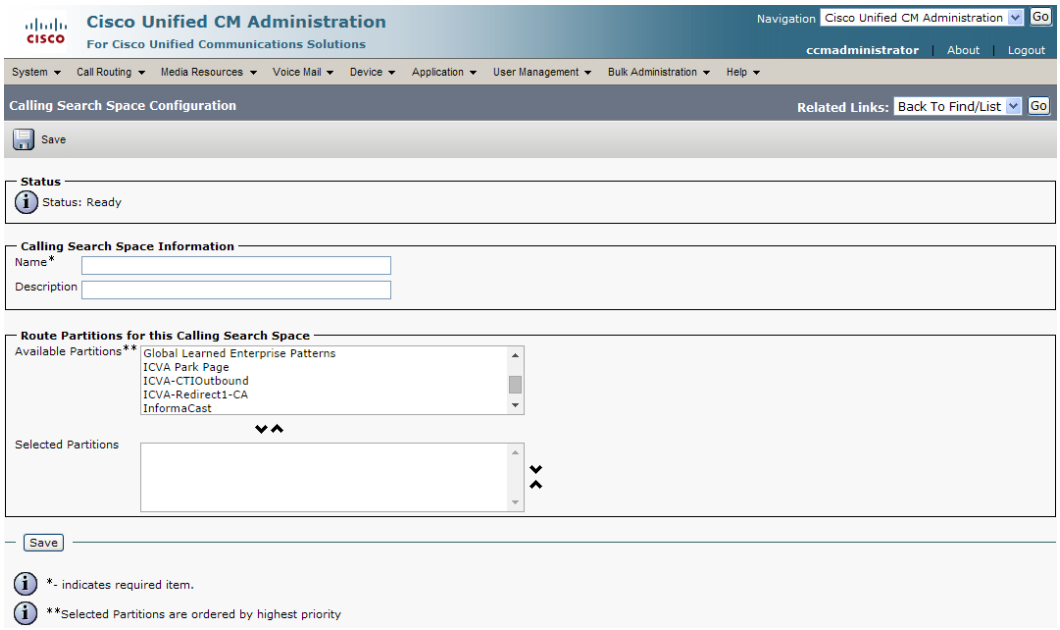
Create a Calling Search Space

InformaCast places a call to your Cisco IP phone to record the audio that will be broadcast. This is a phone call just like any other call. You must ensure that your CUCM's calling search space allows calls to your SIP trunk or all the partitions within which your Cisco IP phone directory numbers are located.

Step 1 Go to **Call Routing** | **Class of Control** | **Calling Search Space**. The Find and List Calling Search Spaces page appears.



Step 2 Click the **Add New** button. The Calling Search Space Configuration page appears.



Step 3 Enter **ICVA** in the **Name** field.

Step 4 Select the following partition(s):

- The partition you created in "Create a Route Partition" on page 2-42
- The partition(s) housing your users' extensions

Step 5 Move these partitions from the *Available Partitions* area into the *Selected Partitions* area using the down arrow.

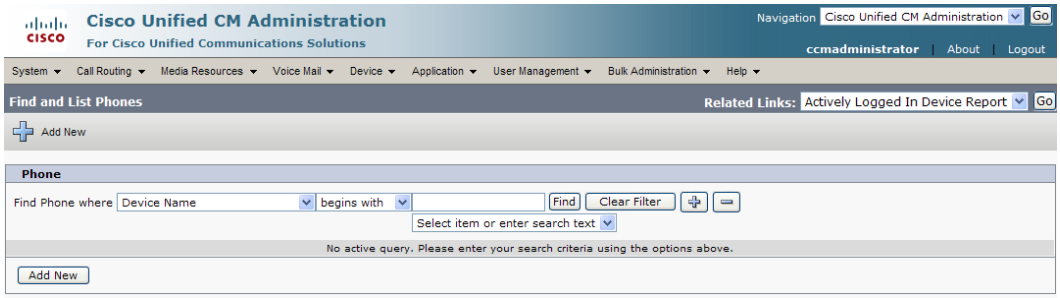
Tip Do not add your voicemail platform to the *Selected Partitions* area.

Step 6 Click the **Save** button.

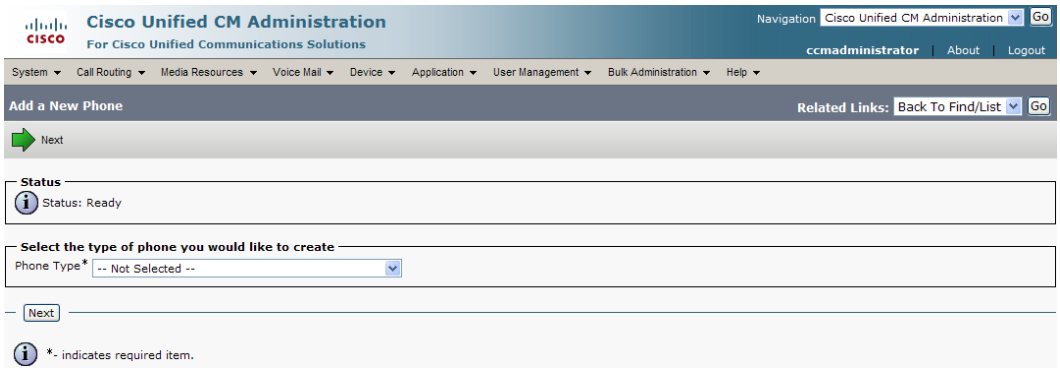
Create CTI Ports

Use the following steps to create CTI ports for InformaCast.

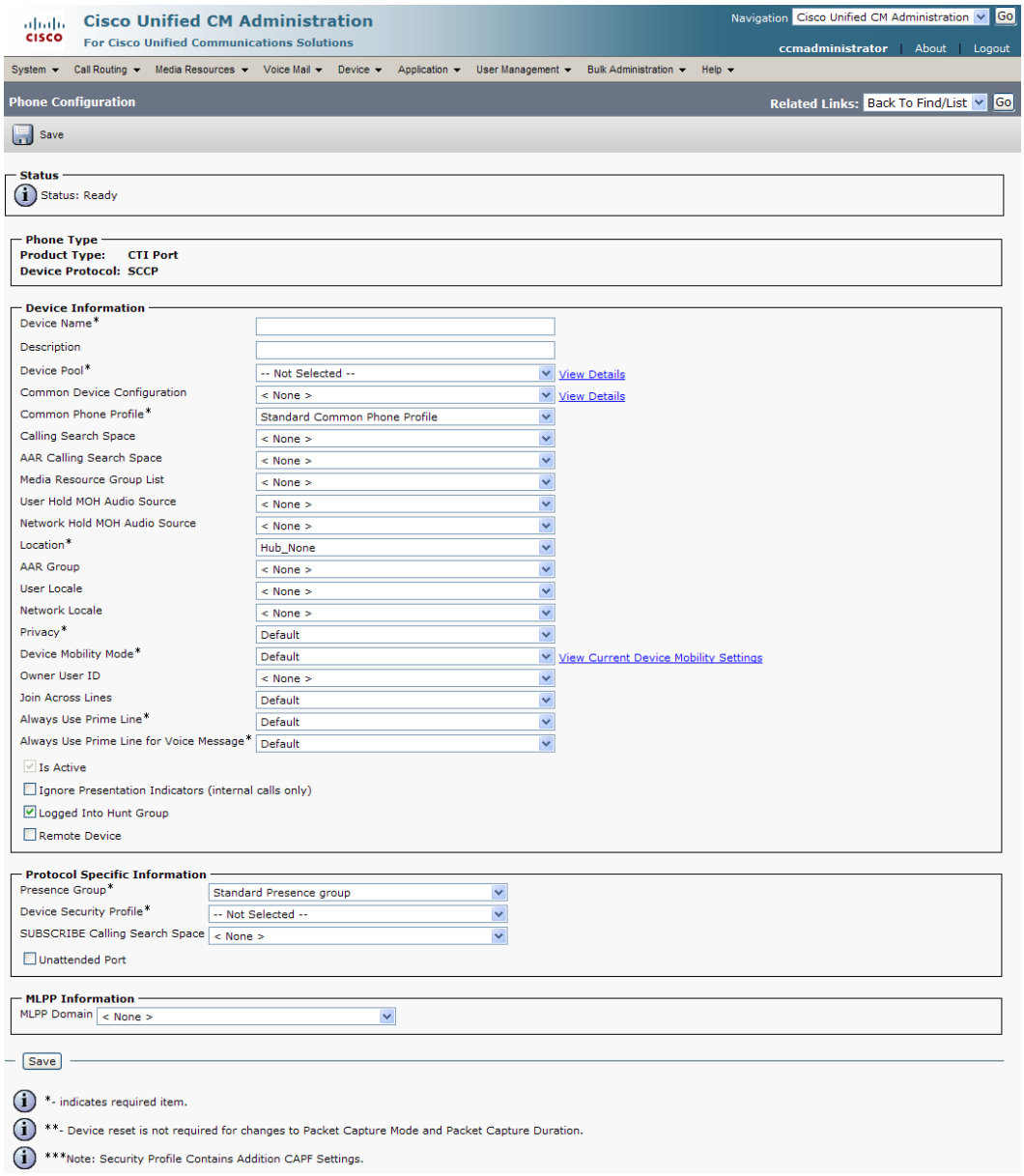
Step 1 Go to **Device | Phone**. The Find and List Phones page appears.



Step 2 Click the **Add New** button. The Add a New Phone page appears.



Step 3 Select **CTI Port** from the **Phone Type** dropdown menu and click the **Next** button. The Phone Configuration page appears.



Step 4 Enter an appropriate name in the **Device Name** field for the new CTI port, e.g. ICVA-IC-001. As you add ports, you can simply append a number to this name, for example: ICVA-IC-002, ICVA-IC-003, etc.

Step 5 Enter a description in the **Description** field, e.g. InformaCast Port.

Step 6 Select **ICVA** from the **Device Pool** dropdown menu.

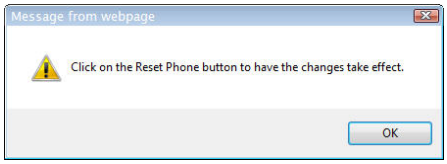
Note The device pool must use a region that will allow a G.711 μLaw call to phones.

Step 7 Select **ICVA** from the **Calling Search Space** dropdown menu. This calling search space must allow calls to the partitions in which phones reside. Calling search spaces are unable to detect when voicemail answers a phone. If a phone extension is called with the expectation that the person answering will dictate a message, InformaCast will end up broadcasting the voicemail prompt until the broadcast is canceled.

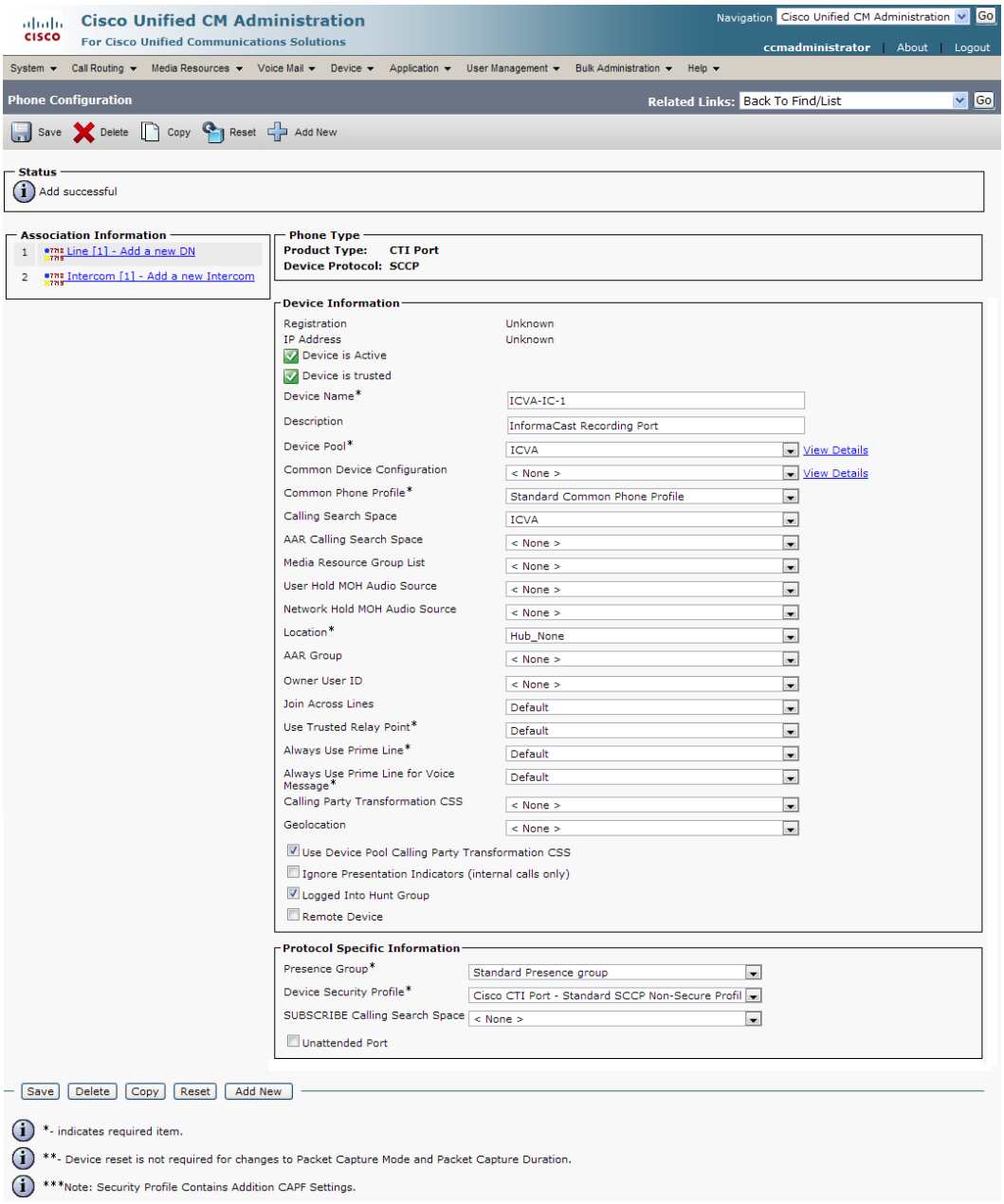
Note In CUCM 9.0 and later, the **Owner ID** field is required. Select the **Anonymous/Public Shared Space** radio button above the **Owner ID** field, which will remove the required setting.

Step 8 Scroll to the *Protocol Specific Information* area and select **Cisco CTI Port - Standard SCCP Non-Secure Profile** from the **Device Security Profile** dropdown menu.

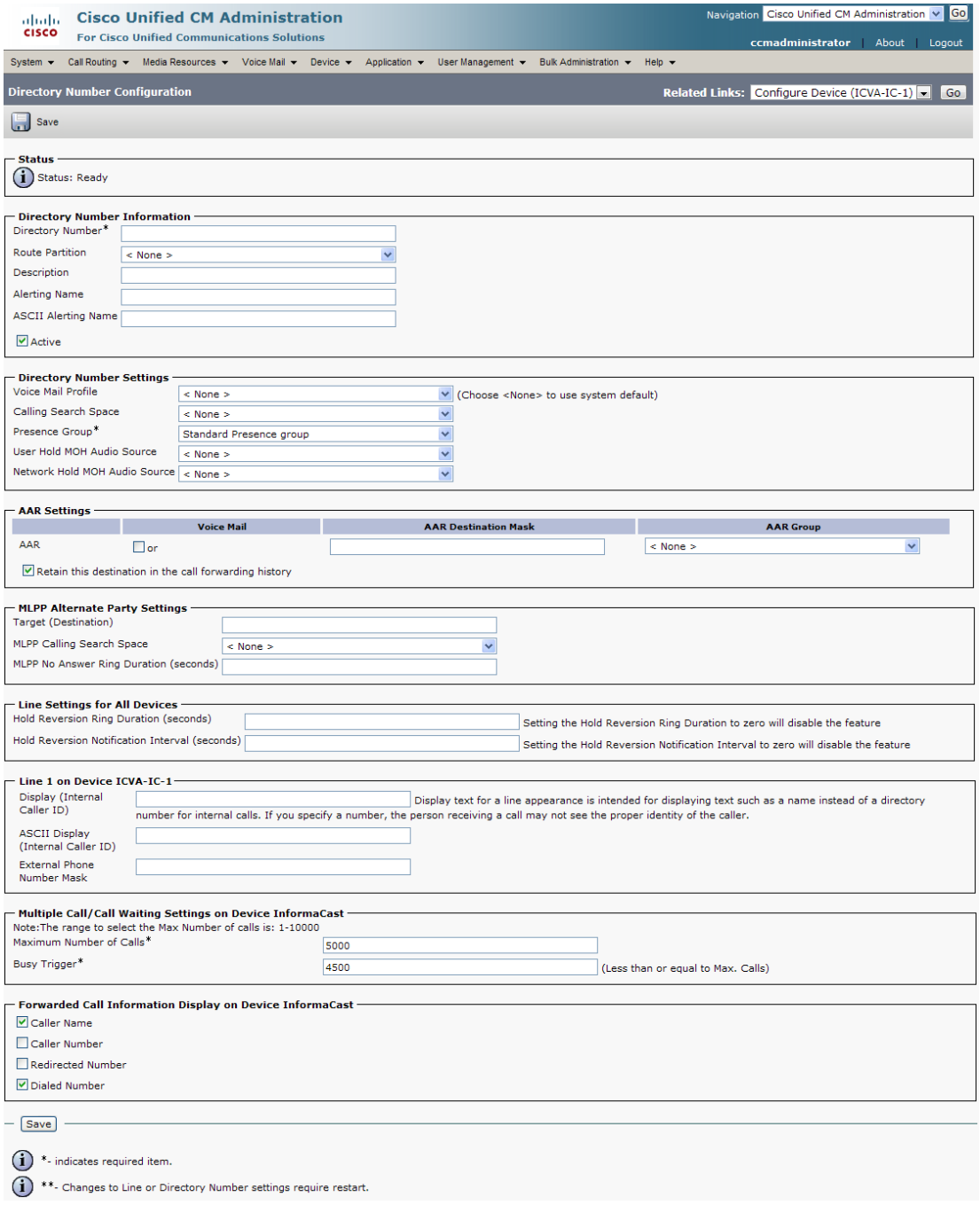
Step 9 Click the **Save** button. A warning dialog box appears.



Step 10 Click the **OK** button if you are prompted to restart the CTI port. The Phone Configuration page refreshes, and you are given the opportunity to create a Directory Number (DN) for the new port.



Step 11 Click the **Line[1] - Add an New DN** link. The Directory Number Configuration page appears.



Step 12 Enter a value in the **Directory Number** field that will not be used for any other purpose at your organization, and which is not within a direct-inward-dialing range. Nothing will call this number. It's purely for InformaCast's use when placing calls.

Step 13 Select **ICVA-CTIOutbound** from the **Route Partition** dropdown menu.

Step 14 Scroll to the *Line 1 on Device ICVA-IC-001* area and enter **InformaCast** in the **Display (Internal Caller ID)** field.

Step 15 Enter **InformaCast** in the **ASCII Display (Caller ID)** field. This will cause "from InformaCast" to display on phones when they are called by InformaCast.

Step 16 Click the **Save** button to add the directory number.

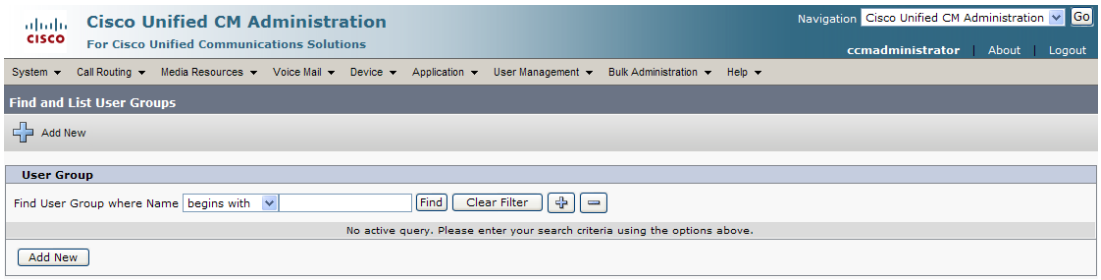
Step 17 Repeat Steps 1 through 16 as many times as needed to create the number of CTI ports that you need (minimum two).

Create an AXL User Group/Access Control Group

In "Create an Application User" on page 2-53, you will create an application user. First, you need to create a user group/access control group that has only the Standard AXL API Access role, which you will then assign to your application users.

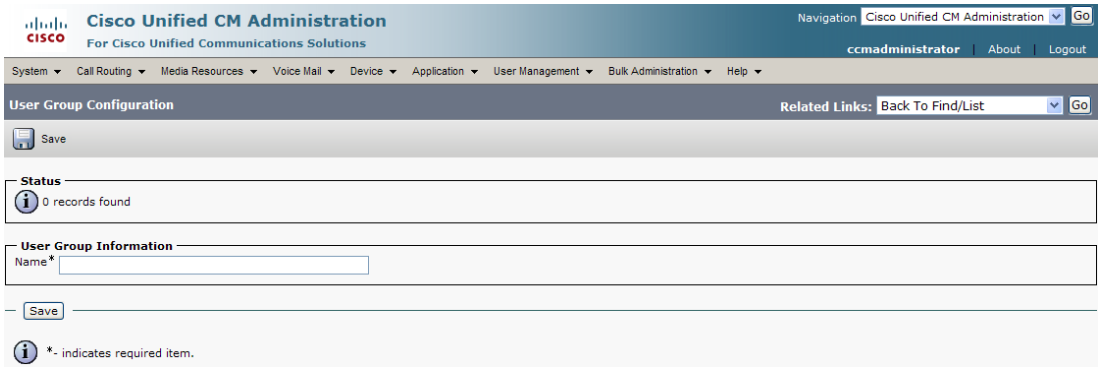
Note If you are using CUCM 9.0 or later, AXL user groups have been renamed to access control groups, the Find and List User Groups page has been renamed to Find and List Access Control Groups, and the navigation to that page has changed to **User Management** | **User Settings** | **Access Control Group** instead of **User Management** | **User Group**. Because of this name change, the User Group Configuration page has been renamed to the Access Control Group Configuration page. However, all the rest of the steps in this section remain the same. Only the way to access the Find and List Access Control Groups page and its naming convention have changed.

Step 1 Go to **User Management** | **User Group**. The Find and List User Groups page appears.

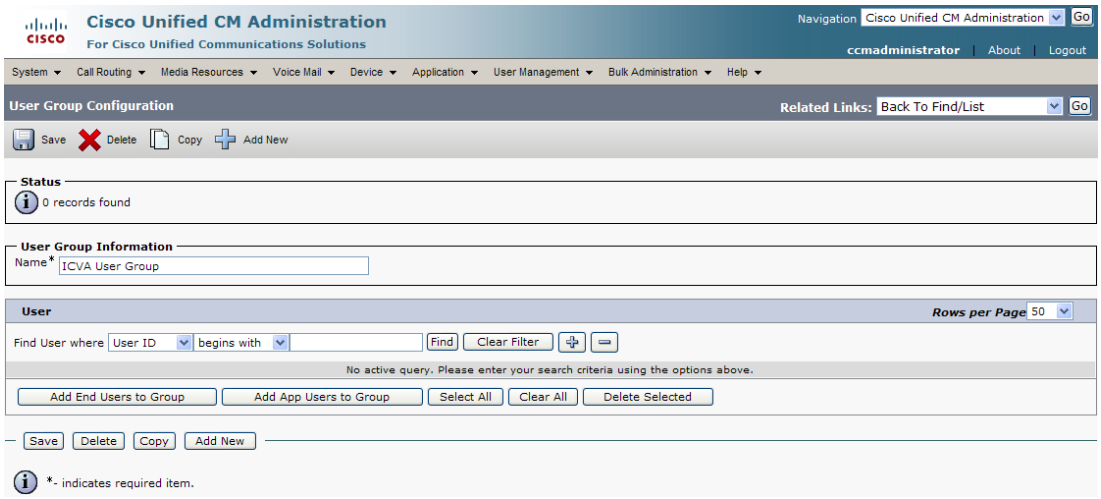


Note If you are using CUCM 9.0 or later, go to **User Management** | **User Settings** | **Access Control Group**. The Find and List Access Control Groups page then appears.

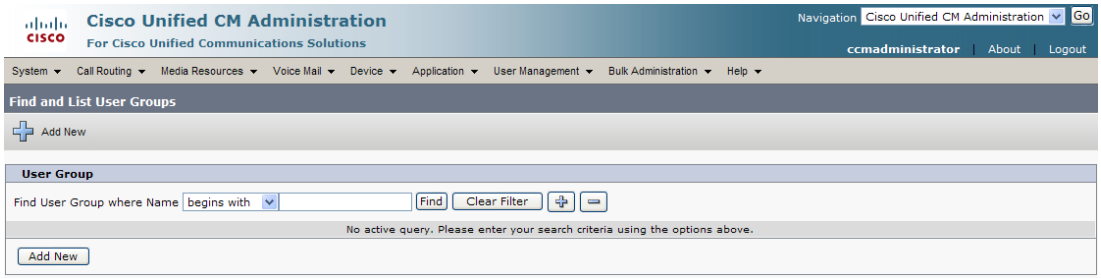
Step 2 Click the **Add New** button. The User Group Configuration page appears.



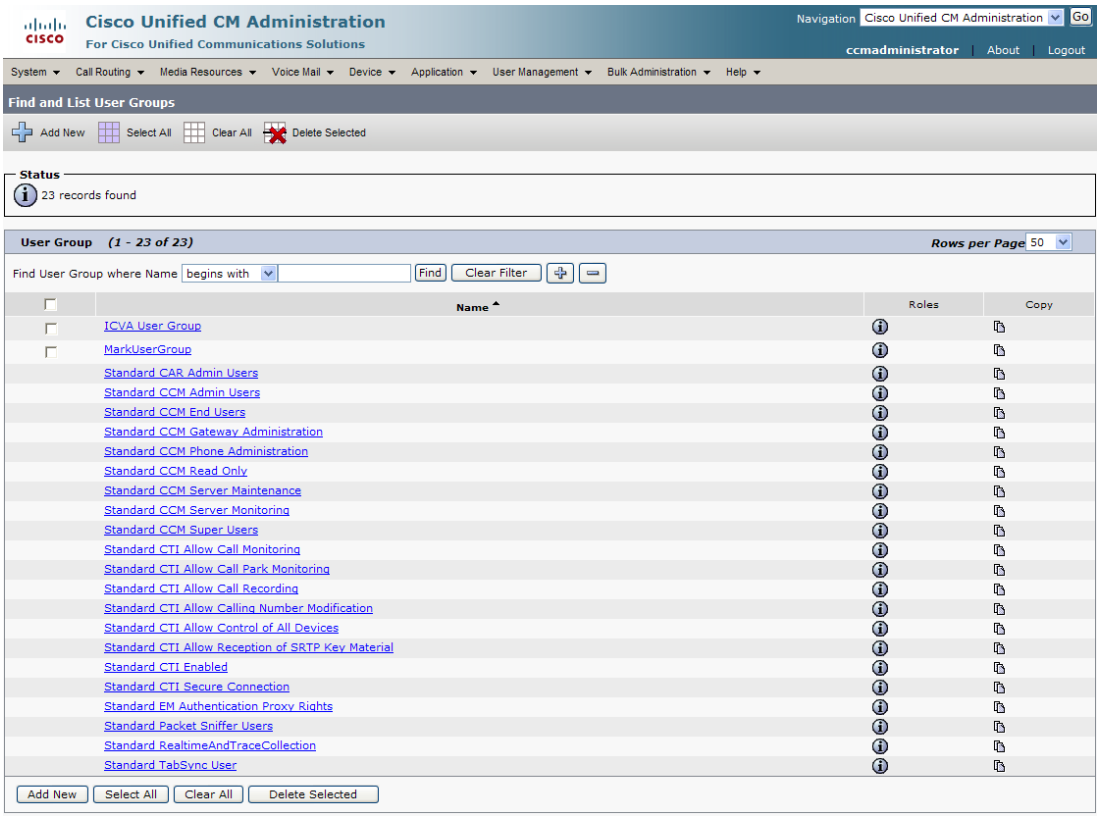
Step 3 Enter **ICVA User Group** in the **Name** field and click the **Save** button. The User Group Configuration page refreshes.



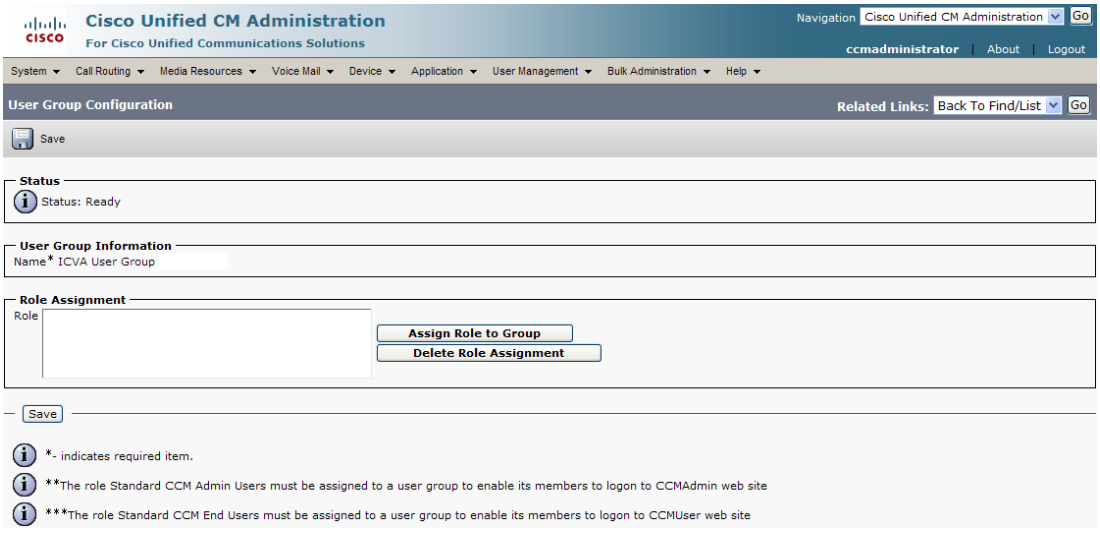
Step 4 Make sure **Back to Find/List** is selected in the **Related Links** dropdown menu and click the **Go** button. The Find and List User Groups page appears.



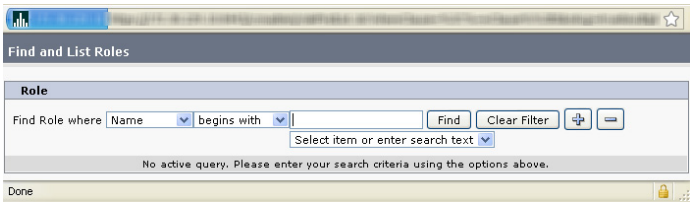
Step 5 Click the **Find** button. The Find and List User Groups page refreshes and you should see your new user group.



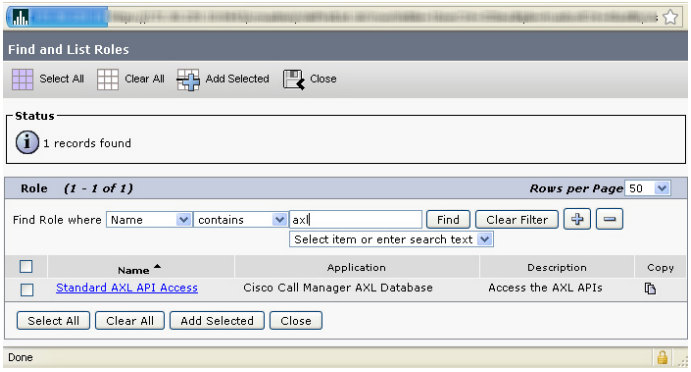
Step 6 Click the **i** icon in the Roles column next to your new user group. The User Group Configuration page appears.



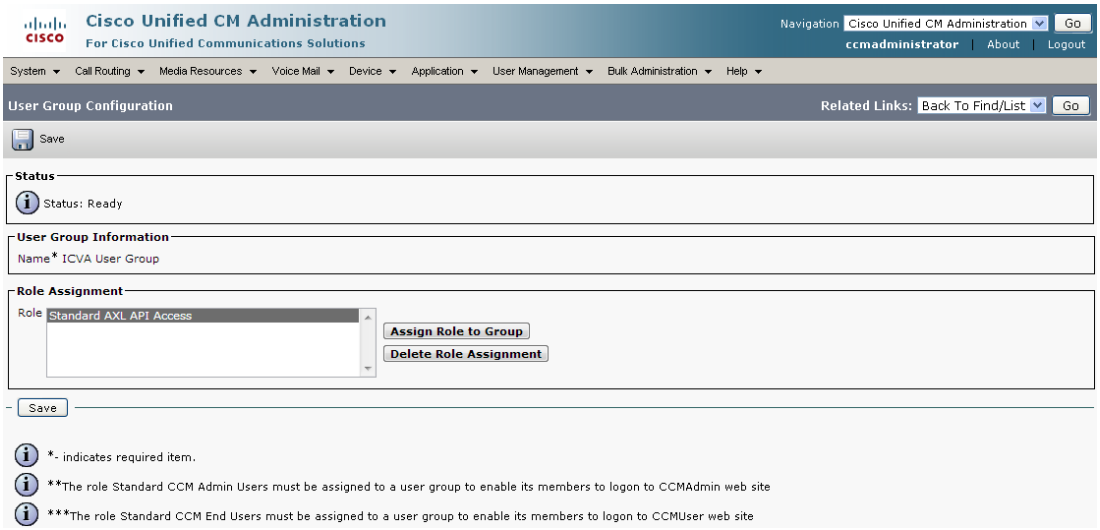
Step 7 Click the **Assign Role to Group** button. The Find and List Roles window appears.



Step 8 Click the **Find** button. The Find and List Roles window refreshes.



Step 9 Select the **Standard AXL API Access** checkbox and click the **Add Selected** button. The User Group Configuration page refreshes.



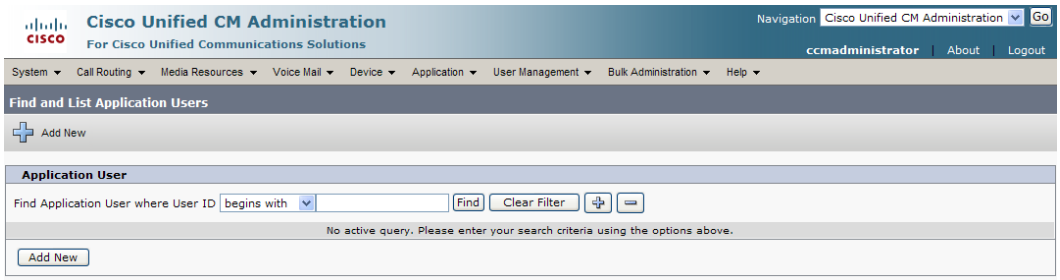
Step 10 Click the **Save** button.

Create an Application User

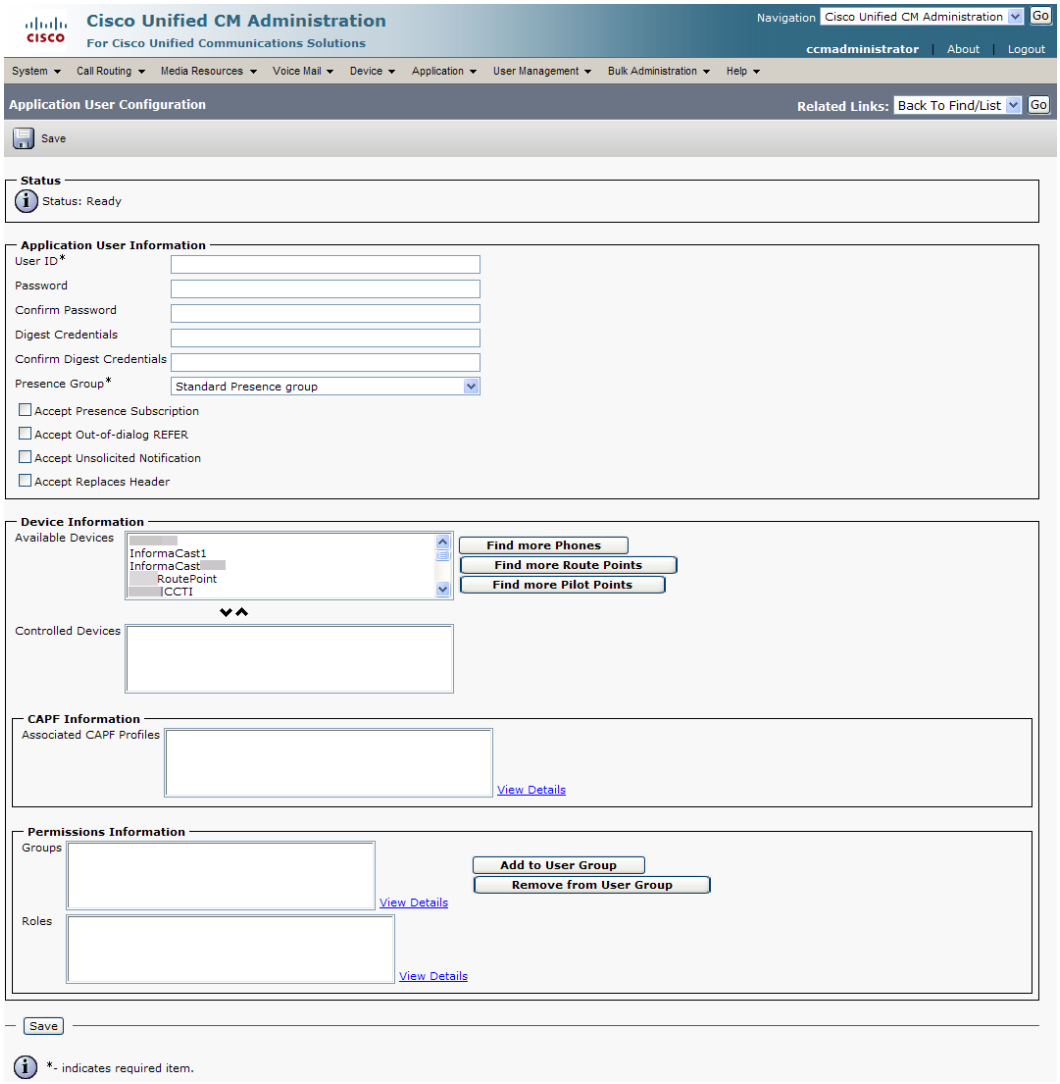
InformaCast needs an application user set in CUCM so that it can establish a CTI connection and gain access to the telephony features CUCM offers (e.g. making phone calls, using JTAPI to determine the busy status of a phone, etc.). You also need an application user for AXL phone data requests. Those requests must include the credentials for a user who has been granted access to the AXL API. Several roles/groups need to be associated with your InformaCast application user:

- **ICVA User Group.** Allows you access to the Standard AXL API Access role through the group you created in "Create an AXL User Group/Access Control Group" on page 2-49.
- **Standard CTI Allow Control of All Devices.** Allows an application to control or monitor any CTI-controllable device in the system. This is optional; when combined with InformaCast, it allows you to communicate using JTAPI instead of HTTP (see "Manage Broadcast Parameters" on page 4-44).
- **Standard CTI Allow Control of Phones Supporting Connected Xfer and Conf.** Allows JTAPI to determine the busy status of a phone, communicating to InformaCast whether to skip it in a broadcast (for phones that support the connected transfer and conference feature).
- **Standard CTI Allow Control of Phones Supporting Rollover Mode.** Allows JTAPI to determine the busy status of a phone, communicating to InformaCast whether to skip it in a broadcast (for phones that support rollover mode).
- **Standard CTI Enabled.** Enables users to execute CTI applications that control/monitor devices.

Step 1 Go to **User Management** | **Application User**. The Find and List Application Users page appears.



Step 2 Click the **Add New** button. The Application User Configuration page appears.



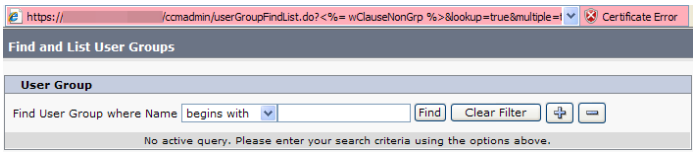
Step 3 Enter an appropriate user ID in the **User ID** field, e.g. ICVA InformaCast.

Step 4 Enter a password into the **Password** field, and enter it again in the **Confirm Password** field.

You will need to remember the user ID and password values because you will enter them into InformaCast's own Edit Telephony Configuration page once you install InformaCast (see "Configure Your Default CUCM Cluster" on page 4-2).

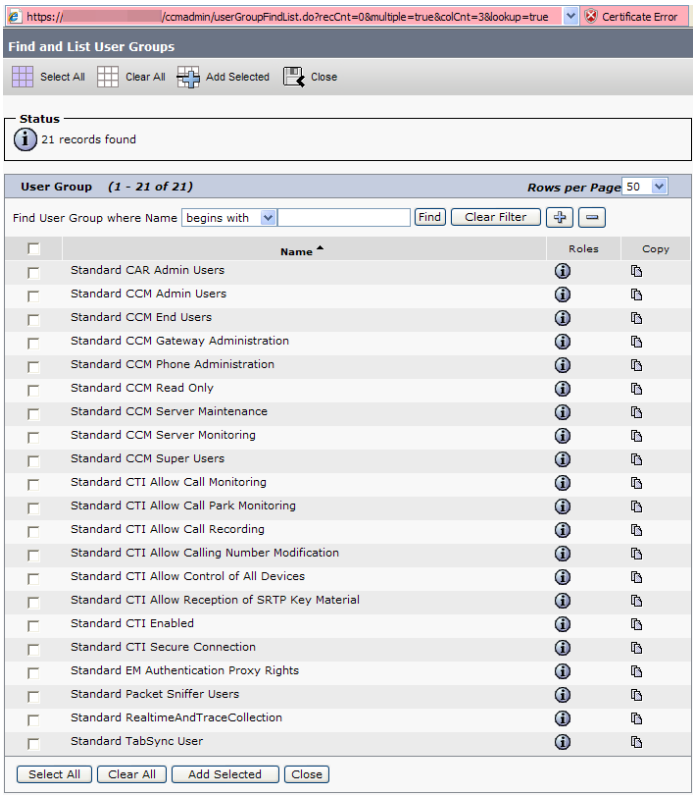
Step 5 Select the CTI ports (created in "Create CTI Ports" on page 2-44) in the *Device Information* area and move them from the **Available Devices** field to the **Controlled Devices** field using the down arrow.

Step 6 Scroll down to the *Permissions Information* area on the Application User Configuration page and click the **Add to User Group** button. The Find and List User Groups window appears.



Note If you are using CUCM 9.0 or later, "user groups" changed to "access control groups" (see "Create an AXL User Group/Access Control Group" on page 2-49), which means that you will now click the **Add to Access Control Group** button instead of the **Add to User Group** button. Clicking the **Add to Access Control Group** button will open the Find and List Access Control Groups pop-up window.

Step 7 Click the **Find** button. The Find and List User Groups window refreshes with a list of user groups.



Step 8 Select the **ICVA User Group**, **Standard CTI Allow Control of All Devices** (optional), **Standard CTI Allow Control of Phones supporting Connected Xfer and conf**, **Standard CTI Allow Control of Phones supporting Rollover Mode**, and **Standard CTI Enabled** checkboxes and click the **Add Selected** button. You will be returned to the Application User Configuration page.

Step 9 Verify the application user has been added to the correct groups by scrolling down to the *Permissions Information* area and viewing the entries in the **Groups** field.

Step 10 Click the **Save** button to save your changes.

Enable Web Access for Cisco IP Phones

You must enable web access for all phones to which InformaCast will broadcast. To enable web access, you can:

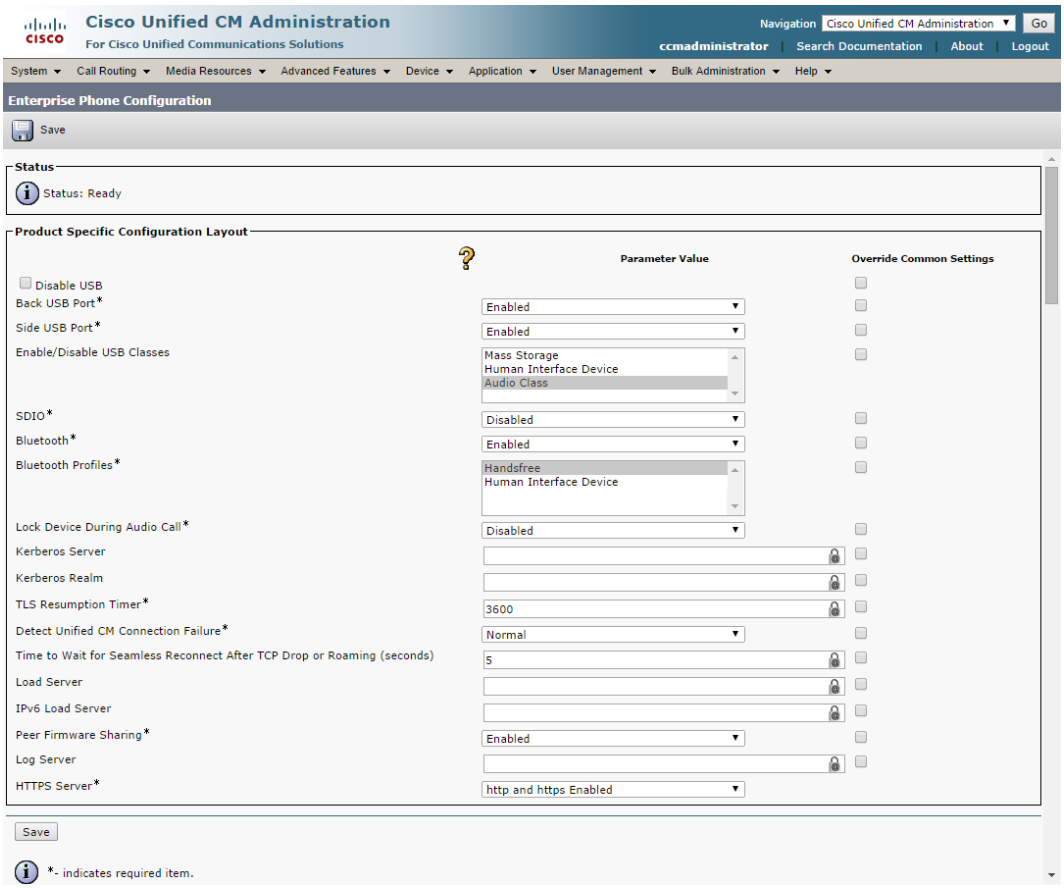
- Enable phones en masse by changing their enterprise phone configurations
- Enable phones en masse by changing their profiles
- Enable individual phones

Enable Web Access for Multiple Phones by Changing Their Enterprise Phone Configurations

Use the following steps to enable web access for multiple phones by changing their enterprise phone configurations.

Note This option is only available to you if you are using CUCM 9.x or later.

Step 1 Go to **System | Enterprise Phone Configuration**. The Enterprise Phone Configuration page appears.



Step 2 Scroll down to the **Web Access** dropdown menu and select **Enabled**.

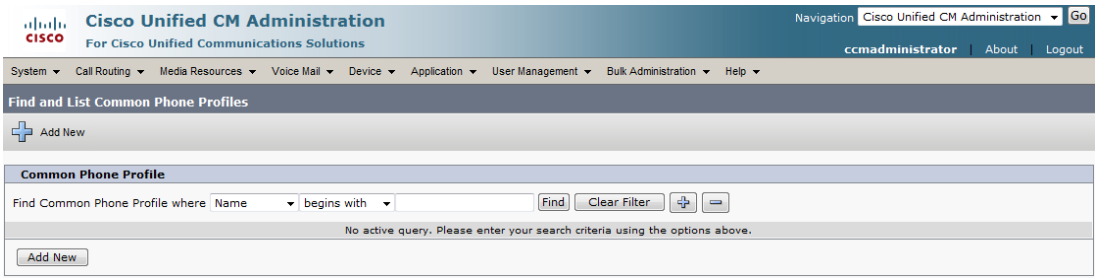
Step 3 Click the **Save** button.

Note You will need to reboot your phones for this change to take effect; however, you will also need to reboot your phones after performing the steps in "Set Your Authentication URL" on page 2-64. If you have a lot of phones, this process can be time-consuming. If you only want to reset your phones once, wait to do so until prompted in "Reboot Your Phones" on page 2-65.

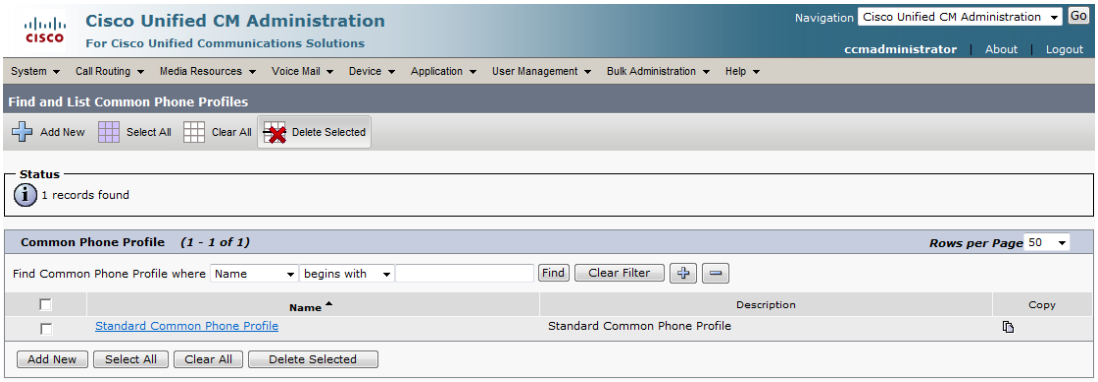
Enable Web Access for Multiple Phones by Changing Their Profiles

Use the following steps to enable web access for multiple phones by changing their profiles.

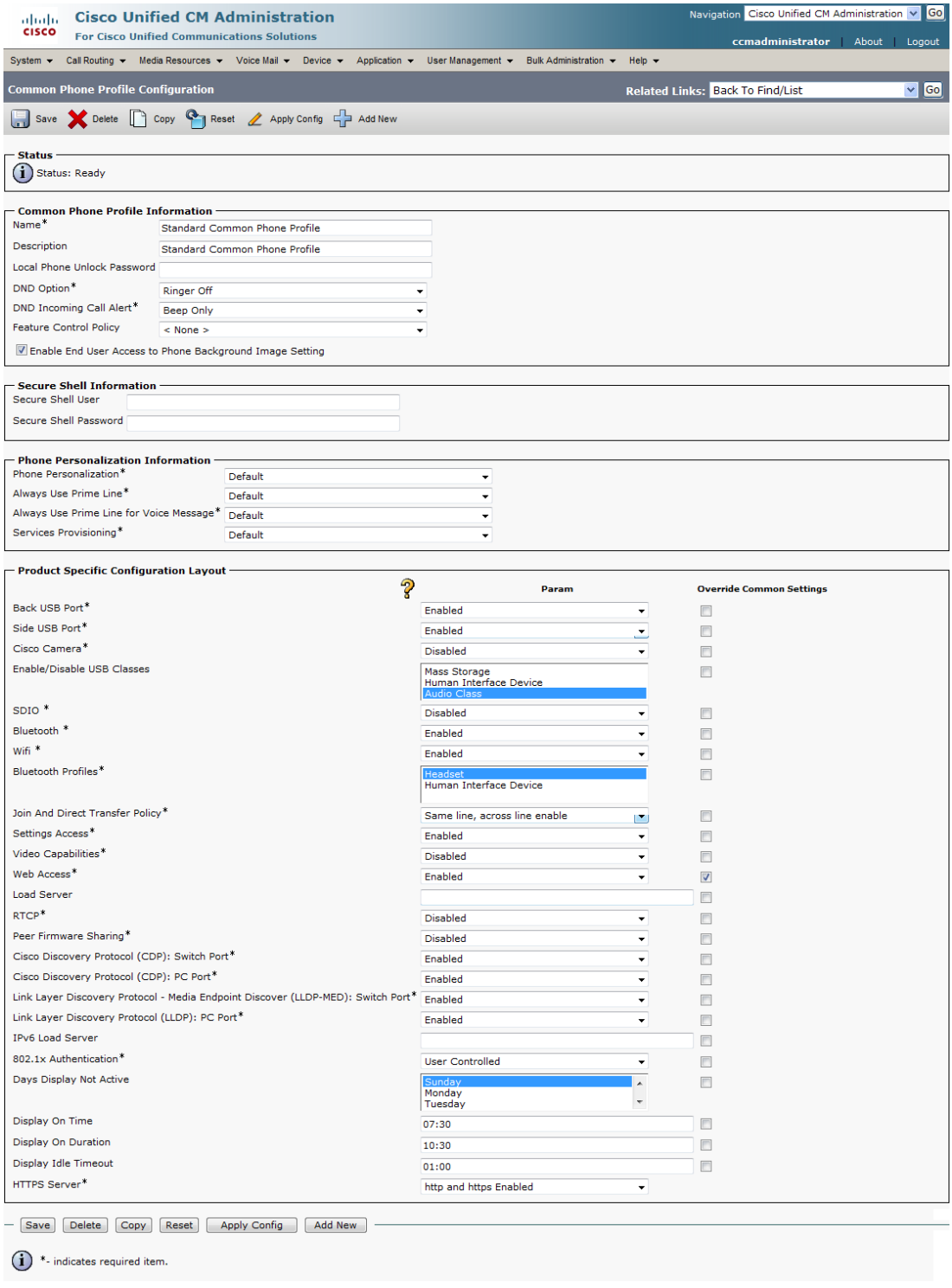
Step 1 Go to **Device** | **Device Settings** | **Common Phone Profile**. The Find and List Common Phone Profiles page appears.



Step 2 Click the **Find** button to display all the phone profiles of which CUCM knows or use the filter fields at the top of the page to narrow your list of profile results before clicking the **Find** button. The Find and List Common Phone Profiles page refreshes.



Step 3 Click the **Name** link of the profile in which you want to enable web access. Make sure you select the profile that applies to the phones where web access needs to be enabled. The Common Phone Profile Configuration page for that phone appears.



Step 4 Scroll down to the *Product Specific Configuration Layout* area and select **Enabled** from the **Web Access** dropdown menu.

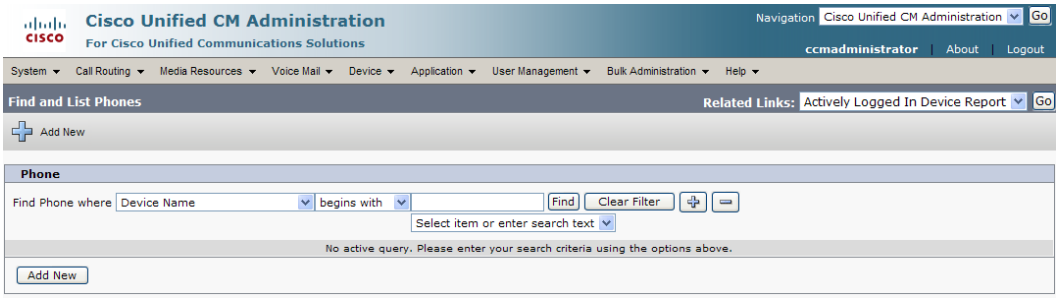
Step 5 Click the **Save** button.

Note You will need to reboot your phones for this change to take effect; however, you will also need to reboot your phones after performing the steps in "Set Your Authentication URL" on page 2-64. If you have a lot of phones, this process can be time-consuming. If you only want to reset your phones once, wait to do so until prompted in "Reboot Your Phones" on page 2-65.

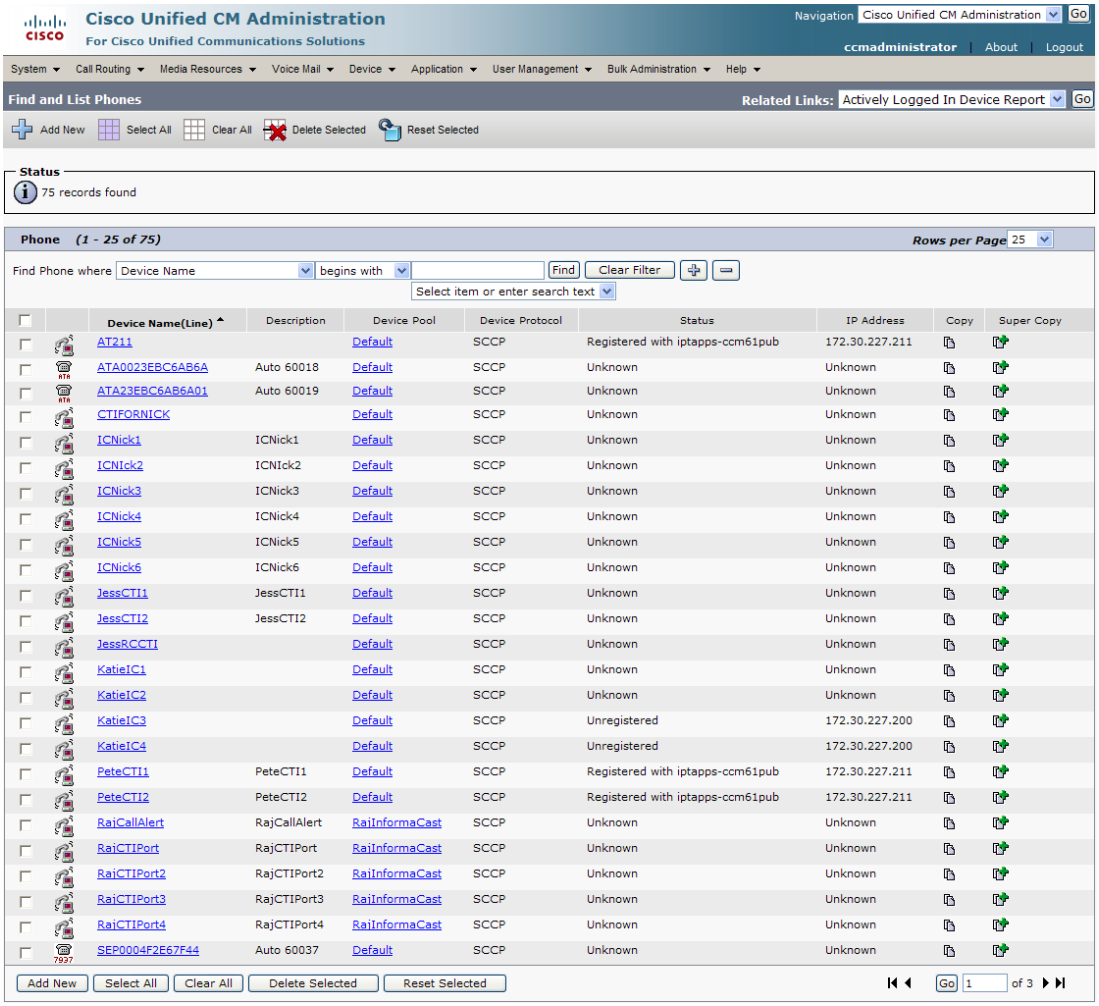
Enable Web Access for Individual Phones

Use the following steps to enable web access for individual phones.

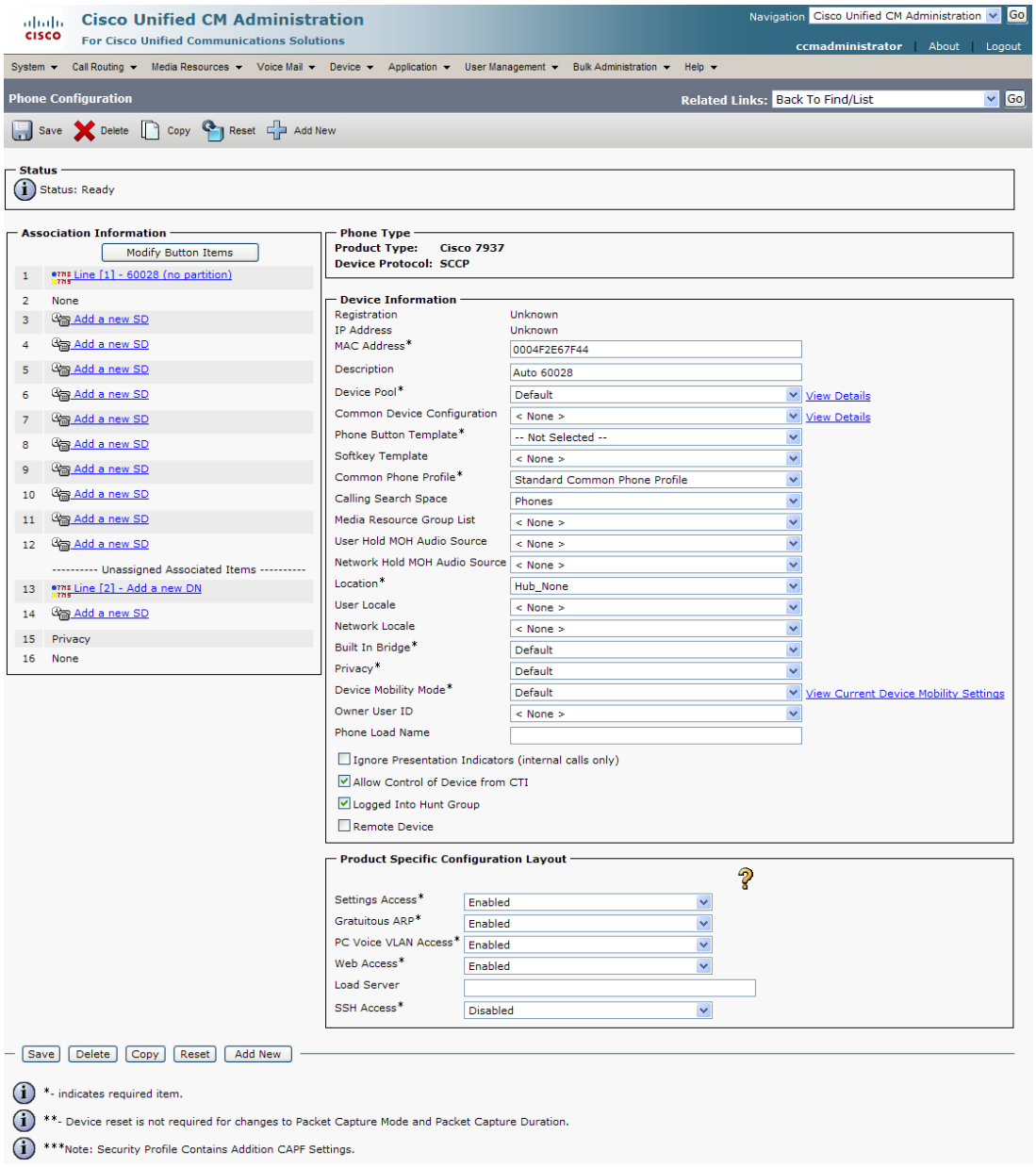
Step 1 Go to **Device** | **Phone**. The Find and List Phones page appears.



Step 2 Click the **Find** button to display all phones of which CUCM knows or use the filter fields at the top of the page to narrow your list of phone results before clicking the **Find** button. The Find and List Phones page refreshes.



Step 3 Click the **Device Name** link of the phone in which you want to enable web access. The Phone Configuration page for that phone appears.



Step 4 Scroll down to the *Product Specific Configuration Layout* area and select **Enabled** from the **Web Access** dropdown menu.

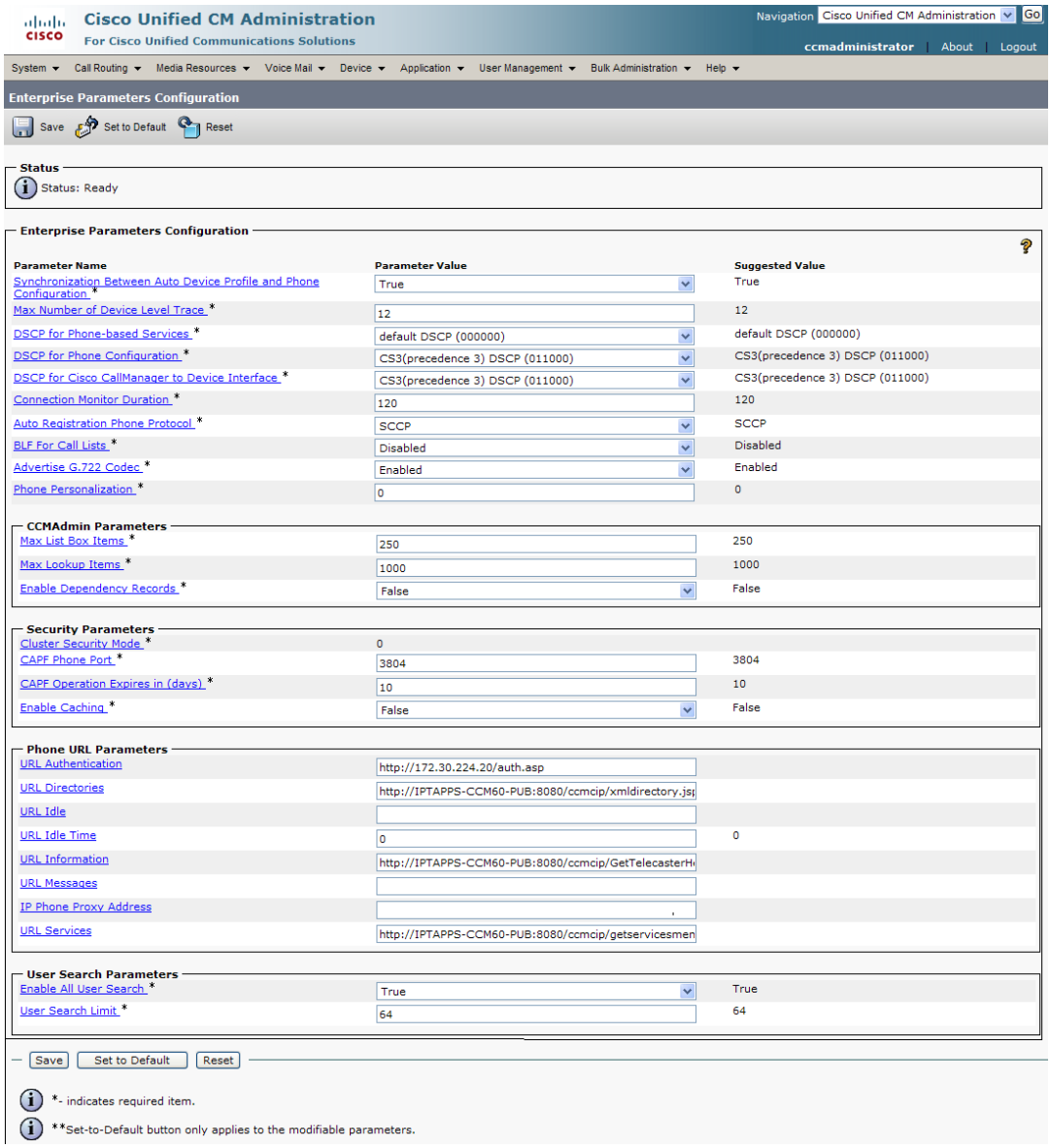
Step 5 Click the **Save** button.

Note You will need to reboot your phones for this change to take effect; however, you will also need to reboot your phones after performing the steps in "Set Your Authentication URL" on page 2-64. If you have a lot of phones, this process can be time-consuming. If you only want to reset your phones once, wait to do so until prompted in "Reboot Your Phones" on page 2-65.

Set Your Authentication URL

When InformaCast sends broadcasts to your phones, it needs to be able to push commands to them, which requires that you point CUCM's Authentication URL to InformaCast.

Step 1 Go to **System** | **Enterprise Parameters**. The Enterprise Parameters Configuration page appears.



Note Once you make this change, InformaCast must be running when any XML push application is used, because the phones will query the InformaCast authentication server.

Step 2 Scroll down the page to the *Phone URL Parameters* area.

Step 3 Make a note of the URL in the **URL Authentication** field. You may need this in Step 10 on page 4-6.

Step 4 Enter **http://<InformaCast Virtual Appliance IP Address>:8081/InformaCast/phone/auth** in the **URL Authentication** field, where <InformaCast Virtual Appliance IP Address> is replaced with your Virtual Appliance's actual IP address.

Note The URL is case sensitive, so make sure that the I and C in the word InformaCast are capitalized.

Step 5 Scroll to the *Secured Phone URL Parameters* area and enter **http://<InformaCast Virtual Appliance IP Address>:8081/InformaCast/phone/auth** in the **Secured Authentication URL** field as well.

Step 6 Click the **Save** button.

Note You must reboot your phones for the new authentication URL to take affect. See "Reboot Your Phones" on page 2-65.

Reboot Your Phones

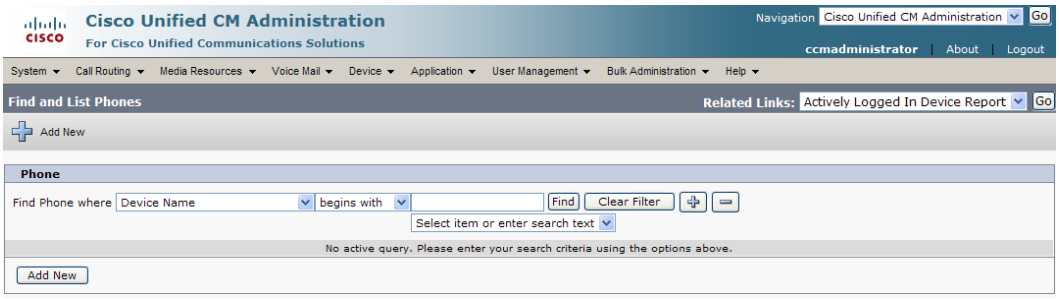
Enabling web access for your phones and setting your authentication URL both require you to reboot your phones. There are many methods that can be used to reboot your phones. Use your best judgment for how and when this can be done in your environment. Some possible options for rebooting your phones include:

- Bulk Administration Tool (BAT), which allows you to schedule your reboots for off hours and not deal with manually executing the reboot
- Enterprise parameters, which allows you to reboot all devices in a cluster
- Device pools, which allow you to reboot phones on a site-by-site basis
- Device defaults, which allows you to reboot phones by their model type
- Individual phones, which allows you to do phone-by-phone reboots

This guide will illustrate a popular option for rebooting phones: rebooting by device pool.

Note By resetting the device pool you reset all devices associated with it, e.g. analog ports, voice gateways, conference bridges, etc. This option is best performed during off-peak hours.

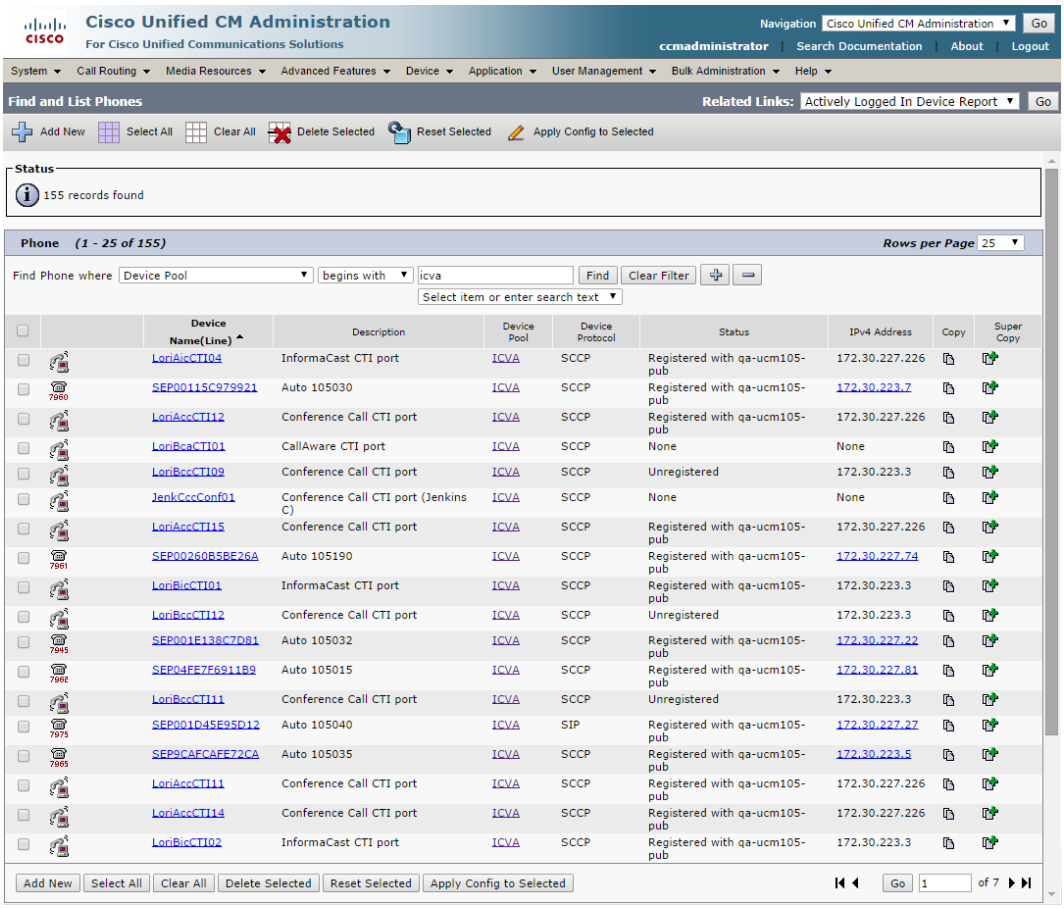
Step 1 Go to **Device** | **Phone**. The Find and List Phones page appears.



Step 2 Select **Device Pool** from the **Find Phone where** dropdown menu.

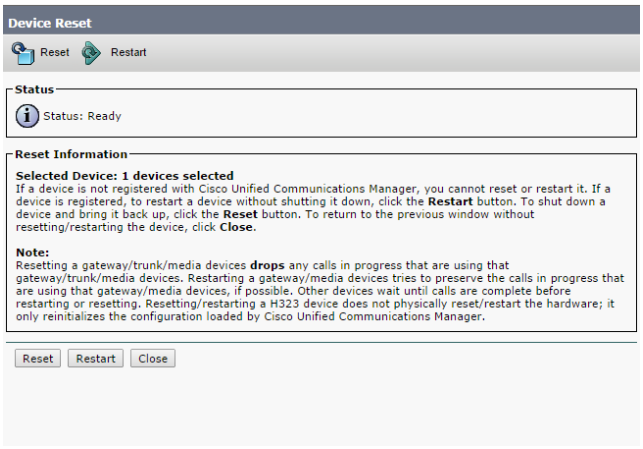
Step 3 Set the other dropdown menu and field to the parameters most likely to bring up the device pool(s) in which you'd like to reboot your phones.

Step 4 Click the **Find** button. The Find and List Phones page refreshes with your search results.



Step 5 Select the device pool(s) that house the phones you'd like to reboot.

Step 6 Click the **Reset Selected** button. The Device Reset dialog box appears.

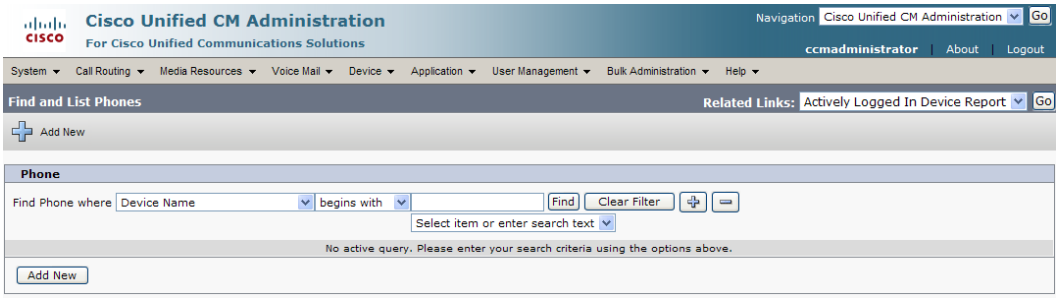


Step 7 Click the **Reset** button. Your phone(s) will reboot.

Test Your Phones

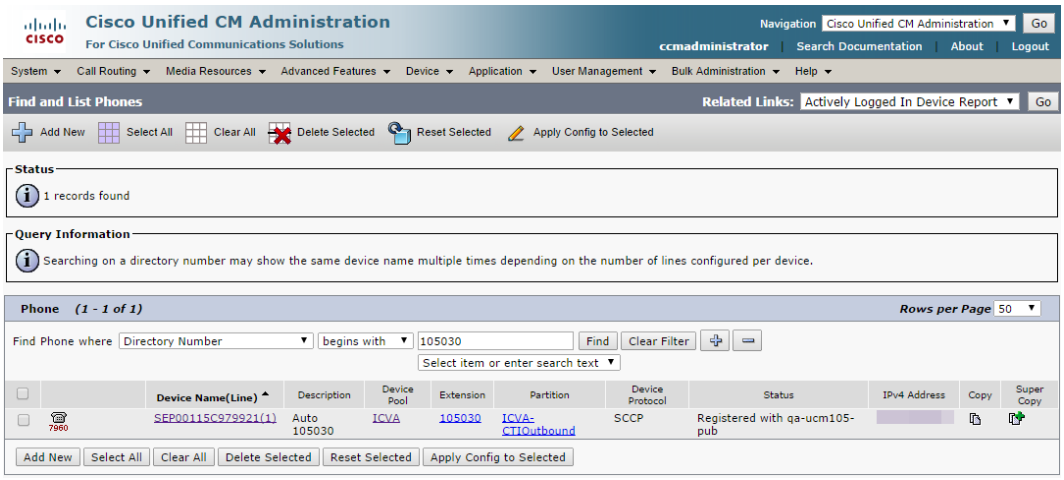
Rebooting your phones should have caused them to pick up their new settings. You can verify their new settings through a web browser.

Step 1 Go to **Device** | **Phone**. The Find and List Phones page appears.

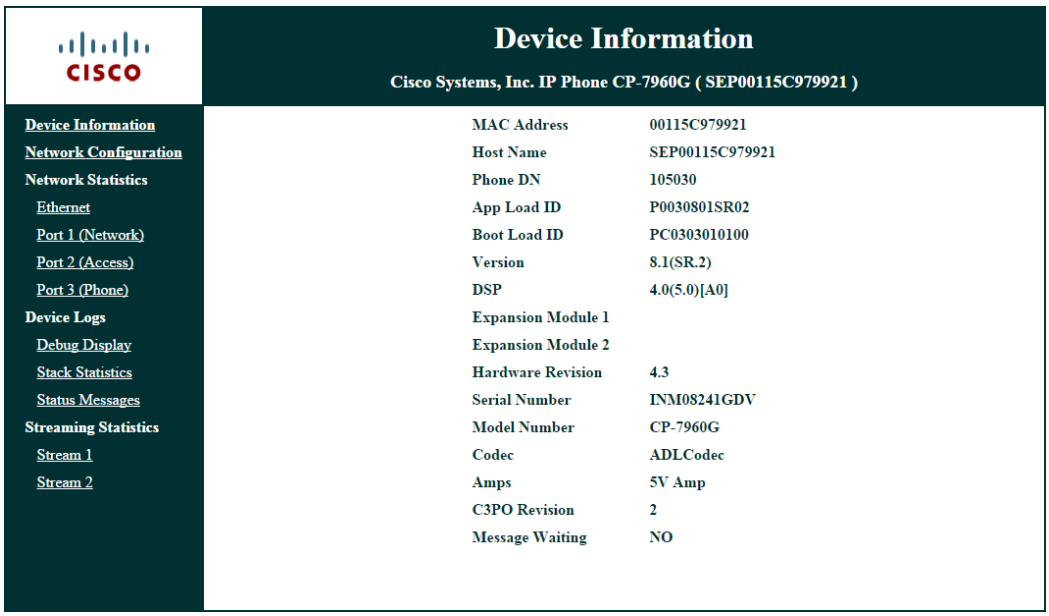


Step 2 Use the dropdown menus and fields to filter for a phone that should have picked up your new settings.

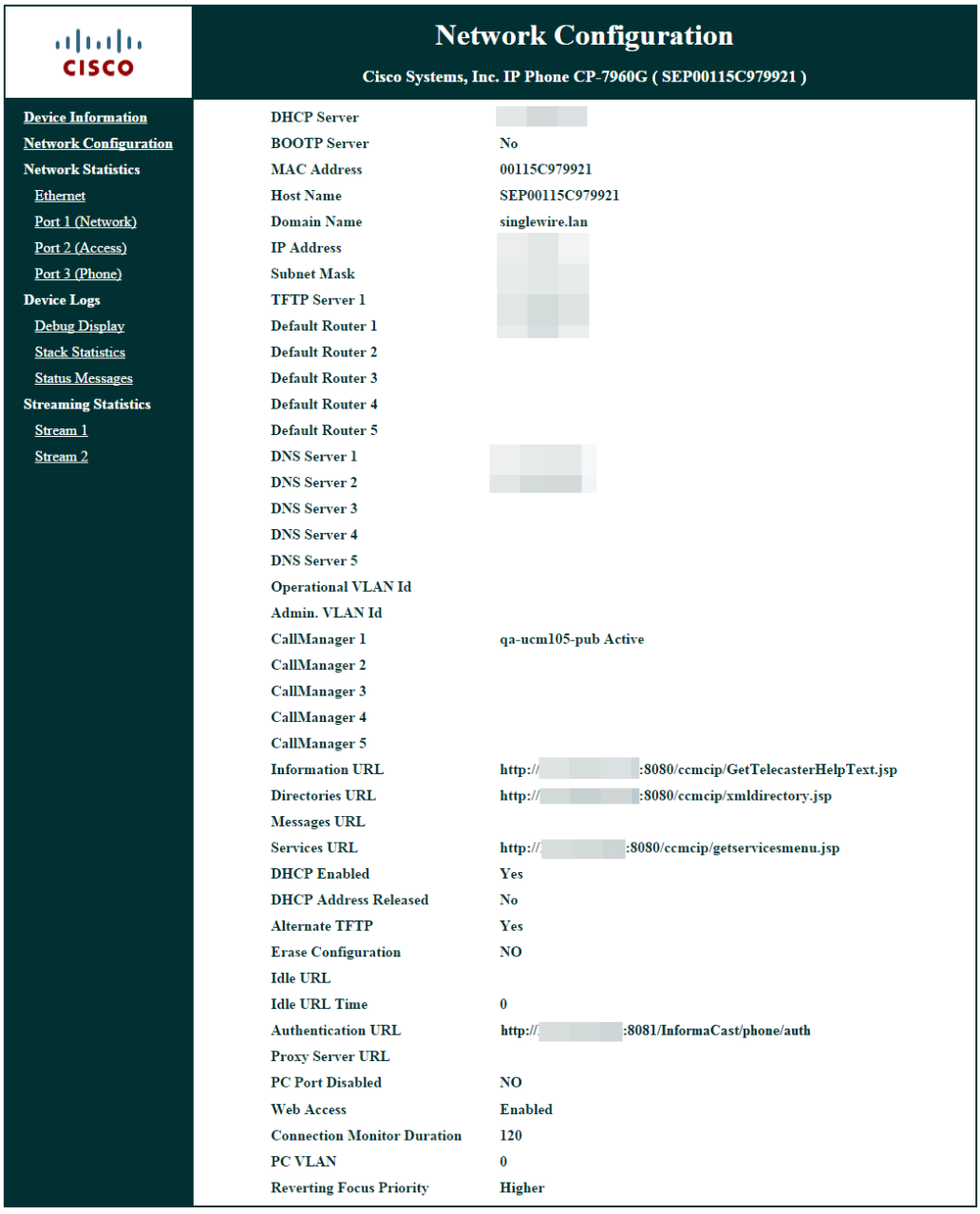
Step 3 Click the **Find** button. The Find and List Phones page refreshes with your search results.



Step 4 Click the **IP address** link in the IPv4 Address column. The Device Information page should open in a new window/tab. If the webpage does not display, you most likely do not have web access enabled for this phone (see "Enable Web Access for Cisco IP Phones" on page 2-56 for more information).



Step 5 Click the **Network Configuration** link. The Network Configuration page appears.



Step 6 Scroll down the page until you come to Authentication URL. It should list the IP address you entered in the **URL Authentication** field in Step 4 on page 2-65. If it does not, see "Set Your Authentication URL" on page 2-64.

Manage Installation Administration

Installation administration covers a number of topics that pertain the administration of your InformaCast installation, namely multicast administration, such as obtaining and viewing traffic captures to verify multicast functionality.

Review Multicast Configuration

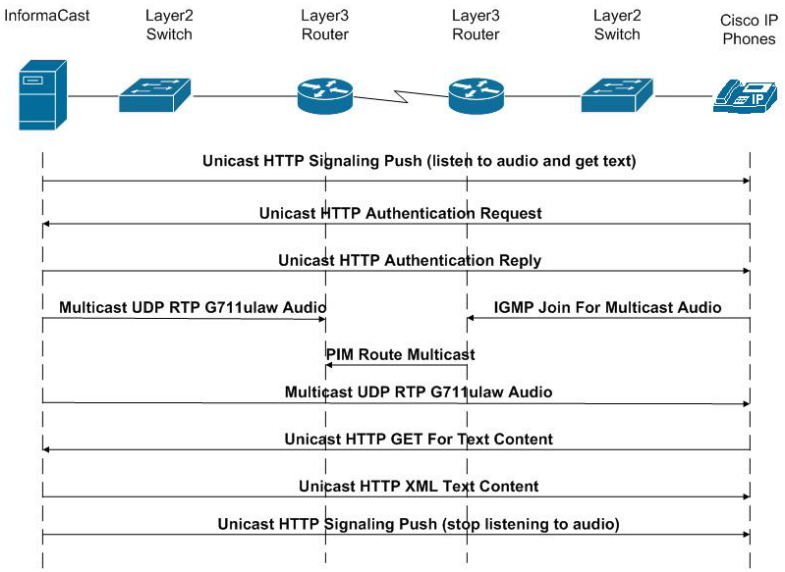
Multicast must be configured in order for InformaCast broadcasts to properly play on your recipients. The following recommendations can also apply:

- Protocol Independent Multicast (PIM) should be deployed in either sparse or dense mode across your Layer 3 devices (PIM is the most common protocol, but there are others)
- Your MPLS network provider should route multicast on its network; otherwise you will need to use GRE tunnels

In addition, sometimes Internet Group Management Protocol (IGMP) snooping can cause issues with varying revisions of IOS on some Cisco switches and may need to be turned off. Lastly, for recipients to receive the audio portion of InformaCast broadcasts, they make requests using IGMP. While most networks default to IGMPv2, newer recipients may use IGMPv3. If newer recipients are being deployed, be sure to enable the newer protocol version on network devices.

Verify Multicast with a Network Traffic Capture

Another way to verify multicast is configured (besides by using the Multicast Testing Tool) is through a network traffic capture. It is important to note that the only piece of traffic that travels through the network via multicast routing is the audio portion of a broadcast. All signaling traffic is done with unicast HTTP. The diagram below outlines the traffic that occurs during an InformaCast broadcast that contains both text and audio.



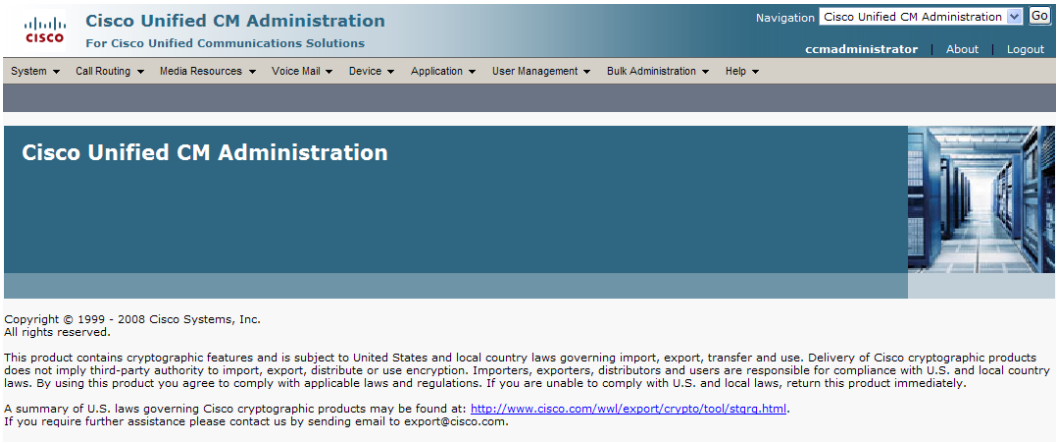
Now that you are familiar with the traffic flow created by InformaCast, you can use a protocol analyzer, such as Wireshark, to sniff the traffic on the network to see that multicast is enabled.

Obtain a Network Traffic Capture

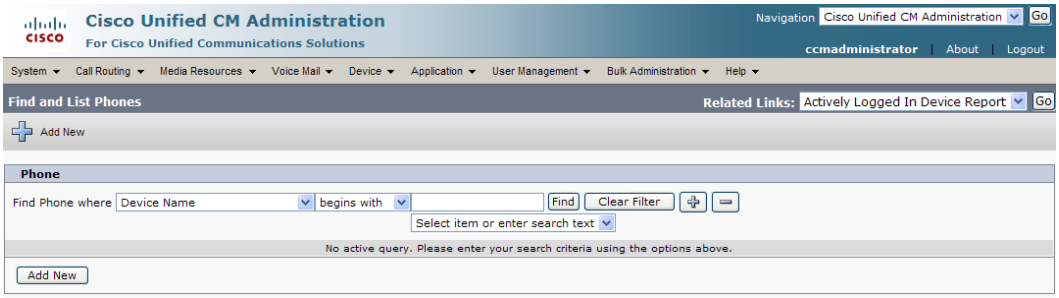
Use the following steps to obtain a network traffic capture from a phone to determine if multicast traffic is routing to that network segment.

Step 1 Download and install a protocol analyzer like Wireshark (http://www.wireshark.org/) on a PC that's attached to a phone on your network on which you want to obtain a traffic capture.

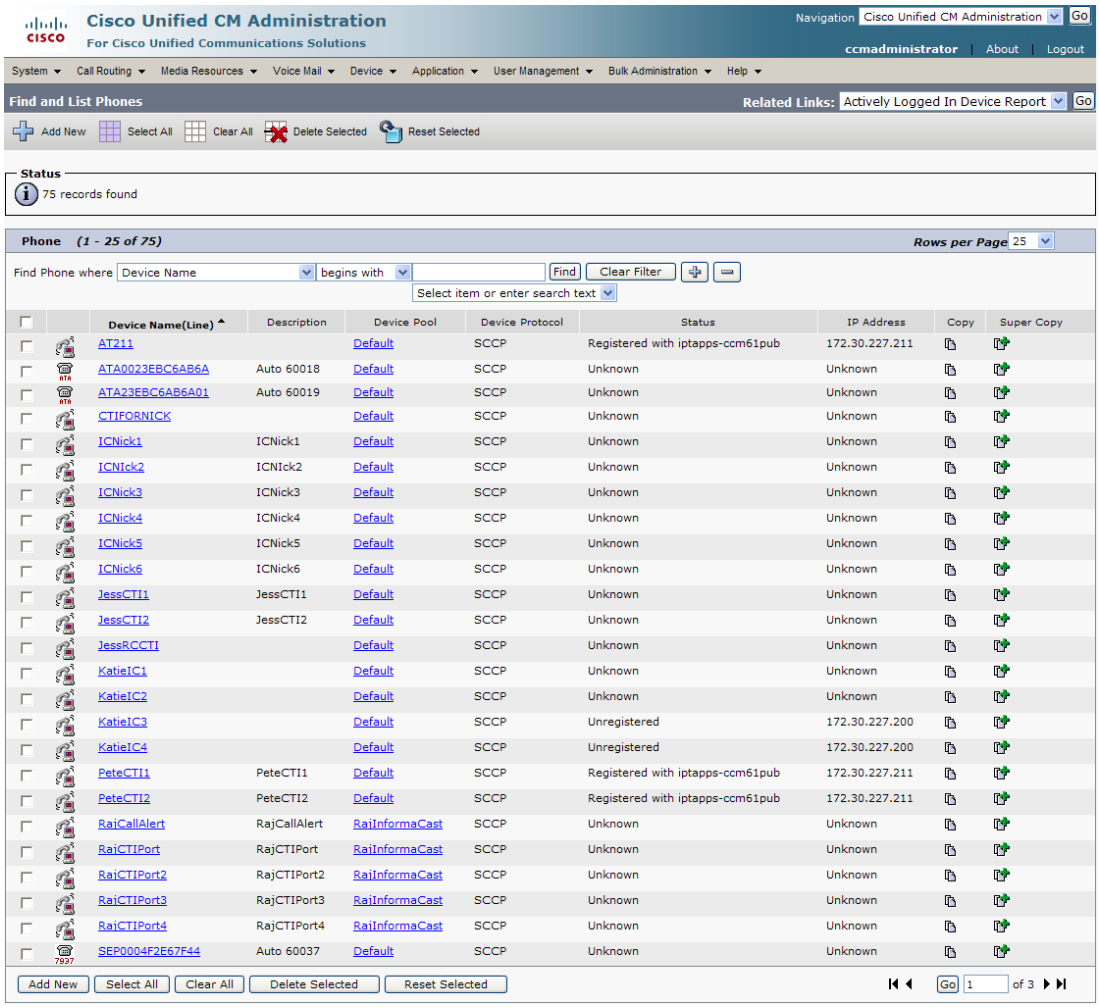
Step 2 Open and log into your CUCM's administrative interface. The Cisco Unified CM Administration page appears.



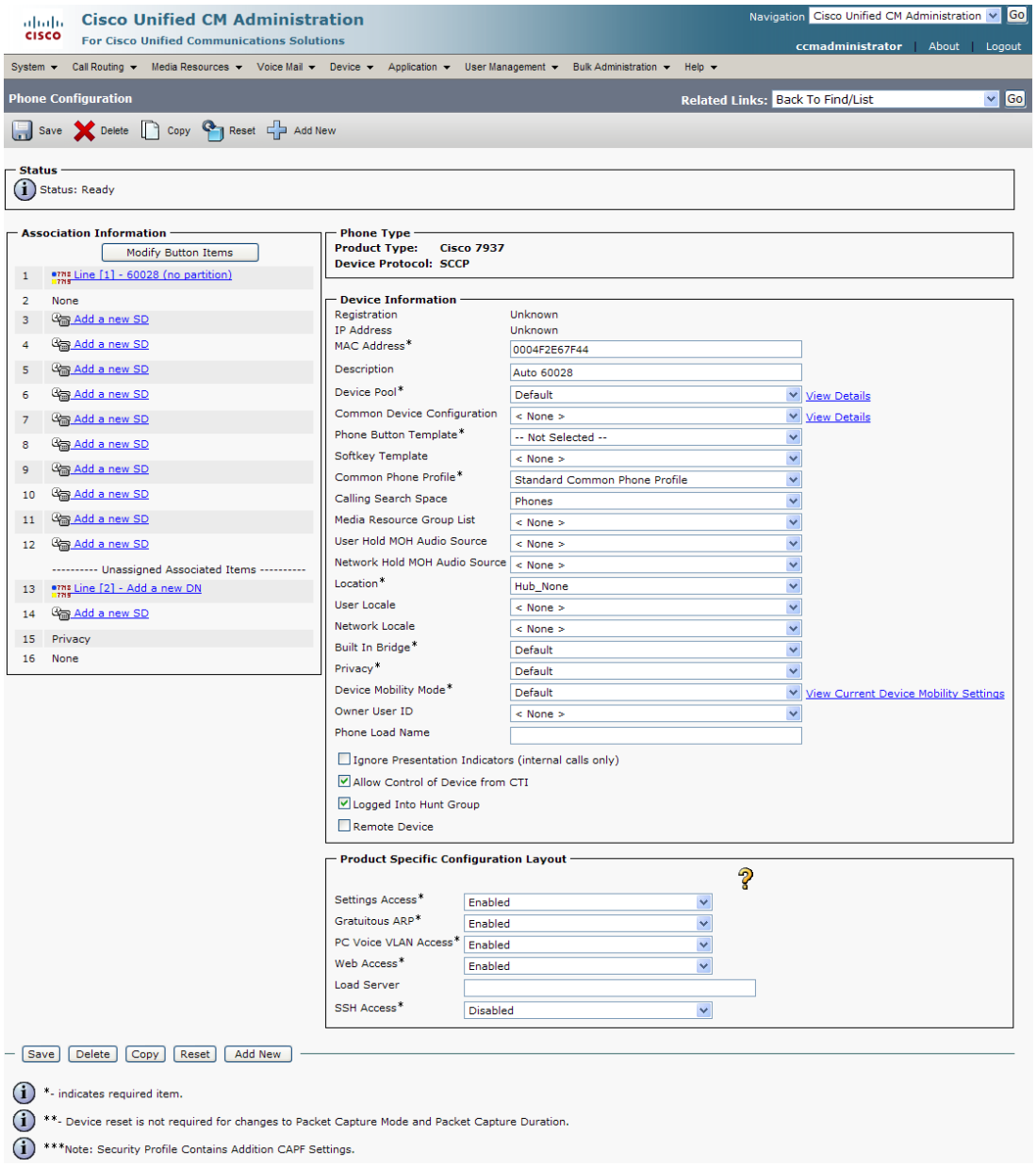
Step 3 Go to **Device** | **Phone**. The Find and List Phone page appears.



Step 4 Use the dropdown menus and fields to locate the phone attached to the PC on which you downloaded Wireshark. Your results will appear below the fields.



Step 5 Select the phone attached to your PC with Wireshark on it. The Phone Configuration page for that phone appears.

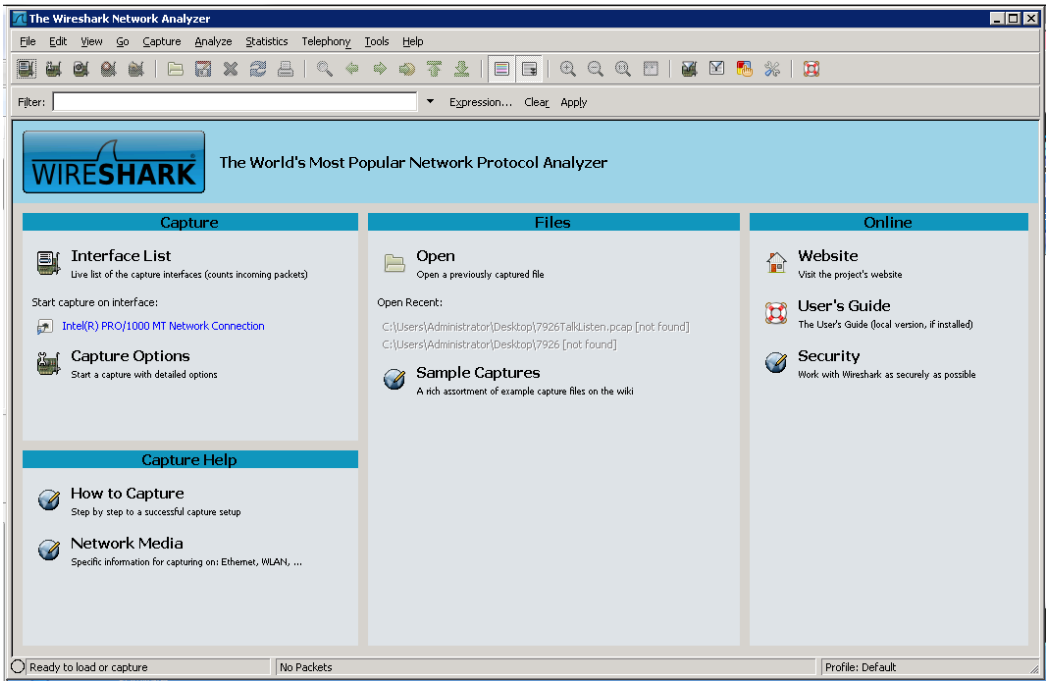


Step 6 Scroll down to the *Product Specific Configuration Layout* area.

Step 7 Make sure that both the **Web Access** and **Span to PC Port** dropdown menus have **Enabled** selected.

Step 8 Click the **Reset** button.

Step 9 Start Wireshark. The Wireshark window appears.



Step 10 Send an InformaCast broadcast to the phone attached to the PC with Wireshark on it.

Step 11 Wait until the broadcast has finished and stop the network traffic capture.

Read a Network Traffic Capture

When analyzing a network traffic capture, look for the following:

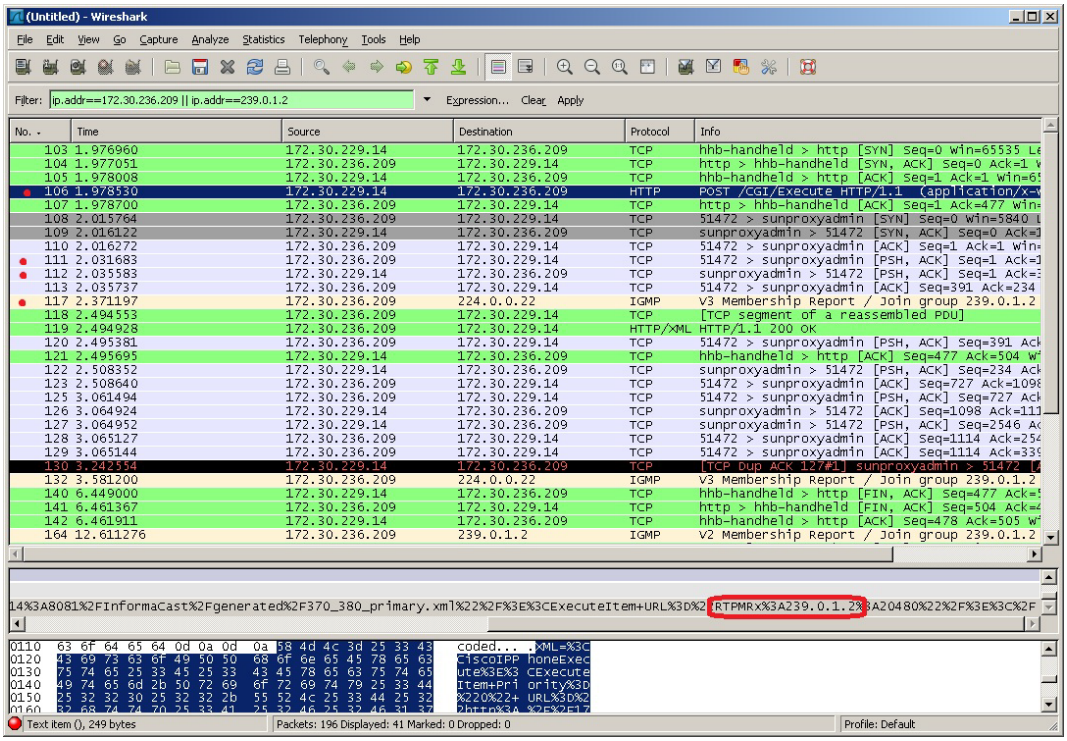
- A unicast HTTP command from InformaCast to the recipient to join the multicast group
- Successful authentication
- An IGMP join from the recipient to the multicast group
- A multicast audio stream

When there is no multicast audio present, InformaCast audio will not play through a recipient, and you'll notice the following things in your traffic capture (reference with the following graphic):

- **Frame 106.** InformaCast pushes the unicast HTTP command to a recipient to listen to audio. In the middle pane, the multicast IP address to listen for is circled in red.
- **Frame 111.** The recipient makes a unicast HTTP authentication request. The protocol doesn't show as HTTP because the communication took place on port 8444. You can view the contents of the packet for the actual data or decode as HTTP.
- **Frame 112.** InformaCast replies in unicast HTTP to the authentication request as OK.
- **Frame 117.** The recipient makes an IGMP join request for a multicast audio stream.

- **Frame 164.** There is a timestamp nine seconds after the IGMP join, but no multicast traffic is seen in the capture. Thus, multicast is not routing and no audio will be received at the recipient.

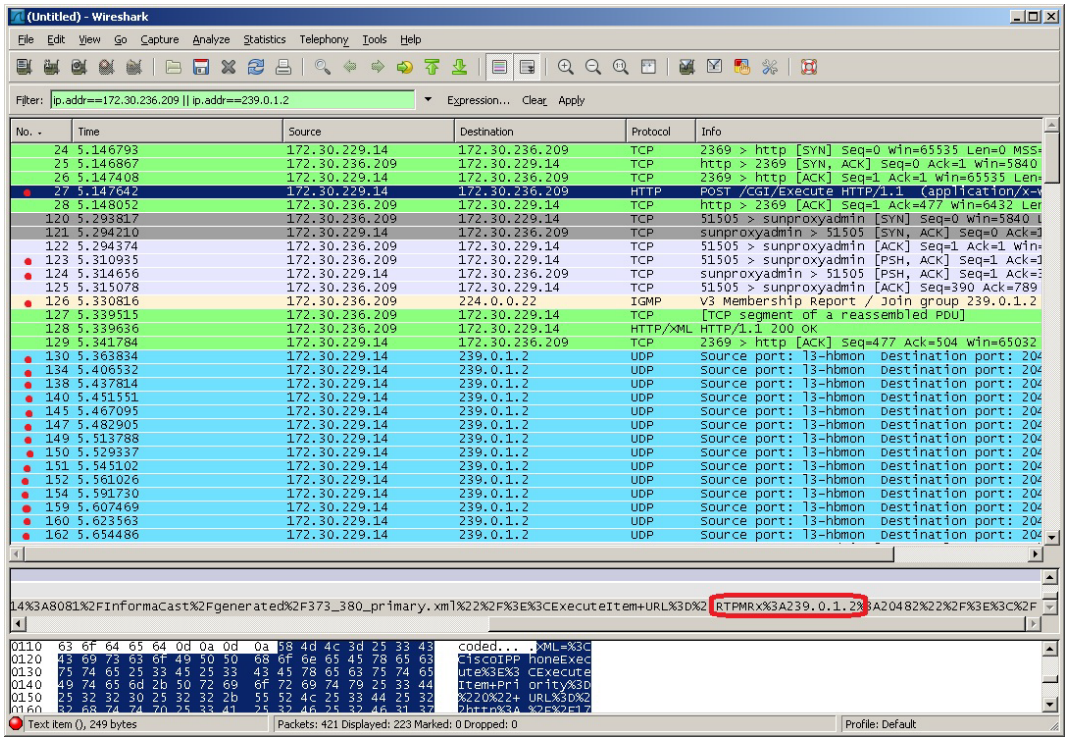
Each of the things to look for are marked with red in the following graphic.



When there is multicast audio present, InformaCast audio plays through recipient, and you'll notice the following things in your traffic capture (reference with the following graphic):

- **Frame 27.** InformaCast pushes the unicast HTTP command to a recipient to listen to audio. In the middle pane, the multicast IP address to listen for is circled in red.
- **Frame 123.** The recipient makes a unicast HTTP authentication request. The protocol doesn't show as HTTP because the communication took place on port 8444. You can view the contents of the packet for the actual data or decode as HTTP.
- **Frame 124.** InformaCast replies in unicast HTTP to the authentication request as OK.
- **Frame 126.** The recipient makes an IGMP join request for a multicast audio stream.
- **Frames 130 - 62 (plus more).** The multicast UDP is present. Audio should have played through the recipient.

Each of the things to look for are marked with red in the following graphic.

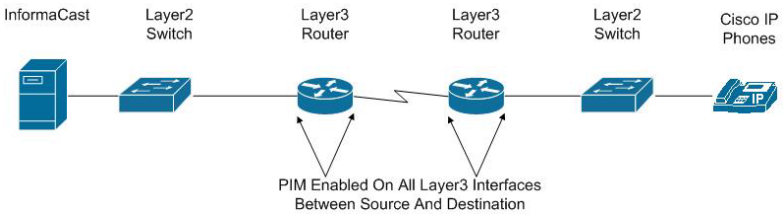


If multicast isn't working, troubleshoot the problems singly by frame(s). Work with your network administrator to configure multicast appropriately.

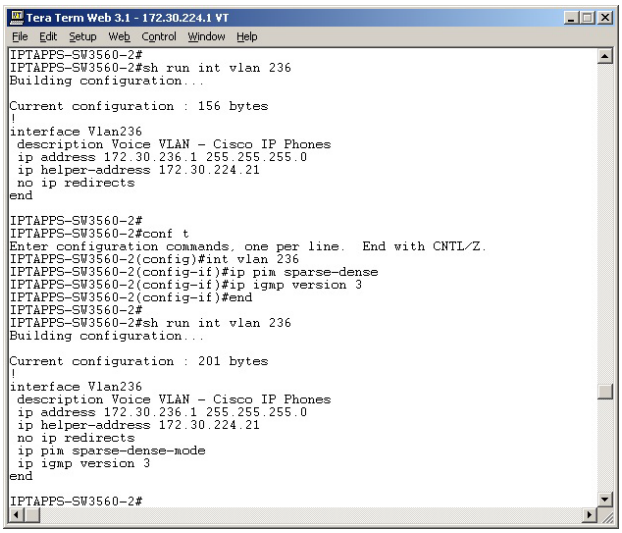
Verify PIM is Configured on All Layer 3 Interfaces

For audio broadcast traffic to route from a source (InformaCast) to a destination (IP phones), every Layer 3 interface in between must have PIM configured. If the switches on the network are also providing Layer 3, then PIM must be enabled on the VLANs configured on those switches providing Layer 3 functionality. PIM is deployed in either sparse or dense mode, and InformaCast will work with either.

The following graphic shows PIM enabled on all Layer 3 interfaces between the IP phones/speakers and InformaCast.



The following graphic shows an interface before PIM is properly configured and that same interface after applying PIM.



If PIM isn't configured properly, work with your network administrator to configure PIM appropriately.

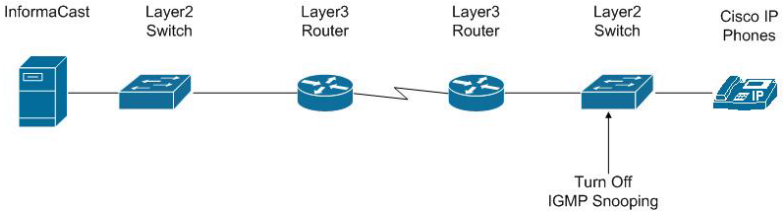
Verify your MPLS Provider Routes Multicast

When InformaCast audio broadcasts are successful at the same location where InformaCast is located, but remote locations do not receive the audio, that indicates that the multicast audio traffic is not routing across the WAN link. Many Multiprotocol Label Switching (MPLS) network providers will not route multicast traffic on their networks; check with your circuit provider to see if they do/will route your multicast.

For WAN links where your circuit provider will not route your multicast, you can use GRE tunnels, which carry your multicast traffic from the location where InformaCast is located to its recipients. The only traffic that needs to traverse these GRE tunnels is the multicast traffic you might want to route. The tunnels do not need to create a full mesh between sites; they only need to be configured from the hub location to the spoke location(s). Please see the following link for details: http://www.cisco.com/en/US/tech/tk828/technologies_configuration_example09186a00801a5aa2.shtml

Test Whether IGMP Snooping is Interrupting Multicast

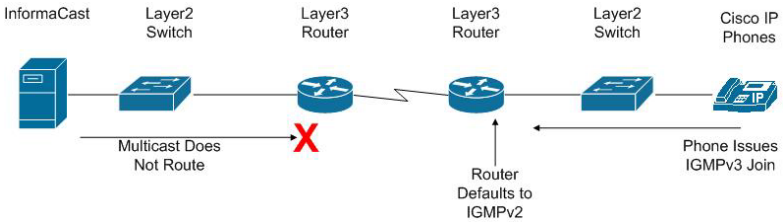
IGMP snooping has been seen to cause issues with Layer 2 switches. For this reason, if there are issues receiving the multicast audio stream at the phones, it would be worth testing if turning off IGMP snooping on the switches where phones are connected solves the problem. The following graphic illustrates where IGMP snooping should be turned off on the network.



Work with your network administrator to test if IGMP snooping is causing multicast to not function properly.

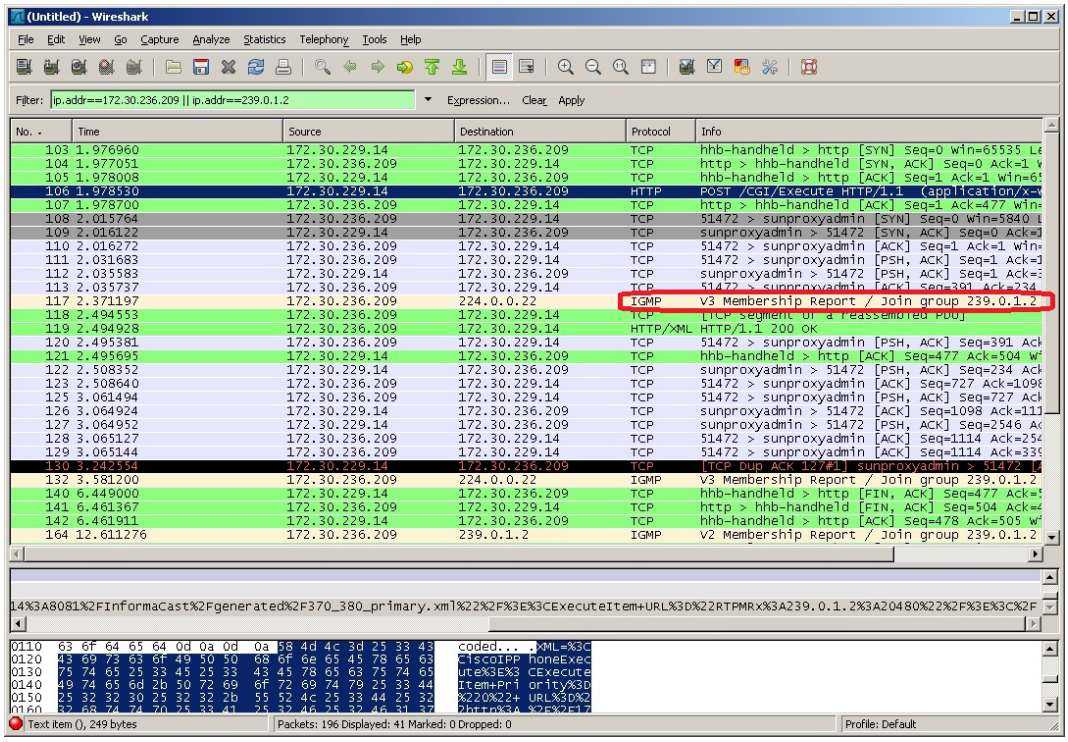
Ensure IGMPv3 is Enabled for Newer Phone Models

Newer phone models are using IGMPv3 where earlier phone models used IGMPv2. This is important because by default, IOS uses IGMPv2. If your network segment has a combination of older phones and newer phones, you may not perceive any issues. However, if a broadcast is sent only to devices using IGMPv3 on a network segment and the network has not been programmed for IGMPv3, the end result will be that multicast does not route to that network segment. The following graphic illustrates how the differences between IGMPv3 and IGMPv2 can affect your multicast traffic.

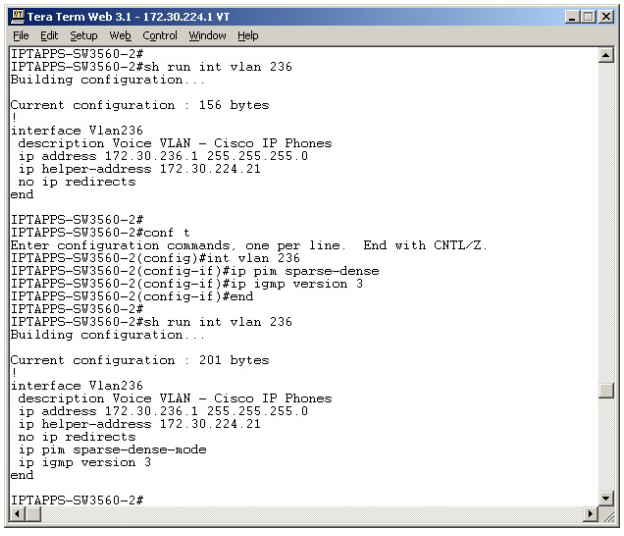


To verify if your phone(s) are using IGMPv3, you can take a network traffic capture using a protocol analyzer like Wireshark (see "Verify Multicast with a Network Traffic Capture" on page 2-70). In the capture, the phone will issue an IGMP join to listen to the multicast audio.

The version of the IGMP join can be seen on the packet (circled in red in the following graphic).



To ensure multicast audio will route to network segments where the phones are using IGMPv3, the Layer 3 device must be programmed for IGMPv3. The following graphic shows an interface before and after configuring IGMPv3.



Work with your network administrator to test if enabling IGMPv3 solves your multicast issues.

CHAPTER 3

Access InformaCast

Note Before proceeding with configuring InformaCast, you must have properly configured your environment for multicast (see "Prepare Your Multicast Environment" on page 2-1) and successfully installed InformaCast Virtual Appliance (see "Install InformaCast Virtual Appliance" on page 2-6). Do not continue with configuring InformaCast until you have completed these steps.

InformaCast's web interface—where you will set up your InformaCast environment, e.g. recipient groups, SIP functionality, DialCasts, etc.—is accessed through the Singlewire Start page. When first accessing InformaCast, you will want to:

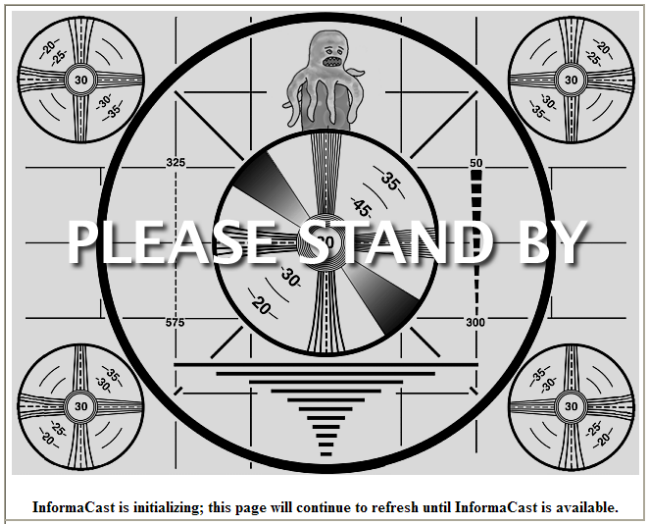
- "Log into InformaCast for the First Time" on page 3-2
- "Change the Administrator's Password" on page 3-6
- "View Your License Key" on page 3-7

Log into InformaCast for the First Time

Once the Virtual Appliance is started and you've accessed the Singlewire Start page, you can log into InformaCast.

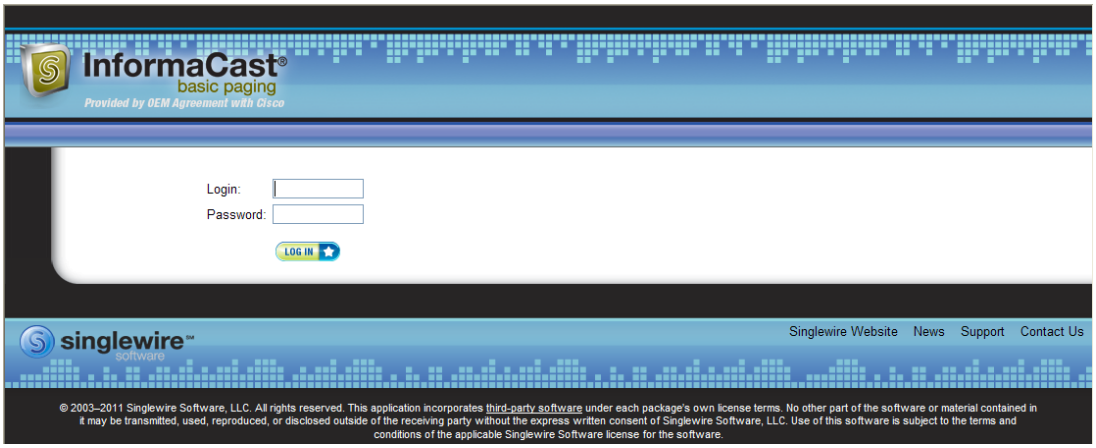
Step 1 Open a web browser, enter the IP address of the InformaCast Virtual Appliance, and press the **Enter** key. The Singlewire Start page appears.

Step 2 Click the **InformaCast** link. A separate tab/window opens to InformaCast's Startup page. Depending on your system, there may be a delay of several minutes while InformaCast initializes.



Note If you are using Internet Explorer to access InformaCast, you will receive an error, "There is a problem with this website's security certificate." Since InformaCast, like CUCM, is a locally-installed server rather than a global, public Internet site, there is no practical way for web browsers to recognize its encryption certificate as safe. To permanently bypass this error, install the self-signed SSL certificate present on InformaCast. See the question on page 8-1 for details on installing this certificate.

Once InformaCast initializes, you will be presented with InformaCast's Login page.

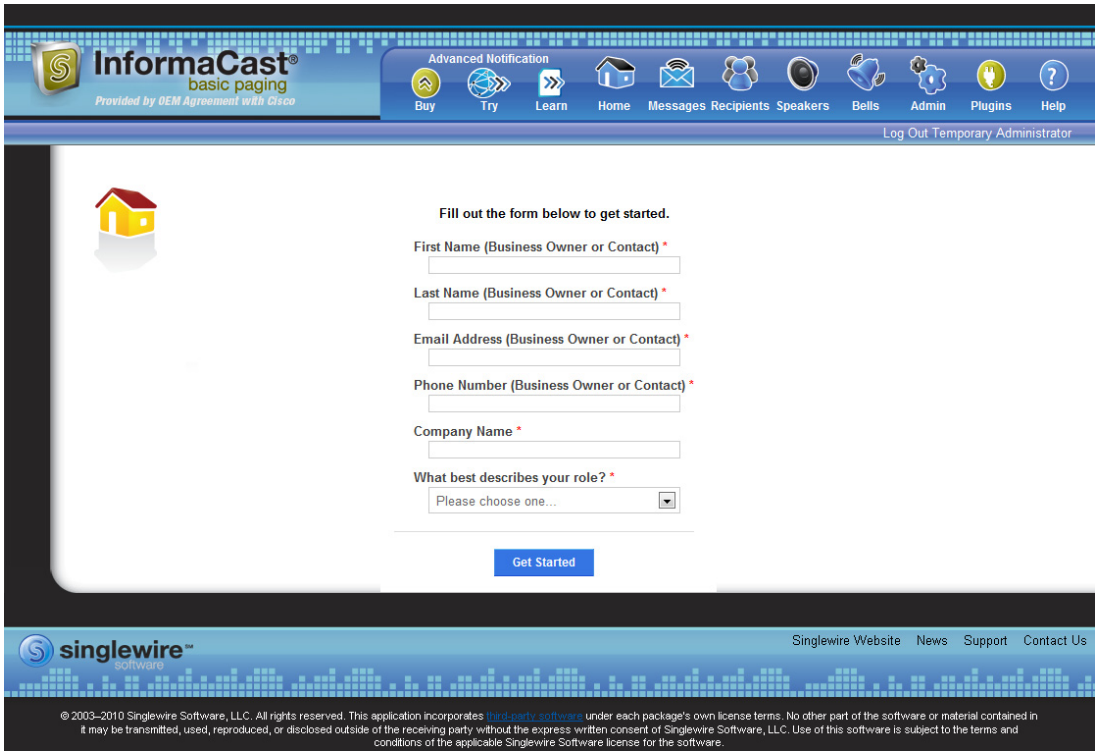


Step 3 Enter **admin** in the **Login** field. The **Login** field is case sensitive.

Step 4 Enter **changeMe** in the **Password** field. The **Password** field is also case sensitive.

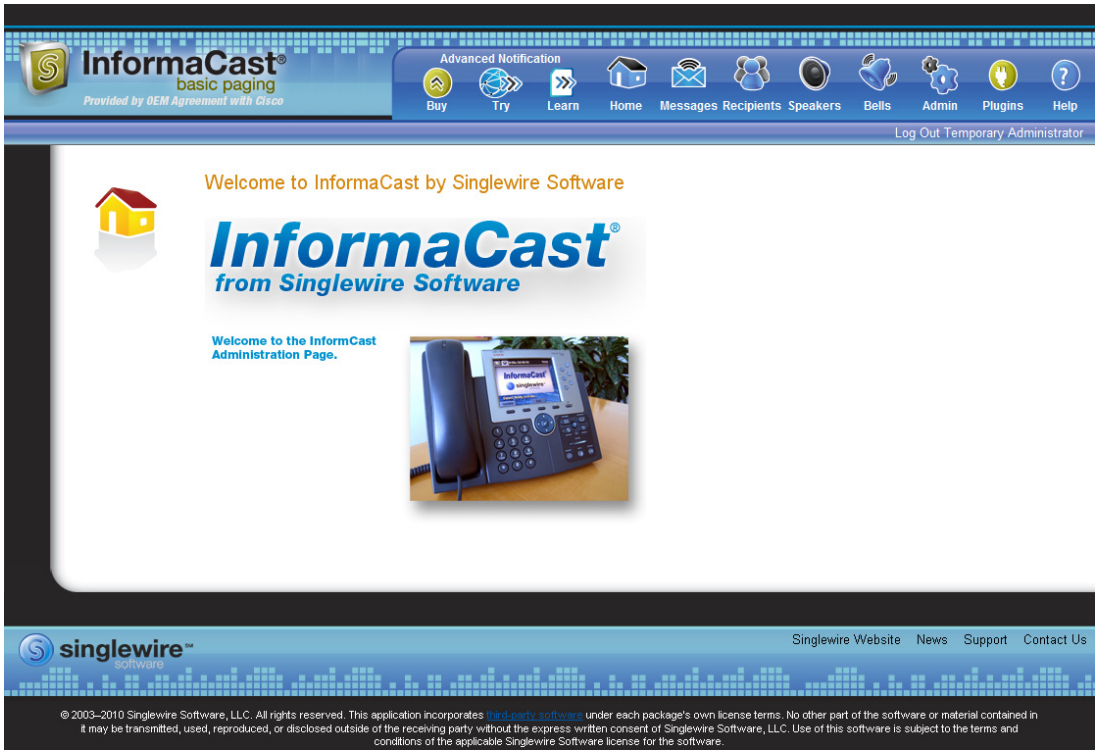
Note These are your default credentials. "Change the Administrator's Password" on page 3-6 will show you how to change your credentials, which will make your InformaCast installation more secure.

Step 5 Click the **Log In** button. If the machine on which InformaCast is installed has Internet access, the Getting Started Form page appears. Continue with Step 6 on page 3-6.

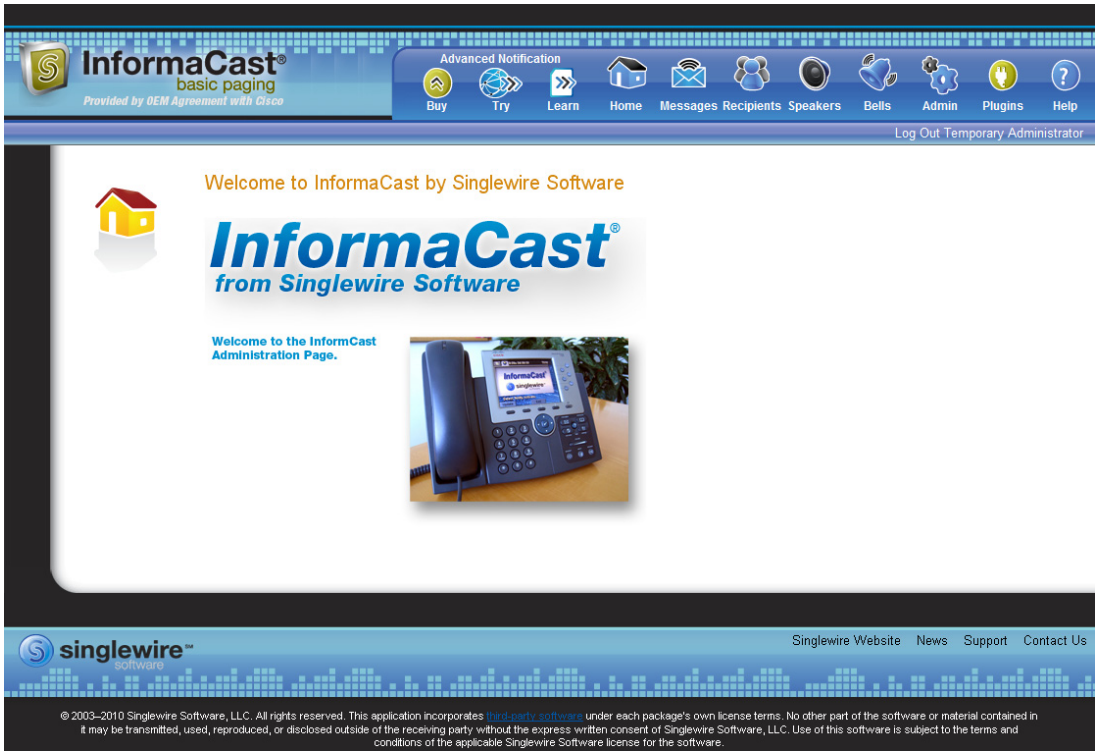


Note Completing this form is required in order to access InformaCast's functionality.

If the machine on which InformaCast is installed does not have Internet access, you will see InformaCast's homepage. Skip the rest of this section and continue with "Change the Administrator's Password" on page 3-6.



Step 6 Fill out the form and click the **Get Started** button. The InformaCast homepage appears.

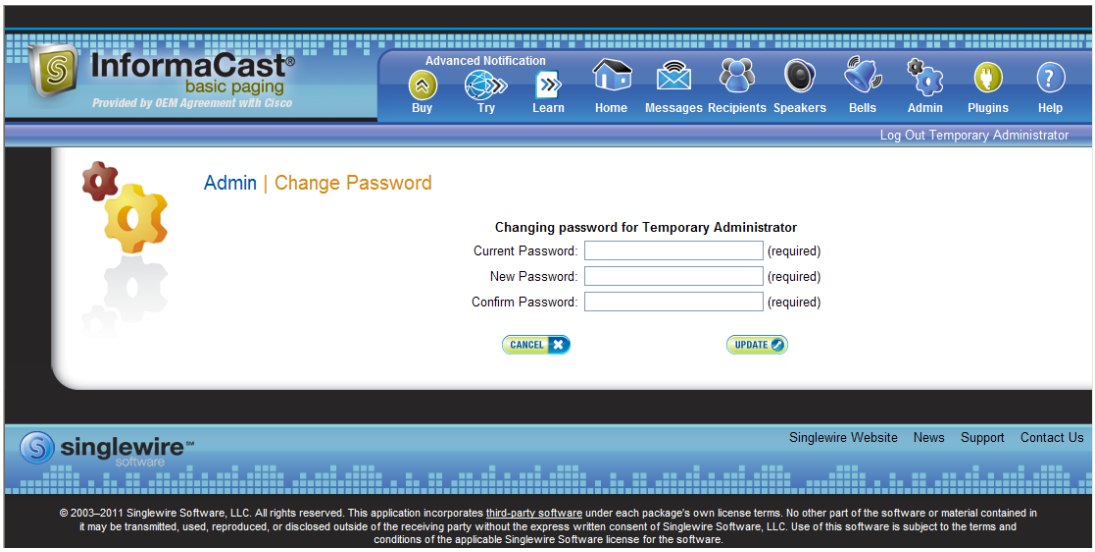


Change the Administrator's Password

InformaCast ships with a default administrative user, *admin*, so that you can log in and configure the system. In this section, you will change it so that other people familiar with InformaCast won't have complete access to your configuration.

Warning **If you change your password in Basic InformaCast, upgrade to Advanced InformaCast, then downgrade to Basic InformaCast, your password will revert to your original Basic InformaCast password.**

Step 1 Go to **Admin** | **Change Password**. The Change Password page appears.



Step 2 Enter the current password in the **Current Password** field.

Step 3 Enter your new password in the **New Password** and **Confirm Password** fields. Choose a password that you will be able to remember (or record it in a secure location).

Step 4 Click the **Update** button.

Note If the passwords you entered in the **New Password** and **Confirm Password** fields do not match or if you entered the wrong password, you will be prompted to try again.

You have now established a new password that you will use (along with the admin username) to log into InformaCast.

View Your License Key

Your InformaCast license key (**Admin** | **Manage License Key**) contains your designated functionality for InformaCast (e.g. Basic vs. Advanced, the number of phones to which you can broadcast, trial vs. demonstration vs. subscription vs. perpetual, etc.). For a further discussion of how licensing works in InformaCast, see "Licensing Information" on page 1-5.

Note Once you have exceeded the number of phones allowed by your license, you will receive a warning that you've attempted to broadcast to more phones than are allowed by your license key, causing some phones to be skipped. Consult the InformaCast Performance log (**Help** | **Support**) to see the phones that have been skipped and contact Singlewire about obtaining a larger license. You can also retry your

broadcast with a smaller group of phones. Your license limits you to 50 phones. If you want to broadcast to more than 50 phones (i.e. 100 phones), you can send out one broadcast to 50 phones and a second broadcast to the next 50 phones.

Configure Recipients

Messages sent by dialing a pre-configured number are called *DialCasts* or *broadcasts*. InformaCast's *messages* contain the building blocks of your broadcast: endpoints, audio, etc. Before endpoints can receive InformaCast's broadcasts, you must configure their communication with InformaCast and include them in *recipient groups*.

When working with InformaCast's recipients, you can:

- "Manage InformaCast's Telephony" on page 4-2
- "Manage Recipient Groups" on page 4-11
- "Manage Recipient Administration" on page 4-37

Manage InformaCast's Telephony

When you click the **Admin** icon, you will be brought to the Overview page. On this page, you can view various statistics associated with the configuration of InformaCast, such as how long the current session of InformaCast has been running, your version of InformaCast, and the configuration of your backups and phone updates.

Configure Your Default CUCM Cluster

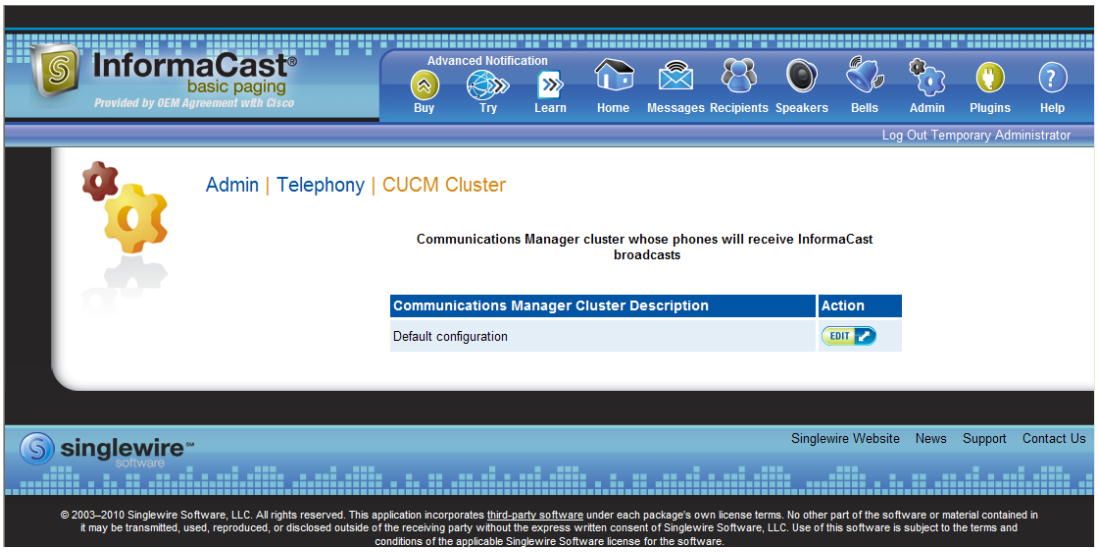
When configuring InformaCast:

- Basic installations are limited to one cluster; however, Advanced installations can be run with multiple clusters (contact Singlewire for details)
- Neither Cisco nor Singlewire supports combining both Basic and Advanced InformaCast instances

Follow these steps to set up the configuration of your default CUCM cluster. These steps should be performed by your CUCM administrator.

Warning **If you fail to configure CUCM in Basic InformaCast, upgrading to Advanced InformaCast and then configuring CUCM before downgrading to Basic InformaCast will require you to perform all the steps in this section again.**

Step 1 Go to **Admin** | **Telephony** | **CUCM Cluster**. The CUCM Cluster page appears.



Step 2 Click the **Edit** button next to Default configuration. The Edit Telephony Configuration page appears.

Step 3 Change name of your cluster (if necessary) in the **Communications Manager Cluster Description** field.

Step 4 Enter the username of the application user that you created earlier into the **Communications Manager Application User** field (see Step 3 on page 2-54).

Step 5 Enter the password of the application user that you created earlier into the **Communications Manager Application Password** and **Confirm Application Password** fields (see Step 4 on page 2-54). The password is entered twice to double-check for typing errors since its value is masked.

Step 6 Decide if you will use your application user or AXL user's credentials.

Tip Using your AXL credentials means that potentially more people have administrative access to CUCM, which may pose a security risk. To close this potential security hole, your CUCM Administrator should grant AXL API access to the application user and tell your InformaCast administrator what the credentials are. The InformaCast administrator then only knows the application user credentials and does not have administrative access to CUCM.

Note Different fields will appear on this page depending on whether the **Use Application User for AXL** checkbox is selected.

For application user credentials, select the **Use Application User for AXL** checkbox and skip to Step 7 on page 4-5.

For AXL credentials:

Step a. Enter the CUCM administrator's username in the **Communications Manager AXL User** field.

Note This is the same username you use to access the CUCM Administrator interface, often **CCMAdministrator**.

The username and password of the administrative login to the CUCM server are required for gathering phone information to enable broadcast messages.

Step b. Enter the CUCM administrator's password in the **Communications Manager AXL Password** and **Confirm AXL Password** fields. The password is entered twice to double-check for typing errors since its value is masked.

Note This is the same password you use to access the CUCM Administrator interface.

Step 7 Enter your AXL IP address(es) in the **AXL IP Address(es)** field. Separate addresses with commas. If you leave this field blank, InformaCast will attempt to find a server running the AXL service among those servers running the CallManager service.

Tip You can find which cluster members are running the AXL service by logging into your CUCM, selecting **Cisco Unified Serviceability** from the **Navigation** dropdown menu, and going to **Tools** | **Service Activation**. Scroll down the Service Activation page to see whether the **Cisco AXL Web Service** checkbox is selected.

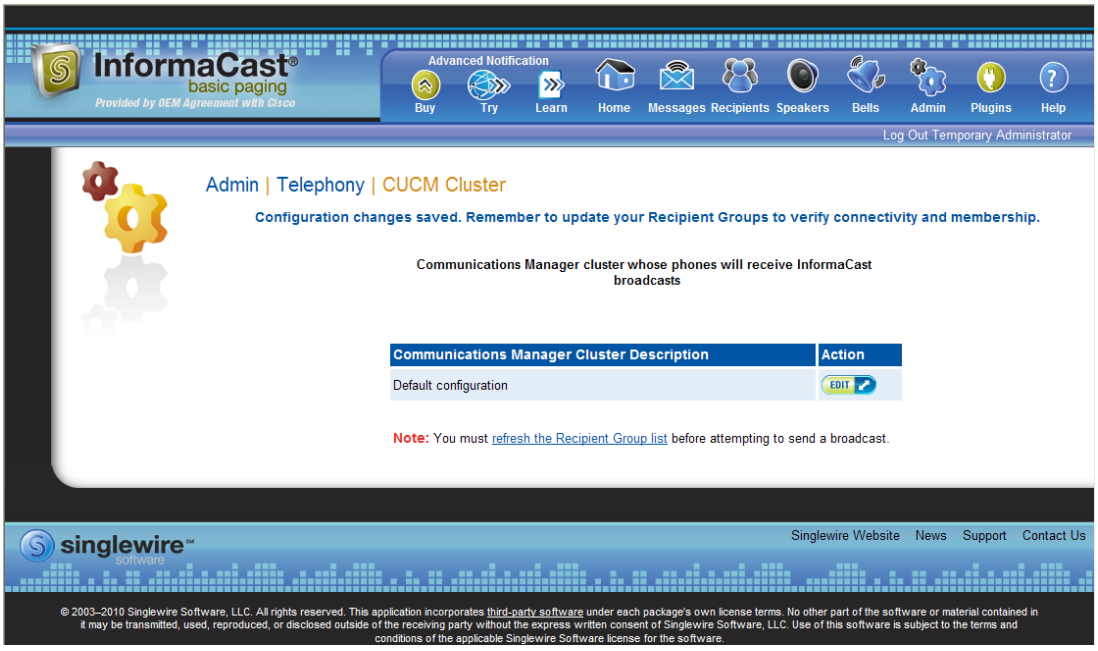
Step 8 Enter the IP address of the CUCM server(s) in the **Communications Manager IP Address(es)** field, which will be used when establishing a CTI (JTAPI) connection with CUCM. You can enter any and all CUCMs running the CTI Manager service. Use the numeric IP addresses rather than DNS names.

When InformaCast needs to interact with the CUCM, it will use this address. If you have a cluster of servers for redundancy and failover, you can list all of their addresses, separated by commas. InformaCast will use the first one when it is available, and will automatically try the next ones if it cannot reach the primary server.

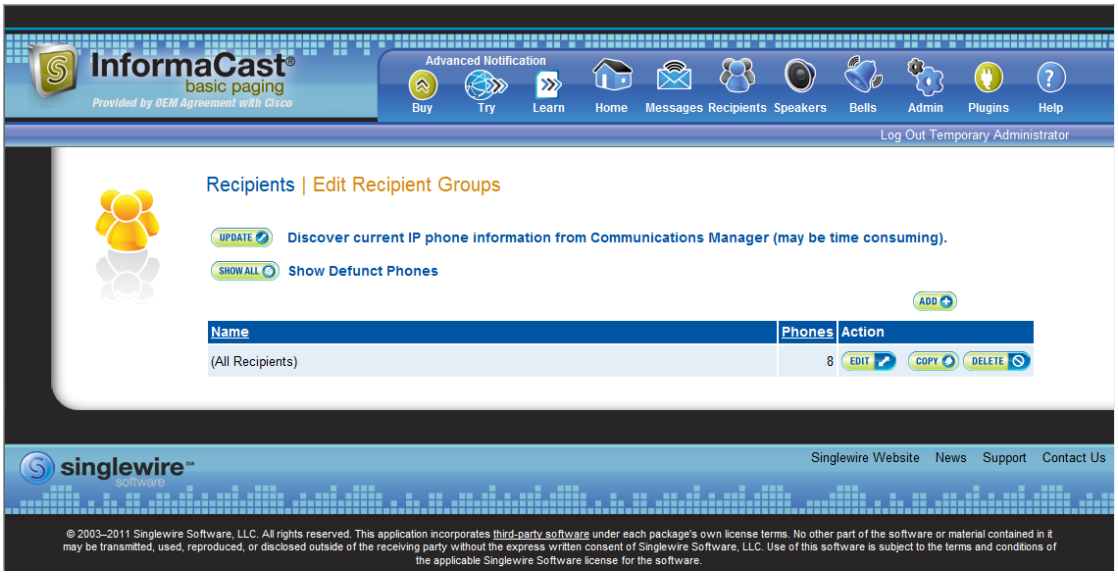
Step 9 Enter the appropriate name in the **SNMP Community Name** and **Confirm SNMP Community Name** fields. You made a note of this name when you configured your CUCM's SNMP in "Create an InformaCast SNMP Community String" on page 2-33. The community name is entered twice to double-check for typing errors since its value is masked.

Step 10 Enter the original value of CUCM's **URL Authentication** field in the **Next Authentication URL** field. You made note of this in Step 3 on page 2-65.

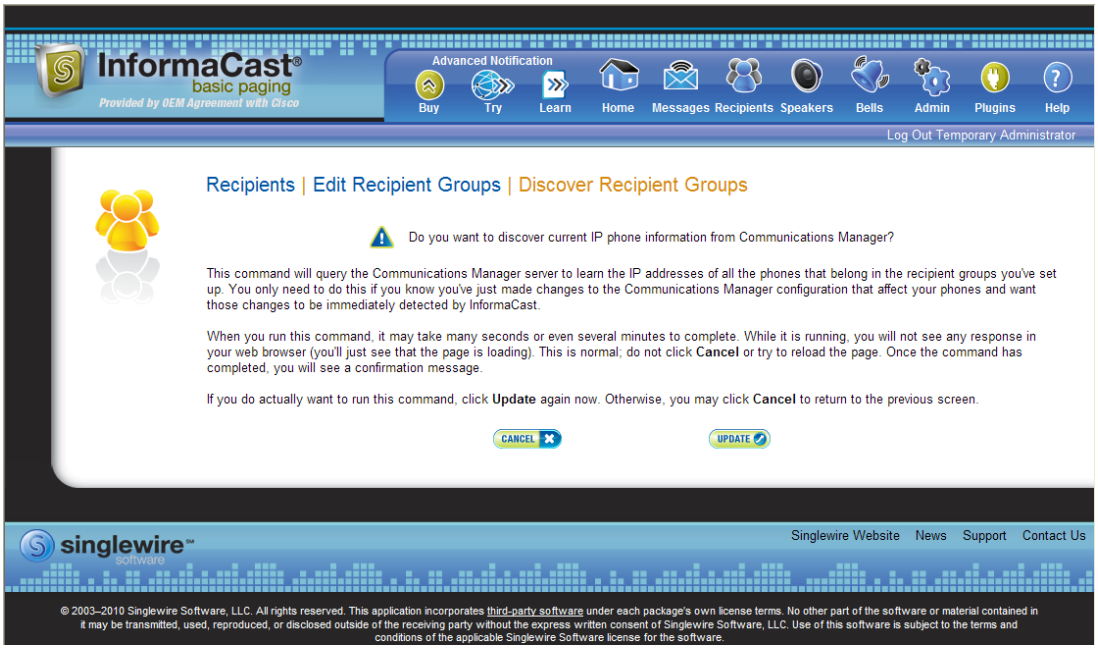
Step 11 Click the **Update** button. You will be redirected to the CUCM Cluster page.



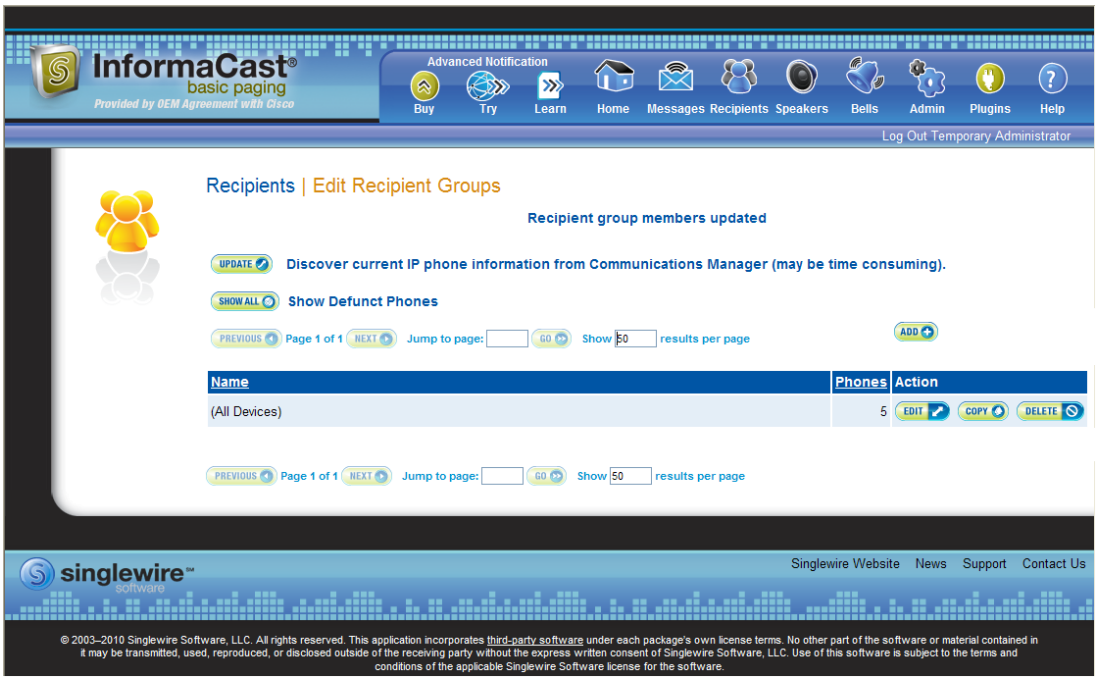
Step 12 Click the **refresh the Recipient Group list** link. You will be redirected to the Edit Recipient Groups page.



Step 13 Click the **Update** button to refresh InformaCast's information pertaining to recipient groups. You will be redirected to the Discover Recipient Groups page.



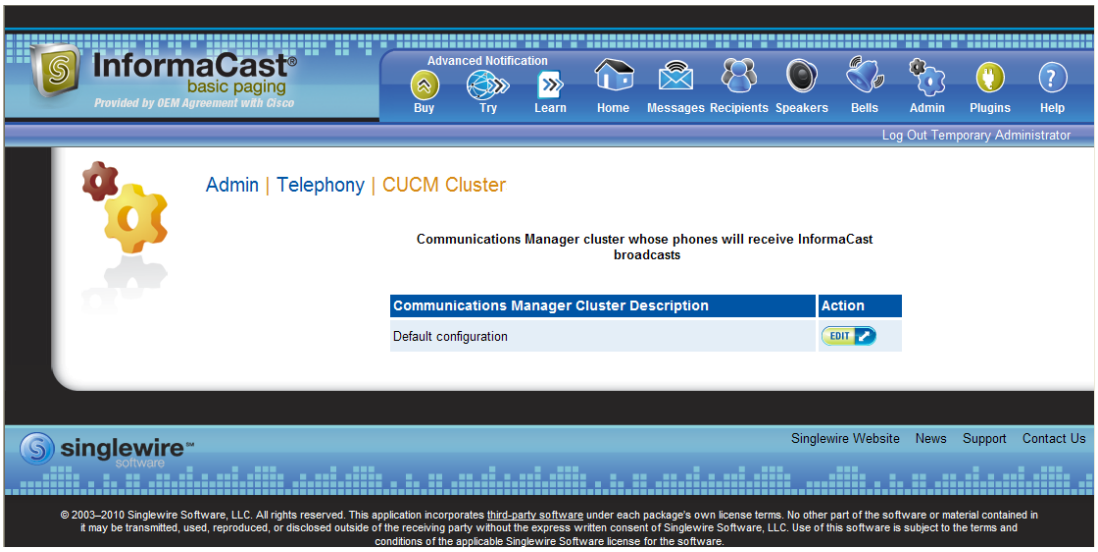
Step 14 Click the **Update** button again. You will be redirected to the Edit Recipient Groups page that will now have a note that recipient group members have been updated.



Edit Your Default Cluster

Once you've configured your default CUCM cluster in InformaCast, you may need to edit its information.

Step 1 Go to **Admin** | **Telephony** | **CUCM Cluster**. The CUCM Cluster page appears.



Step 2 Click the **Edit** button next to Default configuration. The Edit Telephony Configuration page for that cluster opens.

Step 3 Edit the information for that cluster.

Step 4 Click the **Update** button.

Note You will need to ensure your cluster's configuration matches that which you have set up in CUCM.

Manage Recipient Groups

If you'd like to be able to send messages to smaller groups of recipients (rather than all the recipients in your system), you must set up appropriate recipient groups within InformaCast. If you have a relatively small number of recipients, from a few to a few hundred, you can simply select the recipients you want included as members. If you have a large (or very dynamic) number of recipients, you can select multiple existing recipient groups and combine them into one larger group and/or construct matching rules that specify the members of a recipient group.

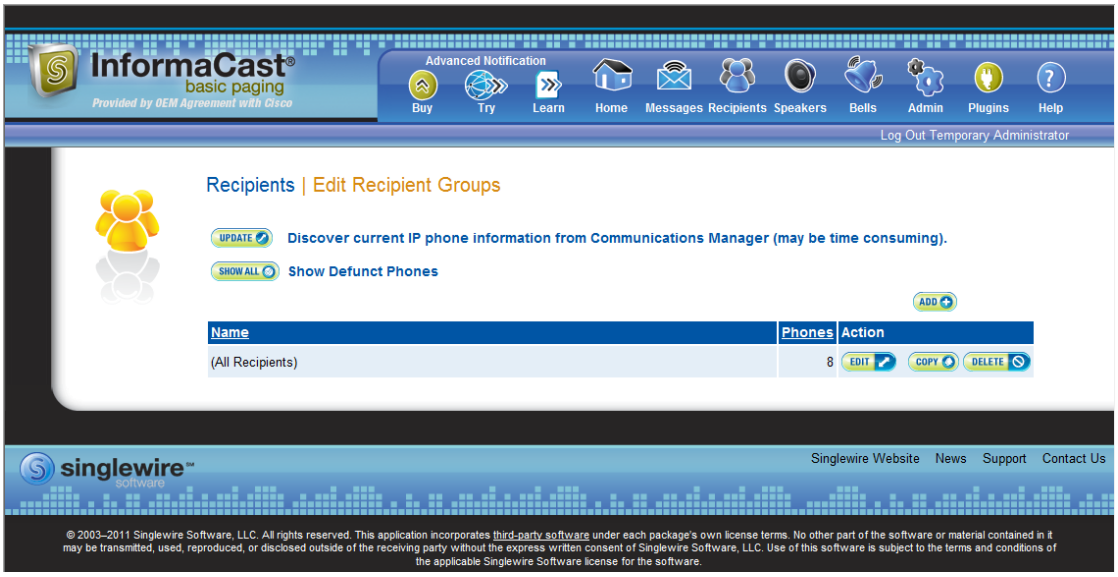
Once you've added recipients by selecting multiple existing recipient groups and/or constructing rules, you can also create exclusions, which allow recipients that had been included in a recipient group by a certain rule or through a recipient group to now be excluded.

Note By default, InformaCast initially creates an "(All Recipients)" group, which contains all the recipients that can be discovered.

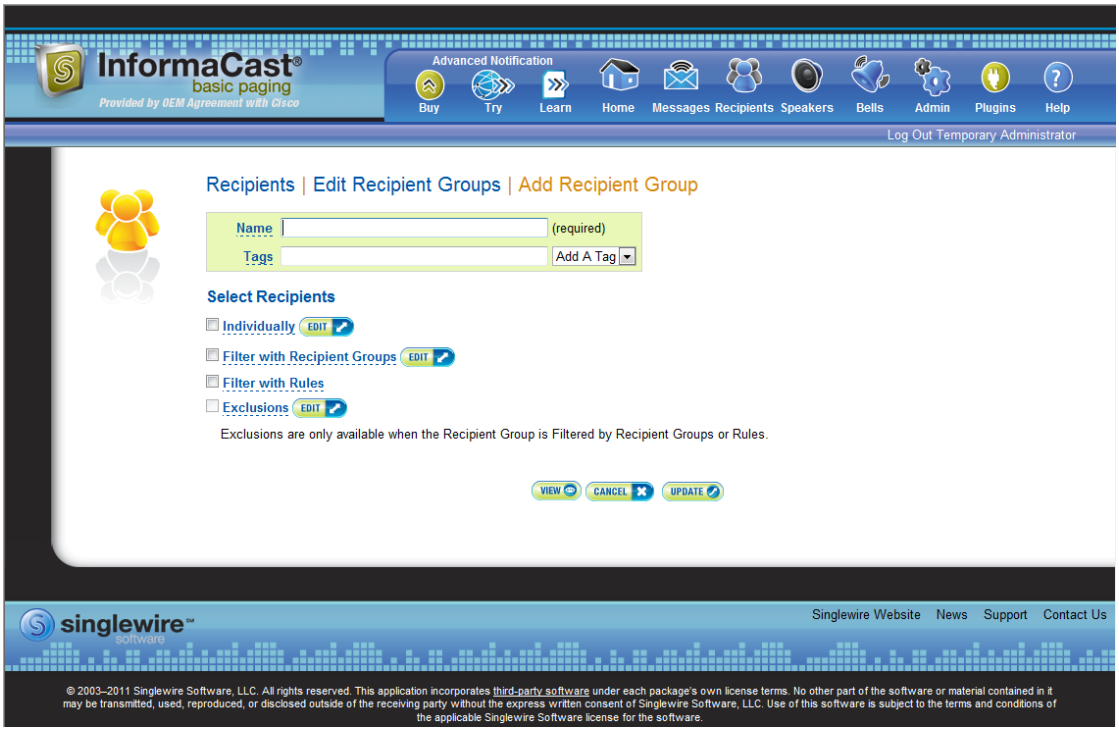
Add a Recipient Group

Use the following steps to add a recipient group.

Step 1 Go to **Recipients** | **Edit Recipient Groups**. The Edit Recipient Groups page appears. This page shows the number of phones for each group.



Step 2 Click the **Add** button. The Add Recipient Group page appears.



Step 3 Enter the name of your group in the **Name** field. This name is what users will select when configuring DialCast messages, so make it as self-explanatory as possible.

Step 4 Optionally, enter a name for a recipient group tag in the **Tags** field, which will create a new tag. Recipient group tags allow you finer control over the display results for recipient groups.

Note You can also create recipient group tags by going to **Recipients** | **Edit Tags** (see "Configure Recipient Group Tags" on page 4-34). Existing tags will appear in the **Add a Tag** dropdown menu on the Add Recipient Group page.

Decide whether you will add members to the group by selecting individual recipients, selecting existing recipient groups, or making rules:

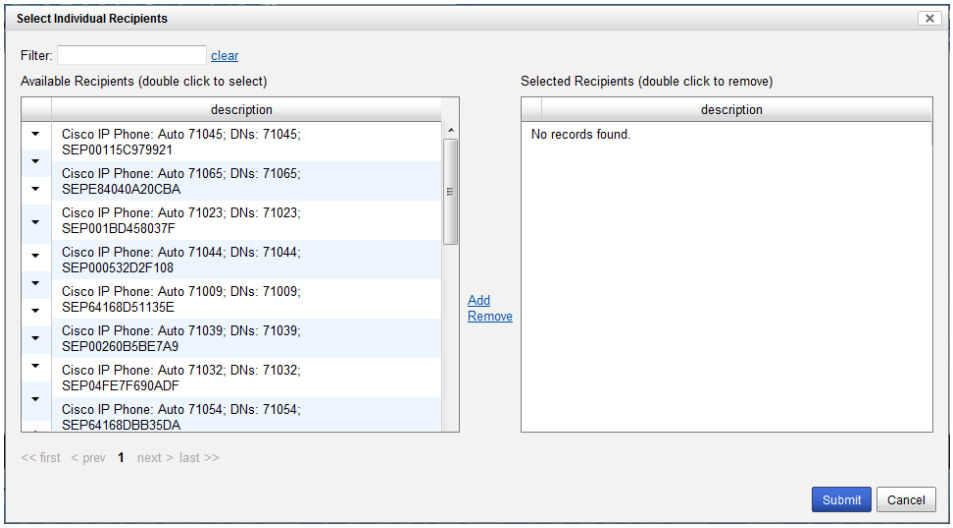
- If you have chosen to select recipients, continue with Step 2 in "Create a Recipient Group by Selecting Individual Recipients" on page 4-13.
- If you have chosen to select existing recipient groups, continue with Step 2 in "Create a Recipient Group by Selecting Multiple, Existing Recipient Groups" on page 4-15.
- If you have chosen to make rules, continue with Step 2 in "Create a Recipient Group Using Rules" on page 4-18.

Create a Recipient Group by Selecting Individual Recipients

Use these steps to add members to a recipient group by selecting the individual recipients to appear within it.

Step 1 Complete the steps in "Add a Recipient Group" on page 4-11.

Step 2 Select the **Individually** checkbox on the Add Recipient Group page and click its **Edit** button. The Select Individual Recipients pop-up window appears.



Tip Click the down arrow next to a recipient to see its parameters.

Step 3 Filter your list by entering text in the **Filter** field. This text will be matched to values of the following constraints, which can be held by your recipient:

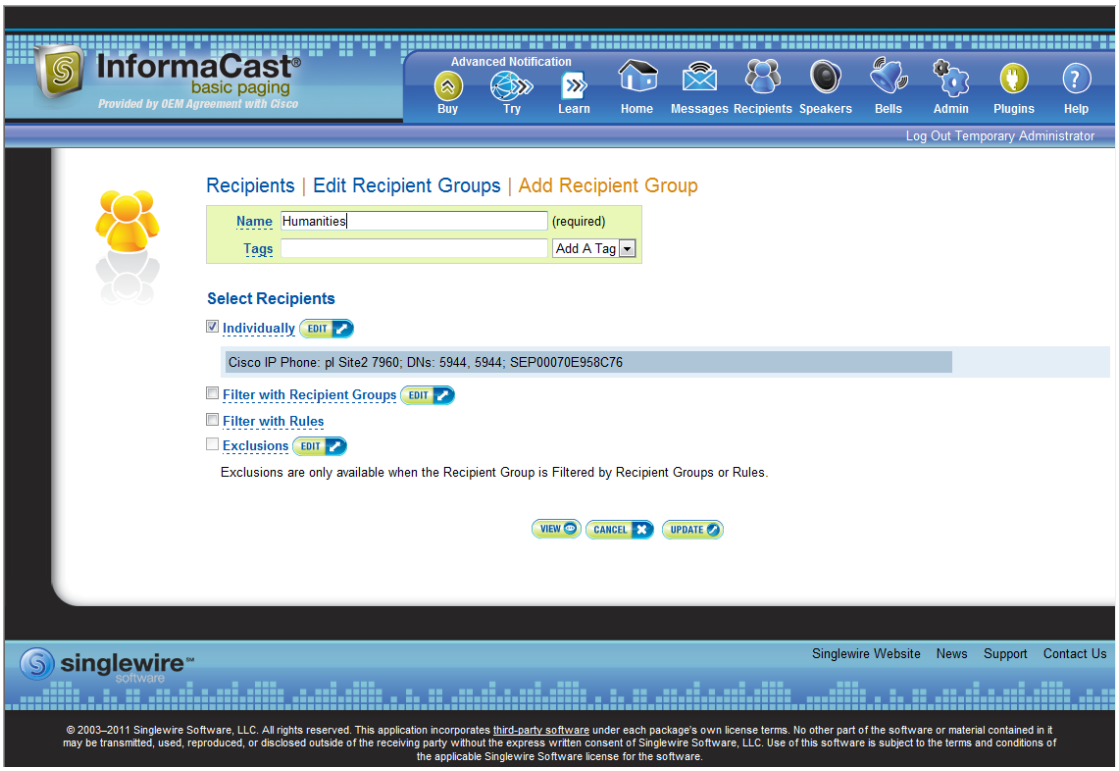
Matching Parameter	Description
Communications Manager Calling Search Space	Phones that match the specified search space.[a]
Communications Manager Cluster Name	Phones that match the specified CUCM cluster name.
Communications Manager Device Pool	Phones that match the specified pool.
Communications Manager Device Type	Phones that match the specified model, as reported by the CUCM.

Matching Parameter	Description
Description	Recipients that match the supplied description value. This is often a useful grouping tool because you have control over the description of the recipients in your system, so you can set up your descriptions in ways that facilitate grouping. The text you enter will be compared against the Device Description entries of phones registered with your CUCM. Any recipients whose descriptions match with the rule you've specified will be considered part of the recipient group.Any recipients whose descriptions match with the rule you've specified will be considered part of the recipient group.
Directory Numbers	Phones that match the supplied phone number(s) assigned to them in CUCM.
IP Address	Recipients that match the supplied subnet boundaries.
InformaCast Device Type	Recipients that match in their functionality as an IP phone.
Location	Recipients that match the supplied location value.
Name	Recipients that match the supplied name. Like the **Description** parameter, you have control over names, so they may useful for grouping, but should be concise.
Partition Names	Phones that match the supplied dial plan partition assigned to each directory number, a.k.a. phone number, assigned to an IP phone in CUCM.

a. Warning: If your site is using extension mobility, bear in mind that the calling search space, and even the directory number, assigned to a phone can change when a user logs in. Because of this, you should avoid using **Communications Manager Calling Search Space** as the criterion for setting up any recipient groups that are supposed to reflect geographic (rather than personnel) divisions. For such geographic divisions, **IP Address** is likely a better choice when extension mobility is a factor.

Step 4 Double-click the recipients you want to include in your group to move them from the *Available Recipients* area to the *Selected Recipients* area. You can also click on a recipient and click the **Add** link to move it from the *Available Recipients* area to the *Selected Recipients* area.

Step 5 Click the **Submit** button to save your selection(s). The Add Recipient Group page now shows the recipient(s) you selected.



Step 6 Click the **Update** button if you are done creating your recipient group. Your recipient group is added to InformaCast.

Tip At any point, you can click the **View** button to list the recipients included in your recipient group. Within the View Recipients pop-up window that appears, you can click the down arrow next to a recipient and view its details.

If you would like to further refine your recipient group, continue with "Create a Recipient Group by Selecting Multiple, Existing Recipient Groups" on page 4-15 and/or "Create a Recipient Group Using Rules" on page 4-18.

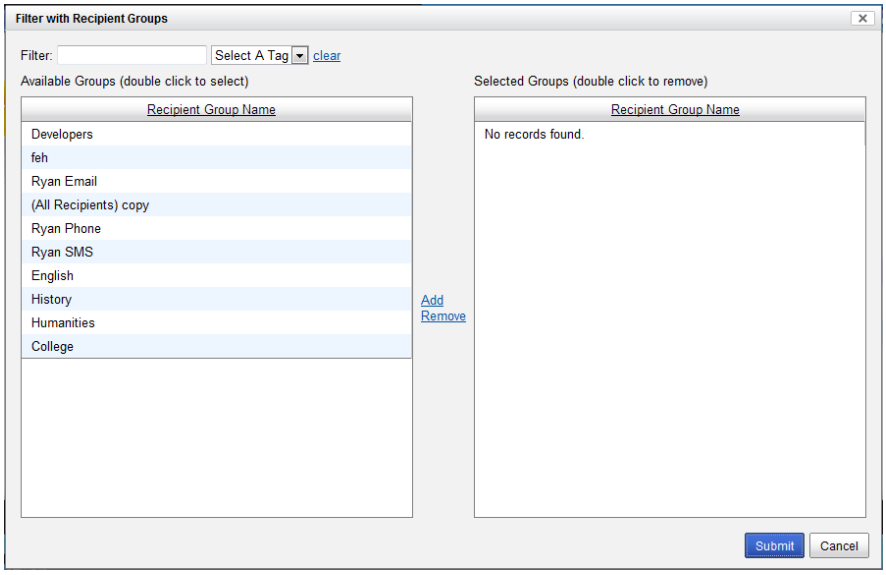
Create a Recipient Group by Selecting Multiple, Existing Recipient Groups

Use the following steps to create a recipient group that includes the members of existing recipient groups.

Note If you further refine your recipient group by using rules, the rules will also apply to the existing recipient groups you select in this section.

Step 1 Complete the steps in "Add a Recipient Group" on page 4-11.

Step 2 Select the **Filter with Recipient Groups** checkbox and click its **Edit** button. The Filter with Recipient Groups pop-up window appears.

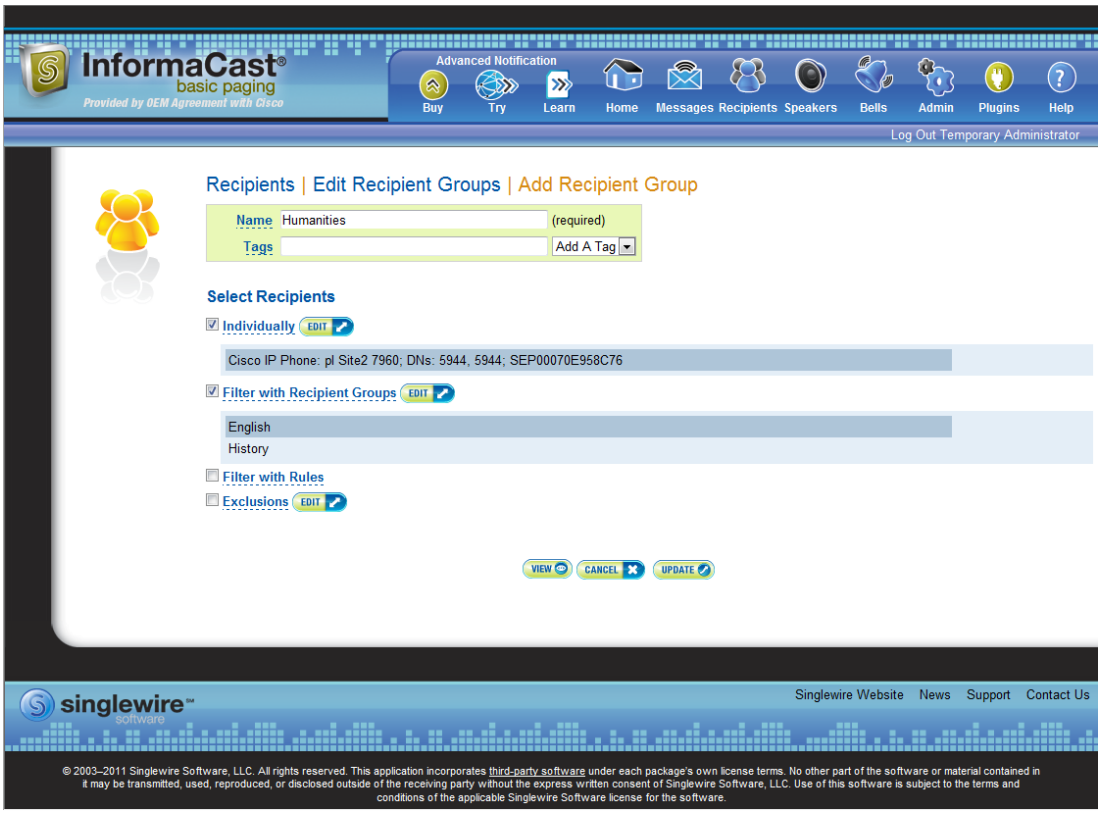


Step 3 Filter the results of your existing recipient groups by entering partial or full recipient group names in the **Filter** field or by selecting a particular recipient group tag from the **Select a Tag** dropdown menu.

Note The filter value is case-sensitive and applied to both the recipient group name and tag. If the recipient group tag matches the filter value, the recipient group will show up in the match list (e.g. a filter value of **AAA** will match tags aaa or AAA). Also, if the recipient group name contains the filter value, the recipient group will show up in the match list (e.g. a filter value of **phone** will match the names Phones, phone, PHONE, All phones, etc.).

Step 4 Double-click the existing recipient groups you want to include in your group to move them from the *Available Groups* area to the *Selected Groups* area. You can also click on a recipient group and click the **Add** link to move it from the *Available Groups* area to the *Selected Groups* area.

Step 5 Click the **Submit** button to save your selection(s). The Add Recipient Group page now shows the recipient(s) you selected.



Step 6 Click the **Update** button if you are done creating your recipient group. Your recipient group is added to InformaCast.

Tip At any point, you can click the **View** button to list the recipients included in your recipient group. Within the View Recipients pop-up window that appears, you can click the down arrow next to a recipient and view its details.

If you would like to further refine your recipient group, continue with "Create a Recipient Group by Selecting Individual Recipients" on page 4-13, "Create a Recipient Group Using Rules" on page 4-18, and/or "Add Exclusions to a Recipient Group" on page 4-21.

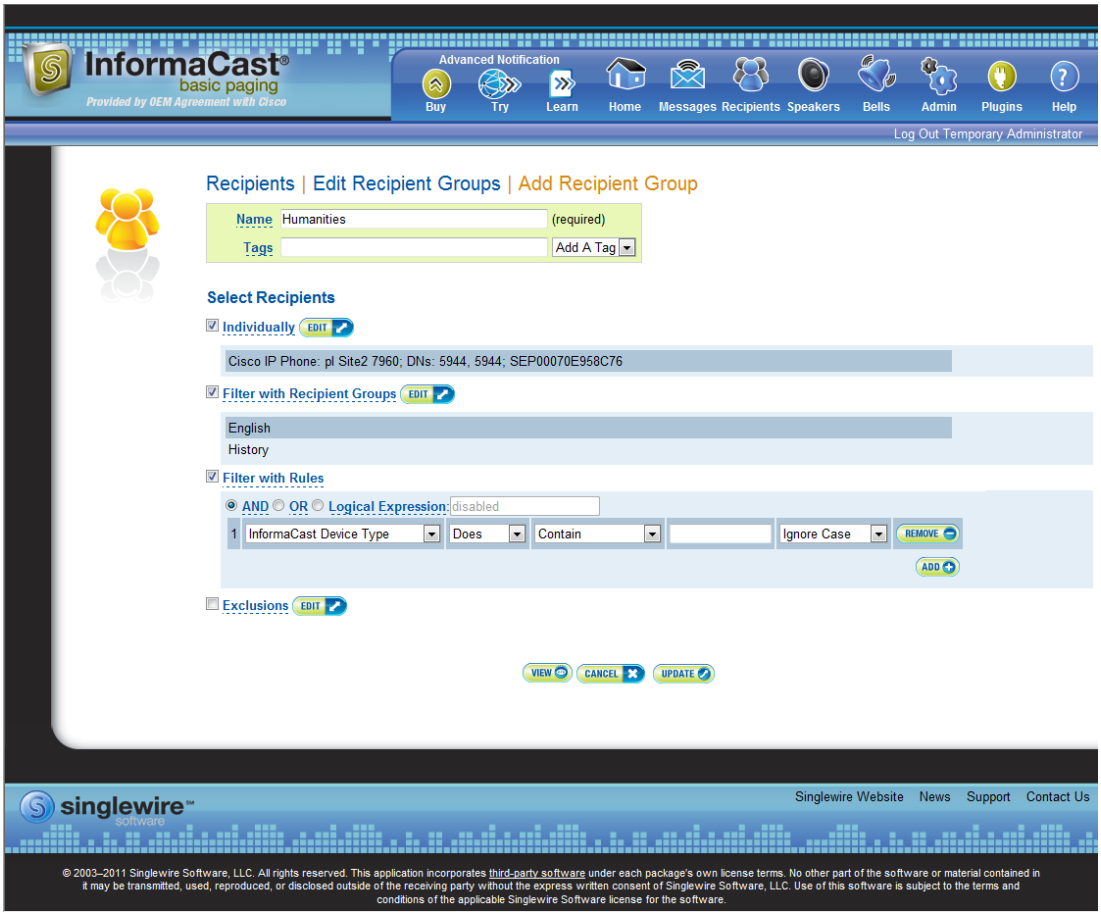
Create a Recipient Group Using Rules

Use the steps in the following section to add members to a recipient group by creating rules that the recipients must follow in order to be included. The rules can be general or extremely specific.

Note Rules added in this section will also affect recipients added through selecting existing recipient groups (as described in "Create a Recipient Group by Selecting Multiple, Existing Recipient Groups" on page 4-15).

Step 1 Complete the steps in "Add a Recipient Group" on page 4-11.

Step 2 Select the **Filter with Rules** checkbox. The Add Recipient Group page refreshes.



Tip Adjust your browser window so the rule elements all fit on a single line.

Note The **AND**, **OR**, and **Logical Expression** radio buttons control which rules will be applied to your recipients. **AND** means that your recipients have to match every rule you specify. **OR** means that your recipients must match at least one specified rule. **Logical Expression** means that your recipients must match a combination of specified rules based on the number in the first column of the Rules table and the words "and" and "or." For example, (1 or 2) and not (3 and 4 and not 5).

Step 3 Select a parameter from the first dropdown menu just underneath the Filter with Rules heading. (Initially, this dropdown menu has the selection **InformaCast Device Type**.) The parameters you can select are described in the following table:

Matching Parameter	Description
Communications Manager Calling Search Space	Phones that match (or don't match) the specified search space.[a]
Communications Manager Cluster Name	Phones that match (or don't match) the specified CUCM cluster name.
Communications Manager Device Pool	Phones that match (or don't match) the specified pool.
Communications Manager Device Type	Phones that match (or don't match) the specified model, as reported by the CUCM server.
Can Display Text	Recipients that match (or don't match) in their ability to display text.[b]
Description	Recipients that match (or don't match) the supplied description value. This is often a useful grouping tool because you have control over the description of the recipients in your system, so you can set up your descriptions in ways that facilitate grouping. The text you enter will be compared against the Device Description entries of phones registered with your CUCM server Any recipients whose descriptions match with the rule you've specified will be considered part of the recipient group.
Directory Numbers	Phones that match (or don't match) the supplied phone number(s) assigned to them in the CUCM server.[b]

Matching Parameter	Description
IP Address	Recipients that match (or don't match) the supplied subnet boundaries. When choosing this parameter, you are given a new Comparison Type choice, **Belong to Subnet**, which allows you to enter a subnet mask like 172.17.30.0/8. See "Configure Advanced Matching for Recipient Groups" on page 4-37 for more information about this approach.
InformaCast Device Type	Recipients that match (or don't match) in their functionality as an IP phone.
Location	Recipients that match (or don't match) the supplied location value.
MAC Address	Recipients that match (or don't match) the supplied network hardware address of the recipient, which is guaranteed to be unique across your network.
Name	Recipients that match (or don't match) the supplied name. Like the **Description** parameter, you have control over names, so they may useful for grouping, but should be concise.
Partition Names	Phones that match (or don't match) the supplied dial plan partition assigned to each directory number, a.k.a. phone number, assigned to an IP phone in CUCM.
Profile Description	Phones that match (or don't match) the CUCM's user device profile description. Phones that are using extension mobility or a profile when logged out are eligible to be filtered in this way.

a. Warning: If your site is using extension mobility, bear in mind that the calling search space, and even the directory number, assigned to a phone can change when a user logs in. Because of this, you should avoid using **Communications Manager Calling Search Space** as the criterion for setting up any recipient groups that are supposed to reflect geographic (rather than personnel) divisions. For such geographic divisions, **IP Address** is likely a better choice when extension mobility is a factor.

b. The recipient must be currently registered for this parameter to match. InformaCast has no information about the detailed features of unregistered recipients.

Step 4 Select **Does** or **Does Not** from the second dropdown menu.

Step 5 Select the matching constraint from the third dropdown menu, which has context-sensitive choices. For example, if you select **IP Address** as the rule parameter to match, a choice of **Belong to Subnet** will appear as a matching relationship choice; this choice is not available for other matching parameters.

Note If you select the **Match Expression** relationship, InformaCast expects a regular expression in the last field. See "Configure Advanced Matching for Recipient Groups" on page 4-37 for a description of regular expressions.

Step 6 Enter the criteria to be matched in the next field. (If you selected the **Equal** relationship, the criteria element may facilitate your selection by changing from a field to a dropdown menu.)

Step 7 Select **Ignore Case** or **Case Sensitive** from the last dropdown menu to further refine your recipients.

Step 8 Click the **Add** button to add your rule. Automatically, another rule line shows up.

Step 9 Decide if your rule is sufficient as it stands or follow Steps 3 through 8 to add another rule.

Tip If you want to remove a rule, click the **Remove** button to the right of the rule's definition.

Step 10 Click the **Update** button if you are done creating your recipient group. Your recipient group is added to InformaCast.

Tip At any point, you can click the **View** button to list the recipients included in your recipient group. Within the View Recipients pop-up window that appears, you can click the down arrow next to a recipient and view its details.

If you would like to further refine your recipient group, continue with "Create a Recipient Group by Selecting Individual Recipients" on page 4-13, "Create a Recipient Group by Selecting Multiple, Existing Recipient Groups" on page 4-15, and/or "Add Exclusions to a Recipient Group" on page 4-21.

Add Exclusions to a Recipient Group

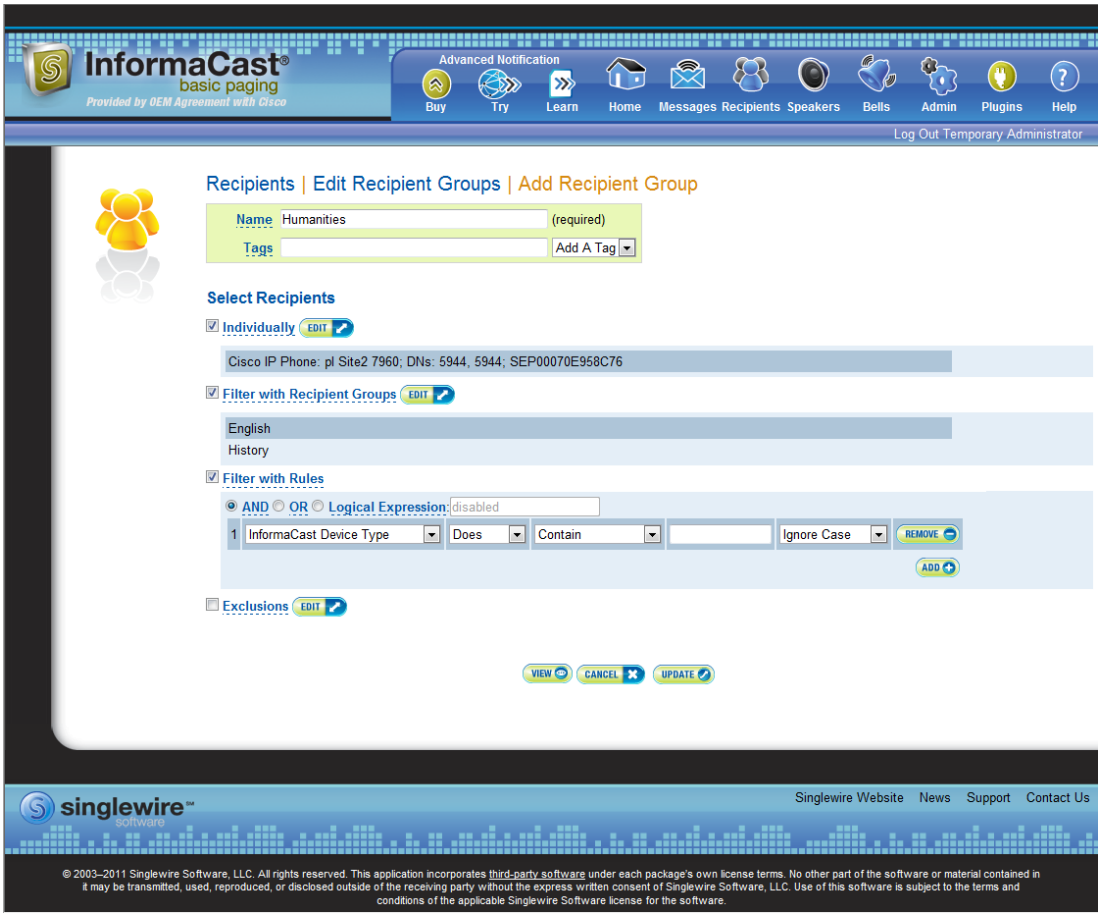
Use the steps in the following section to add exclusions to a recipient group, which allow recipients that had been included in a recipient group by a certain rule or through a recipient group to now be excluded.

Step 1 Complete the steps in "Add a Recipient Group" on page 4-11.

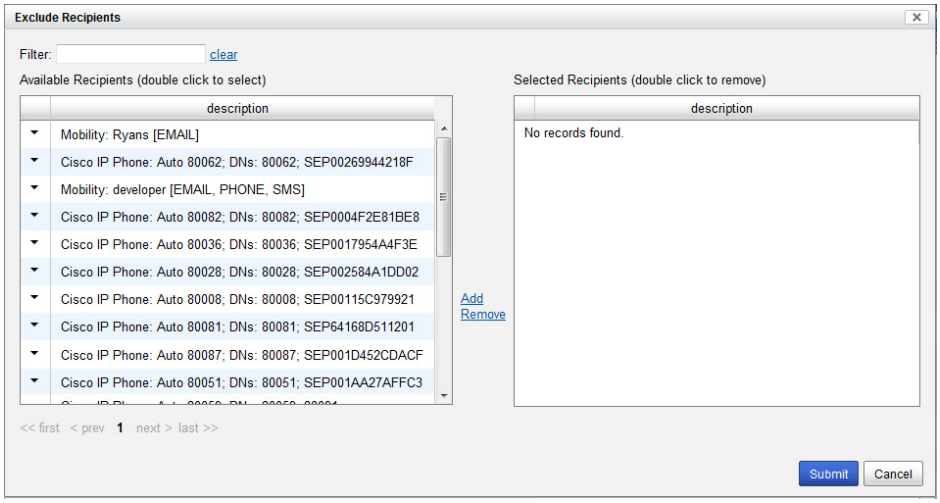
Step 2 Complete the steps in either "Create a Recipient Group by Selecting Multiple, Existing Recipient Groups" on page 4-15 or "Create a Recipient Group Using Rules" on page 4-18 (or both).

Note The Exclusions checkbox is only available if you select multiple existing recipient groups or create rules.

You'll be viewing the Add Recipient Group page.



Step 3 Select the **Exclusions** checkbox and click its **Edit** button. The Exclude Recipients pop-up window appears.



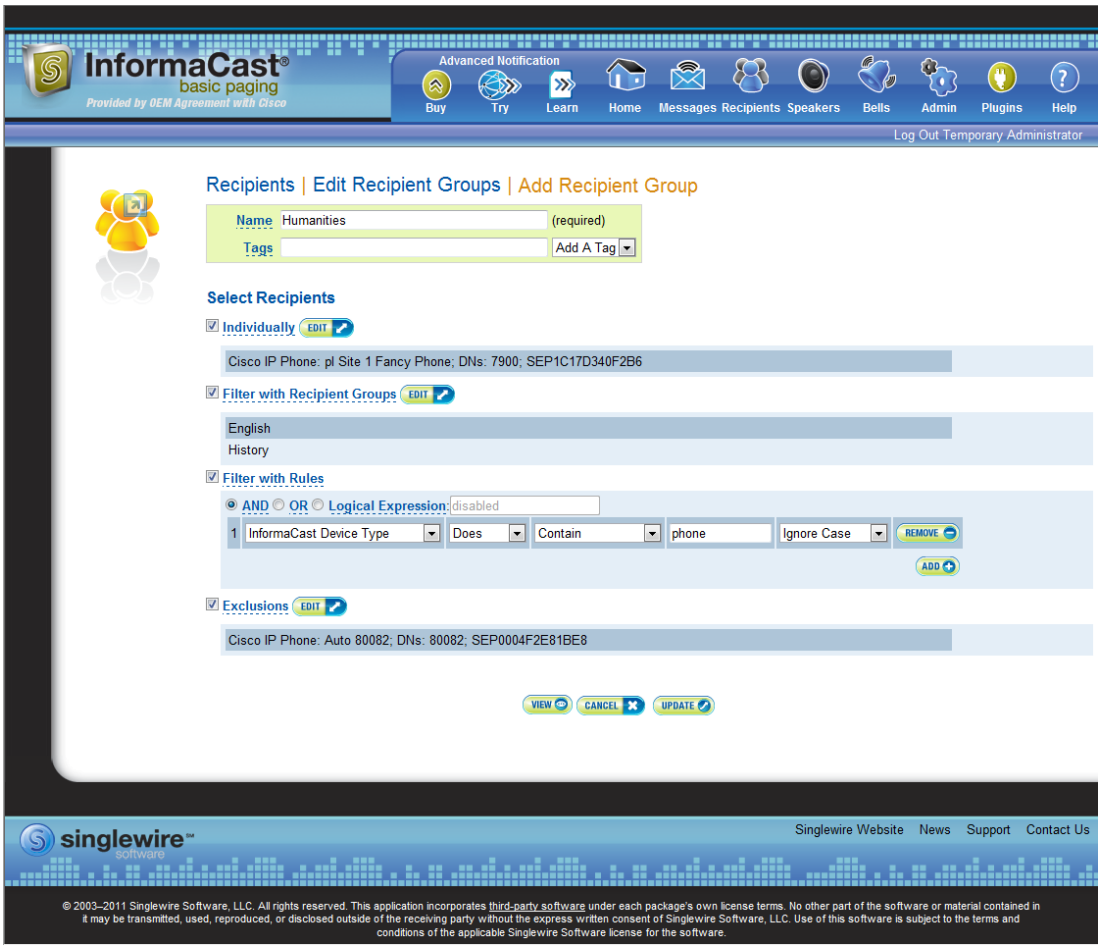
Step 4 Filter your list by entering text in the **Filter** field. This text will be matched to values of the following constraints, which can be held by your recipient:

Matching Parameter	Description
Communications Manager Calling Search Space	Phones that match the specified search space.[a]
Communications Manager Cluster Name	Phones that match the specified CUCM cluster name.
Communications Manager Device Pool	Phones that match the specified pool.
Communications Manager Device Type	Phones that match the specified model, as reported by the CUCM server.
Description	Recipients that match the supplied description value. This is often a useful grouping tool because you have control over the description of the recipients in your system, so you can set up your descriptions in ways that facilitate grouping. The text you enter will be compared against the Device Description entries of phones registered with your CUCM server
Directory Numbers	Phones that match the supplied phone number(s) assigned to them in the CUCM server.
IP Address	Recipients that match the supplied subnet boundaries.
InformaCast Device Type	Recipients that match in their functionality as an IP phone.
Location	Recipients that match the supplied location value.
Name	Recipients that match the supplied name. Like the **Description** parameter, you have control over names, so they may useful for grouping, but should be concise.
Partition Names	Phones that match the supplied dial plan partition assigned to each directory number, a.k.a. phone number, assigned to an IP phone in CUCM.

a. Warning: If your site is using extension mobility, bear in mind that the calling search space, and even the directory number, assigned to a phone can change when a user logs in. Because of this, you should avoid using **Communications Manager Calling Search Space** as the criterion for setting up any recipient groups that are supposed to reflect geographic (rather than personnel) divisions. For such geographic divisions, **IP Address** is likely a better choice when extension mobility is a factor.

Step 5 Double-click the recipients you want to exclude from your group to move them from the *Available Recipients* area to the *Selected Recipients* area. You can also click on a recipient and click the **Add** link to move it from the *Available Recipients* area to the *Selected Recipients* area.

Step 6 Click the **Submit** button to apply your selection(s). The Add Recipient Group page now shows the recipient(s) you selected.



Step 7 Click the **Update** button if you are done creating your recipient group. Your recipient group is added to InformaCast.

Tip At any point, you can click the **View** button to list the recipients included in your recipient group. Within the View Recipients pop-up window that appears, you can click the down arrow next to a recipient and view its details.

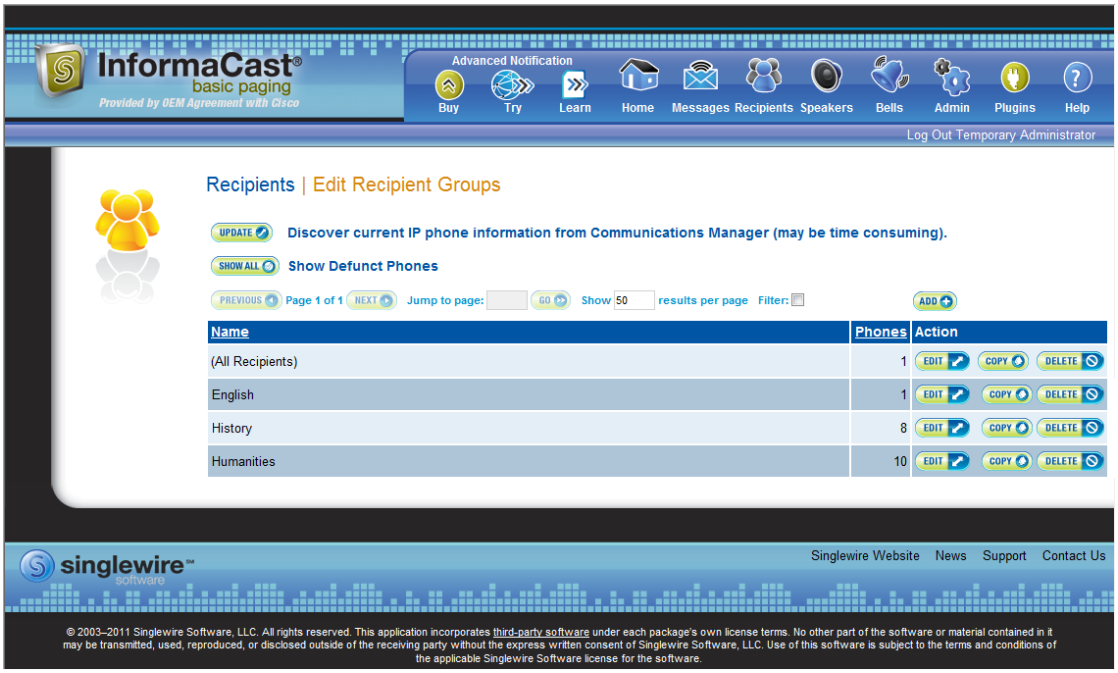
If you would like to further refine your recipient group, continue with "Create a Recipient Group by Selecting Individual Recipients" on page 4-13, "Create a Recipient Group by Selecting Multiple, Existing Recipient Groups" on page 4-15 and/or "Create a Recipient Group Using Rules" on page 4-18.

Edit a Recipient Group

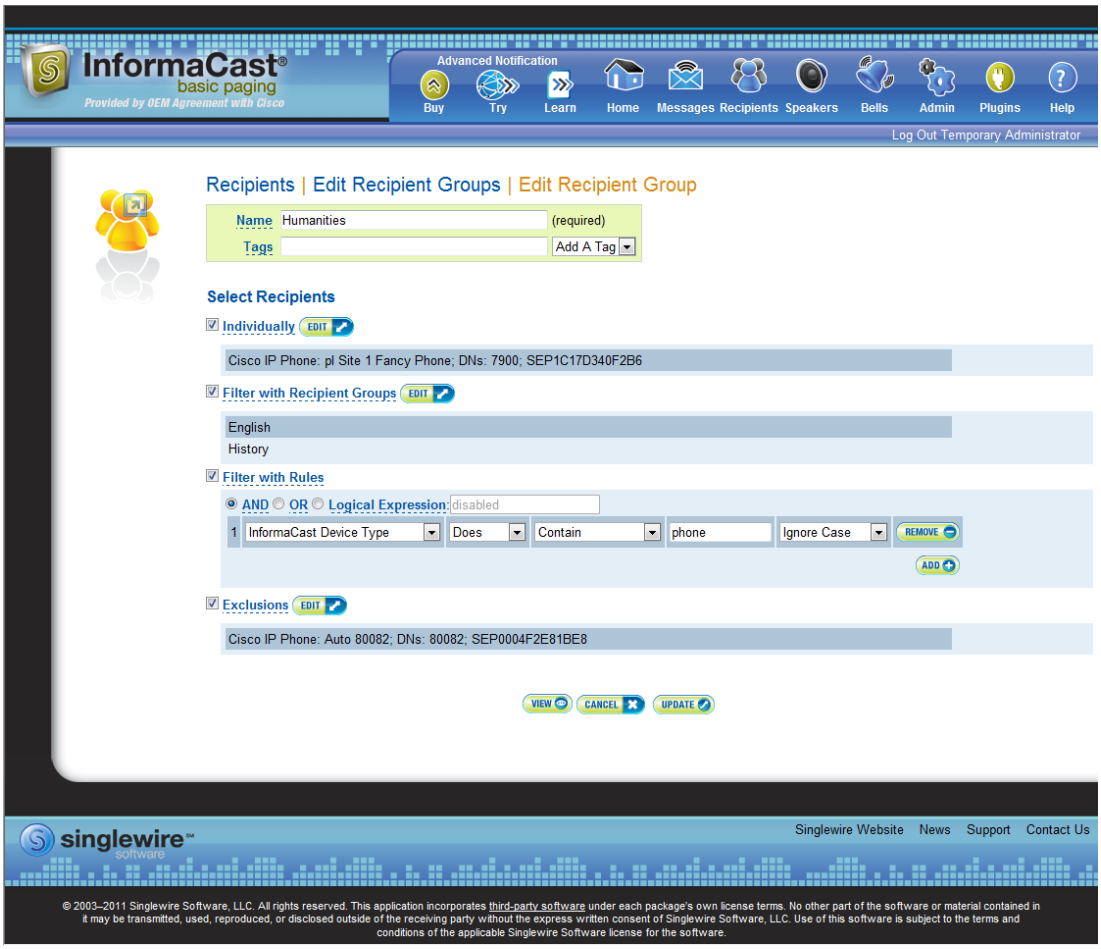
After you have added recipient groups to InformaCast, you may need to edit their information.

Tip If you upgraded from Basic to Advanced InformaCast, but then returned to Basic functionality and you're now seeing empty recipient groups and/or unsuccessful broadcasts, ensure that you have the most up-to-date recipients by clicking the **Update** button on the Edit Recipient Groups page.

Step 1 Go to **Recipients** | **Edit Recipient Groups**. The Edit Recipient Groups page appears.



Step 2 Click the **Edit** button next to the recipient group you'd like to edit. The Edit Recipient Group page appears.



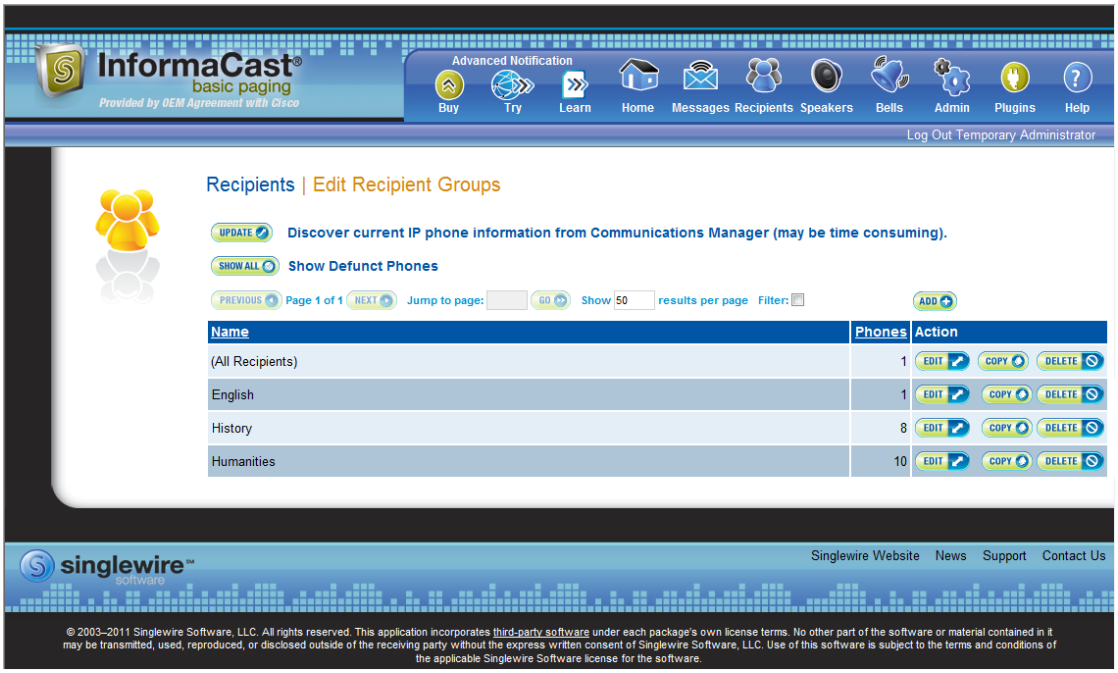
Step 3 Make your desired changes. See "Create a Recipient Group by Selecting Individual Recipients" on page 4-13, "Create a Recipient Group by Selecting Multiple, Existing Recipient Groups" on page 4-15, "Create a Recipient Group Using Rules" on page 4-18, or "Add Exclusions to a Recipient Group" on page 4-21 for more information on recipient group creation.

Step 4 Click the **Update** button when you are finished.

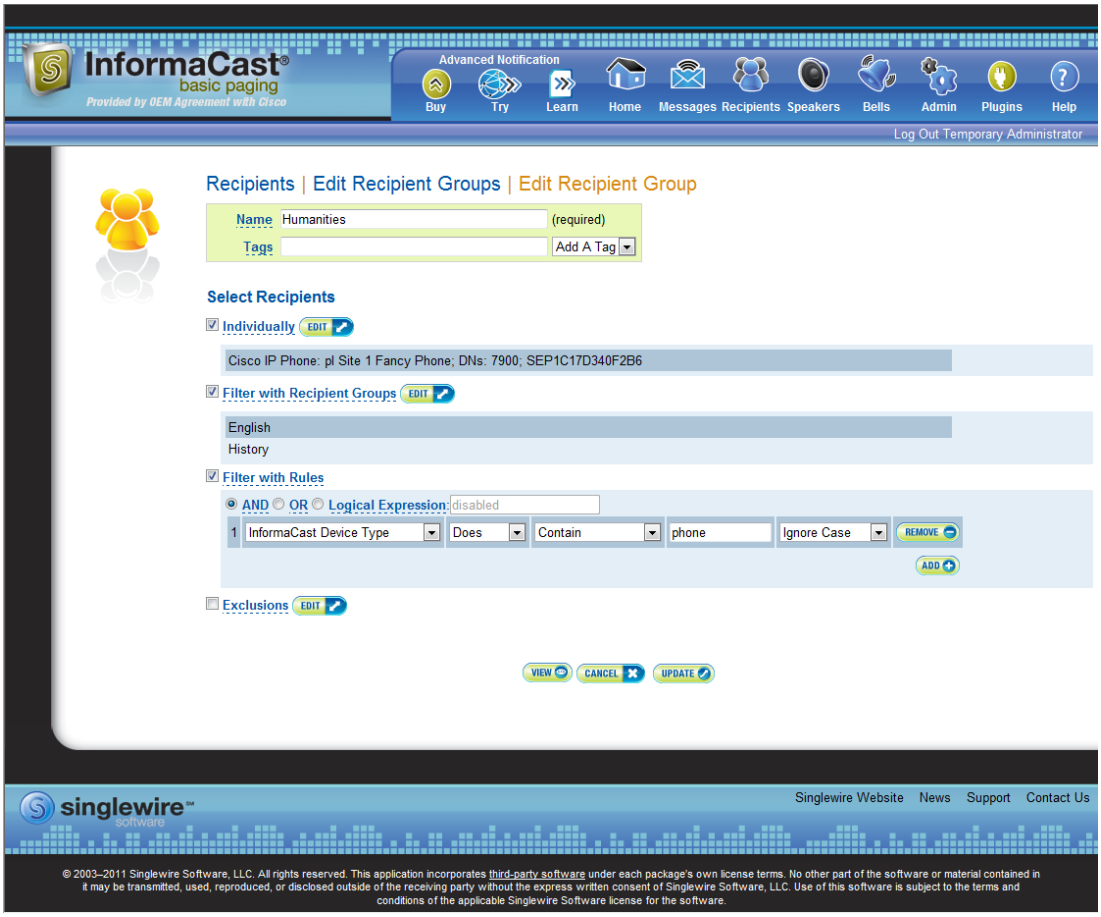
View Recipients in a Recipient Group

Once you have created a recipient group, you may want to review the recipients you've included.

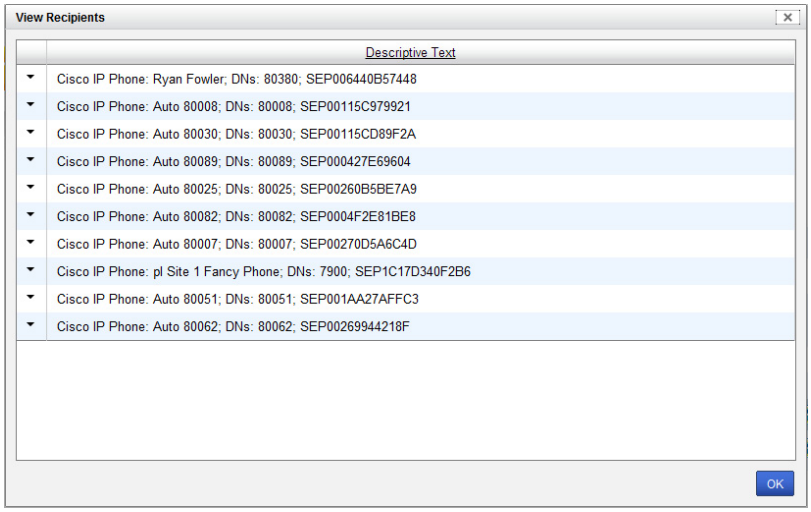
Step 1 Go to **Recipients** | **Edit Recipient Groups**. The Edit Recipient Groups page appears.



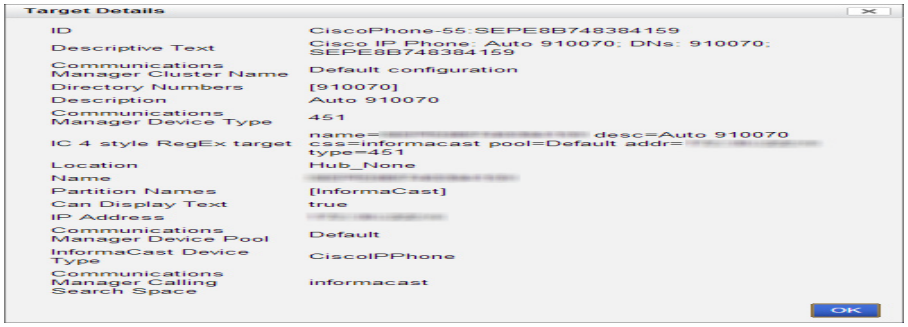
Step 2 Click the **Edit** button of the recipient group you want to view. The Edit Recipient Group page appears.



Step 3 Click the **View** button to list the recipients included in your recipient group. The View Recipients pop-up window appears.



Step 4 Click the down arrow next to a recipient to view its details. The Target Details pop-up window appears.



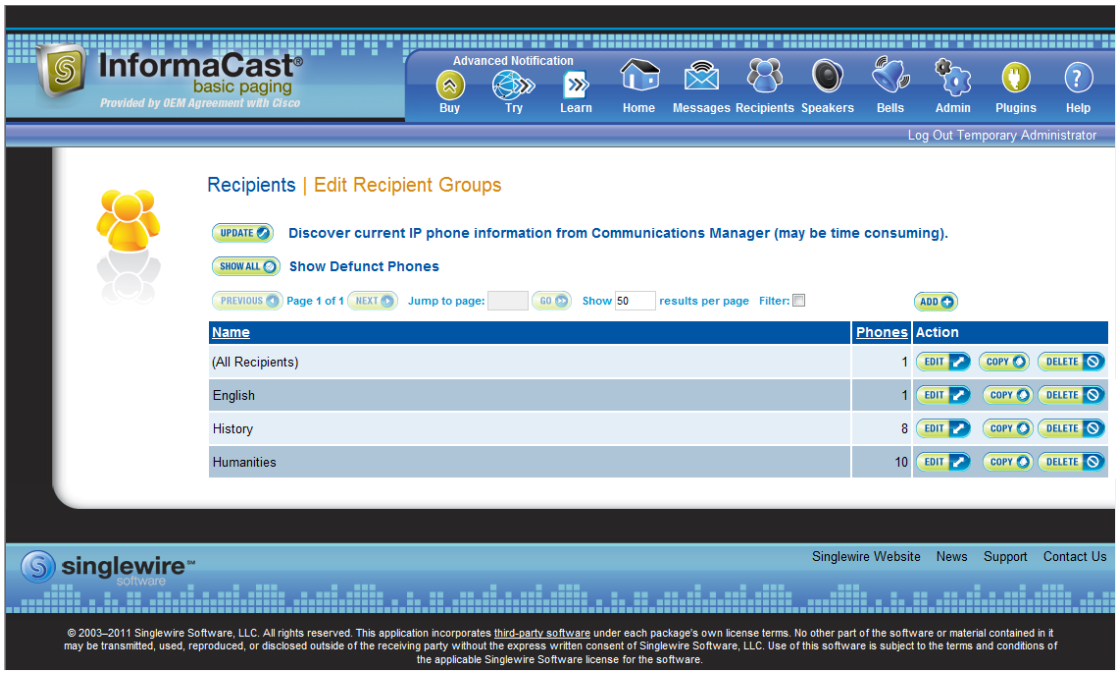
Step 5 Click the **OK** buttons in the Target Details and View Recipients pop-up windows to close them.

Step 6 Click the **Cancel** button to go back to the Edit Recipient Groups page or click the **Update** button to save any changes you've made.

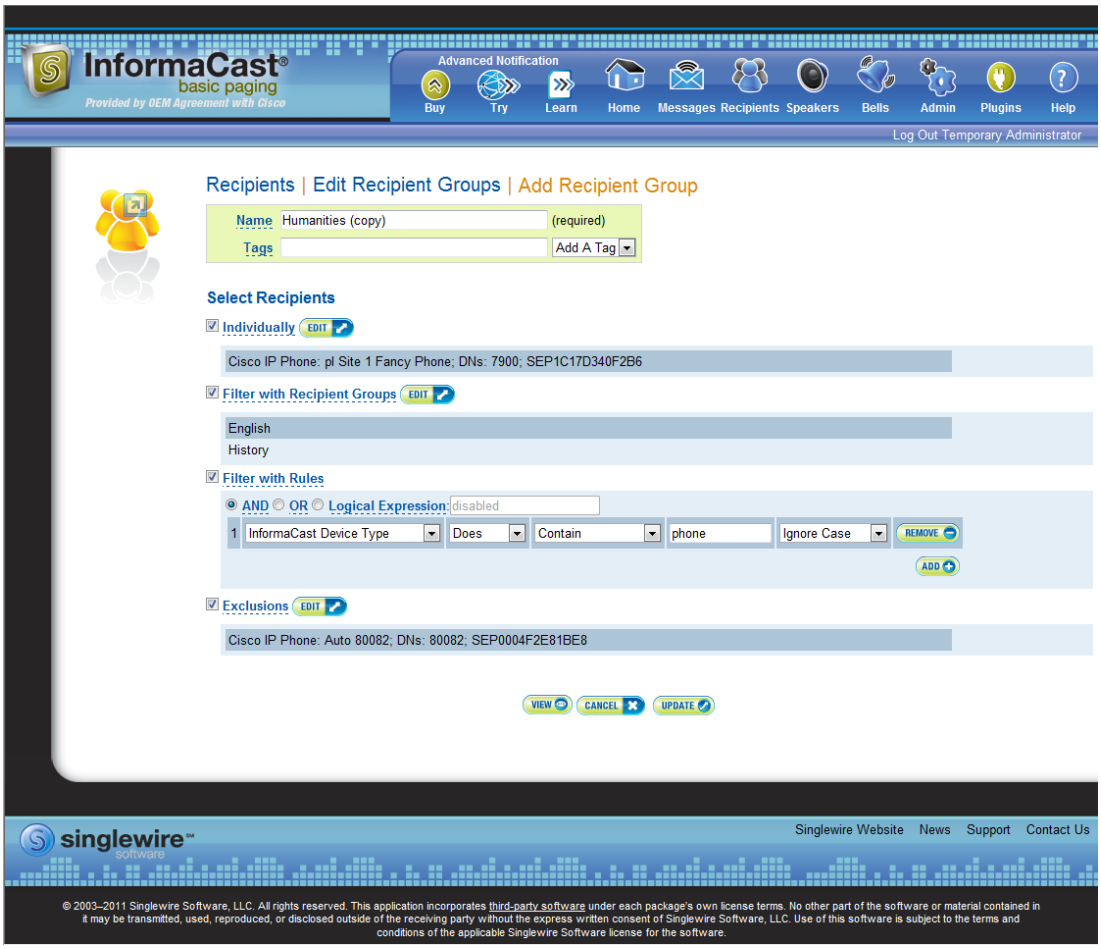
Copy a Recipient Group

When creating new recipient groups, you may want to start from a pre-existing recipient group that is close to the configuration you'd like for your new recipient group and make small changes from there.

Step 1 Go to **Recipients** | **Edit Recipient Groups**. The Edit Recipient Groups page appears.



Step 2 Click the **Copy** button next to the recipient group you'd like to copy. The Add Recipient Group page appears.



Note The **Name** field will automatically populate with the original recipient group's name and "copy" appended to it.

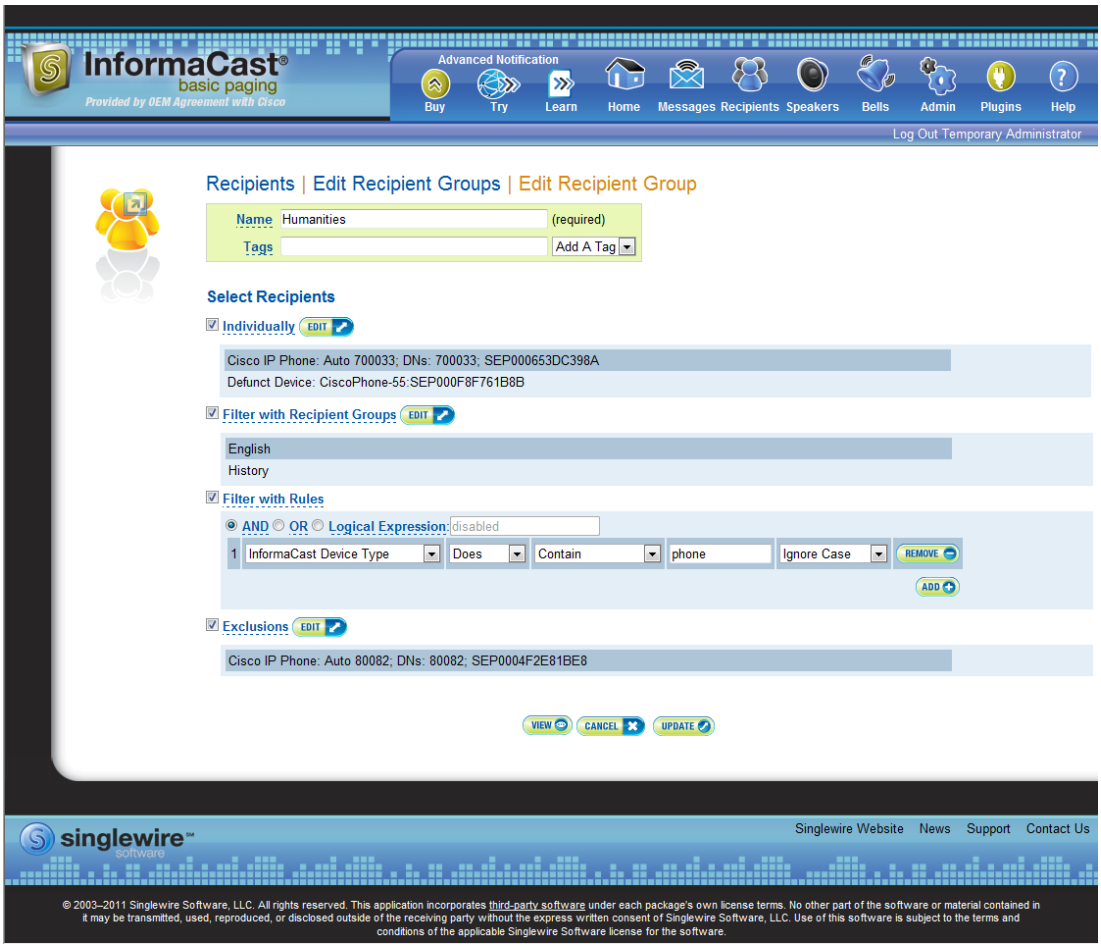
Step 3 Make your desired changes. See "Create a Recipient Group by Selecting Individual Recipients" on page 4-13, "Create a Recipient Group by Selecting Multiple, Existing Recipient Groups" on page 4-15, "Create a Recipient Group Using Rules" on page 4-18, or "Add Exclusions to a Recipient Group" on page 4-21 for more information on recipient group creation.

Step 4 Click the **Update** button when you are finished.

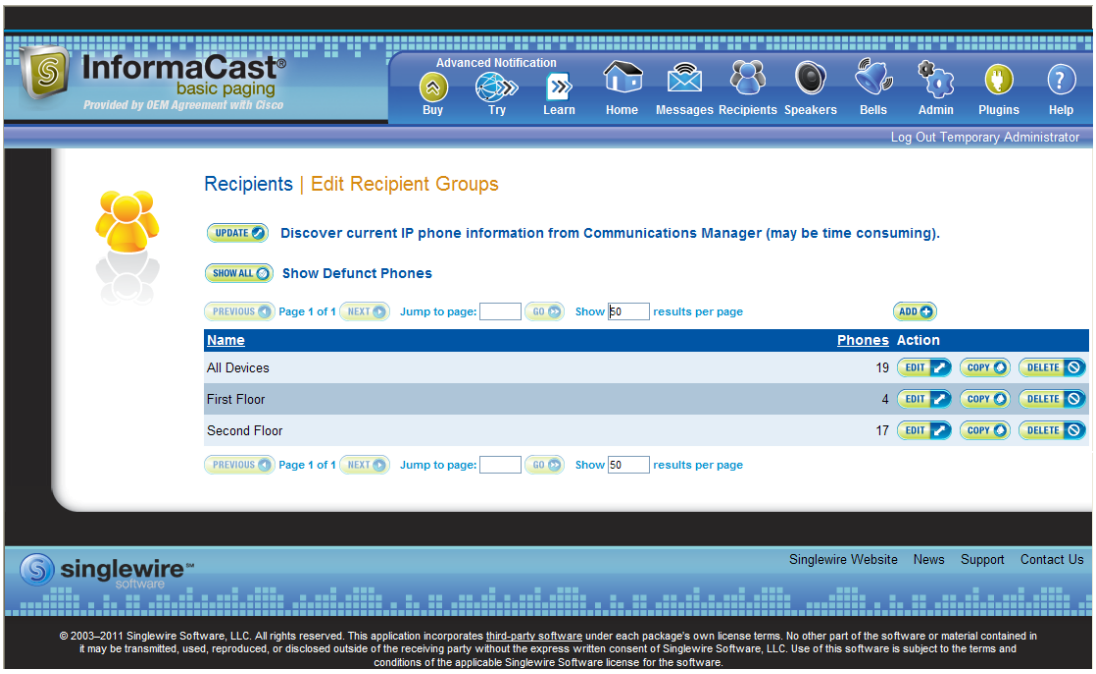
Remove Defunct Phones from Recipient Groups

Defunct phones are recipients that are no longer available to CUCM when the regular polling interval occurs. Recipients can become defunct if they lose power and/or are accidentally unplugged. A large number of defunct phones can degrade InformaCast's performance, and they should be removed.

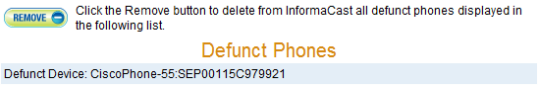
When phones become defunct, they will display as "Defunct" in your list of recipients on the Add/Edit Recipient Group page (see picture).



Step 1 Remove defunct phones by clicking the **Recipients** icon or going to **Recipients** | **Edit Recipient Groups**. The Edit Recipient Groups page appears.



Step 2 Click the **Show All** button near the top of the page. The Defunct Phones window appears.



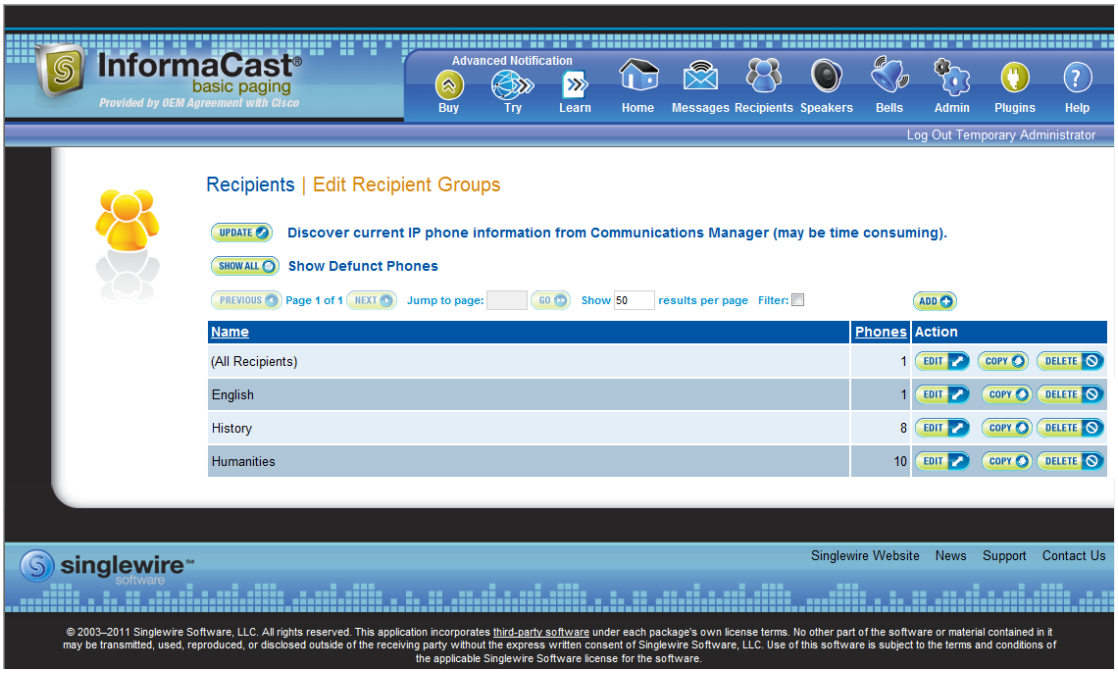
Step 3 Click the **Remove** button. Your defunct phones are removed from any recipient group to which they had been manually included or excluded.

Note Recipient groups using rules do not recognize defunct phones as viable recipients for inclusion in recipient groups.

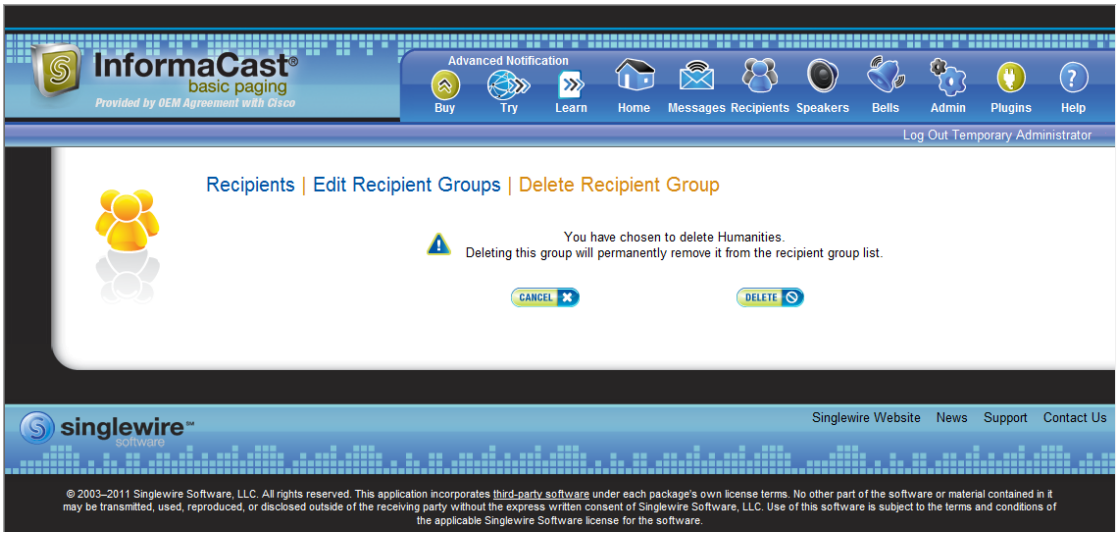
Delete a Recipient Group

As your needs change, you may want to delete unused recipient groups from the system.

Step 1 Go to **Recipients** | **Edit Recipient Groups**. The Edit Recipient Groups page appears.



Step 2 Click the **Delete** button next to the recipient group you'd like to delete. The Delete Recipient Group page appears.



Step 3 Click the **Delete** button again. Your recipient group is removed.

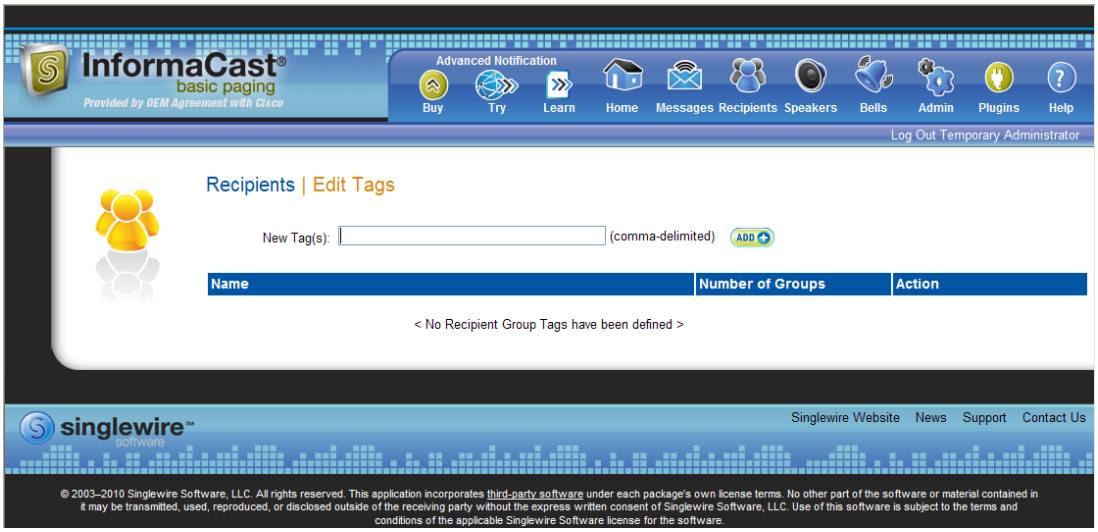
Configure Recipient Group Tags

Recipient group tags allow you finer control over the display results for recipient groups.

Add a Recipient Group Tag

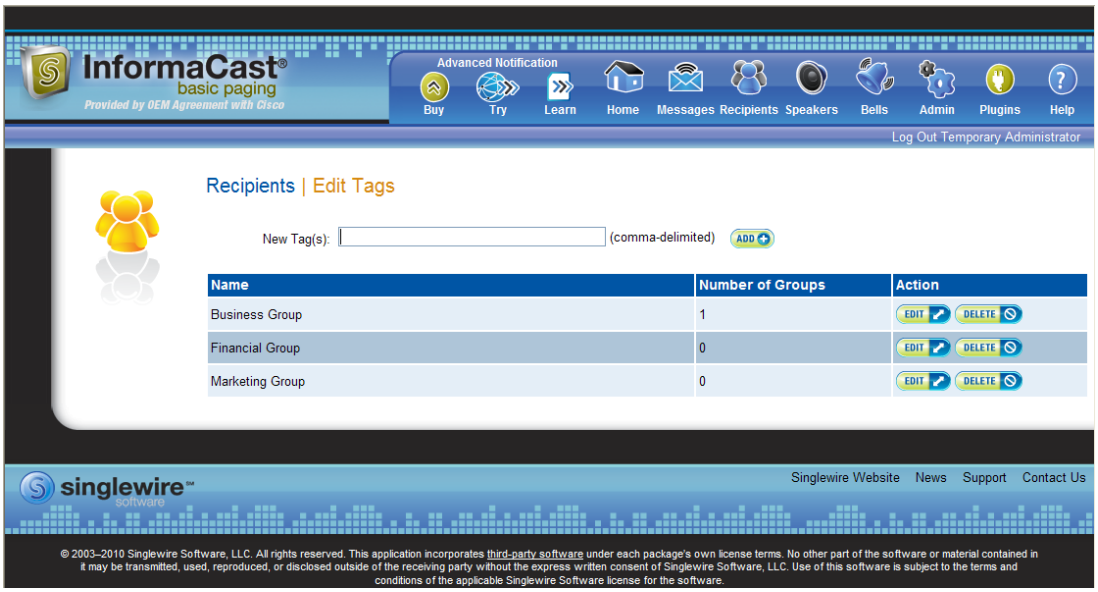
Before you can filter recipient groups through tags, you need to add them to InformaCast.

Step 1 Go to **Recipients** | **Edit Tags.** The Edit Tags page appears.



Step 2 Enter a name for your tag in the **New Tag(s)** field. Separate multiple tag names with a comma.

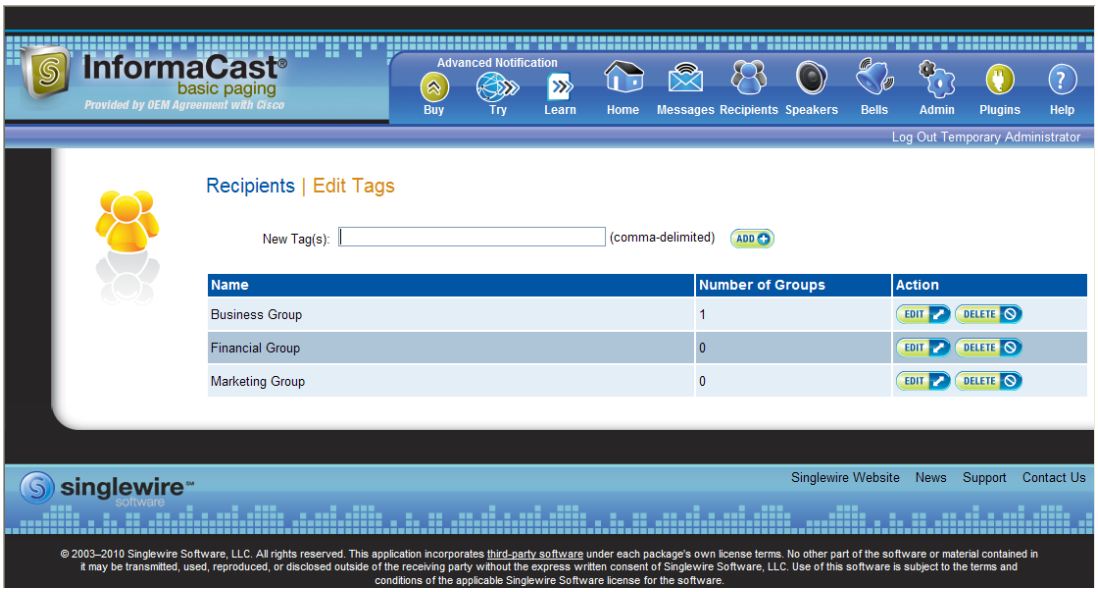
Step 3 Click the **Add** button. The Edit Tags page now shows the tag(s) you added. When you assign your tags to recipient groups, the number of recipient groups assigned to that tag will appear in the table.



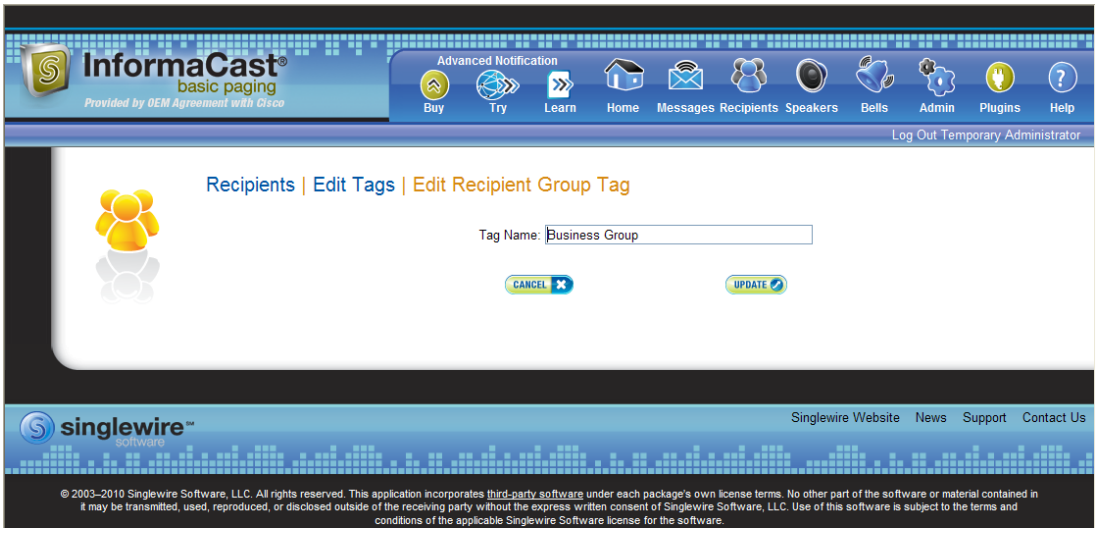
Edit a Recipient Group Tag

Once you've added recipient group tags, you may need to edit their names.

Step 1 Go to **Recipients** | **Edit Tags**. The Edit Tags page appears.



Step 2 Click the **Edit** button next to the tag you'd like to change. The Edit Recipient Group Tag page appears.



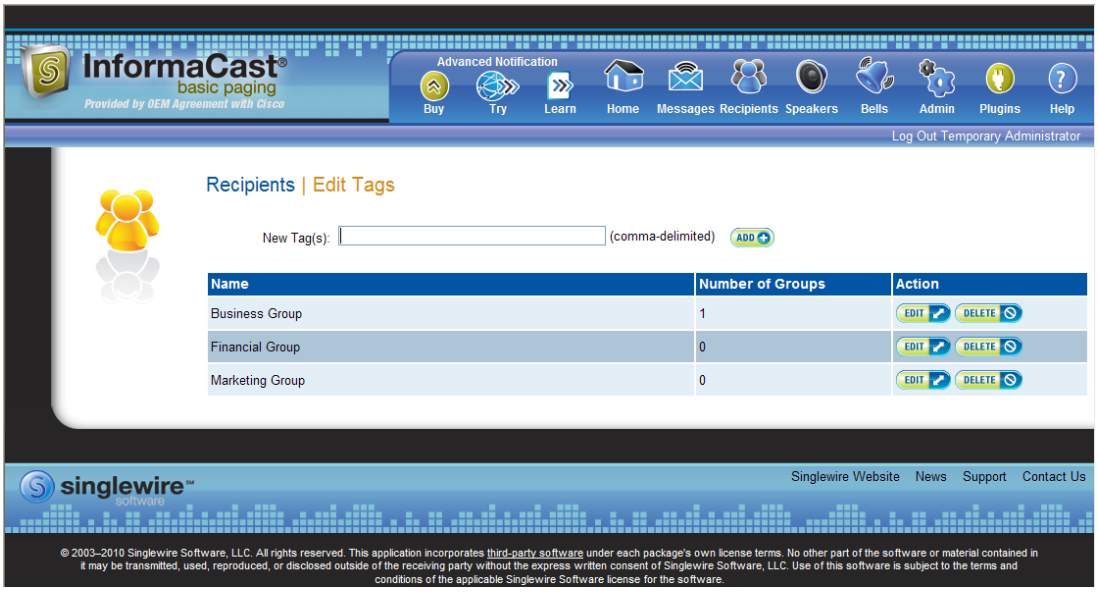
Step 3 Make your changes.

Step 4 Click the **Update** button. Your changes are saved.

Delete a Recipient Group Tag

As your needs change, you may want to delete existing tags from InformaCast.

Step 1 Go to **Recipients** | **Edit Tags**. The Edit Tags page appears.



Step 2 Click the **Delete** button next to the tag you want to delete.

Step 3 Click the **OK** button to accept the warning. Your tag is deleted.

Manage Recipient Administration

Recipient administration covers a number of topics that pertain the administration of your InformaCast phones.

Configure Advanced Matching for Recipient Groups

InformaCast has a variety of powerful methods for creating very precise matches of recipients for recipient groups:

- **Subnet matching.** For when you want to match all recipients on a particular network based on the IP address range assigned to that network.
- **Regular expressions.** For when the value of a particular device parameter will let you select devices, but in a more complex way than literally matching all of or part of the value. For example, you may want to check that the description contains numeric digits, or a particular pattern of text that would be tedious or impossible to set up as an individual rule.

Subnet Matching

When you are setting up a recipient group rule based on recipients' IP addresses, in addition to the normal matching types, you will see a **Belong to Subnet** choice. This allows you to include or exclude recipients based on whether their network address falls within the range assigned to a particular network.

To specify a subnet in IP networking, you need to provide two pieces of information: an address that is part of the network, and information about how much of that address is allowed to vary. There are a variety of approaches for formatting this information, and the one InformaCast uses reflects the underlying Java networking system on which it is built.

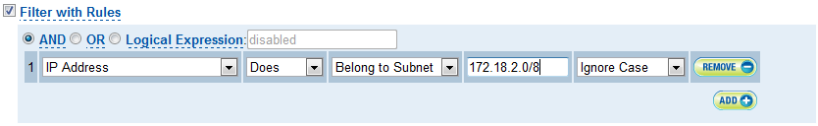
To specify a subnet within InformaCast, supply an address and the number of "host bits" that should be ignored in that address. For example, look at how you'd match a very common style of LAN, which uses what is known as "Class C" addressing. In a Class C network, there are 24 bits of network address, which are always the same, and eight bits that identify the host, so they vary from device to device. (IP addresses always contain a total of 32 bits; when written in decimal notation with dots, as they are in InformaCast, each number contains eight of the bits).

So, assume your hypothetical network has a network address portion of 172.18.2 (since there are 24 bits of network address information, there are three eight-bit numbers that make up the network portion). Valid addresses on this network would range from 172.18.2.0 to 172.18.2.255 (although in practice some of those addresses are reserved for special purposes, that goes beyond the depth of this introduction.

To match this subnet in InformaCast, select **IP Address** from the first dropdown menu in the *Filter with Rules* area, **Does** from the second dropdown menu, **Belong to Subnet** from the third dropdown menu, and enter the pattern **172.18.2.0/8** in the fourth field. The portion before the slash is the sample address that is part of the network, and the part after the slash tells InformaCast how many bits of the address are used for host information. In fact, the last value in the network address doesn't need to be zero in this case—it could be any valid value, 0 to 255—and will be ignored, since all eight bits of that value are reserved for host information.

Note If you are coming from other tools that perform subnetting, or using one of the online subnet calculators, keep in mind that they often work differently, placing the number of "network" or "mask" bits after the slash. In the example above, using such a tool, you would see "172.18.2.0/24" instead of what would actually work in InformaCast. To convert from network bits to host bits, you must subtract from 32.

Trying to use a subnet pattern of "172.18.2.0/24" in InformaCast will match many more recipients than you intend because it says that there are 24 host bits, meaning there are only eight network bits, so any address from 172.0.0.0 to 172.255.255.255 will match.



Regular Expressions

Regular expressions are an extremely powerful way to specify patterns to be matched. InformaCast lets you use them to choose recipients that belong in a recipient group. To use this feature you need to have a solid basic understanding of the syntax and use of regular expressions, and in particular, the variety used in the Perl programming language. This section does not attempt to provide this background information. If you need a reference for Perl regular expressions, consider picking up *Programming Perl* (O'Reilly & Associates) and looking at the relevant parts of Chapters 1 and 2. If you want to start at an even more basic level, O'Reilly also publishes *Learning Perl*, and if you want a great deal of detail, depth, and practical advice, they have an entire book on *Mastering Regular Expressions*.

The basic structure of an expression you will enter is as follows:

```
[m]/pattern/[i][m][s][x]
```

The `m` prefix is optional and the meaning of the optional trailing options are:

Option	Description
`i`	Case-insensitive match
`m`	The input is treated as consisting of multiple lines
`s`	The input is treated as consisting of a single line
`x`	Enable extended expression syntax incorporating white space and comments

As with Perl, any non-alphanumeric character can be used in lieu of the slashes.

You'll generally want to match things regardless of whether they are uppercase or lowercase, so you'll usually want the trailing "i" option (regular expressions control whether matches are case-sensitive directly, rather than using a checkbox in the rule to determine this). So, most recipient group regular expressions will look like:

```
m/pattern/i
```

For example, assume for a moment the descriptions of all recipients in your installation contain the name of the corporate division in parentheses. To select everyone in Marketing, we want all recipients whose description attribute contains the word "Marketing" surrounded by parentheses. Parentheses have a special meaning in regular expressions, so you'll have to escape them using backslashes, but other than that, it's pretty straightforward. Create a rule for the **Description** parameter to match this expression:

```
m/\(Marketing\)/i
```

This pattern searches the parameter for the string "(Marketing)." The "i" modifier just means you don't care about capitalization, so "(marketing)" would match just as well. Of course, you wouldn't need a regular expression for this, you could just use a **Contain** match (using the dropdown menus and fields provided in the *Filter with Rules* area) for "(Marketing)."

In something a bit trickier, suppose you want to have a group containing all phones whose extensions are 27xx. In other words, four digits long, starting with "27." Set up a rule with the **Directory Numbers** parameter, and set it to match this expression:

```
m/27[0-9][0-9]/
```

This rule will match any phone whose list of directory numbers contains the digit "2" followed by the digit "7," then any two additional digits.

These examples convey the basics of setting up regular expressions. The references cited at the beginning of the section will help in constructing even more sophisticated and powerful expressions.

There's a trick you can use to quickly see the data that is available for forming your regular expressions. Within the Add Recipient Group page, set the rule to **InformaCast Device Type Does Contain**, make sure there is nothing in the last field, and click the **View** button. This will open the View Recipients pop-up window, showing you all the recipients about which InformaCast knows. You can click on down arrow next to any recipient to pop up the Target Details window that shows you all the parameters available that describe that recipient and their values. Once you've figured out how to proceed, set the rule back to the parameter you want to use, pick **Logical Expression** for the constraint, and start setting it up.

Manage Phone Updates

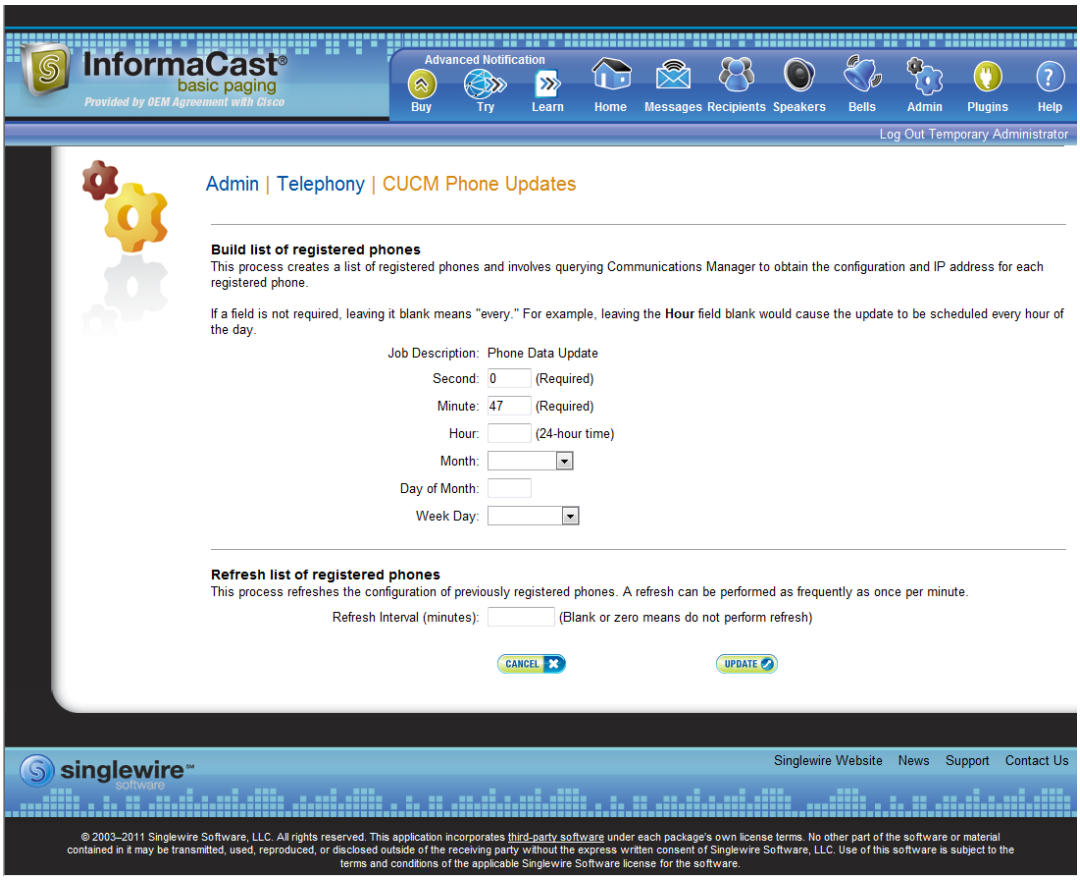
Phone updates allow you to configure the timing for two scheduled jobs of how often InformaCast will update its phone information: build a list of registered phones and refresh a list of registered phones.

The time it takes for InformaCast to *rebuild* a list of phones is directly related to the number of phones you have. During a build of registered phones, CUCM's SNMP service obtains the IP address of all registered phones in the cluster. Because SNMP is throttled for each piece of data it sends, minutes may pass if many thousands of phones are registered. By comparison, the AXL requests used to *refresh* a list of registered phones are relatively quick.

Refreshing a list of registered phones picks up the changes to phones that use extension mobility as well as other configuration changes, e.g. adding/deleting/modifying a line, changing the phone description, etc. Updates can be performed as frequently as once per minute or even disabled if desired.

Note Refreshing the list only updates the phones already in InformaCast's phone cache. Newly registered phones will not be seen in the cache until the next rebuild of registered phones.

Step 1 Go to **Admin** | **Telephony** | **CUCM Phone Updates**. The CUCM Phone Updates page appears.



Note By default, building a list of registered phones will occur at 10 minutes past the hour, every hour.

Step 2 Enter numeric values in the **Second**, **Minute**, and **Hour** fields to specify when you'd like InformaCast to rebuild its list of registered phones.

Step 3 Select **Every Month** or a specific month from the **Month** dropdown menu.

Step 4 Enter a numeric value in the **Day of Month** field if you'd like InformaCast to only rebuild its phone information on a specific day.

Step 5 Select **Every Day** or a specific day from the **Week Day** dropdown menu.

Step 6 Enter a numeric value in the **Refresh Interval (minutes)** field. A positive numeric value enables updates. Zero or no value disables updates.

Note Refreshing a list of registered phones picks up the changes to phones that use extension mobility as well as other configuration changes. Refreshing the list only updates the phones already in InformaCast's phone cache. Newly registered phones will not be seen in the cache until the next rebuild of registered phones.

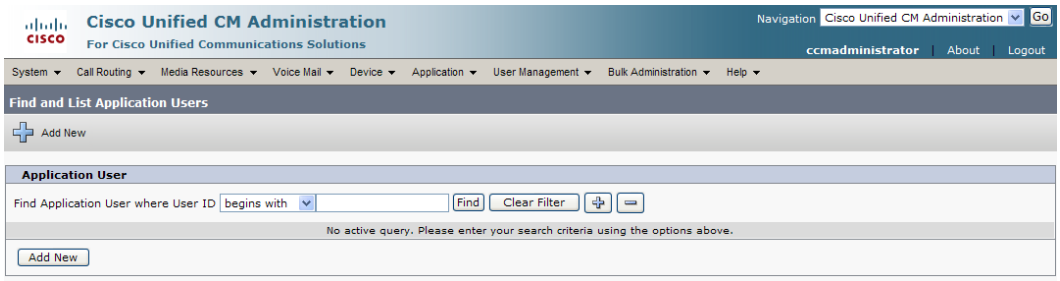
Step 7 Click the **Update** button. On the Overview page, you can see your changes reflected in the *Phone Updates* section.

Determine the Busy State of a Phone with JTAPI

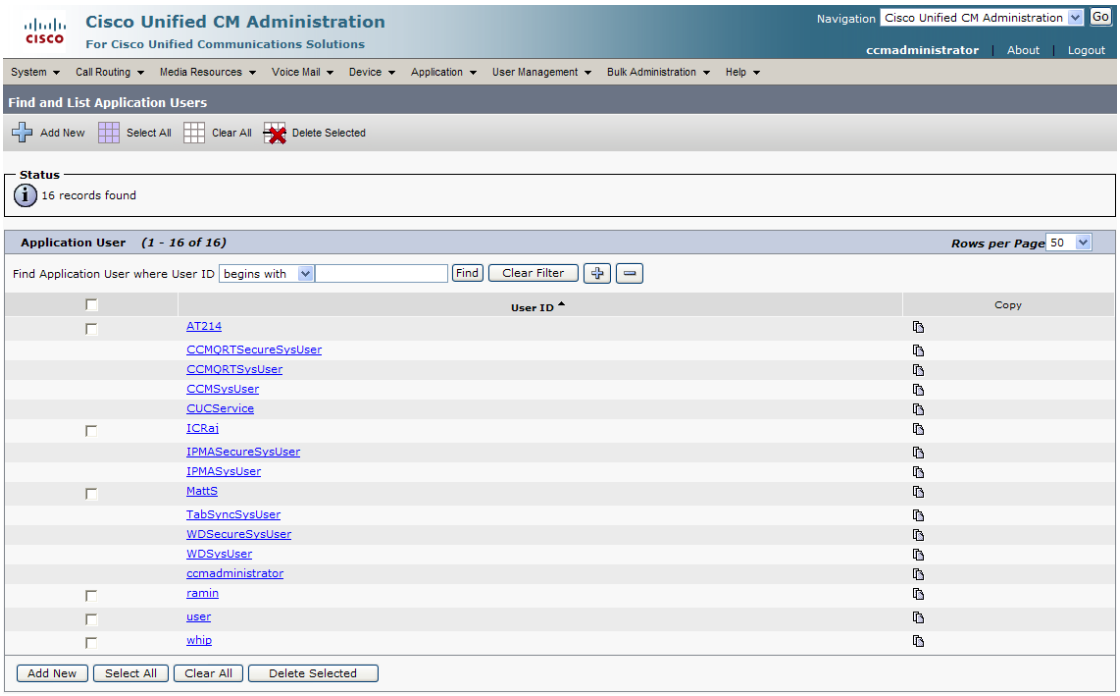
Cisco IP phones have become progressively less reliable at reporting whether they are in use during a broadcast. For those small number of phones where it is very important to be sure that message audio is always and only delivered if the phone is idle (a requirement for Basic InformaCast), it is now possible to associate these specific phones with InformaCast's application user, which will give InformaCast more accurate information about their status. Unfortunately, because of scalability limitations within CUCM itself, it is not practical or possible to monitor all phones in medium-to-large installations.

Note This procedure will only work when using CUCM 8.x or newer. It is not intended to be used with a medium or large number of phones, and must be applied in a targeted manner.

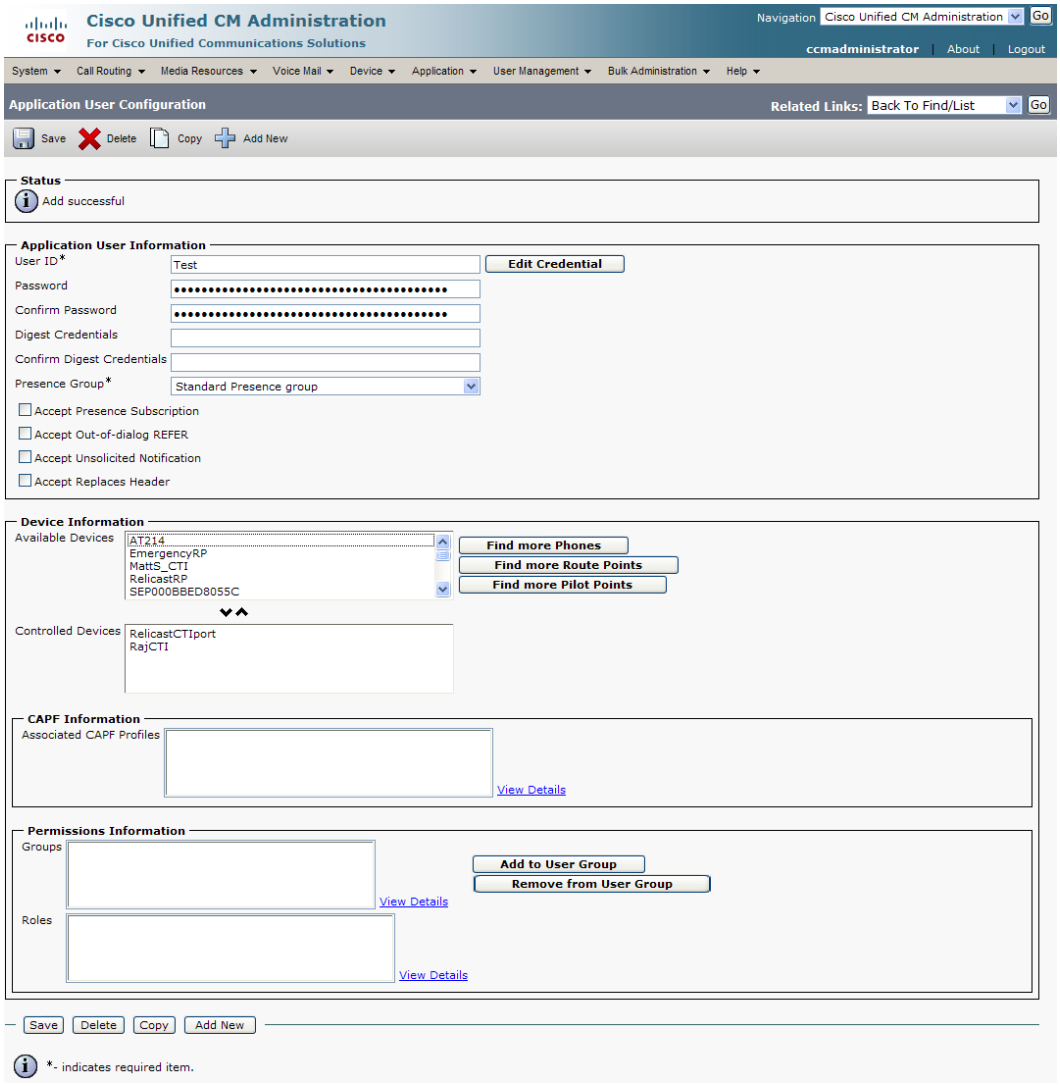
Step 1 Log into your CUCM's administrative interface and go to **User Management** | **Application User**. The Find and List Application Users page appears.



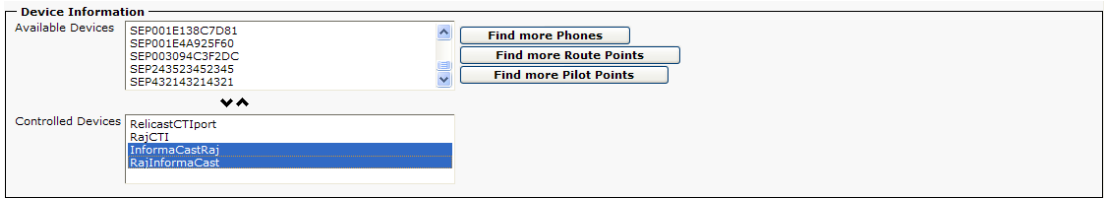
Step 2 Use the filters to search for the name of the application user you are using. Click the **Find** button. The Find and List Application Users page refreshes with your results.



Step 3 Click the **User ID** link of your user. The Application User Configuration page appears.



Step 4 Scroll down to the **Device Information** area. Highlight all of the phones on which you would like to enable JTAPI monitoring and click the down arrow to move them into the lower box. All phones in the lower box will look to JTAPI for their current phone status.

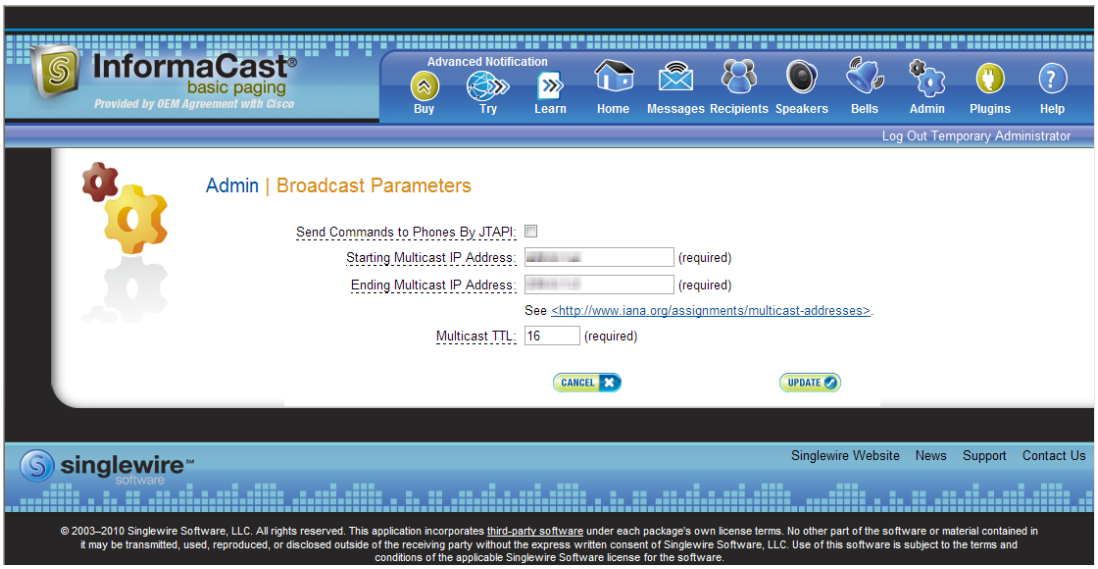


Step 5 Click the **Save button** to save your changes.

Manage Broadcast Parameters

If your InformaCast license includes audio broadcast capability, you'll need to set up your audio parameters.

Step 1 Go to **Admin** | **Broadcast Parameters**. The Broadcast Parameters page appears.



Step 2 Select the **Send Commands to Phones by JTAPI** checkbox if you would like to use JTAPI to communicate between InformaCast and your phones. If you select this checkbox, you must have also selected the **Standard CTI Allow Control of All Devices** checkbox when configuring your application user (see "Create an Application User" on page 2-53).

Step 3 Verify that there is an entry in the **Starting Multicast IP Address** and **Ending Multicast IP Address** fields. This is the address that InformaCast will use to send IP multicast packets when broadcasting audio messages to IP phones. You will need to ensure that your network is configured to treat this address as a multicast address, and that your switches mark traffic to this address from InformaCast as having the highest priority.

Note The multicast IP address needs to be a valid IP multicast address, not your subnet's IP broadcast address. The default address InformaCast provides usually works; don't change it unless you have checked with your network administrator.

Alternatively, you can enter a range of IP addresses in the **Starting Multicast IP Address** and **Ending Multicast IP Address** fields, which will cause InformaCast to cycle through this range of addresses, using the next address in the range for each broadcast. You will need to ensure that your network is configured to treat each address in this range as a multicast address and that your switches mark traffic to this address range from InformaCast as having the highest priority.

Note Click the http://www.iana.org/assignments/multicast-addresses/ link for information on how multicast addresses are assigned.

Step 4 Enter a numerical value in the **Multicast TTL** field to set the multicast time-to-live value used with RTP streams. Time-to-live is the number of routers that an RTP packet can be passed through on a network. Each time it goes through a router, the time-to-live is decremented. When it reaches zero, the packet won't pass through any more routers. The default value is 16.

Step 5 Click the **Update** button to save your changes.

Configure Messages and Broadcasts

InformaCast allows you to send a live audio broadcast through its DialCast functionality combined with proper session initiation protocol (SIP) configuration.

When working with messages and broadcasts, you can:

- "Manage Messages" on page 5-1
- "Manage SIP Functionality" on page 5-4
- "Manage DialCasts" on page 5-40
- "Send a DialCast/Broadcast" on page 5-45
- "Cancel a DialCast/Broadcast" on page 5-46

Manage Messages

Messages are the basis of any InformaCast broadcast. A message predefines the characteristics of the broadcast.

A message can be composed of text, audio, or both; however, with Basic InformaCast functionality, you only have access to Live Audio broadcasts. In these messages, the audio is not recorded at all; it is streamed to recipient groups in real time when the message is broadcast. These broadcasts will skip any phones that are in use when the broadcast occurs, wait until all recipients capable of playing audio are ready to play the broadcast, play the broadcast at the volume at which the phone is set when the broadcast occurs, and if there are simultaneous broadcasts attempted, will play the first broadcast first (the second broadcast will be bumped) With Advanced InformaCast, you'd have access to all the messages described in the following table.

Message Type	Description
Text	These messages consist of only text and appear on the phone's display and in a pop-up window on computers running the InformaCast Desktop Notifier.
Text and Pre-recorded Audio	These messages have the same display features as Text messages, but add an audible component.
Text and Live Audio	These messages are the combination of a Text message (whose content is predetermined, although it may be dynamic) with Live Audio that is streamed to recipient groups in real time when the message is broadcast.

Message Type	Description
Text and Ad-hoc Audio	These messages are the combination of a Text message (whose content is predetermined, although it may be dynamic) with an Ad-hoc Audio message, whose content is determined when the message is broadcast. Ad-hoc broadcasts are sent immediately after the audio is recorded. They are used to rapidly respond to unpredictable events.
Pre-Recorded Audio	These messages are audio only and are sent to the specified combination of phones, IP speakers, and computers running the InformaCast Desktop Notifier. These messages have no display component; they do not affect the display of the phone (other than a small animation showing incoming stream activity, and the illumination of the Mute and Speaker lights during the audio broadcast).
Live Audio	In these messages, the audio is not recorded at all; it is streamed to recipient groups in real time when the message is broadcast.
Ad-hoc Audio	These messages are a form of Audio message in which the audio is not recorded in advance; instead, it is recorded each time the message is sent. Ad-hoc broadcasts are sent immediately after the audio is recorded. They are used to rapidly respond to unpredictable events.
Talk and Listen	Talk and Listen messages allow any phone in a recipient group to speak, in real time ("live"), to all the other phones receiving the broadcast by pressing a **Talk** softkey. Other listeners can respond by pressing the **Talk** softkey on their own phones.

Click the **Messages** icon or go to **Messages** | **Send or Edit Messages**. The Send or Edit Messages page appears.

Note With Basic InformaCast functionality, you can view all of the potential InformaCast messages, but you cannot configure any of them unless you have Advanced InformaCast functionality. Contact Singlewire to obtain an Advanced InformaCast license, which is available as a free trial or for purchase, and gain access to all of InformaCast's functionality.

Aside from viewing potential InformaCast messages, you can also view active broadcasts by clicking the **View** button (only visible on the Send or Edit Messages page when there is an active broadcast) and cancel any ongoing broadcasts (see "Cancel a DialCast/Broadcast" on page 5-46).

Manage SIP Functionality

Session Initiation Protocol (SIP) is supported by a growing number of PBXs and telephony devices, and provides InformaCast with the capability to receive SIP calls, allowing other SIP devices (in this case, CUCM) to locate and call InformaCast. InformaCast's SIP functionality provides these important features:

- **Access control.** Controls the devices from which InformaCast will accept SIP packets.
- **Authentication of incoming requests.** Allows incoming SIP requests to be authenticated using digest authentication.
- **Secure signalling.** Enables the exchange of SIP messages in a secure fashion by using the Transport Layer Security (TLS) protocol.
- **Authentication challenges.** Enables InformaCast to respond to authentication challenges issued by other SIP devices when sending a request.

In order to configure SIP functionality, you will need to configure a SIP trunk and InformaCast's SIP pages.

Note In the past, CTI route points were recommended for use with DialCast functionality. For easier troubleshooting, it is now recommended that DialCast functionality be used in conjunction with SIP instead. You should update your DialCast configurations accordingly.

Configure a SIP Trunk

Configuring a SIP trunk is comprised of three basic components: a SIP trunk security profile, the SIP trunk itself, and a route pattern.

When configuring a SIP trunk, you can choose between a non-secure SIP trunk (TCP only) or a secure SIP trunk (TCP with TLS).

For a non-secure SIP trunk, follow these steps:

- "Add a SIP Trunk Security Profile" on page 5-5
- "Add a SIP Trunk" on page 5-7
- "Add a Route Pattern" on page 5-25

For a secure SIP trunk, follow these steps:

- "Manage SIP Certificates to Facilitate TLS Protocol" on page 5-9
- "View the InformaCast SIP Certificate" on page 5-10
- "Install the InformaCast SIP Certificate on CUCM" on page 5-12
- "Add a SIP Trunk Security Profile That Uses TLS" on page 5-15
- "Add a SIP Trunk That Uses TLS" on page 5-17
- "Install CUCM Certificates on InformaCast" on page 5-20

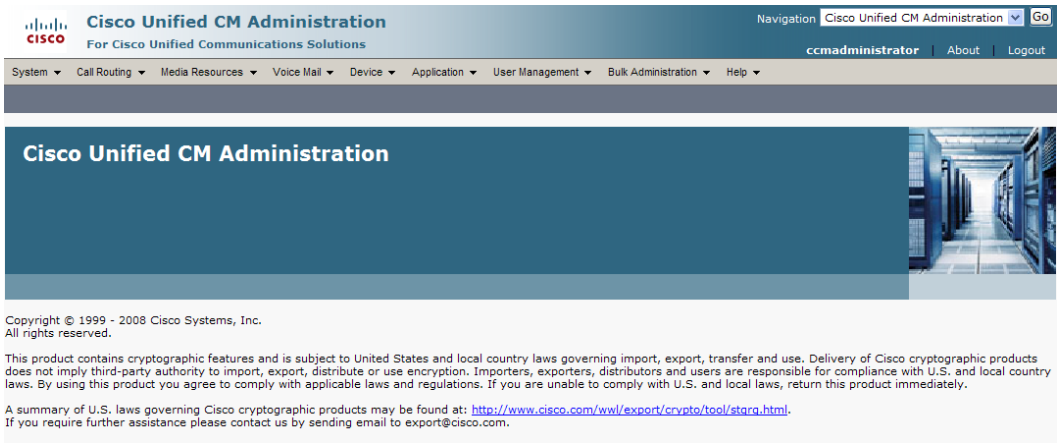
- "Add a Route Pattern" on page 5-25

Add a SIP Trunk Security Profile

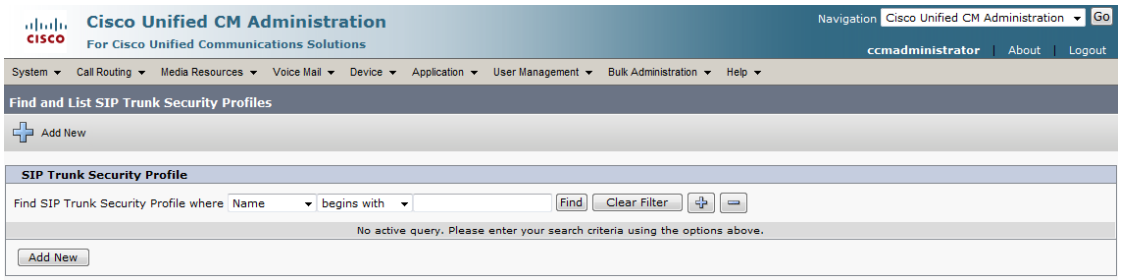
A SIP trunk security profile specifies things such as the transport protocol to be used, whether digest authentication should be performed, etc.

Note If you want to use TLS with your SIP trunk, follow the steps in "Add a SIP Trunk Security Profile That Uses TLS" on page 5-15.

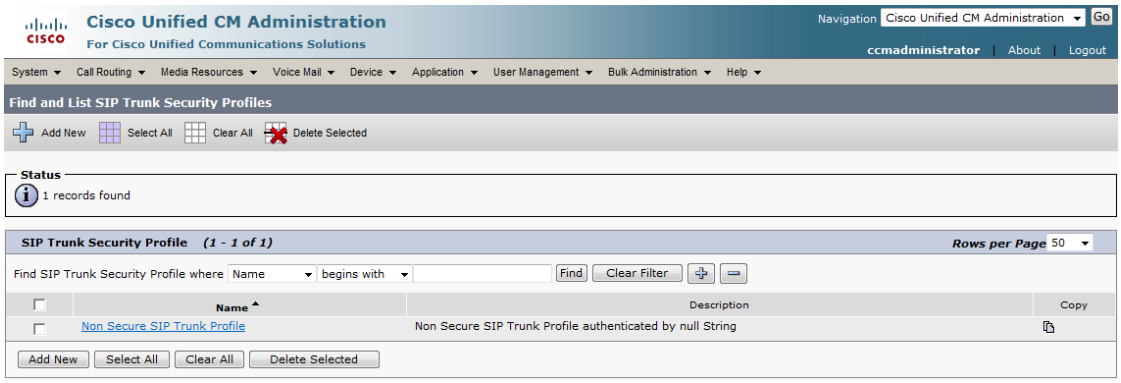
Step 1 Open a web browser and log into the administration interface of the CUCM server (the address will be similar to https://<CUCM IP Address>/ccmadmin). The Cisco Unified CM Administration page appears.



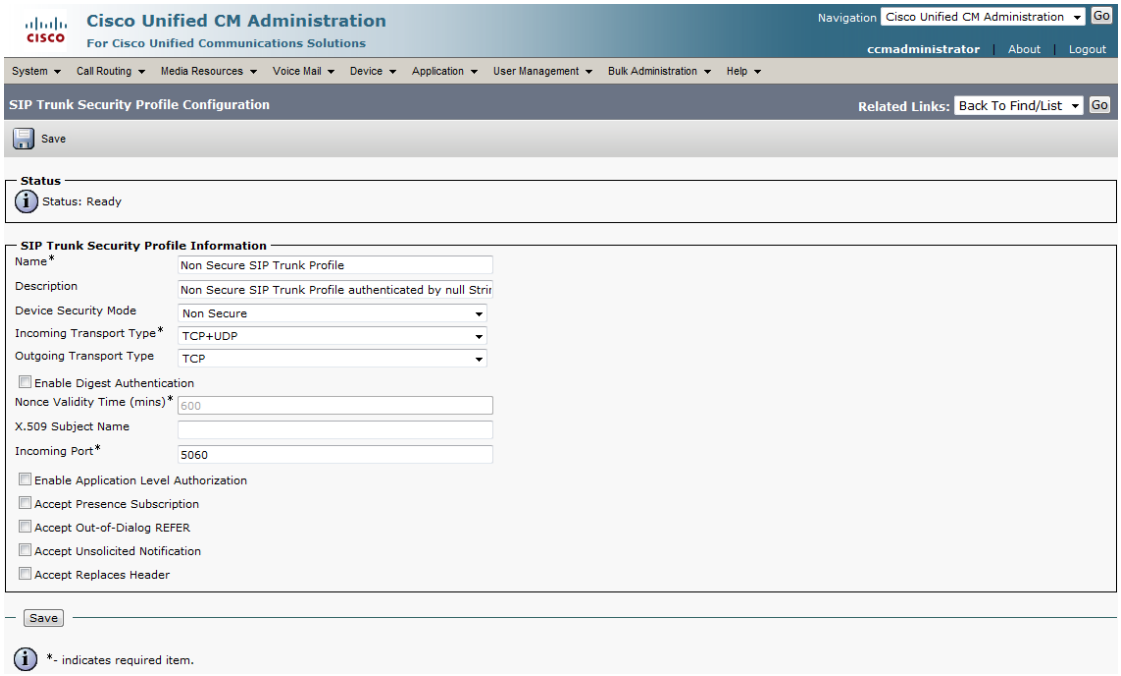
Step 2 Go to **System** | **Security** | **SIP Trunk Security Profile**. The Find and List SIP Trunk Security Profiles page appears.



Step 3 Click the **Find** button. The Find and List SIP Trunk Security Profiles page refreshes with a list of SIP trunk security profiles.



Step 4 Click the **Copy** icon in the row of your default profile, **Non Secure SIP Trunk Profile**. The SIP Trunk Security Profile Configuration page appears.



Step 5 Enter a unique name for your SIP trunk security profile in the **Name** field, e.g. InformaCast.

Step 6 Enter a description of your SIP trunk security profile in the **Description** field.

Step 7 Select **Non Secure** from the **Device Security Mode** dropdown menu.

Once you select a Device Security mode, the **Incoming** and **Outgoing Transport Type** fields will automatically fill with information.

Step 8 Select **TCP** from the **Outgoing Transport Type** dropdown menu.

Step 9 Leave the **Incoming Port** field as **5060**.

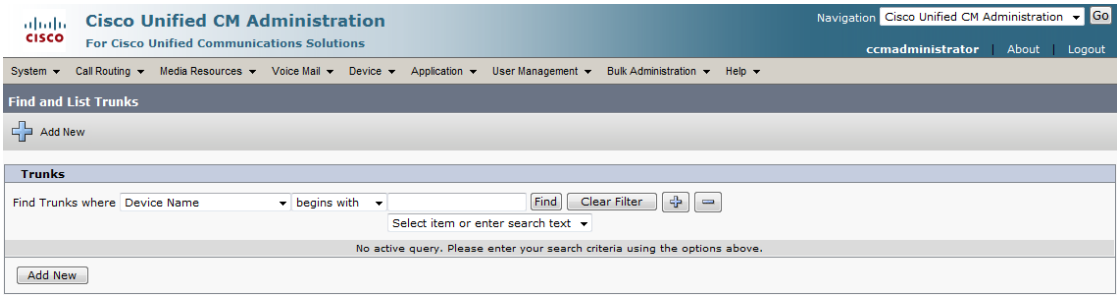
Step 10 Click the **Save** button.

Add a SIP Trunk

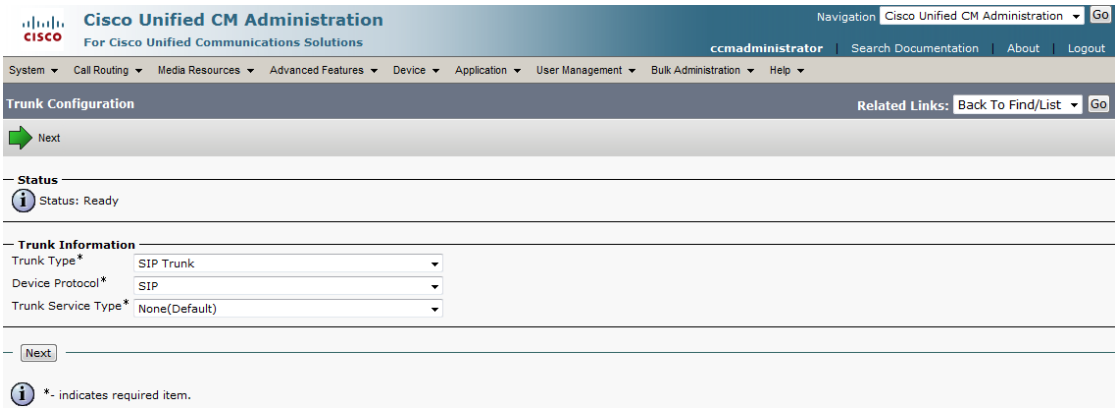
Use the following steps to create a SIP trunk that uses the security profile you just created.

Note If you want to use TLS with your SIP trunk, follow the steps in "Add a SIP Trunk That Uses TLS" on page 5-17.

Step 1 Go to **Device** | **Trunk**. The Find and List Trunks page appears.



Step 2 Click the **Add New** button. The Trunk Configuration page appears.

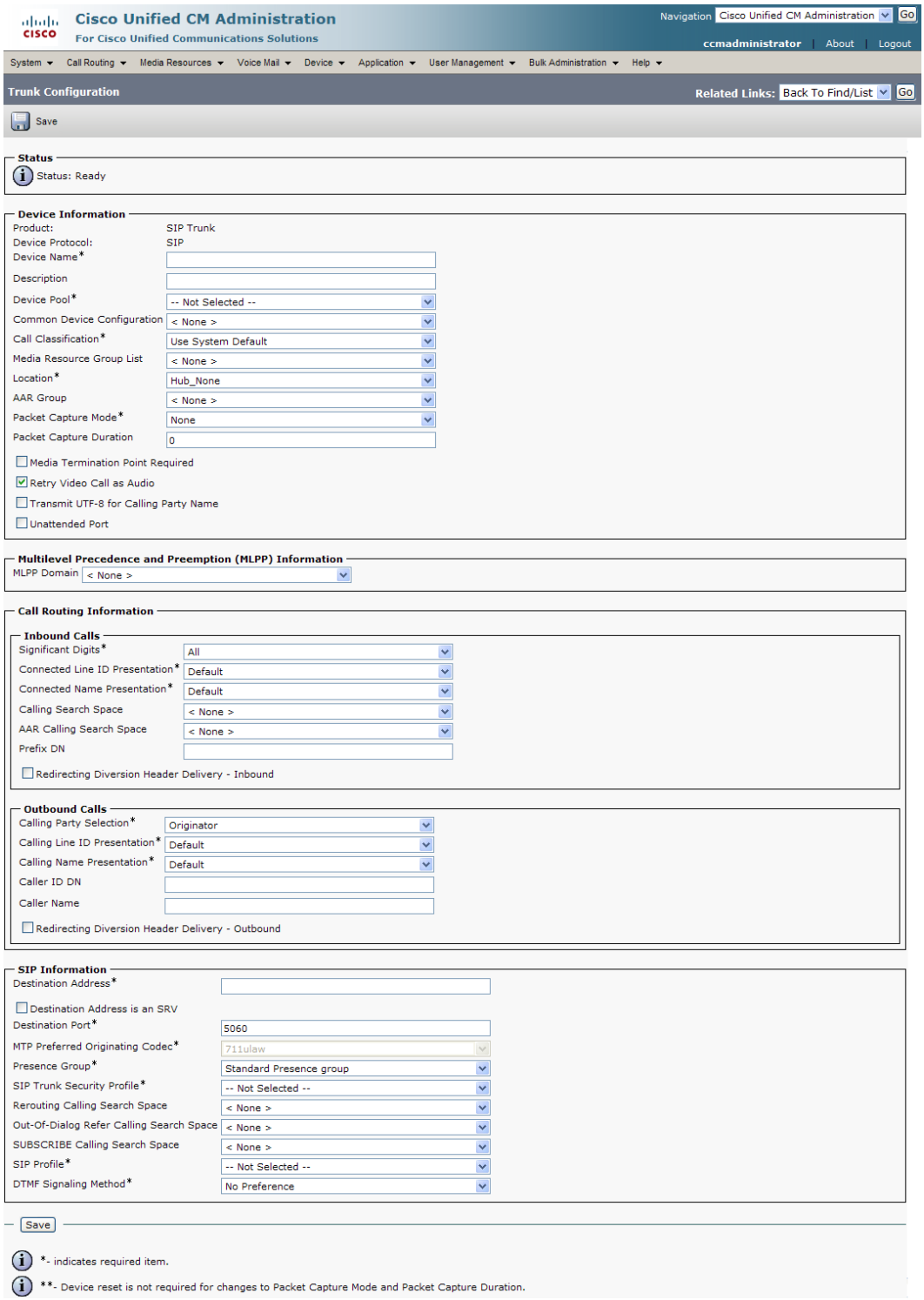


Step 3 Select **SIP Trunk** from the **Trunk Type** dropdown menu.

Step 4 Ensure that **SIP** appears as the **Device Protocol** dropdown menu selection.

Step 5 Leave the **Trunk Service Type dropdown** menu at its default of **None(Default)**.

Step 6 Click the **Next** button. The Trunk Configuration page refreshes.



Step 7 Enter a name for your SIP trunk in the **Device Name** field, e.g. InformaCast.

Step 8 Select the device pool you created in "Create a Device Pool" on page 2-40 from the **Device Pool** dropdown menu.

Step 9 Select the **Run On All Active Unified CM Nodes** checkbox.

Step 10 Scroll down to the *Inbound Calls* area and select the calling search space you created in "Create a Calling Search Space" on page 2-43 from the **Calling Search Space** dropdown menu.

Step 11 Scroll down to the *SIP Information* area and enter InformaCast's IP address in the **Destination Address** field.

Step 12 Ensure that the value in the **Destination Port** field is the same as listed in Step 9 on page 5-6.

Step 13 Select the SIP trunk security profile that you created in "Add a SIP Trunk Security Profile" on page 5-5 from the **SIP Trunk Security Profile** dropdown menu.

Step 14 Select **Standard SIP Profile** from the **SIP Profile** dropdown menu.

Step 15 Click the **Save** button.

Step 16 Proceed to "Add a Route Pattern" on page 5-25.

Manage SIP Certificates to Facilitate TLS Protocol

Note This section is optional depending on the security of your environment.

The TLS protocol is used by SIP to provide secure signalling between SIP endpoints. Using TLS between two SIP hosts first requires the sending host to make a TCP connection with other host. Once the TCP connection has been made, the two hosts must agree upon an encryption protocol and cipher suite to be used when exchanging encrypted data with each other. Next, the two hosts must prove to each other that they are who they represent themselves to be. This process involves each host passing its identity certificate to the other host, thereby proving its trustworthiness since a copy of that certificate already resides in the other host's cache of trusted certificates. Once these steps have been successfully completed, the two hosts are ready to exchange SIP requests and responses between themselves over a secure channel.

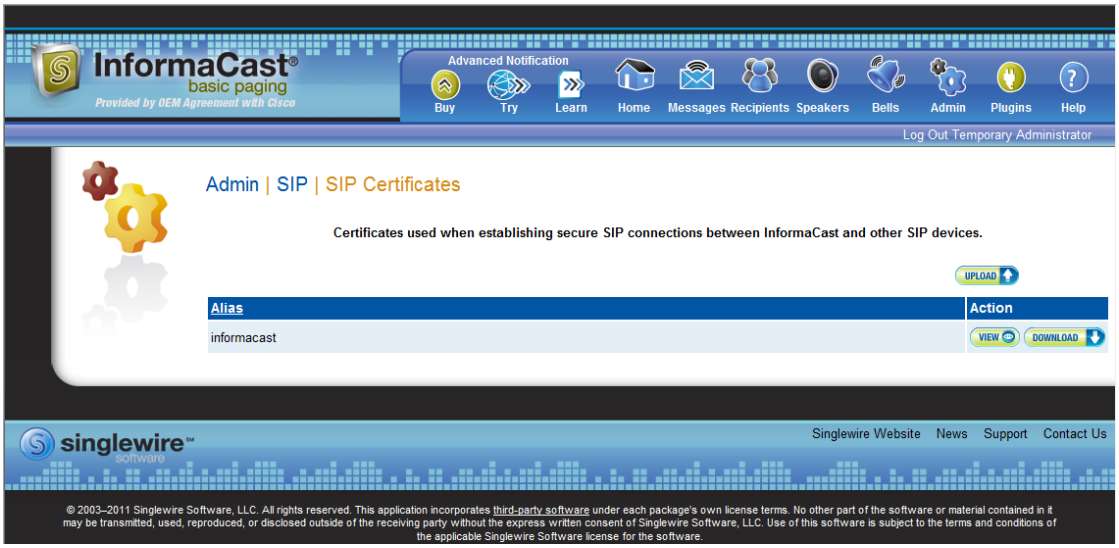
It is essential that the InformaCast certificate be downloaded and installed at each host that expects to use TLS as its SIP transport protocol with InformaCast. It is also essential that a certificate from each of those same hosts be uploaded to InformaCast. You will also need to modify it and its security profile to use TLS.

When InformaCast is first installed, the key store only contains an RSA self-signed certificate for InformaCast. The InformaCast key store file is named keystore.jks (typically located in /usr/local/singlewire/InformaCast/web/WEB-INF/sip) and uses changeMe for its password. Each certificate in the certificate cache has an alias assigned to it. The alias is assigned when the certificate is uploaded and is set to be equal to the lowercase value of the common name in the certificate's subject line (i.e. CN=...).

View the InformaCast SIP Certificate

Use the following steps to view the SIP certificate for InformaCast.

Step 1 Go to **Admin** | **SIP** | **SIP Certificates**. The SIP Certificates page appears.



Note InformaCast installs with its own SIP certificate.

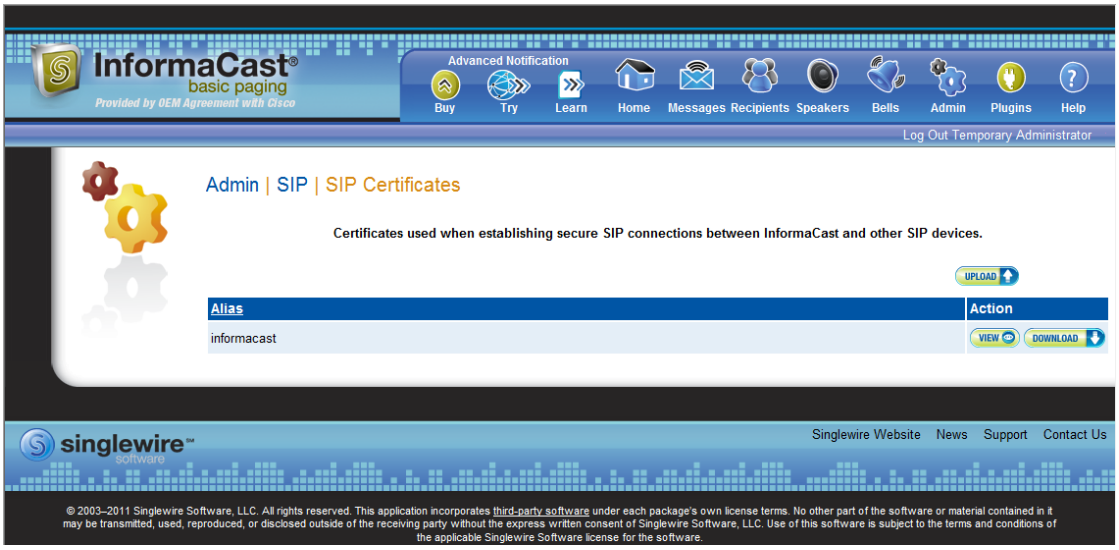
Step 2 Click the **View** button. The SIP Certificate page appears.

Step 3 Click the **Done** button to return to the SIP Certificates page.

Install the InformaCast SIP Certificate on CUCM

To use the TLS protocol between CUCM and InformaCast, you will need to be using a SIP trunk for SIP configuration and install InformaCast's SIP certificate on all nodes in the CUCM group used by the trunk's device pool.

Step 1 Go to **Admin** | **SIP** | **SIP Certificates**. The SIP Certificates page appears.

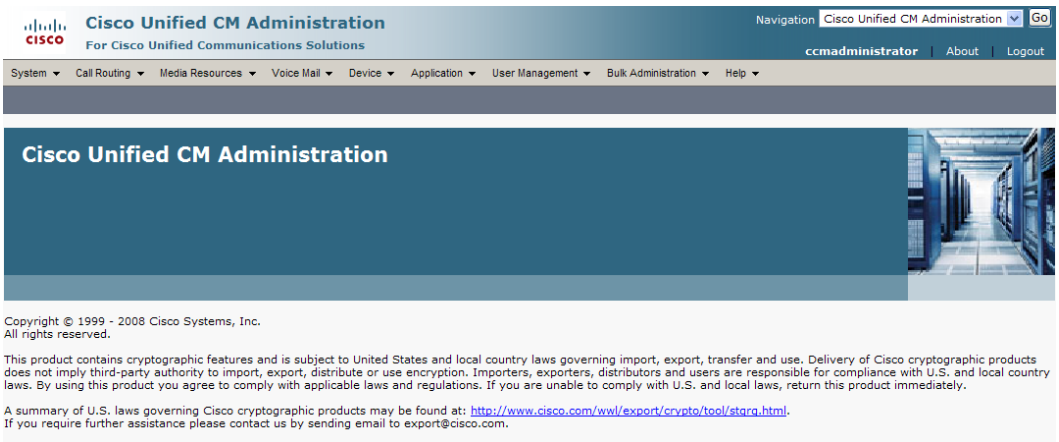


Step 2 Click the **Download** button.

Step 3 Save the PEM file to a location accessible to your CUCM server(s).

Note Leave this window open. You will come back to it.

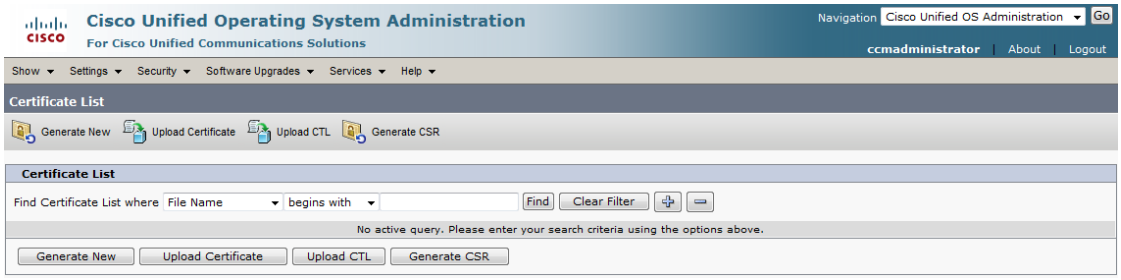
Step 4 Open a web browser and log into the administration interface of the CUCM server (the address will be similar to https://<CUCM IP Address>/ccmadmin). The Cisco Unified CM Administration page appears.



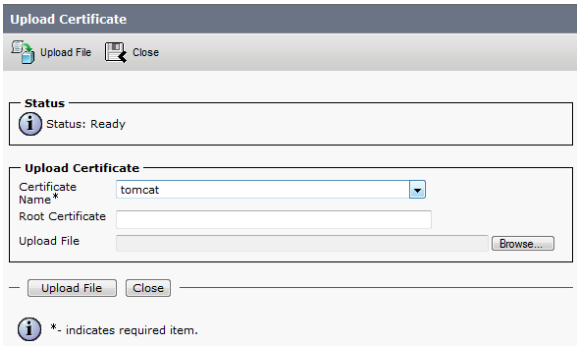
Step 5 Select **Cisco Unified OS Administration** from the **Navigation** dropdown menu and click the **Go** button. The Cisco Unified Operating System Administration page appears.

Step 6 Enter your Operating System Administration username and password in the **Username** and **Password** fields, respectively, and click the **Login** button. The Cisco Unified Operating System Administration page refreshes.

Step 7 Go to **Security** | **Certificate Management**. The Certificate List page appears.

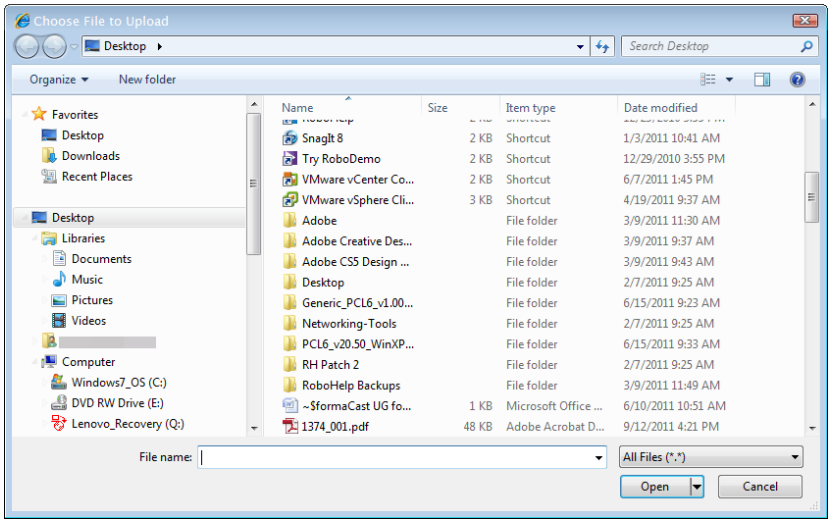


Step 8 Click the **Upload Certificate** button. The Upload Certificate window appears.



Step 9 Select **CallManager-trust** from the **Certificate Name** dropdown menu.

Step 10 Click the **Browse** button. The Choose File to Upload dialog box appears.



Step 11 Navigate to where you saved the InformaCast.pem file, select it, and click the **Open** button.

Step 12 Click the **Upload File** button on the Upload Certificate window.

Step 13 Click the **Close** button to close this window.

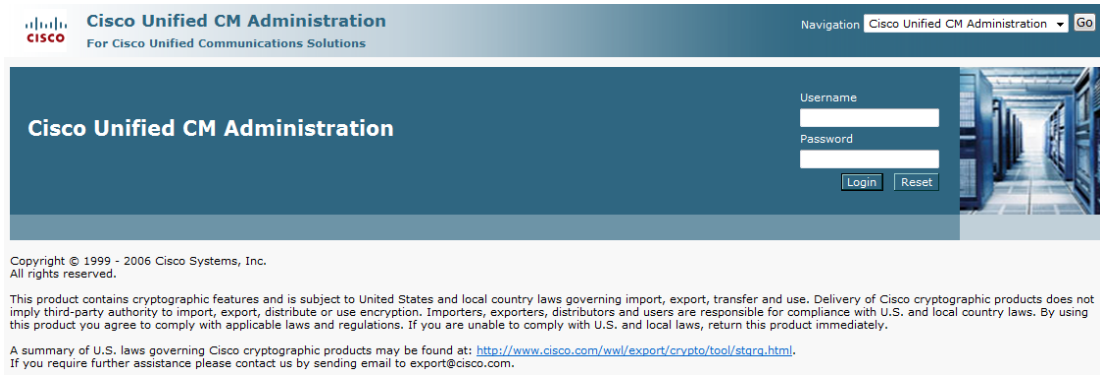
Step 14 Perform these steps for each CUCM server used by the SIP trunk.

Note TLS certificates are regenerated whenever CUCM is installed. So, if the server is restored from backup, these steps may need to be followed again. Also, InformaCast certificates are regenerated whenever InformaCast is installed or its IP address is changed, so this process will need to be followed again if InformaCast is re-installed or its IP address is changed.

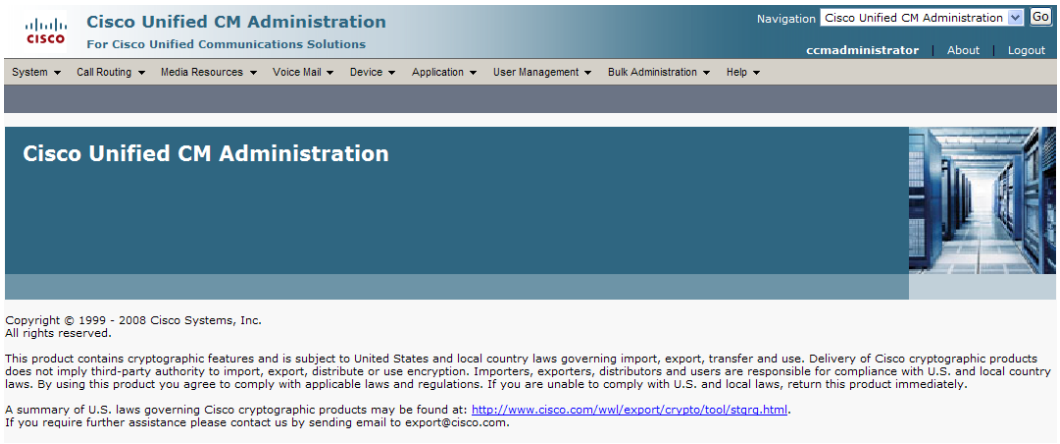
Add a SIP Trunk Security Profile That Uses TLS

Use the following steps to create a SIP trunk security profile that uses TLS.

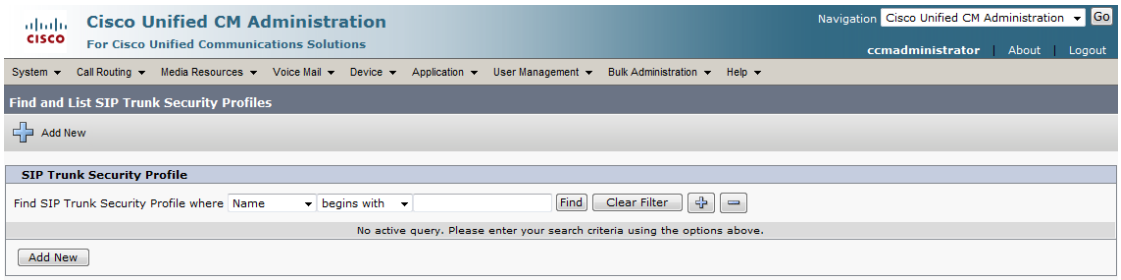
Step 1 Select **Cisco Unified CM Administration** from the **Navigation** menu and click the **Go** button. The Cisco Unified CM Administration page appears.



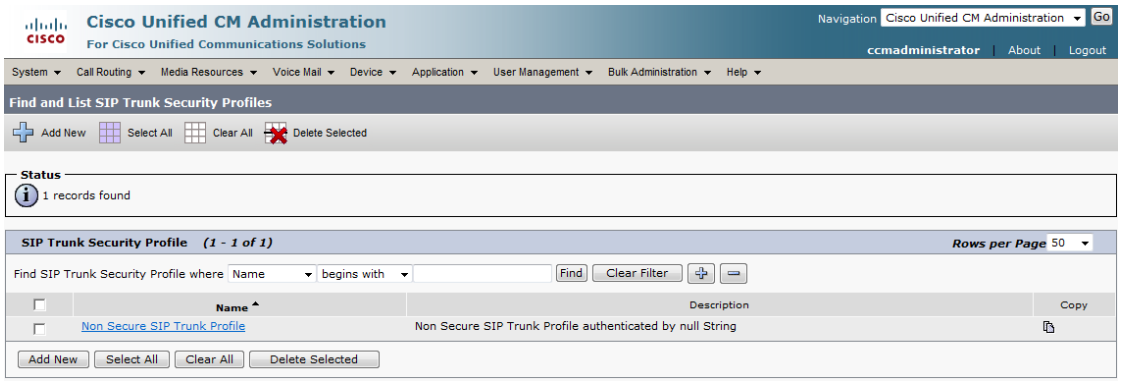
Step 2 Enter your administrative username and password in the **Username** and **Password** fields, respectively, and click the **Login** button. The Cisco Unified CM Administration page refreshes.



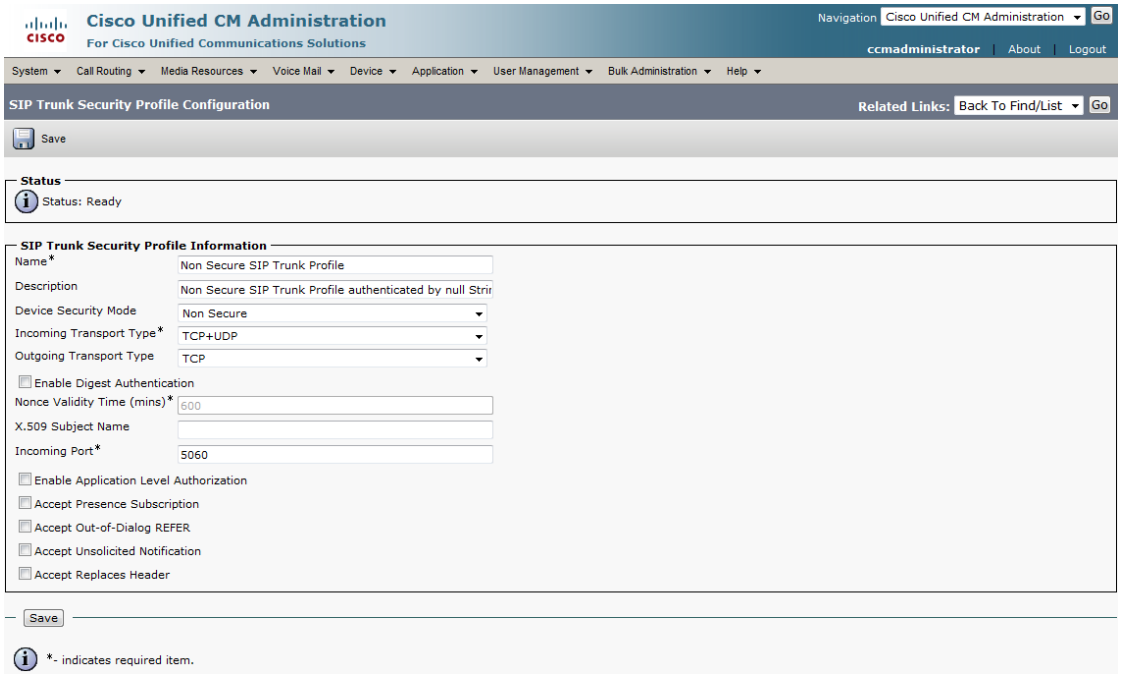
Step 3 Go to **System** | **Security** | **SIP Trunk Security Profile**. The Find and List SIP Trunk Security Profiles page appears.



Step 4 Click the **Find** button. The Find and List SIP Trunk Security Profiles page refreshes with a list of SIP trunk security profiles.



Step 5 Click the **Copy** icon in the row of your default profile, **Non Secure SIP Trunk Profile**. The SIP Trunk Security Profile Configuration page appears.



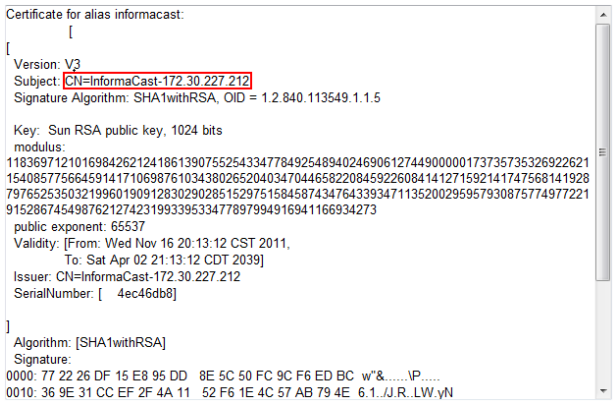
Step 6 Enter a unique name for your SIP trunk security profile in the **Name** field, e.g. InformaCastTLS.

Step 7 Enter a description of your SIP trunk security profile in the **Description** field.

Step 8 Select **Encrypted** from the **Device Security Mode** dropdown menu.

Step 9 Select **TLS** from the **Outgoing Transport Type** dropdown menu.

Step 10 Enter **InformaCast-<x.x.x.x>** in the **X.509 Subject Name** field, where <x.x.x.x> should be replaced with the IP address section of the common name assigned to InformaCast. This information can be found by viewing the SIP certificate.



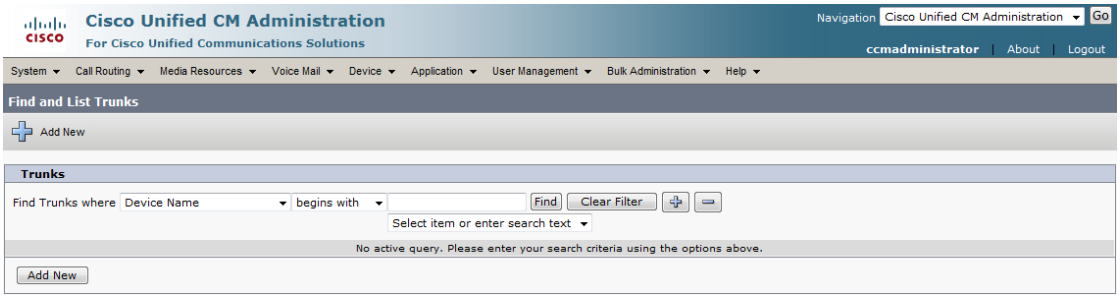
Step 11 Enter **5061** in the **Incoming Port** field.

Step 12 Click the **Save** button.

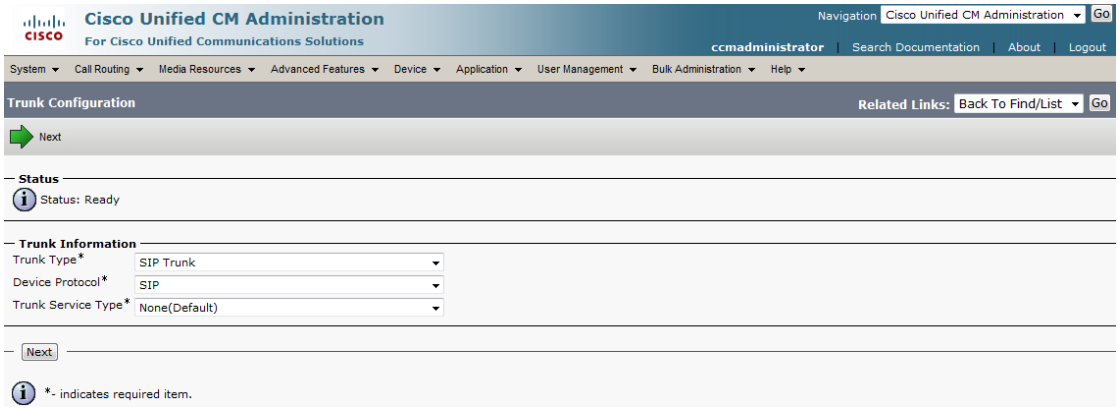
Add a SIP Trunk That Uses TLS

Use the following steps to create a SIP trunk that uses the TLS security profile you created in "Add a SIP Trunk Security Profile That Uses TLS" on page 5-15.

Step 1 Go to **Device** | **Trunk**. The Find and List Trunks page appears.



Step 2 Click the **Add New** button. The Trunk Configuration page appears.

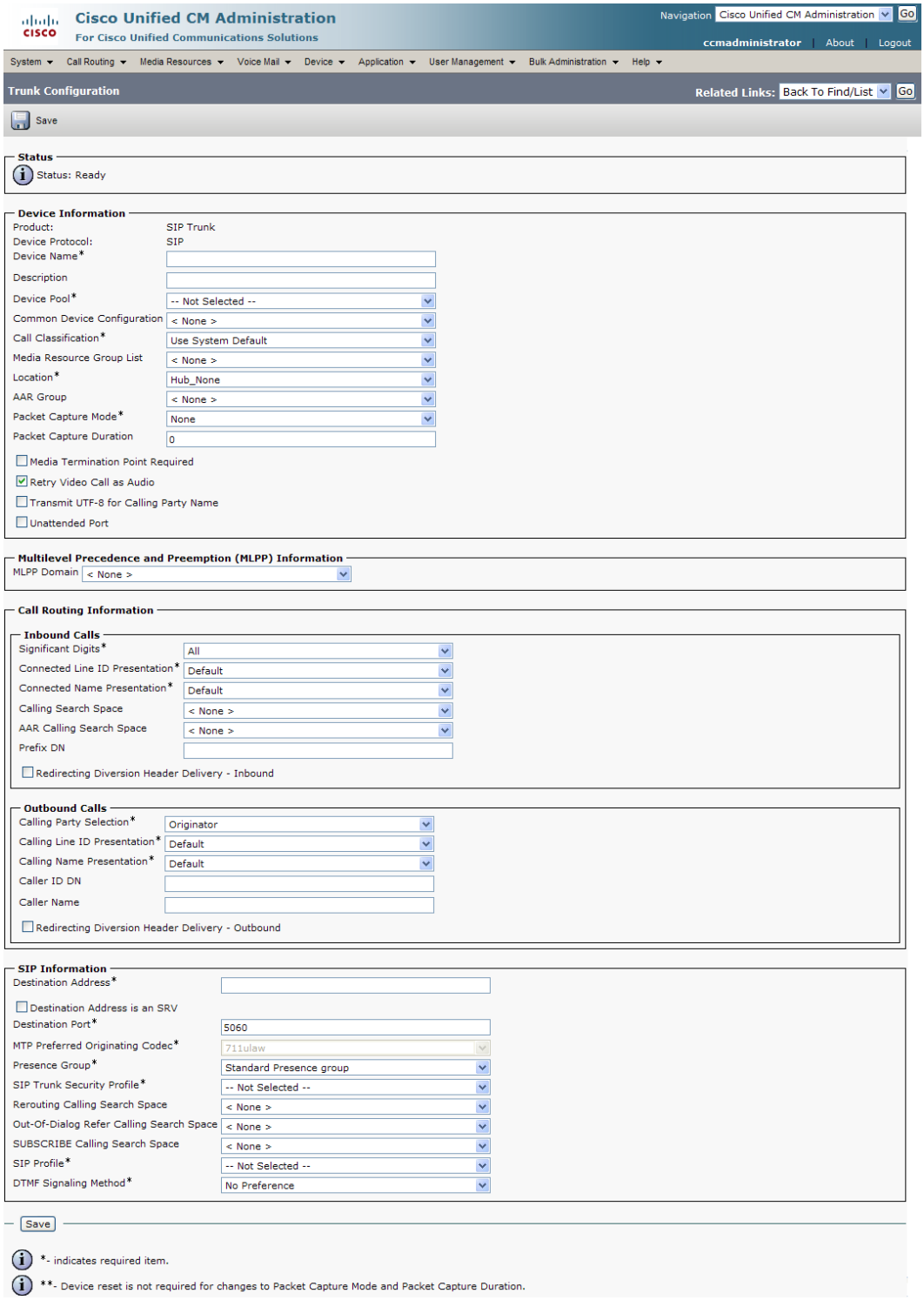


Step 3 Select **SIP Trunk** from the **Trunk Type** dropdown menu.

Step 4 Ensure that **SIP** appears as the **Device Protocol** dropdown menu selection.

Step 5 Leave the **Trunk Service Type dropdown** menu at its default of **None(Default)**.

Step 6 Click the **Next** button. The Trunk Configuration page refreshes.



Step 7 Enter a name for your SIP trunk in the **Device Name** field, e.g. InformaCastTLS.

Step 8 Select the device pool you created in "Create a Device Pool" on page 2-40 from the **Device Pool** dropdown menu.

Step 9 Scroll down to the *Inbound Calls* area and select the calling search space you created in "Create a Calling Search Space" on page 2-43 from the **Calling Search Space** dropdown menu.

Step 10 Scroll down to the *SIP Information* area and enter InformaCast's IP address in the **Destination Address** field (you entered this in Step 10 on page 5-17).

Step 11 Enter **5061** in the **Destination Port** field.

Step 12 Select the SIP trunk security profile you created in "Add a SIP Trunk Security Profile That Uses TLS" on page 5-15 from the **SIP Trunk Security Profile** dropdown menu.

Step 13 Select **Standard SIP Profile** from the **SIP Profile** dropdown menu.

Step 14 Click the **Save** button.

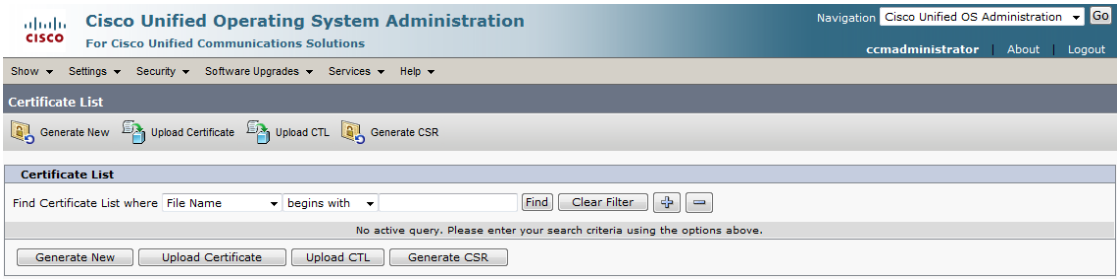
Install CUCM Certificates on InformaCast

To use the TLS protocol between CUCM and InformaCast, you will need to install CUCM's certificate on InformaCast.

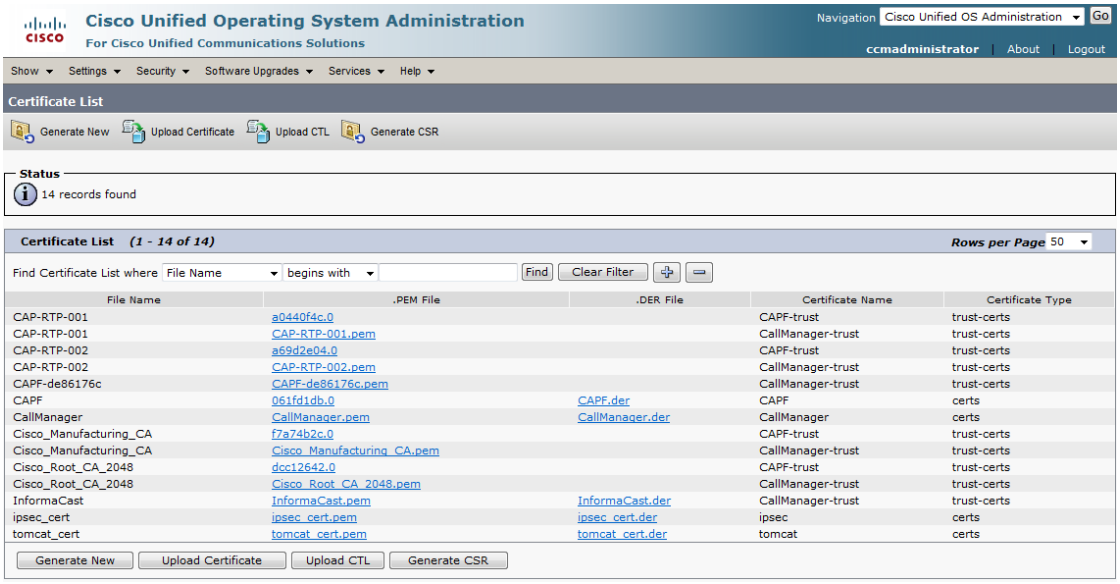
Step 1 Select **Cisco Unified OS Administration** from the **Navigation** dropdown menu and click the **Go** button. The Cisco Unified Operating System Administration page appears.

Step 2 Enter your Operating System Administration username and password in the **Username** and **Password** fields, respectively, and click the **Login** button. The Cisco Unified Operating System Administration page refreshes.

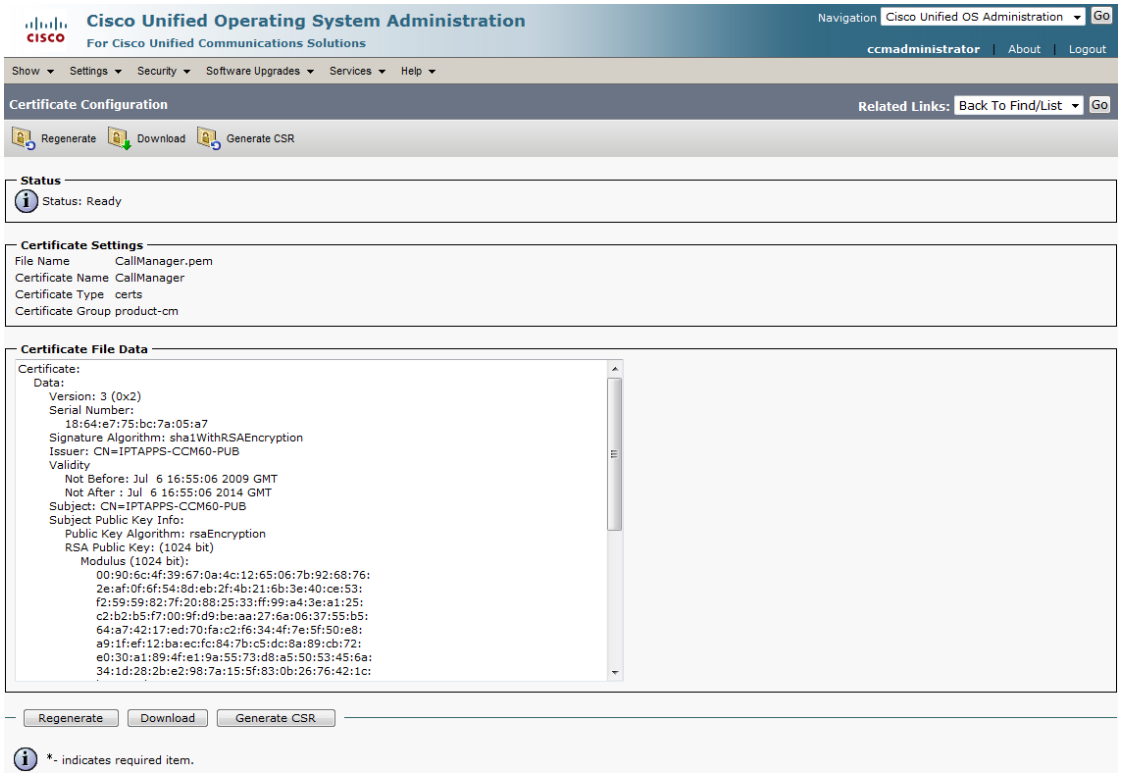
Step 3 Go to **Security** | **Certificate Management**. The Certificate List page appears.



Step 4 Click the **Find** button. The Certificate List page refreshes.

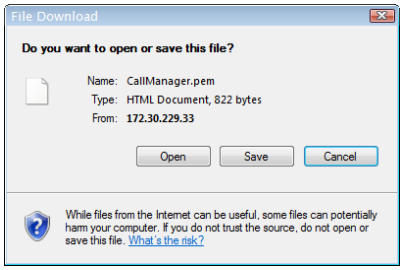


Step 5 Click the **CallManager.pem** link in the .PEM File column. The Certificate Configuration page appears.

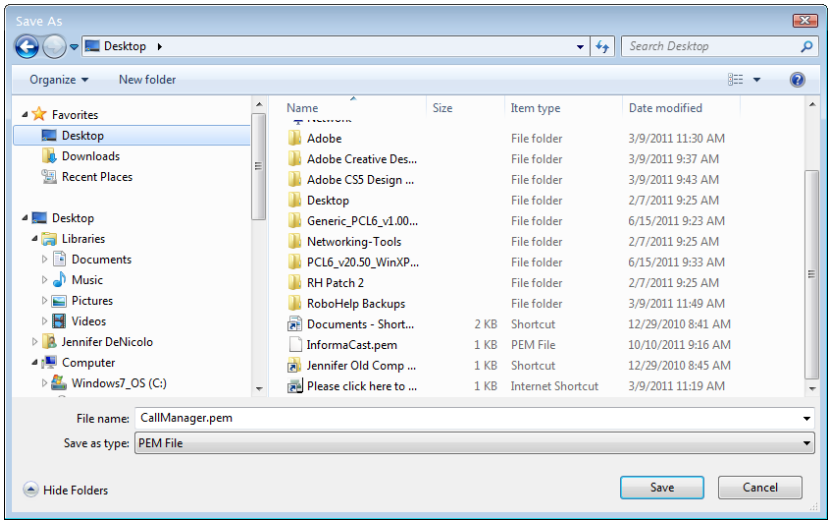


Note If you are using CUCM 10.5 and later, you will click the **Common Name** link of the certificate that displays "CallManager" in the **Certificate** column of the Certificate List table.

Step 6 Click the **Download** button. The File Download dialog box appears.



Step 7 Click the **Save** button. The Save As dialog box appears.

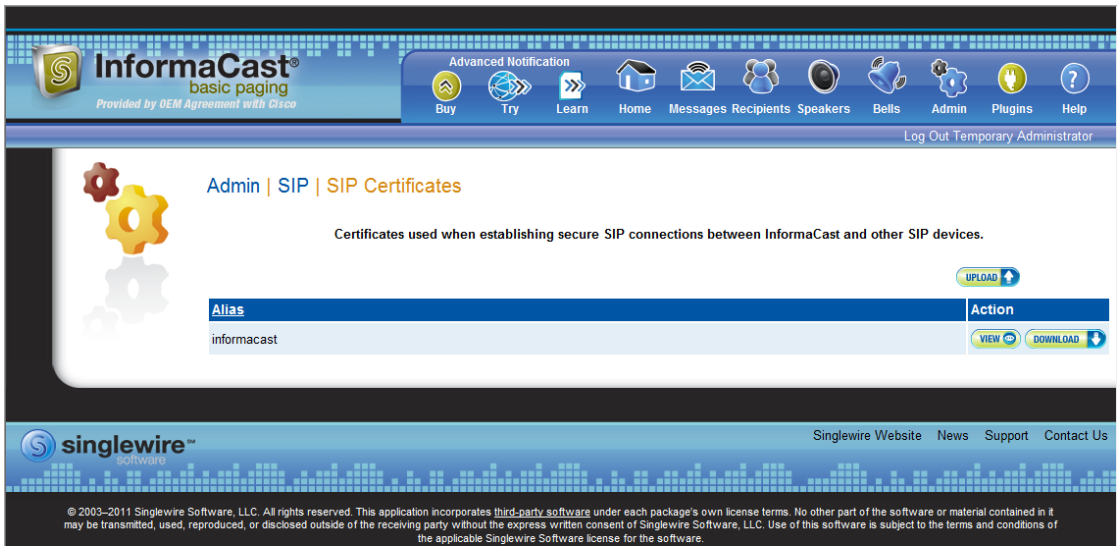


Step 8 Select a location accessible to InformaCast and click the **Save** button.

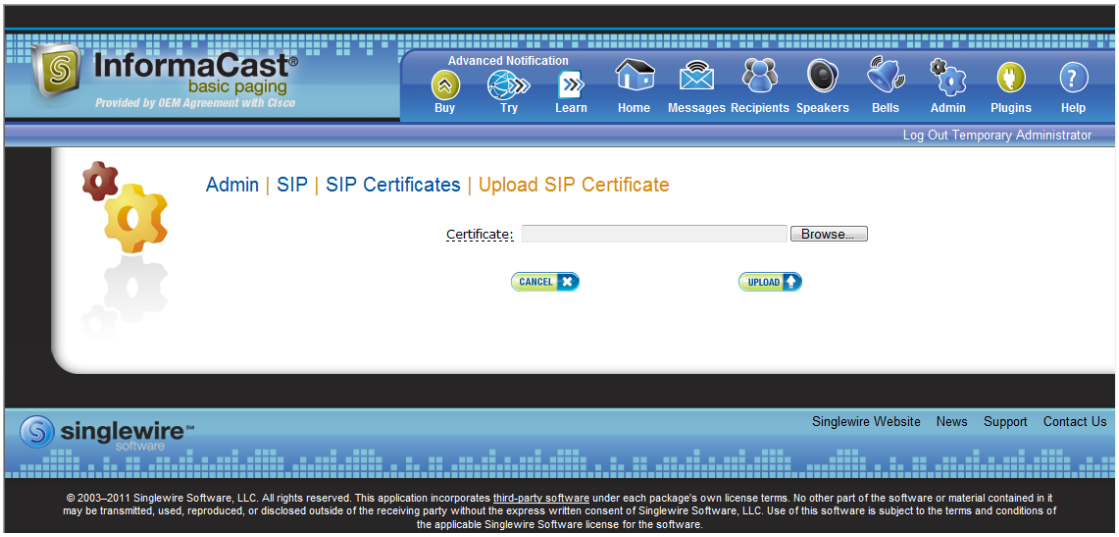
Note Perform Steps 1 through 8 for each CUCM server that will communicating to InformaCast.

Step 9 Go back to your InformaCast window.

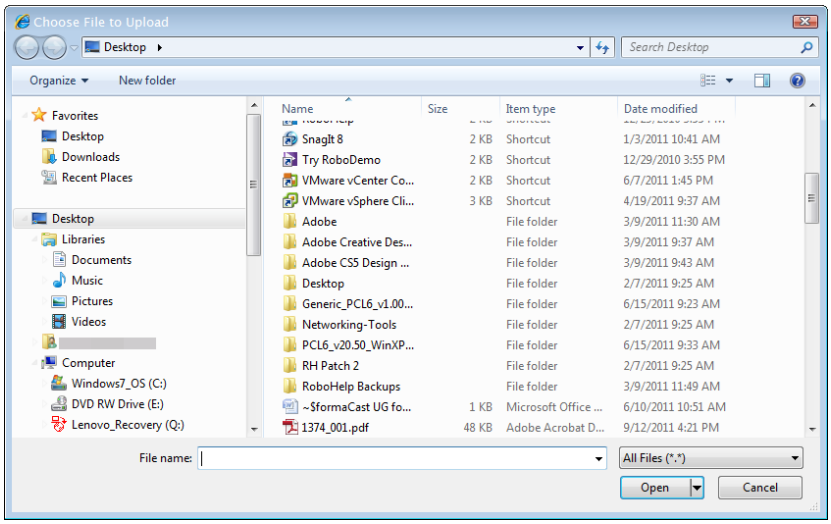
Step 10 Go to **Admin** | **SIP** | **SIP Certificates**. The SIP Certificates page appears.



Step 11 Click the **Upload** button. The Upload SIP Certificate page appears.



Step 12 Click the **Browse** button. The Choose File to Upload dialog box appears.



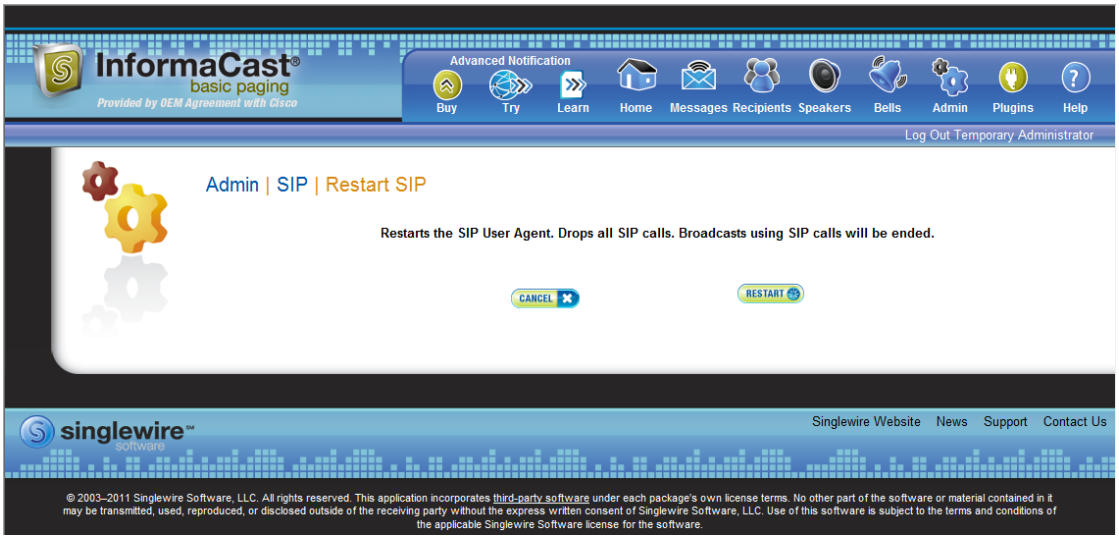
Step 13 Navigate to where you saved your CallManager.pem file, select it, and click the **Open** button.

Step 14 Click the **Upload** button.

Step 15 Perform Steps 11 through 14 for each CallManager.pem file you downloaded.

Note Any changes made to InformaCast's certificate cache, including uploads and deletions, require a SIP restart before they take effect.

Step 16 Go to **Admin** | **SIP** | **Restart SIP**. The Restart SIP page appears.



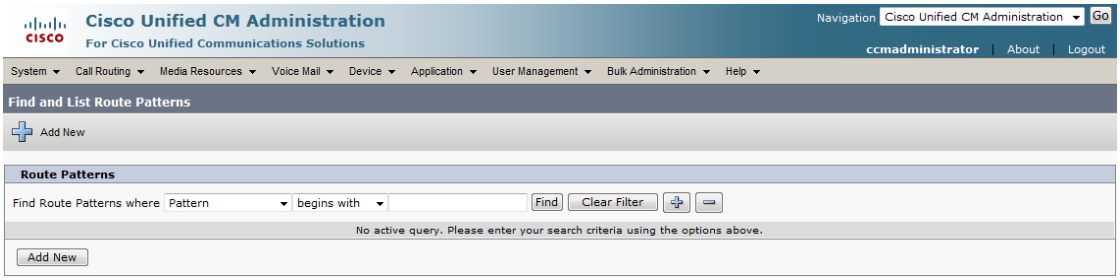
Step 17 Click the **Restart** button. It may take a few moments for SIP to restart.

Caution Restarting SIP causes all SIP calls to be dropped, i.e. any callers interacting with the DialCast IVR will have their calls dropped. Broadcasts using SIP calls will also be impacted by a restart. Live broadcasts using SIP calls will be stopped.

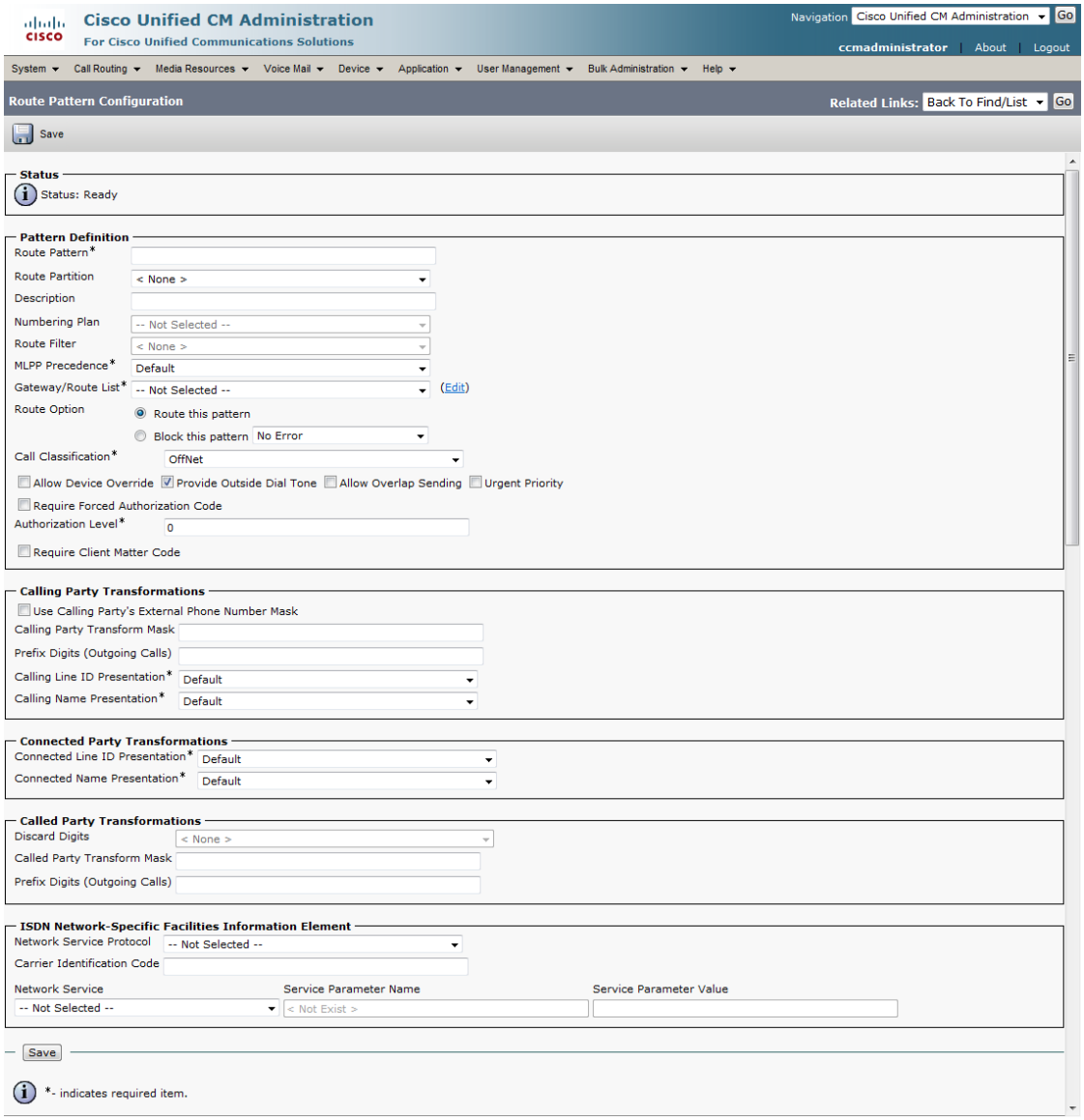
Add a Route Pattern

Use the following steps to create a route pattern that uses the SIP trunk you created in "Add a SIP Trunk" on page 5-7 or "Add a SIP Trunk That Uses TLS" on page 5-17. In your route pattern, specify a range of DNs that, when called, use the SIP trunk. Another option would be to use wild card patterns to match a range numbers.

Step 1 Go to **Call Routing** | **Route/Hunt** | **Route Pattern**. The Find and List Route Patterns page appears.



Step 2 Click the **Add New** button. The Route Pattern Configuration page appears.



Step 3 Enter a route pattern in the **Route Pattern** field, e.g. 12345.

Step 4 Select a route partition from the **Route Partition** dropdown menu. This partition should be reachable from the phones to which you will be sending DialCasts.

Step 5 Enter a description of your route pattern in the **Description** field.

Step 6 Select the SIP trunk you created in "Add a SIP Trunk" on page 5-7 or "Add a SIP Trunk That Uses TLS" on page 5-17 from the **Gateway/Route List** dropdown menu.

Step 7 Select the **Route This Pattern** radio button.

Step 8 Select **OnNet** from the **Call Classification** dropdown menu.

Step 9 Deselect the **Provide Outside Dial Tone** checkbox.

Step 10 Click the **Save** button.

Allow/Deny SIP Access to InformaCast

SIP access permits you to either allow or deny incoming SIP calls. The all-or-nothing scope of these buttons can be tuned by adding exceptions that counteract their setting. For example, when all incoming SIP calls are denied, exceptions serve to allow calls to be answered from those hosts specified by them. On the other hand, when all incoming SIP calls are allowed, exceptions serve to reject calls from those hosts specified by them.

SIP is processed through InformaCast in the following manner: a SIP client sends an INVITE message to a SIP peer when it wants to start or modify a call with that peer. A Via header containing the host's address is added to the request when the client sends the INVITE message. As the message is routed to its destination, additional Via headers are added at each hop. When the message arrives at its final destination, one or more Via headers are present in the request. Via headers are used by SIP to ensure that responses are routed back to the caller through the same hosts that participated in sending the request. InformaCast uses the host in the top Via header when determining if the INVITE should be accepted or denied. The top Via header represents the last host that handled the request before it reached InformaCast.

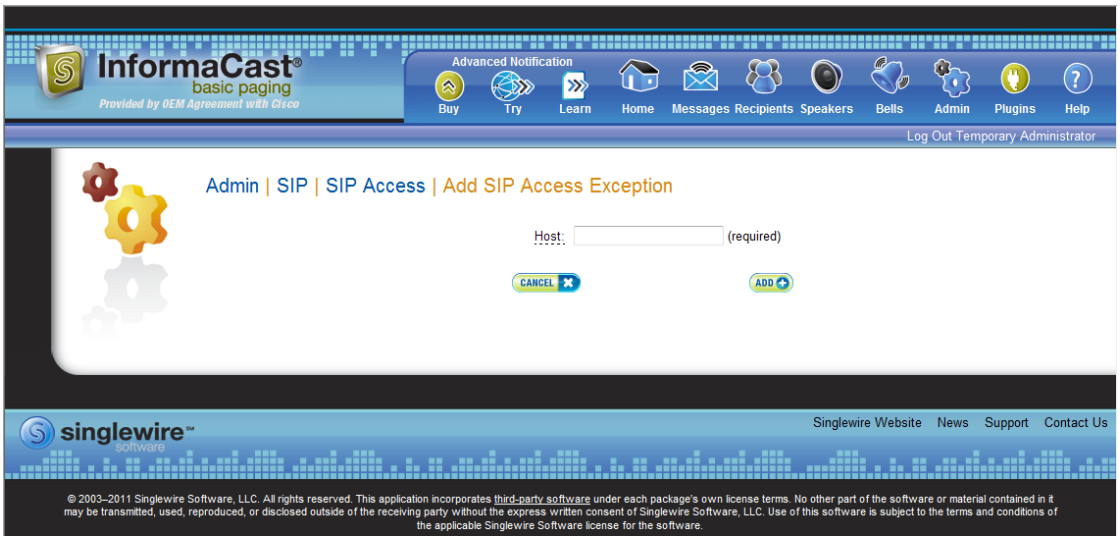
Note Changes made to SIP access take effect immediately and do not require a restart of InformaCast.

Step 1 Go to **Admin** | **SIP** | **SIP Access**. The SIP Access page appears.

Note By default, SIP access is denied.

Step 2 Select the **Allow** radio button to allow SIP calls to be answered.

Step 3 Leave the **Deny** radio button selected and click the **Add** button to add exceptions to the SIP calls that are denied. The Add SIP Access Exception page appears.



Step 4 Enter the IP address or fully qualified domain name of the host you want to includes in the **Host** field.

Tip When defining exceptions, make sure to specify the host that directly sends the INVITE request to InformaCast. This may be a SIP proxy server if proxies stand between InformaCast and the calling host.

Step 5 Click the **Add** button. The SIP Access page appears with your new exception noted.

Note If you had elected to allow SIP access by selecting the **Allow** radio button, you can still deny some SIP access by adding exceptions, as was illustrated in Step 5. In that case, your SIP Access page would appear as follows:

Step 6 Click the **Update** button to save your changes.

Tip Click the **Restore** button to return InformaCast to its default settings.

Enable SIP Authentication for InformaCast

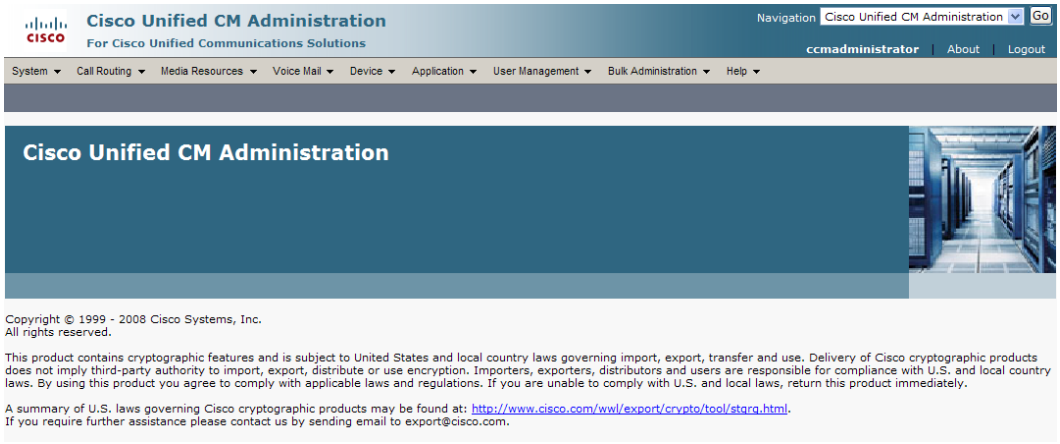
Note This section is optional depending on the security of your environment.

SIP authentication allows you to enable or disable digest authentication of incoming SIP requests. SIP authentication works in the following manner: SIP provides a stateless, challenge-based mechanism for authentication that is based on authentication in HTTP. Any time that a SIP device receives a request (with the exception of ACK messages or the CANCEL method), it may challenge the initiator of the request to provide assurance of its identity. Once the originator has been identified, the recipient of the request should ascertain whether or not this user is authorized to make the request in question.

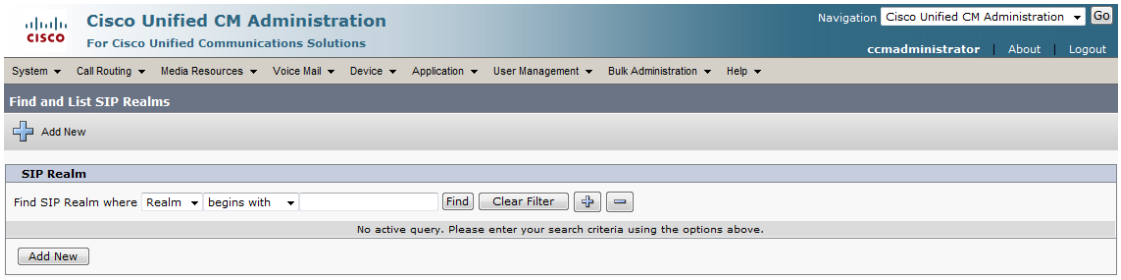
InformaCast responds with an UNAUTHORIZED (401) HTTP status when a request either does not contain an Authorization header or uses an Authorization header containing invalid data. The response sent to the peer contains a WWWAuthenticate header specifying the SIP realm for which credentials

must be provided. The peer must send another request containing a valid Authorization header before InformaCast will accept it. The header must use the same credentials that are given on this page and the same SIP realm.

Step 1 Open a web browser and log into the administration interface of the CUCM server (the address will be similar to https://<CUCM IP Address>/ccmadmin). The Cisco Unified CM Administration page appears.



Step 2 Go to **User Management** | **SIP Realm**. The Find and List SIP Realms page appears.



Step 3 Click the **Find** button. The Find and List SIP Realms page appears with a list of your configured SIP realms OR, if you have no SIP realms set up, it will display no records.

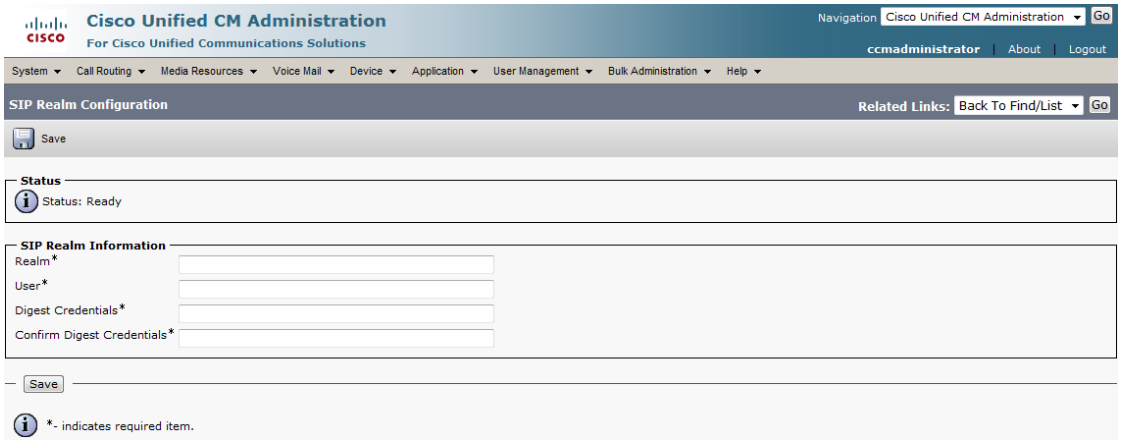
If you have a SIP realm you'd like to use, select it and make note of the values that appear in the following fields on the SIP Realm Configuration page:

- Realm
- User
- Digest Credentials

Skip to Step 10 on page 5-32.

If you have no realms set up, continue with the following steps.

Step 4 Click the **Add New** button. The SIP Realm Configuration page appears.



Step 5 Enter **InformaCast** in the **Realm** field.

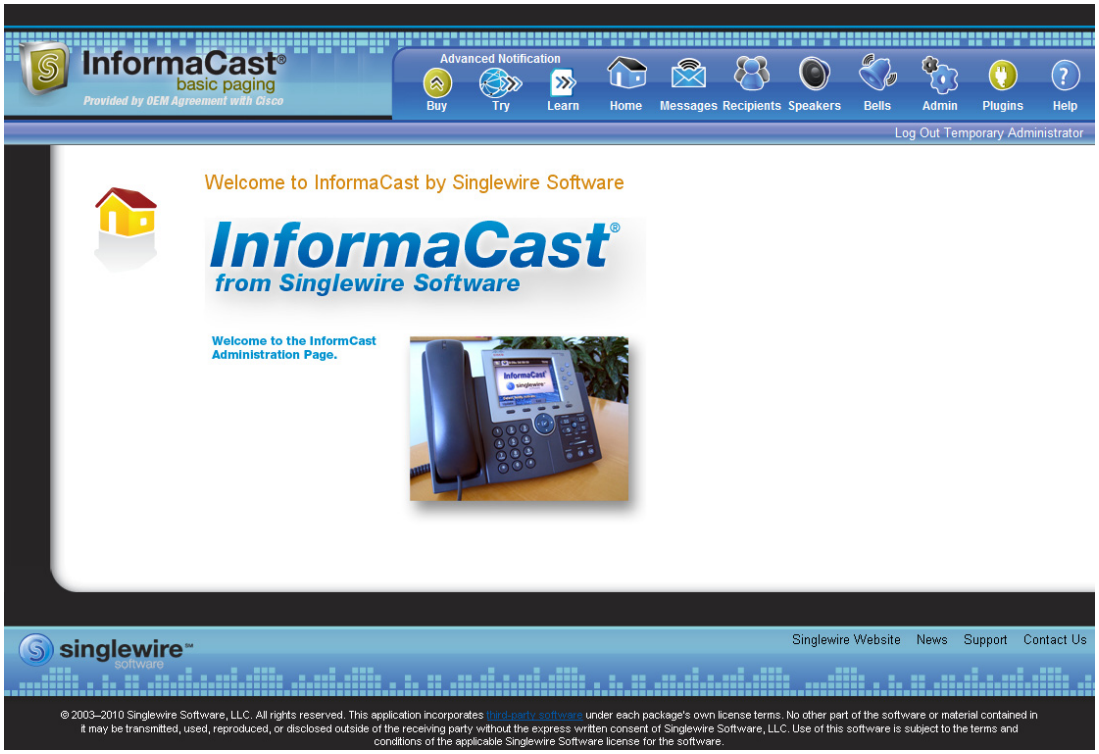
Step 6 Enter **sipuser** in the **User** field.

Step 7 Enter **changeMe** in the **Digest Credentials** field.

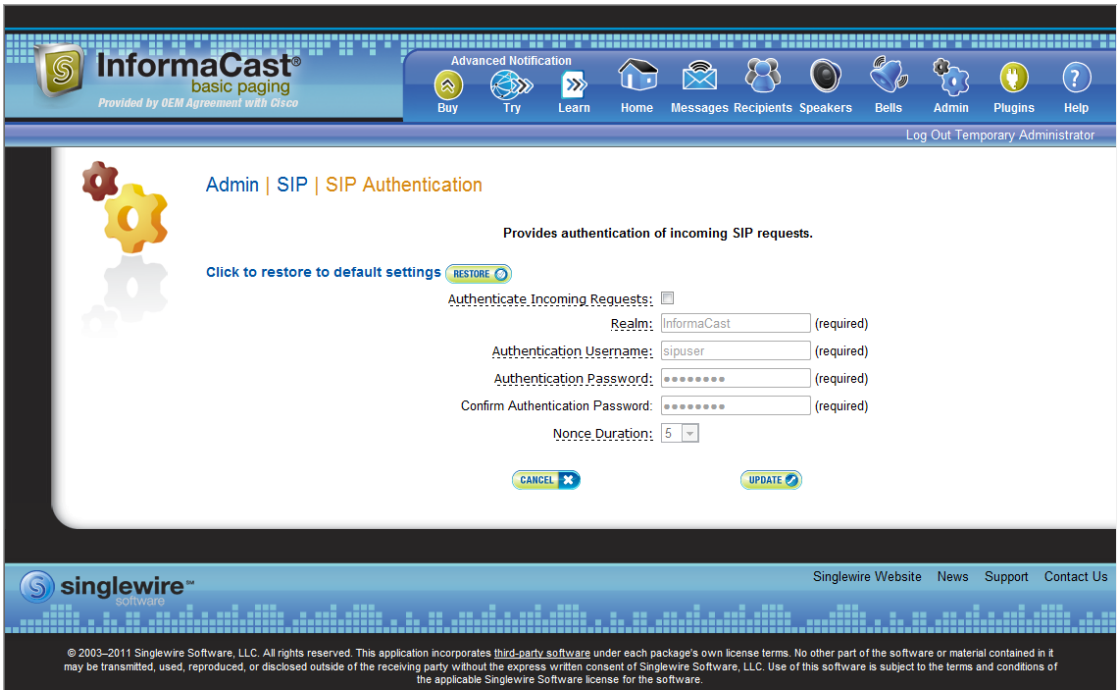
Step 8 Enter **changeMe** in the **Confirm Digest Credentials** field.

Step 9 Click the **Save** button.

Step 10 Log into InformaCast (see "Log into InformaCast" on page 10-3 for specific steps). The InformaCast homepage appears.



Step 11 Go to **Admin** | **SIP** | **SIP Authentication**. The SIP Authentication page appears.



Note By default, SIP authentication is disabled.

Step 12 Select the **Authenticate Incoming Requests** checkbox to enable SIP authentication.

Note The fields on this page come pre-filled. You only need to edit them if you want to change them. By default, the realm is named InformaCast, the authentication username is sipuser, and the authentication password is changeMe.

Step 13 Ensure that the values in the **Realm**, **Authentication Username**, **Authentication Password**, and **Confirm Authentication Password** fields match the values you entered in Steps 5 through 8.

Step 14 Select the length of time InformaCast should allow for a single authentication request from the **Nonce Duration** dropdown menu.

Note The nonce value is used by the digest authentication scheme to provide additional security. Clients making requests will use it until it is deemed by InformaCast to be stale.

Step 15 Click the **Update** button to save your changes.

Enable Digest Authentication with SIP User Credentials

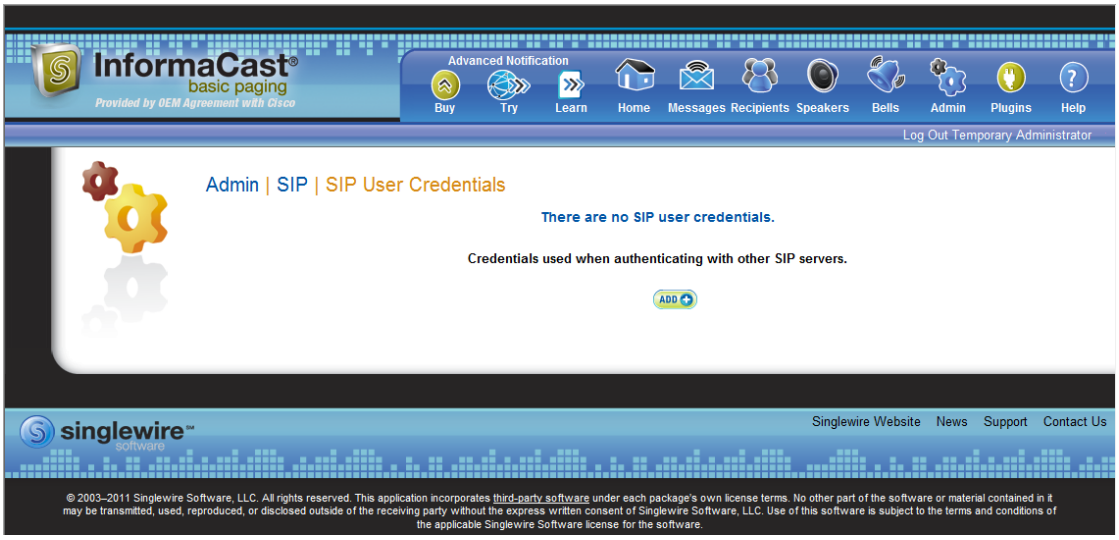
Note This section is optional depending on the security of your environment.

SIP peers may challenge InformaCast to provide valid credentials for its SIP realm when registering or terminating a SIP call. Lack of valid credentials for a challenging realm means that requests to it will be rejected. You should enter valid credentials for each SIP realm where you expect InformaCast to be challenged.

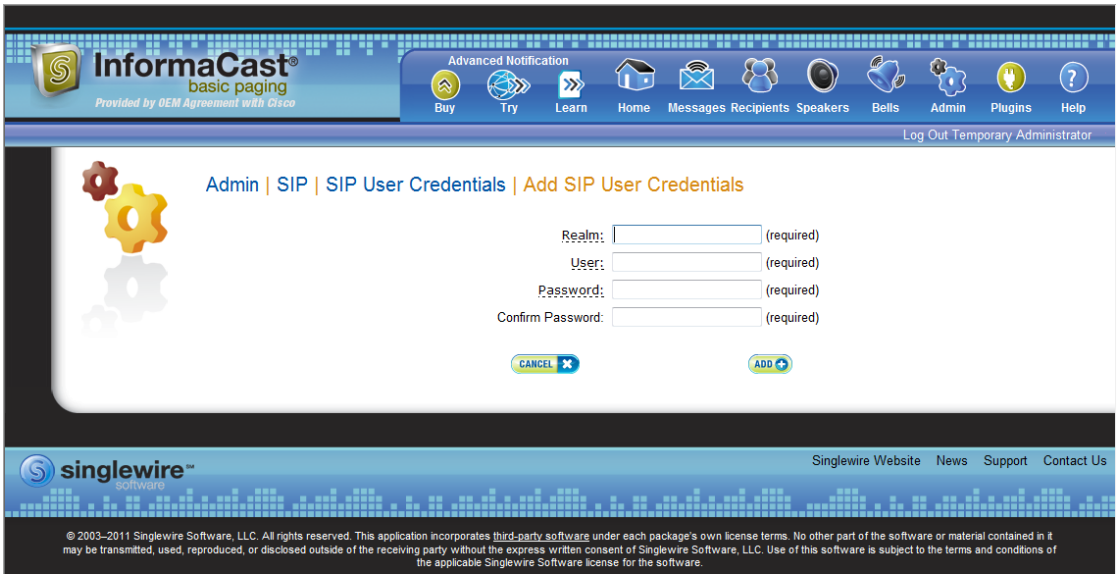
Add SIP User Credentials

Use the following steps to add SIP user credentials to InformaCast.

Step 1 Go to **Admin** | **SIP** | **SIP User Credentials**. The SIP User Credentials page appears.



Step 2 Click the **Add** button. The Add SIP User Credentials page appears.



Step 3 Enter the name of your SIP peer's SIP realm in the **Realm** field.

Step 4 Enter the username associated with the SIP peer's SIP realm in the **User** field.

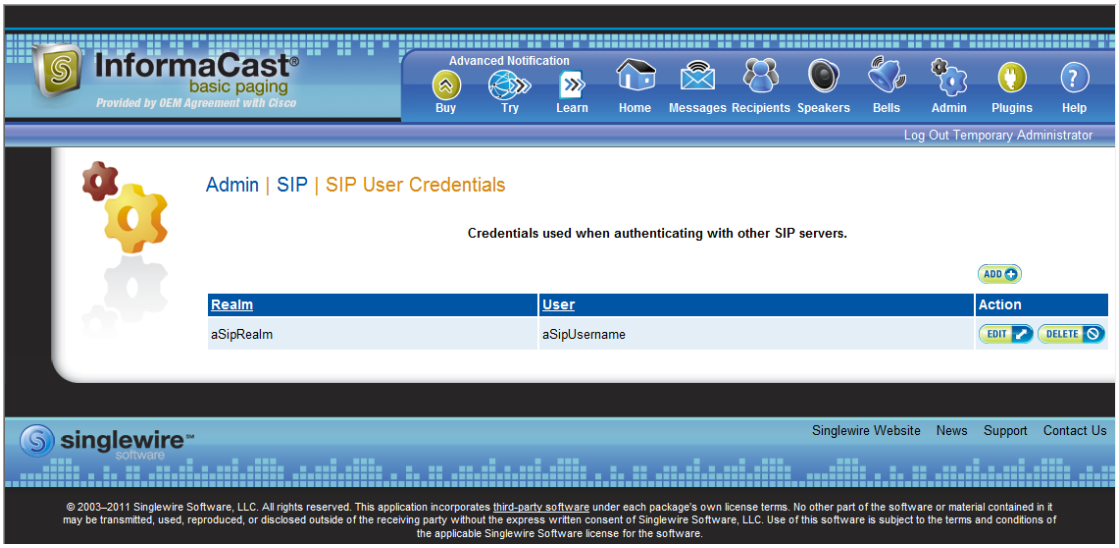
Step 5 Enter the password of the username associated with the SIP peer's SIP realm in the **Password** and **Confirm Password** fields.

Step 6 Click the **Add** button.

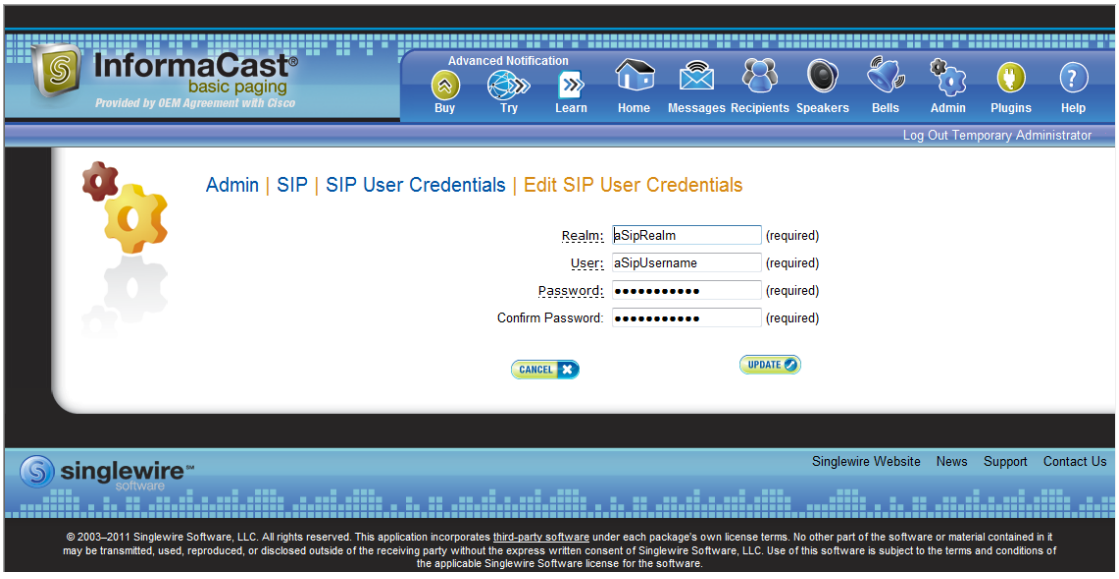
Edit SIP User Credentials

Once you have added SIP user credentials to InformaCast, you may want to edit their information.

Step 1 Go to **Admin** | **SIP** | **SIP User Credentials**. The SIP User Credentials page appears.



Step 2 Click the **Edit** button next to the user credentials you want to modify. The Edit SIP User Credentials page appears.



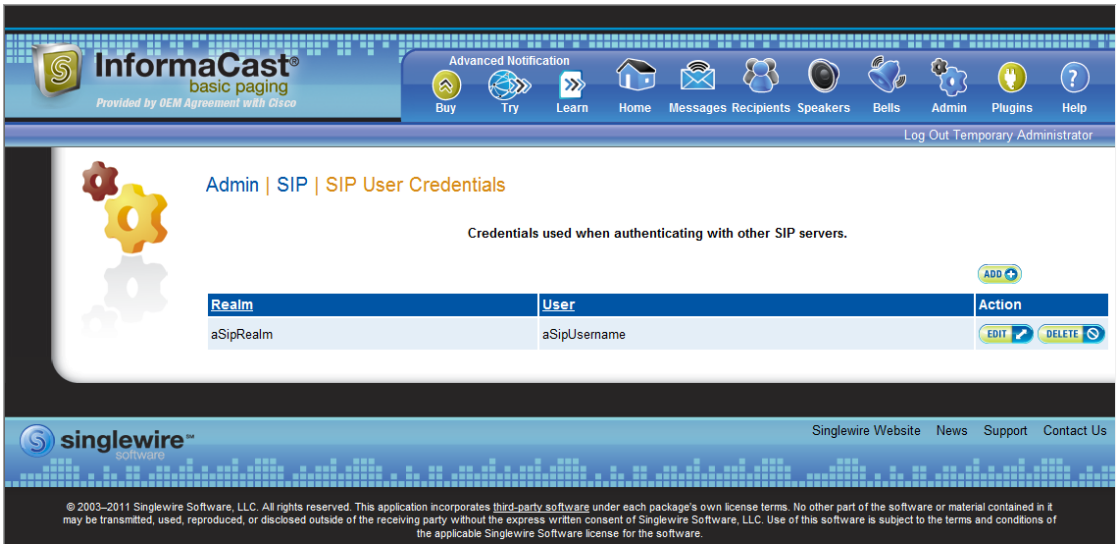
Step 3 Make your desired changes.

Step 4 Click the **Update** button to save your changes.

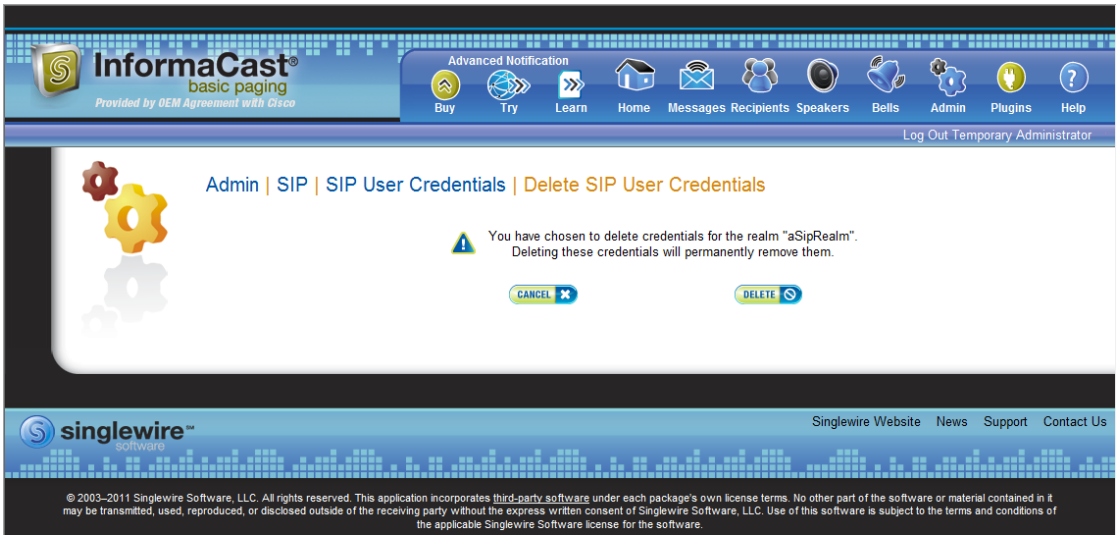
Delete SIP User Credentials

As your needs change, you may want to remove SIP user credentials from InformaCast.

Step 1 Go to **Admin** | **SIP** | **SIP User Credentials**. The SIP User Credentials page appears.



Step 2 Click the **Delete** button next to the SIP user credentials you want to delete. The Delete SIP User Credentials page appears.



Step 3 Click the **Delete** button. Your SIP user credentials are removed.

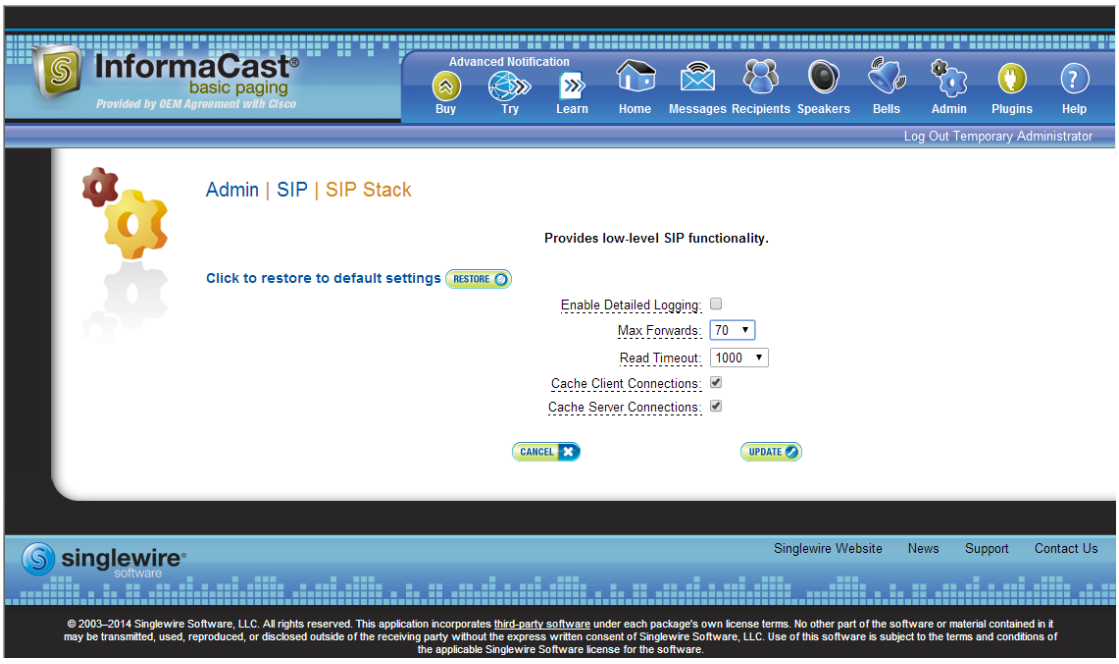
Manage the SIP Stack

InformaCast uses the National Institute of Standards and Technology (NIST) SIP stack to provide it with basic SIP functionality. The SIP stack provides InformaCast with fundamental low-level SIP functionality such as transaction handling, dialogs, utilities for SIP headers, maintenance of SIP timers, etc.

Tip The logs generated for the SIP stack (SIP Stack Log and SIP Stack Debug Log) are accessible through the Support page (**Help** | **Support**).

Caution Caution should be exercised when enabling detailed logging in the SIP stack because of the large size of the log files it produces and the degradation of stack performance due to extensive logging. Detailed logging is intended to be used only when troubleshooting SIP problems and should not be enabled for any longer than necessary. Two log files are generated in the InformaCast logs directory: sipStackDebug.log and sipStackServer.log.

Step 1 Go to **Admin** | **SIP** | **SIP Stack**. The SIP Stack page appears.



Note Most values on this page should not ever need to be changed. The value most likely to be changed is the logging checkbox.

The following fields/dropdown menus can be found on the SIP Stack page:

- **Enable Detailed Logging.** Controls the SIP stack logging level. When checked, extensive and detailed logging of the SIP stack's activities are enabled, likely resulting in decreased performance. When unchecked, logging is confined to reporting problems encountered by the SIP stack, and its ordinary activities. Unless told otherwise by Support personnel, it is recommended that this checkbox remain unchecked.
- **Max Forwards.** The maximum number of forwards allowed while a SIP message is being routed to its destination.
- **Read Timeout.** The read timeout for TCP connections, in milliseconds.
- **Cache Client Connections.** Controls whether the SIP stack frees the resources associated with a client transaction when it reaches its terminated state. When checked, the SIP stack will cache a transaction's resources when it terminates, thereby improving the SIP stack's performance.
- **Cache Server Connections.** Controls whether the SIP stack frees the resources associated with a server transaction when it reaches its terminated state. When checked, the SIP stack will cache a transaction's resources when it terminates, thereby improving the SIP stack's performance.

Step 2 Make your desired changes and click the **Update** button or click the **Restore** button to return to your default settings.

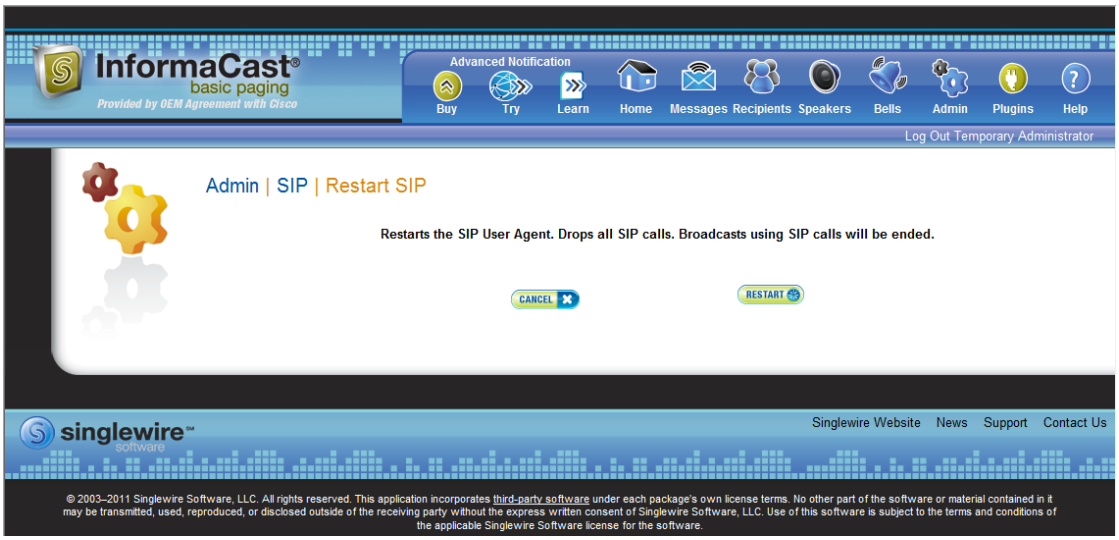
Caution You'll need to restart SIP. Restarting SIP causes all SIP calls to be dropped, i.e. any callers interacting with the DialCast IVR will have their calls dropped. Broadcasts using SIP calls will also be impacted by a restart. Live broadcasts using SIP calls will be stopped.

Restart SIP

Changes to the SIP stack or certificates require a restart before they take effect. Other SIP changes, such as changes to access and authentication, take effect as soon as they are made.

Caution Restarting SIP causes all SIP calls to be dropped, i.e. any callers interacting with the DialCast IVR will have their calls dropped. Broadcasts using SIP calls will also be impacted by a restart. Live broadcasts using SIP calls will be stopped.

Step 1 Go to **Admin** | **SIP** | **Restart SIP**. The Restart SIP page appears.



Step 2 Click the **Restart** button. It may take a few moments for SIP to restart.

Manage DialCasts

InformaCast's DialCast functionality allows you to dial a SIP number to trigger an InformaCast broadcast. InformaCast is notified for each SIP call it receives. The configured dialing pattern that matches the dialed DN determines which InformaCast message should be sent and which recipient groups should receive it.

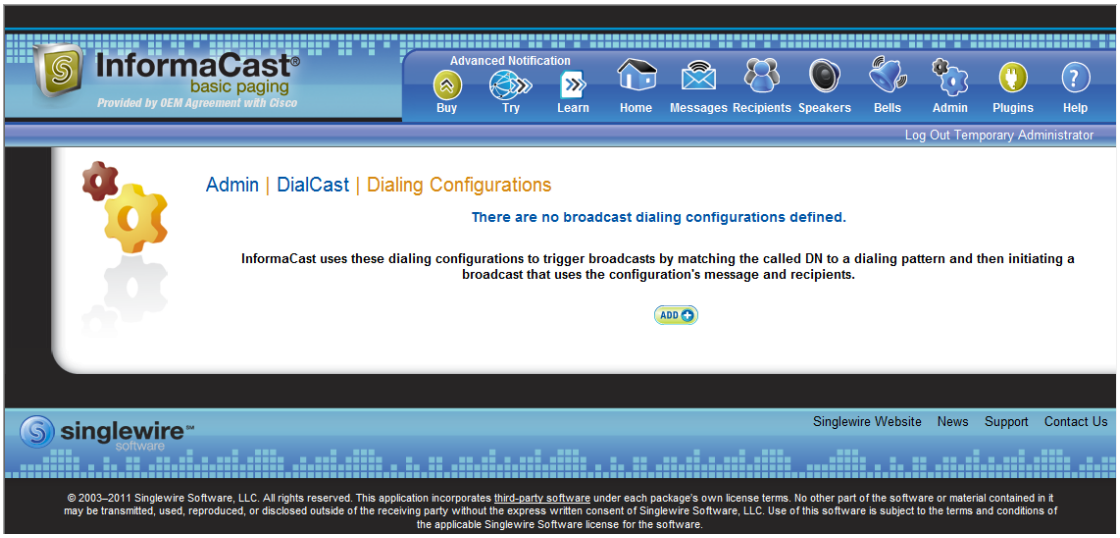
In order to use DialCasts, you must first configure Session Initiation Protocol (SIP), which is supported by a growing number of PBXs and telephony devices. SIP provides InformaCast with the capability to receive SIP calls as well as register with SIP, allowing other SIP devices to locate and call InformaCast. See "Manage SIP Functionality" on page 5-4 for more information.

Once you've finished configuring SIP, you can add and/or modify broadcast dialing configurations, which determine to which recipient group to broadcast based on the number that is dialed.

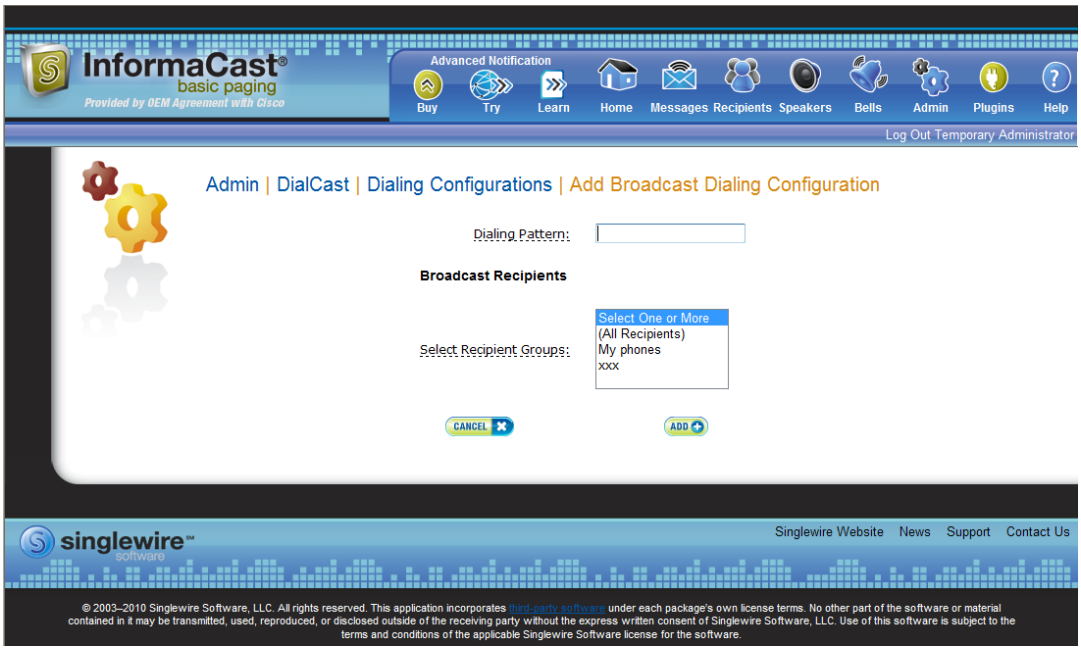
Add a Broadcast Dialing Configuration

Before you can send DialCasts, you must add broadcast dialing configurations to InformaCast.

Step 1 Go to **Admin** | **DialCast** | **Dialing Configurations**. The Dialing Configurations page appears.



Step 2 Click the **Add** button. The Add Broadcast Dialing Configuration page appears.



Step 3 Enter a dialing pattern (e.g. 8811) for a SIP trunk used with InformaCast in the **Dialing Pattern** field. You will need to add at least one dialing pattern configuration for each SIP trunk used with InformaCast.

Tip It is possible to use * or #, when setting up a dial pattern, but you must add \ before the character so that InformaCast doesn't treat it as a wildcard. For example, **1 would have a dial pattern of **1.

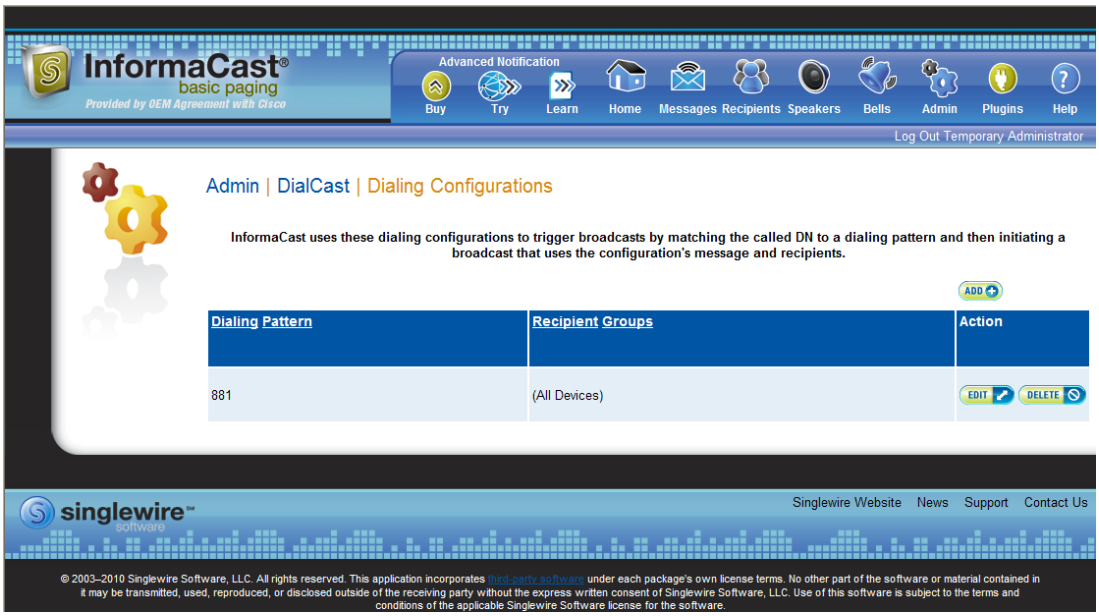
Step 4 Select a recipient group or groups from the **Select Recipient Groups** field.

Step 5 Click the **Add** button to save your current dialing pattern configuration.

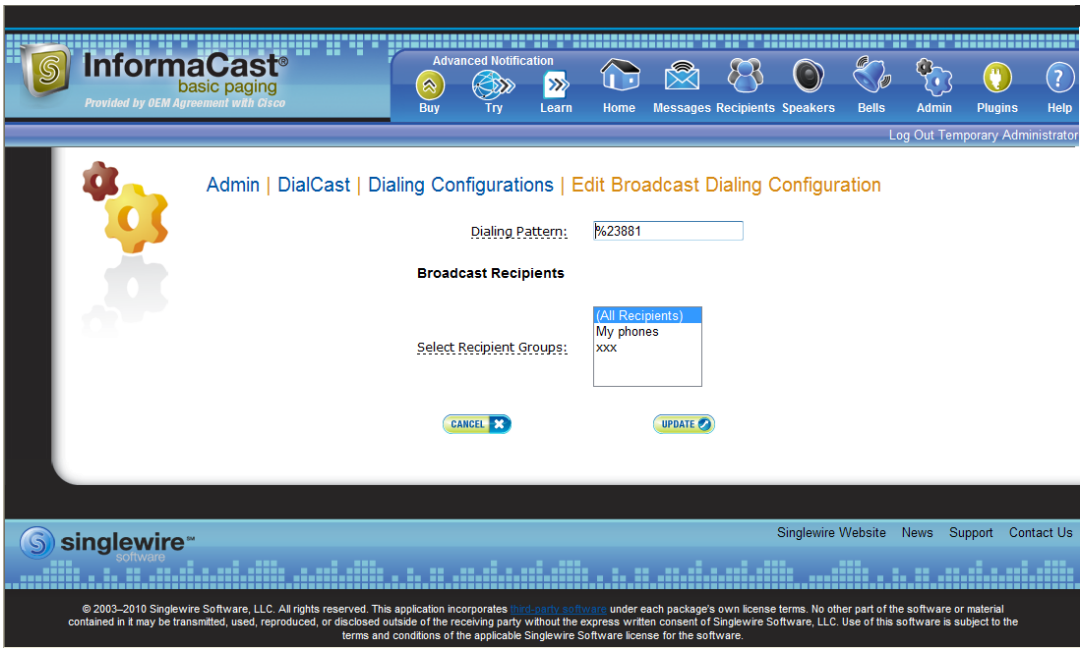
Edit a Broadcast Dialing Configuration

Once you have added dialing configurations, you may need to modify them.

Step 1 Go to **Admin** | **DialCast** | **Dialing Configurations**. The Dialing Configurations page appears.



Step 2 Click the **Edit** button next to the dialing configuration you want to change. The Edit Broadcast Dialing Configuration page appears.



Step 3 Make your changes.

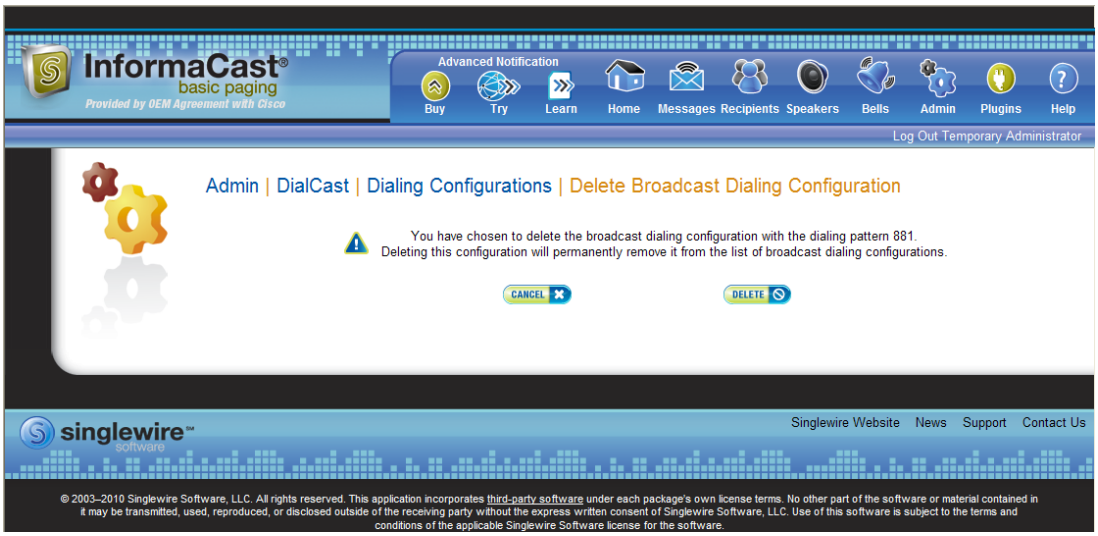
Step 4 Click the **Update** button.

Delete a Broadcast Dialing Configuration

As your needs change, you may want to delete older dialing configurations from InformaCast.

Step 1 Go to **Admin** | **DialCast** | **Dialing Configurations**. The Dialing Configurations page appears.

Step 2 Click the **Delete** button next to the dialing configuration you want to delete. The Delete Broadcast Dialing Configuration page appears.



Step 3 Click the **Delete** button. Your broadcast dialing configuration is deleted.

Send a DialCast/Broadcast

With Basic InformaCast functionality, you only have the ability to send Live Audio messages through InformaCast's DialCast functionality. DialCasts are broadcasts triggered by dialing a SIP number configured with dialing pattern that determines which InformaCast message should be sent and which recipient groups should receive it.

Tip Before you can send a DialCast/broadcast, you must have a SIP trunk configured (see "Configure a SIP Trunk" on page 5-4) as well as DialCasts (see "Manage DialCasts" on page 5-40).

To send a Live Audio broadcast, dial a directory number on your Cisco IP phone that corresponds to a broadcast dialing configuration (see "Add a Broadcast Dialing Configuration" on page 5-41), which is tied to a SIP trunk (see "Configure a SIP Trunk" on page 5-4) in CUCM. The call will be processed, and as soon as all the recipients specified in your broadcast dialing configuration have been activated (minus the phones already in use), you will be broadcasting live.

With Advanced InformaCast functionality, there are eight types of messages that can be grouped into four separate broadcast categories:

- Text, Text and Pre-recorded Audio, and Pre-recorded Audio messages
- Text and Live Audio and Live Audio messages
- Text and Ad-hoc Audio and Ad-hoc Audio messages
- Talk and Listen messages

For more information on these message types, see the table in "Manage Messages" on page 5-1.

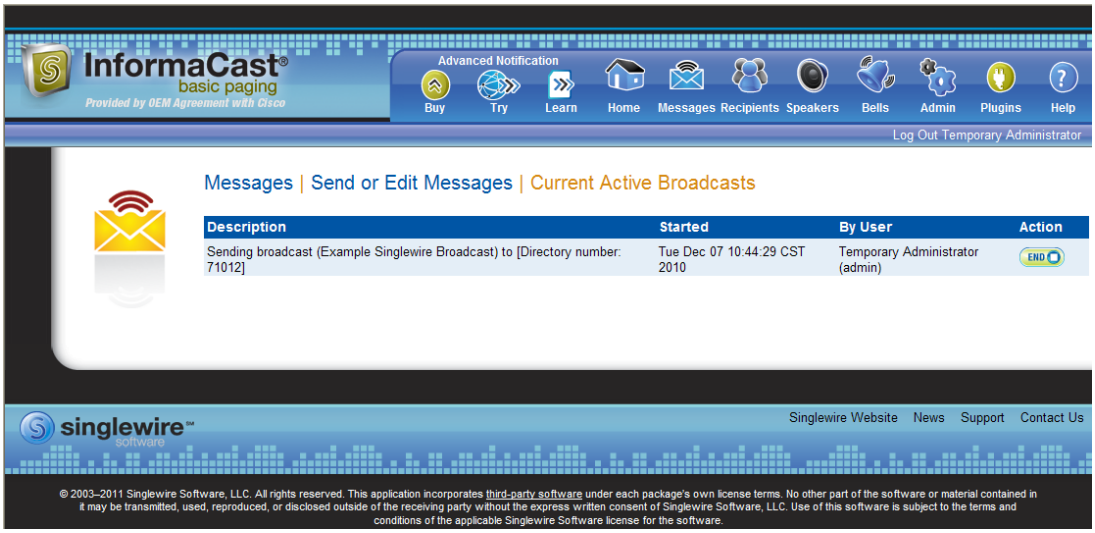
Note If you had Advanced InformaCast, you'd have access to more message types as well as more recipients. For more information on Advanced InformaCast functionality, please contact Singlewire Software.

Cancel a DialCast/Broadcast

Once you have sent a DialCast/broadcast, you may need to cancel it.

Step 1 Go to **Messages** | **Send or Edit Messages**. The Send or Edit Messages page appears with a note at the top of the page that, "InformaCast is currently broadcasting."

Step 2 Click the **View** button to see a list of ongoing broadcasts. The Current Active Broadcasts page appears.



This list offers you the ability to end any of the active broadcasts. This is particularly useful if, for example, an attempt to capture audio has been accidentally directed to a voicemail system.

Step 3 Click the **End** button of the broadcast you'd like to cancel. InformaCast displays a confirmation screen to make sure you picked the right message and that you really want to end the broadcast.

Step 4 Click the **End** button. InformaCast will stop sending the broadcast, and take you back to the Send or Edit Messages page.

If the message ends on its own or is cancelled by another administrator while you're following these steps, InformaCast will tell you that there are no active broadcasts.

Maintain InformaCast

When you click the **Admin** icon, you will be brought to the Overview page. On this page, you can view various statistics associated with the administration of InformaCast, such as how long the current session of InformaCast has been running, your version of InformaCast, and the configuration of your backups and phone updates.

Beyond simply using InformaCast to send broadcasts, you can set up InformaCast backups and manage phone updates, SNMP monitoring, and session timeouts.

Manage InformaCast Backups

Using the native database and file export inside InformaCast, you can configure the timing behind scheduled backups of the InformaCast configuration, which includes the InformaCast database, configuration data, and phone display assets.

Note If you do not set a time for backups, automatic backups will not occur.

Tip The backup process described in the following sections illustrates how to backup to a Windows server. It is possible to back up InformaCast to other operating systems. When backing up to a non-Windows OS, you will need to establish an SFTP client connection to InformaCast and download the InformaCastBackup.zip file from the path that you specify in "Configure InformaCast Backups" on page 6-2. You can use the existing dobackup.cmd file as an example for how backups are triggered on a Windows server, but you will need to adapt dobackup.cmd to work on your operating system.

Configure InformaCast Backups

Follow these steps to configure InformaCast backups.

Step 1 Go to **Admin** | **System** | **Backup**. The Backup page appears.

Step 2 Select the **Backup functionality activated** checkbox.

Step 3 Enter numeric values for when your scheduled backup should occur in the **Second**, **Minute**, and **Hour** fields.

Note The time for scheduled backups is calculated in military time.

Step 4 In the **Path** field, enter **/usr/local/singlewire/InformaCast/backup**, which is the destination for a ZIP file containing all of InformaCast's backup information.

Note You can only back up InformaCast when it is running. In order to achieve a consistent backup, perform it when configuration changes are not expected to be taking place.

If you are transferring your backup files to a Windows machine (described in "Move the InformaCastBackup.zip File to a Secure Location" on page 6-3), you will need to restart InformaCast whenever the content in the **Path** field changes. See "Start/Stop/Restart InformaCast and its Server" on page 9-3 for steps on restarting InformaCast.

Step 5 Click the **Update** button to save your changes. On the Overview page, you can see your changes reflected in the *Backup* section.

Tip After performing these steps, you can also navigate back to the Backup page and click the **click here** link to manually back up InformaCast right away, bypassing the scheduled backup you just set up. New backups will overwrite previous backup files.

Move the InformaCastBackup.zip File to a Secure Location

Note This section is optional. Some VMware environments are automatically backed up using a Storage Area Network (SAN). If this is the case, and you have confidence in your virtual machine recovery process, you can skip moving the InformaCastBackup.zip file.

Once you've configured InformaCast for scheduled backups, you can choose to move the ZIP file InformaCast creates (InformaCastBackup.zip) to a more secure location on a Windows machine that is being backed up at another location. Singlewire has created a script that will facilitate this move, which when paired with a Windows scheduled task, will make backing up InformaCast and ensuring the ZIP file is in a safe location, easy and automatic.

Step 1 Download Plink (http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html), a command-line SCP tool.

Step 2 Download dobackup.txt. If InformaCast is running, the file is available at https://<InformaCast Virtual Appliance IP Address>:8444/InformaCast/tools/dobackup.txt, where <InformaCast Virtual Appliance IP Address> is the IP address of InformaCast. If InformaCast isn't running, the file is available at /usr/local/singlewire/InformaCast/web/tools/dobackup.txt.

Step 3 Save dobackup.txt to a Windows machine that is being backed up to disk.

Step 4 Open dobackup.txt in your preferred text editor.

Step 5 Modify the following lines to suit your environment:

```
rem IP of the InformaCast server
set ip=172.30.238.12
rem OS admin password of the InformaCast server
set admin_password=changeMe
rem Location of plink.exe
set plink=c:\plink.exe
```

Change **172.30.238.12** to InformaCast's IP address. Change **changeMe** to the InformaCast administrator password. Change **c:\plink.exe** to the location of Plink on your Windows machine.

Step 6 Save dobackup.txt as dobackup.cmd.

Step 7 Run dobackup.cmd once to ensure that InformaCastBackup.zip moves from your Linux environment to your backed up Windows machine.

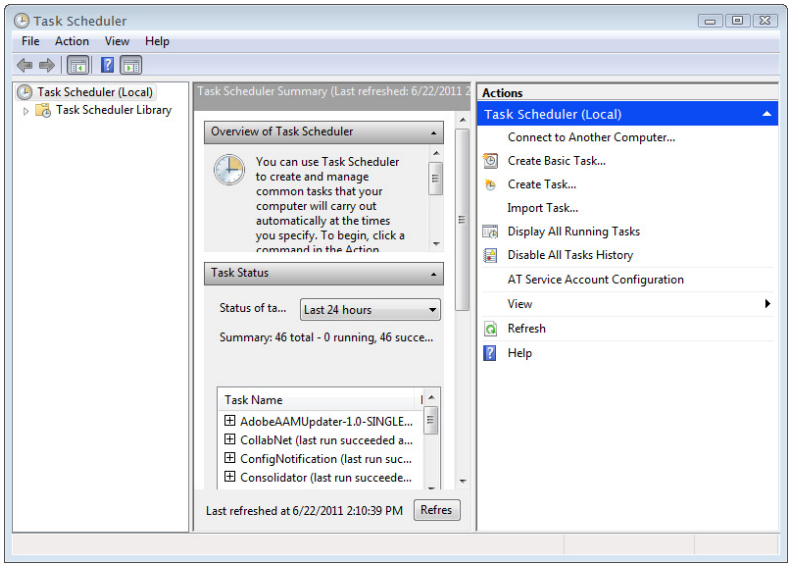
Note Backing up InformaCast using dobackup.cmd does not create multi-generational backups. If this is a requirement for your environment, Singlewire recommends configuring them through your existing backup solution.

Step 8 Set up a Windows scheduled task to move the backup daily:

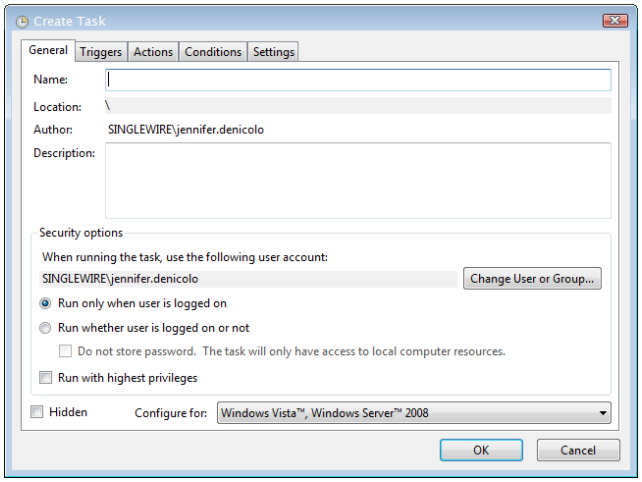
Step a. Go to **Control Panel** | **System and Security** | **Administrative Tools** | **Task Scheduler**.

Note The scheduled tasks process is slightly different, depending on your version of Windows. The documented process may vary slightly from your environment.

The Task Scheduler window appears.



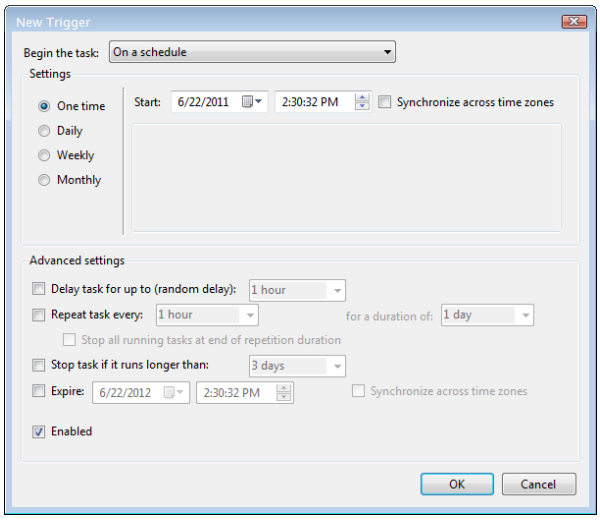
Step b. Go to **Action** | **Create Task.** The Create Task window appears.



Step c. Enter **InformaCast Backup** in the **Name** field.

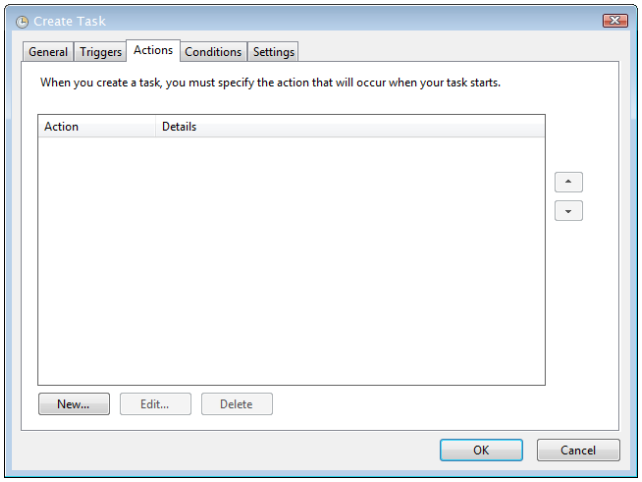
Step d. Select the **Run whether the user is logged on or not** radio button.

Step e. Click the **Triggers** tab and click its **New** button. The New Trigger dialog box appears.

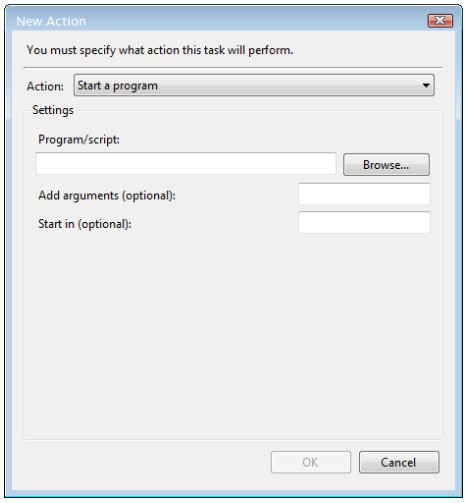


Step f. Configure the New Trigger dialog box to your specific environment and click the **OK** button.

Step g. Click the **Actions** tab. The Create Task window refreshes.



Step h. Click the **New** button. The New Action dialog box appears.



Step i. Choose **Start a program** from the **Action** dropdown menu.

Step j. Click the **Browse** button and navigate to where you saved the dobackup.cmd file.

Step k. Click the **OK** button.

Step l. Click the **OK** button on the New Action dialog box.

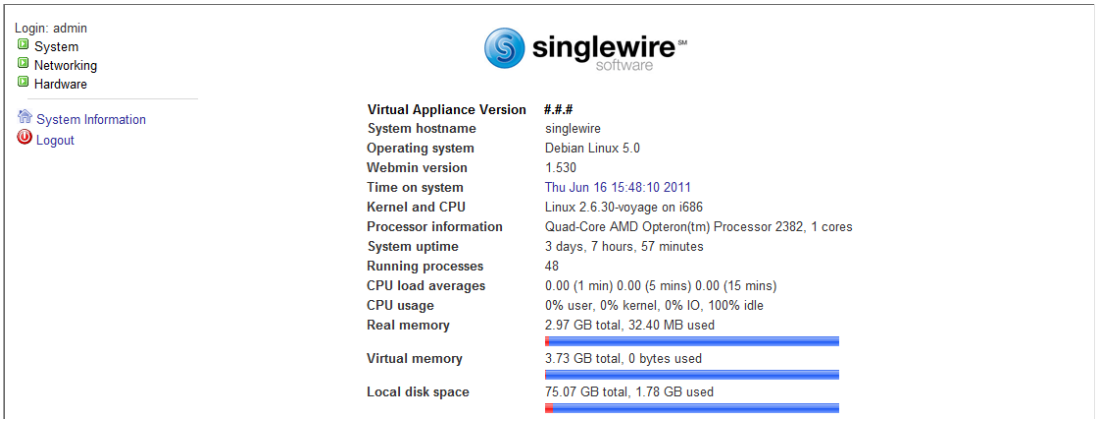
Step m. Click the **OK** button on the Create Task window.

Step n. Close the Task Scheduler. Your schedule task is complete.

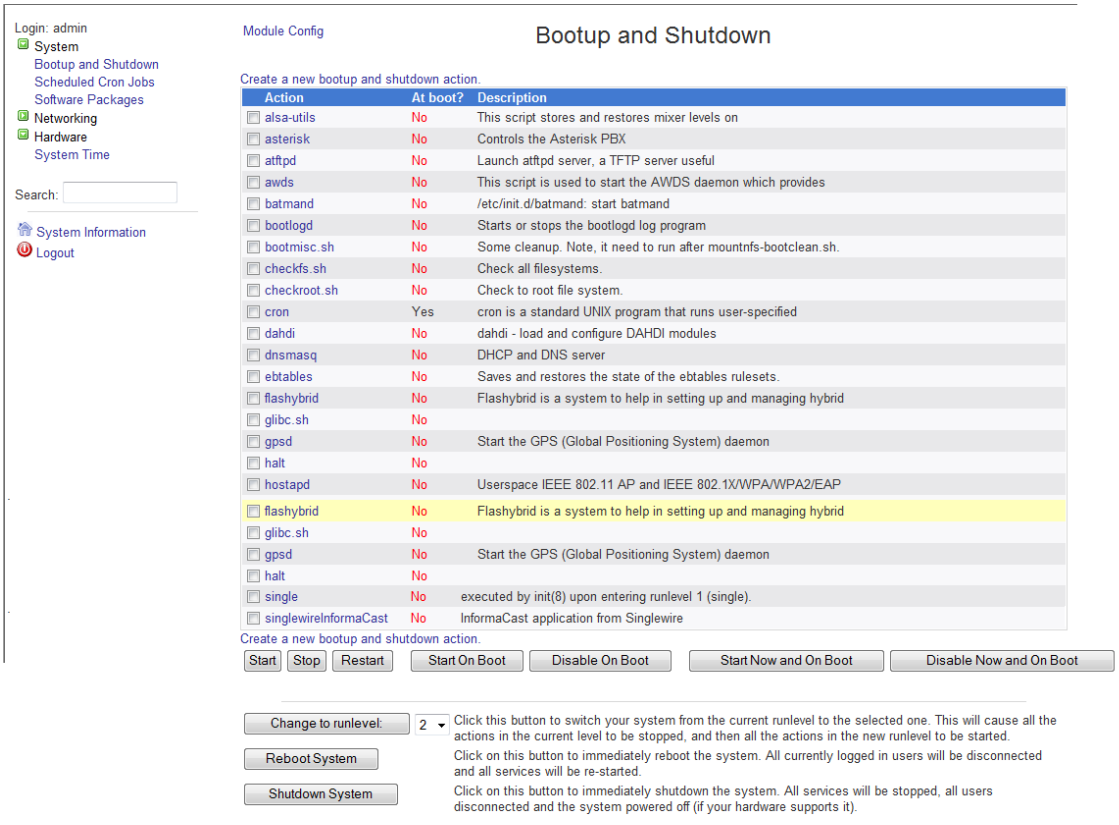
Restore InformaCast

Use the following steps to restore InformaCast from a backup.

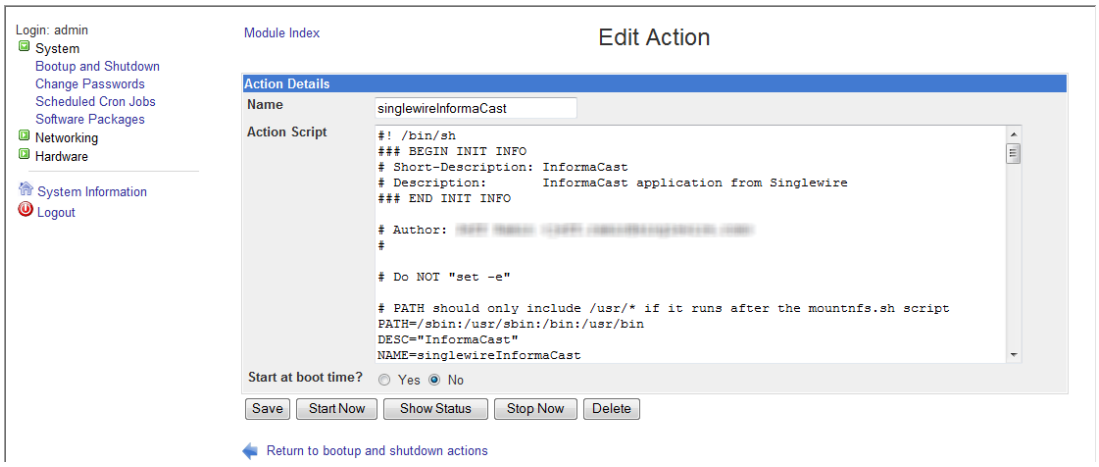
Step 1 Log into Webmin (see "Log into Webmin" on page 10-7 for specific steps). The Webmin homepage appears.



Step 2 Go to **System** | **Bootup and Shutdown**. The Bootup and Shutdown page appears.



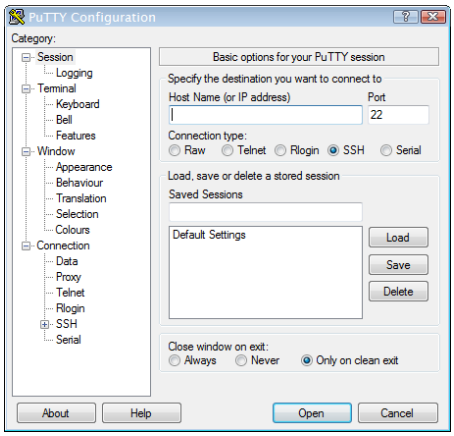
Step 3 Scroll down the list of actions until you come to **singlewireInformaCast**. Click its link. The Edit Action page appears.



Step 4 Click the **Stop Now** button. It will take a minute or so for InformaCast to stop.

Note Leave this window open. You will come back to it.

Step 5 Use an SSH client, like PuTTY (http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html), to access InformaCast's command line interface. The PuTTY Configuration window appears.

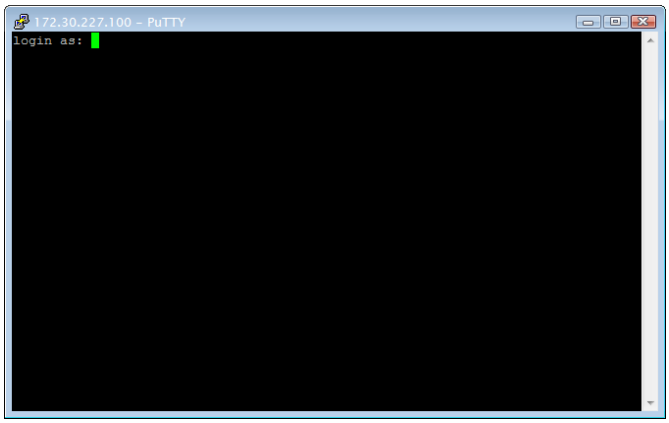


Step 6 Enter InformaCast's IP address in the **Host Name (or IP address)** field.

Step 7 Leave the **Port** field at its default of 22.

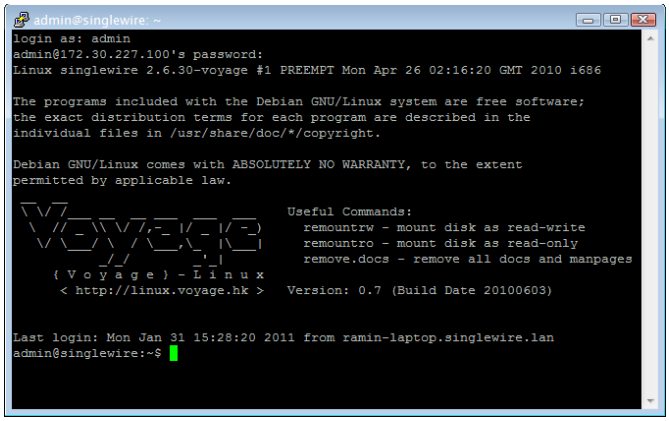
Step 8 Select the **SSH** radio button.

Step 9 Click the **Open** button. The command-line interface for InformaCast appears.

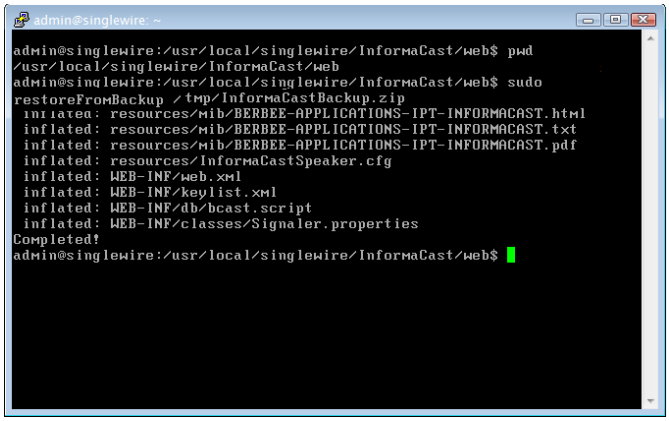


Step 10 Enter **admin** at the prompt and press the **Enter** key.

Step 11 Enter **changeMe** at the prompt and press the **Enter** key. The command-line interface refreshes, showing you that you're logged in.

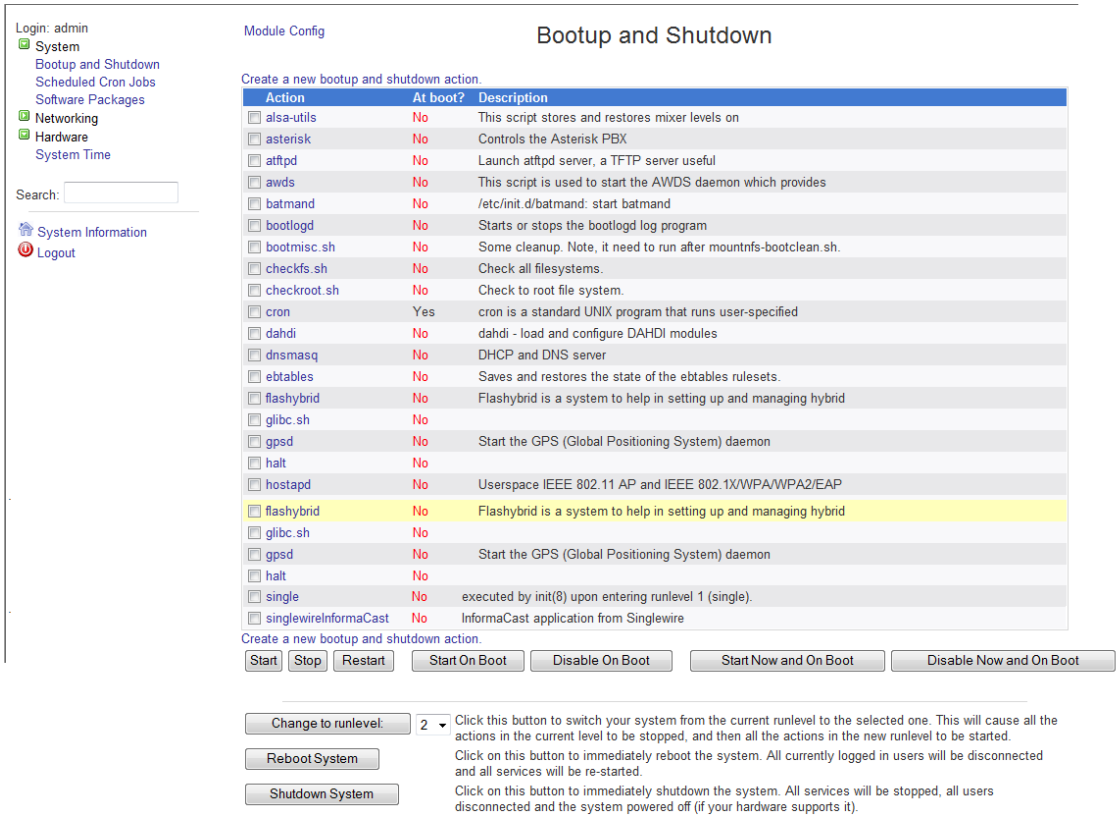


Step 12 Enter **restoreFromBackup /<Directory of Backup>/InformaCastBackup.zip**, where <Directory of Backup> is the location of your InformaCastBackup.zip file, at the prompt and press the **Enter** key. The command-line interface refreshes, detailing the restoration process.

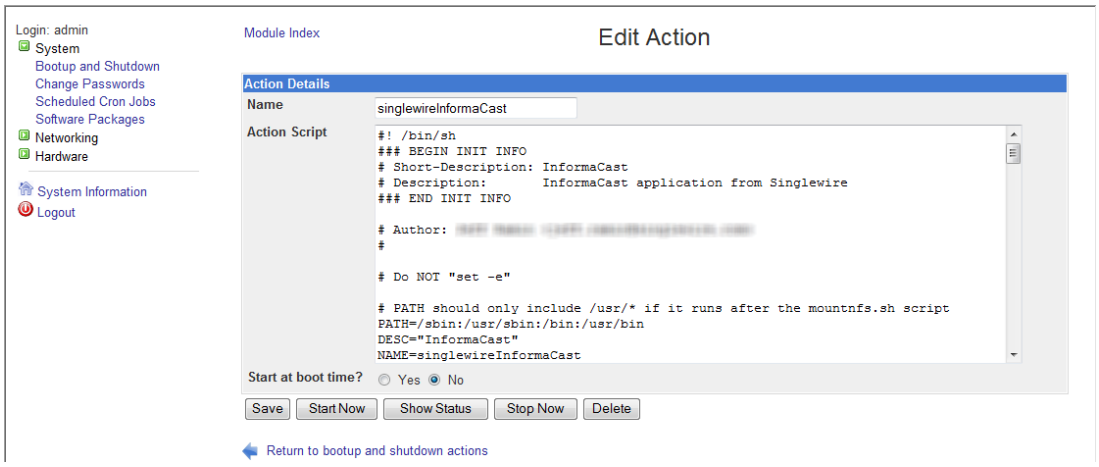


Step 13 Go back to your Stopping Actions page.

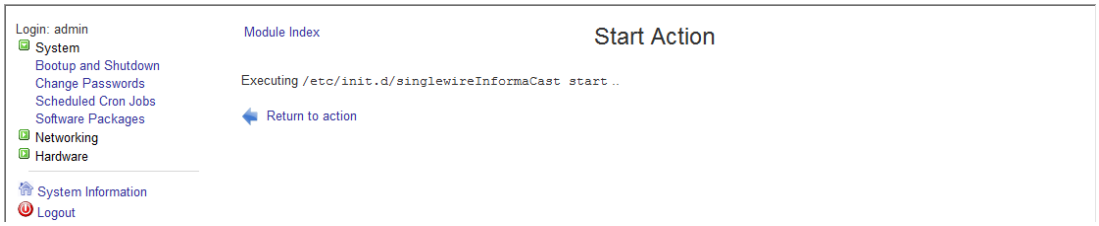
Step 14 Click the **Return to bootup and shutdown actions** link. The Bootup and Shutdown page appears.



Step 15 Scroll down the list of actions until you come to **singlewireInformaCast**. Click its link. The Edit Action page appears.



Step 16 Click the **Start Now** button. It will take a minute or so for InformaCast to start.



Step 17 Test the functionality.

Manage Phone Updates

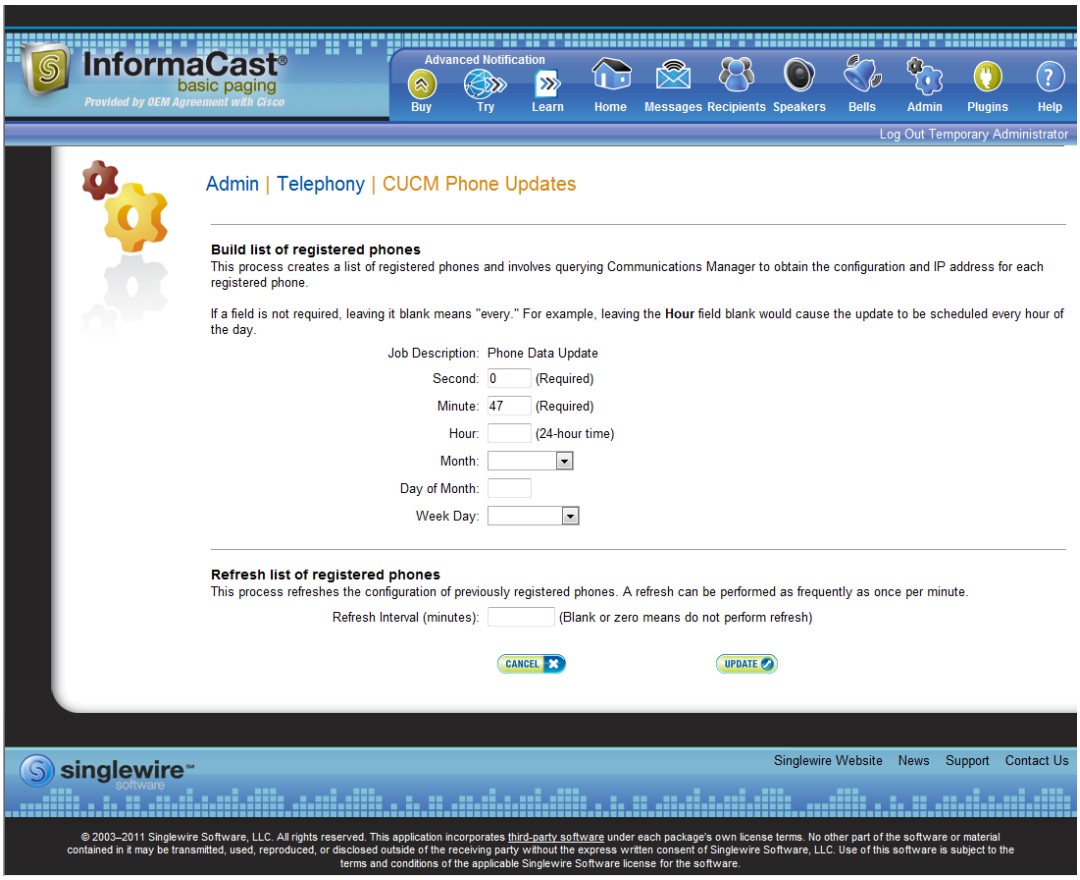
Phone updates allow you to configure the timing for two scheduled jobs of how often InformaCast will update its phone information: build a list of registered phones and refresh a list of registered phones.

The time it takes for InformaCast to *rebuild* a list of phones is directly related to the number of phones you have. During a build of registered phones, CUCM's SNMP service obtains the IP address of all registered phones in the cluster. Because SNMP is throttled for each piece of data it sends, minutes may pass if many thousands of phones are registered. By comparison, the AXL requests used to *refresh* a list of registered phones are relatively quick.

Refreshing a list of registered phones picks up the changes to phones that use extension mobility as well as other configuration changes, e.g. adding/deleting/modifying a line, changing the phone description, etc. Updates can be performed as frequently as once per minute or even disabled if desired.

Note Refreshing the list only updates the phones already in InformaCast's phone cache. Newly registered phones will not be seen in the cache until the next rebuild of registered phones.

Step 1 Go to **Admin** | **Telephony** | **CUCM Phone Updates**. The CUCM Phone Updates page appears.



Note By default, building a list of registered phones will occur at 10 minutes past the hour, every hour.

Step 2 Enter numeric values in the **Second**, **Minute**, and **Hour** fields to specify when you'd like InformaCast to rebuild its list of registered phones.

Step 3 Select **Every Month** or a specific month from the **Month** dropdown menu.

Step 4 Enter a numeric value in the **Day of Month** field if you'd like InformaCast to only rebuild its phone information on a specific day.

Step 5 Select **Every Day** or a specific day from the **Week Day** dropdown menu.

Step 6 Enter a numeric value in the **Refresh Interval (minutes)** field. A positive numeric value enables updates. Zero or no value disables updates.

Note Refreshing a list of registered phones picks up the changes to phones that use extension mobility as well as other configuration changes. Refreshing the list only updates the phones already in InformaCast's phone cache. Newly registered phones will not be seen in the cache until the next rebuild of registered phones.

Step 7 Click the **Update** button. On the Overview page, you can see your changes reflected in the *Phone Updates* section.

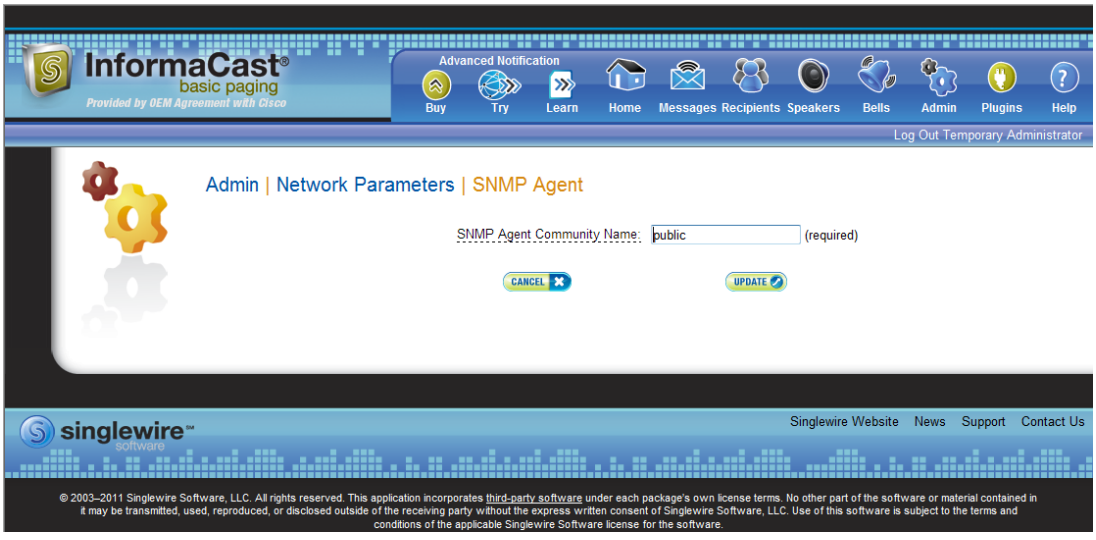
Configure SNMP Monitoring

InformaCast has an embedded SNMP agent that can be paired with your own Network Management Software (NMS) in order to monitor certain aspects of InformaCast (i.e. the number of broadcasts sent, the length of time the application has been running, etc.). Through the import of a Management Information Base (MIB), your NMS will know what InformaCast statistics are available for monitoring. The MIB is available in three formats—HTML, PDF, and TXT—and their default location is:

- https://<InformaCast Virtual Appliance IP Address>:8444/InformaCast/resources/mib/BERBEE-APPLICATIONS-IPT-INFORMACAST.html
- https://<InformaCast Virtual Appliance IP Address>:8444/InformaCast/resources/mib/BERBEE-APPLICATIONS-IPT-INFORMACAST.pdf
- https://<InformaCast Virtual Appliance IP Address>:8444/InformaCast/resources/mib/BERBEE-APPLICATIONS-IPT-INFORMACAST.txt

Note InformaCast's SNMP agent is listening on port 1161.

Step 1 Go to **Admin** | **Network Parameters** | **SNMP Agent**. The SNMP Agent page appears.



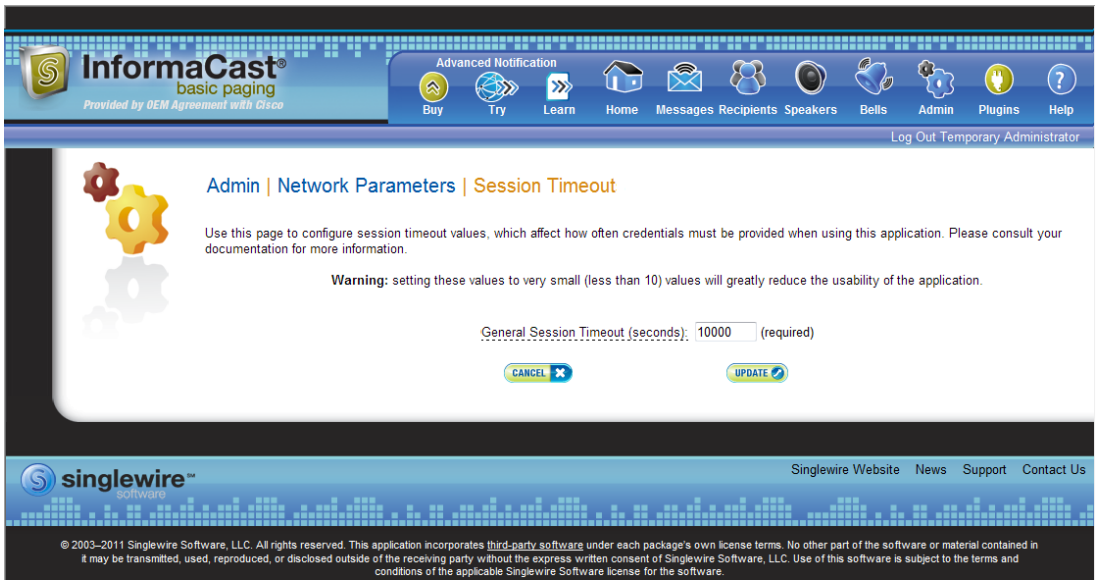
Step 2 Enter an SNMP community name in the **SNMP Agent Community Name** field. This community name and the one that your NMS is configured to use when talking to InformaCast must match in order for SNMP monitoring to work.

Step 3 Click the **Update** button.

Configure Session Timeout

In its default configuration, an InformaCast session will time out after five minutes of inactivity. If you would like a session of InformaCast to remain valid longer, it is possible to change this value.

Step 1 Go to **Admin** | **Network Parameters** | **Session Timeout**. The Session Timeout page appears.



Step 2 Enter a numerical value in the **General Session Timeout (seconds)** field. This field controls when you will be asked to reenter your username and password after a certain amount of inactivity.

Warning **Setting this value to a very small value (i.e. less than 10) will greatly reduce the usability of InformaCast.**

Step 3 Click the **Update** button to save your changes.

Upgrade InformaCast from Basic to Advanced

Note InformaCast Virtual Appliance is part of the larger InformaCast Virtual Appliance suite of products. If you are looking to upgrade your version of InformaCast Virtual Appliance (e.g. 8.3 to 8.5.1), see "Upgrade InformaCast Virtual Appliance" on page 10-25.

InformaCast's functionality is based on its license, and depending on the license you have, you will be able to access all of InformaCast's functionality or only parts of it. Basic InformaCast functionality includes the ability to send live audio broadcasts to up to 50 phones by dialing a number on your Cisco IP phone. Advanced InformaCast functionality includes the ability to send a number of different types of broadcasts (e.g. Live Audio, Pre-recorded Audio, Pre-recorded Audio And Text, etc.) using your Cisco IP phone's interface and/or InformaCast's web interface, interact with InformaCast's plugins (e.g. conduct conference calls, trigger contact closures, post to Twitter, send broadcasts to email addresses, etc.), customize scripts that can be attached to broadcasts, and receive confirmation when broadcasts are sent, among other features.

All InformaCast users start with Basic InformaCast and can upgrade to Advanced InformaCast using the **Try** or **Buy** icons or by contacting Singlewire to obtain a license for a switch in functionality.

Note Downgrading from Advanced InformaCast back to Basic is accomplished by clicking the **Stop Advanced Notification Trial** button on InformaCast's Manage License Key page (**Admin** | **Manage License Key**). This will cause InformaCast to reboot, as will any future change in InformaCast functionality or license type.

InformaCast can be obtained with a basic, trial, demonstration, subscription, or perpetual license. For more information on InformaCast licenses, see "Licensing Information" on page 1-5.

Tip If you want to learn more about InformaCast Advanced Notification, click the **Learn** icon to visit a Singlewire Software website that provides more information on the expanded functionality available to you with your upgrade.

Note the Differences

There are certain caveats to keep in mind when upgrading from Basic to Advanced InformaCast or downgrading from Advanced to Basic:

- If you upgrade from Basic to Advanced InformaCast through either the trial, demonstration, subscription or perpetual licenses and you decide to return to Basic functionality, all additional information entered during your Advanced phase will not be saved (e.g. when you revert to Basic from Advanced, any information you entered after you upgraded initially—dialing configurations, users, recipient groups, etc.—will not be available once you downgrade to Basic InformaCast). If you choose to upgrade back to Advanced InformaCast, that information will reappear; however, any new information you entered after you reverted to Basic functionality will be unavailable.
- You will need a valid license key (if you are using Advanced InformaCast as a trial, your license key is already included), which should have been provided to you by your Singlewire salesperson (contact sales@singlewire.com if you didn't receive one)
- If you are moving from Basic InformaCast to Advanced InformaCast (and you have previously had Advanced InformaCast), InformaCast will be restarted with the installation of this new license. Please plan your upgrades accordingly.
- Because of the differences between Basic and Advanced InformaCast, there are two user guides. When upgrading to Advanced InformaCast from Basic, you should receive a new guide that contains Advanced InformaCast features. Contact Singlewire Software if you have not received a new guide.
- InformaCast's web interface changes dramatically with your move from Basic to InformaCast, adding entirely new menus and richer functionality. Depending on your access level, you'll have access to:
  - **Home.** InformaCast's homepage, complete with RSS news feed.
  - **Messages.** The message administration page, allowing you to create, edit, and send messages as broadcasts.
  - **Recipients.** The recipient group administration page, allowing you to create and manage recipient groups.
  - **Speakers.** The IP speaker administration page, allowing you to detect, add, edit, test, and listen at IP speakers.
  - **Bells.** The bell schedule overview page, allowing you to view and access the ring lists, bell schedules, and exceptions you've created.
  - **Admin.** The configuration overview page, allowing you to view scheduled updates and backups; manage the license key, voice menus, and users; and set up the system, network, and broadcast parameters, along with DialCasts.
  - **Plugins.** The plugin administration page, allowing you to add, disable, and enable plugins and access their configurations.
  - **Help.** InformaCast's help pages, allowing you access to various aspects of the online help system and providing the ability to enter a support request.
- If you change your password in Basic InformaCast, upgrade to Advanced InformaCast, then downgrade to Basic InformaCast, your password will revert to your original Basic InformaCast password.

- If you plan to switch between Basic and Advanced InformaCast and you change your IP address, you will need to redeploy the InformaCast OVA (see "Install InformaCast Virtual Appliance" on page 2-6).
- If you fail to configure CUCM in Basic InformaCast, upgrading to Advanced InformaCast and then configuring CUCM before downgrading to Basic InformaCast will require you to perform all the steps in "Integrate CUCM" on page 2-30 again.

If you have questions about your upgrade, contact Singlewire Support through the online support request form. Please include:

- Account contact information
- Maintenance contract number
- Detailed description of problem
- Product name and version
- CUCM version
- InformaCast logs (go to **Help** | **Support**)

Upgrade InformaCast

All InformaCast users start with Basic InformaCast and can upgrade to Advanced InformaCast using the **Try** or **Buy** icons or by contacting Singlewire to obtain a license for a switch in functionality.

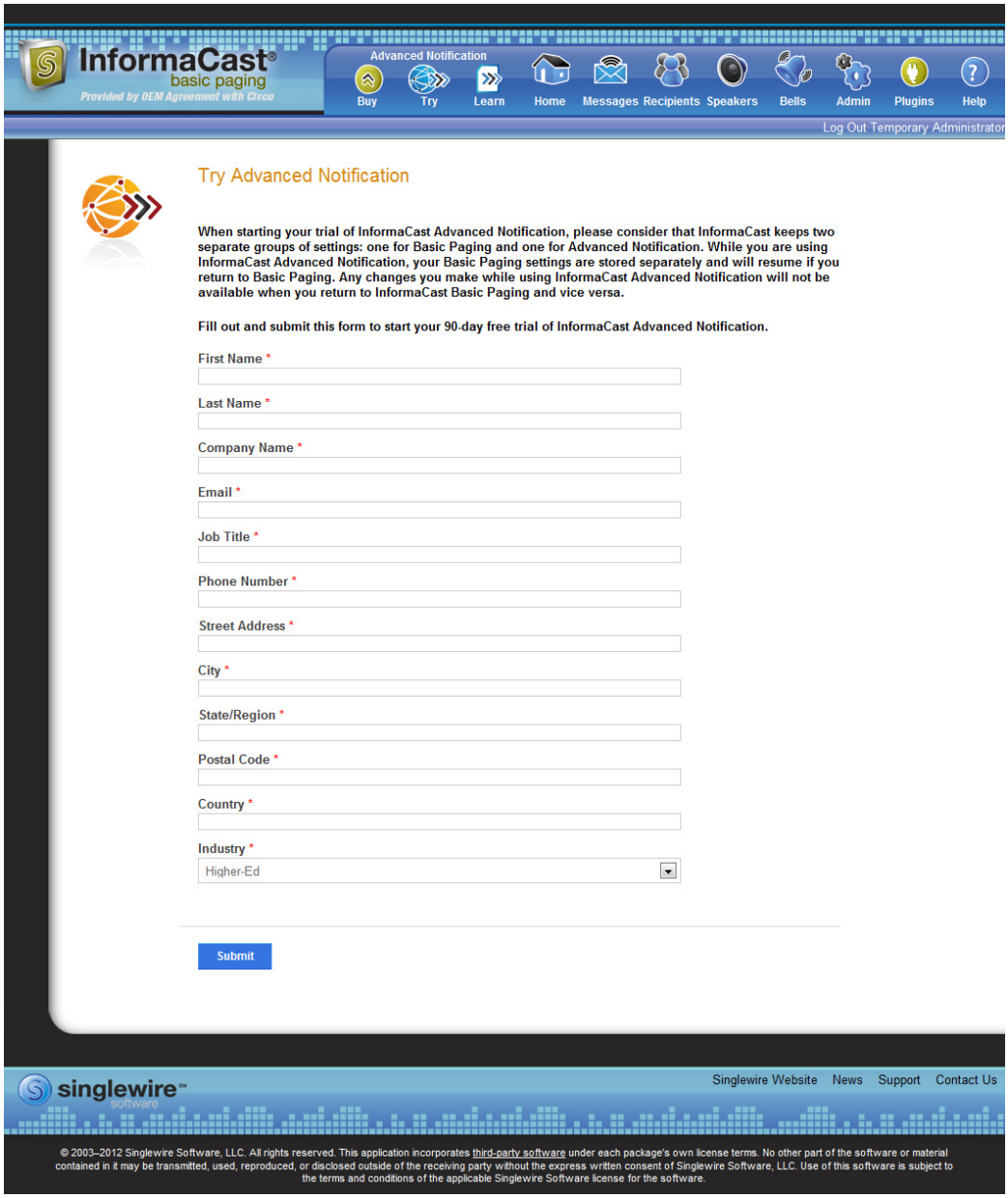
Note You will want to obtain the "InformaCast Virtual Appliance Installation and User Guide" for Advanced Notification in order to make full use of all of InformaCast's functionality. After upgrading, it can be obtained from **Help** | **Install Guide**. If you are using the online help when you upgrade, you will need to close that window and reopen it to view the upgraded help.

Try Advanced Notification

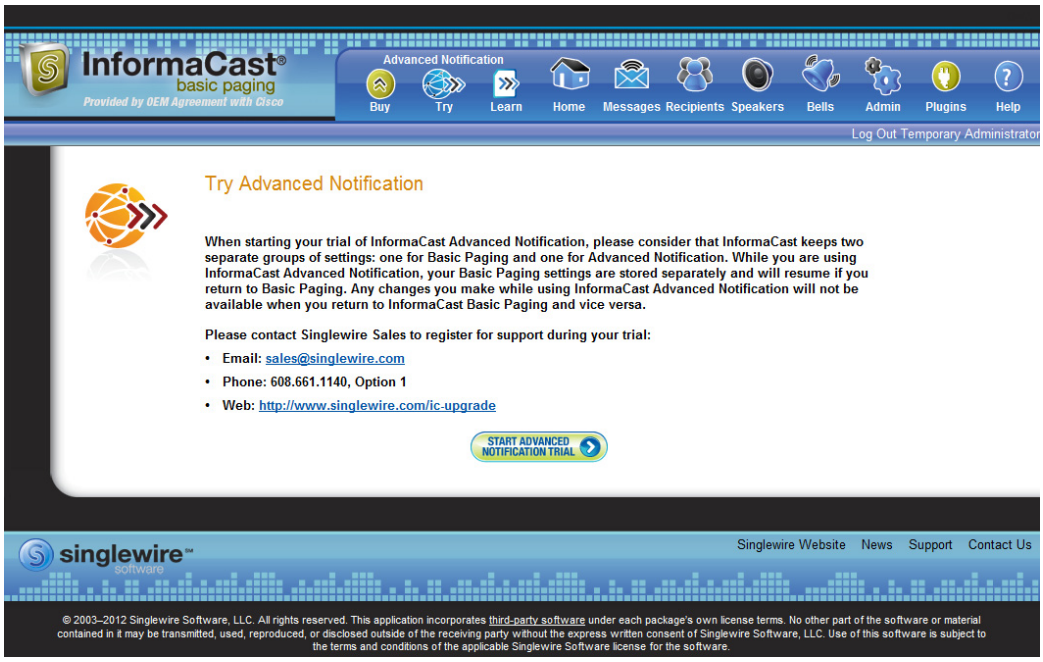
By clicking the **Try** icon (), you start your 60-day free trial of Advanced InformaCast.

Step 1 Click the **Try** icon () any time while using Basic InformaCast.

If your server is connected to the Internet, you will see a form. Fill out the required information and click the **Submit** button.



If your server is not connected to the Internet, you will see Singlewire Sales contact information, which you should use to register for support during your trial.



Click the **Start Advanced Notification Trial** button. The Singlewire InformaCast Software License Agreement page appears.

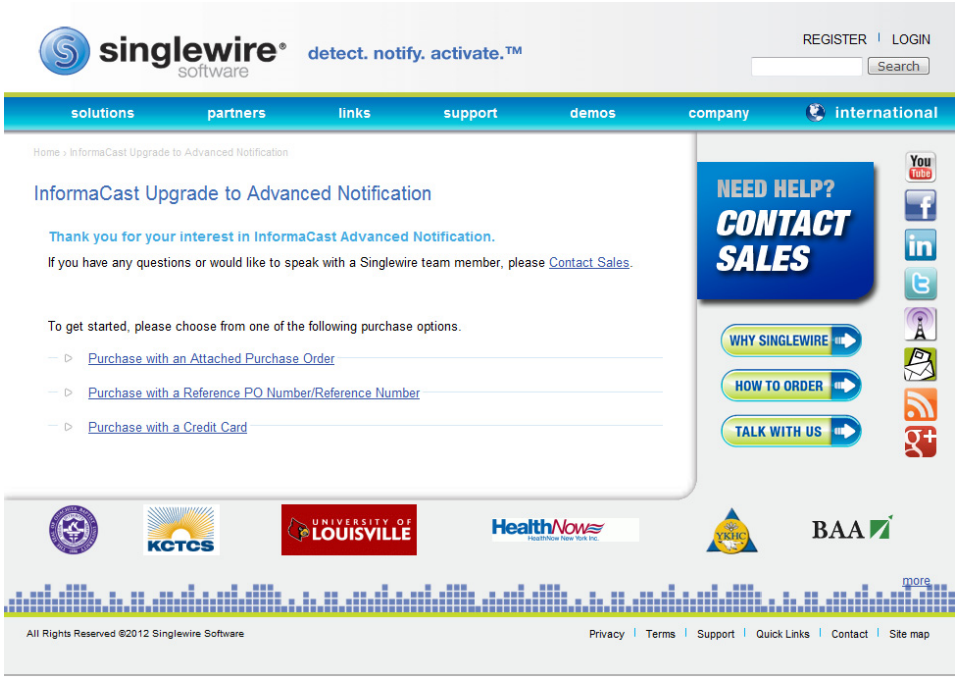
Step 2 Click the **I Accept** button. Your window refreshes with InformaCast's homepage that now shows you are in your trial of InformaCast Advanced Notification.

Buy Advanced Notification

By clicking the **Buy** icon, you start the process of obtaining InformaCast Advanced Notification through either a demonstration, subscription, or perpetual license.

Step 1 Click the **Buy** icon ( ) any time while using Basic InformaCast.

If your server is connected to the Internet, you will be redirected to a Singlewire Software website. Follow the prompts to obtain a new license.



If your server is not connected to the Internet, you will see a QR code that you can scan with your smartphone to access the Singlewire website. Once there, follow the prompts to obtain your new license.

Step 2 Continue with "Enter Your New License Key" on page 7-9.

Enter Your New License Key

Note If you are in your free trial of Advanced InformaCast, you can skip this section.

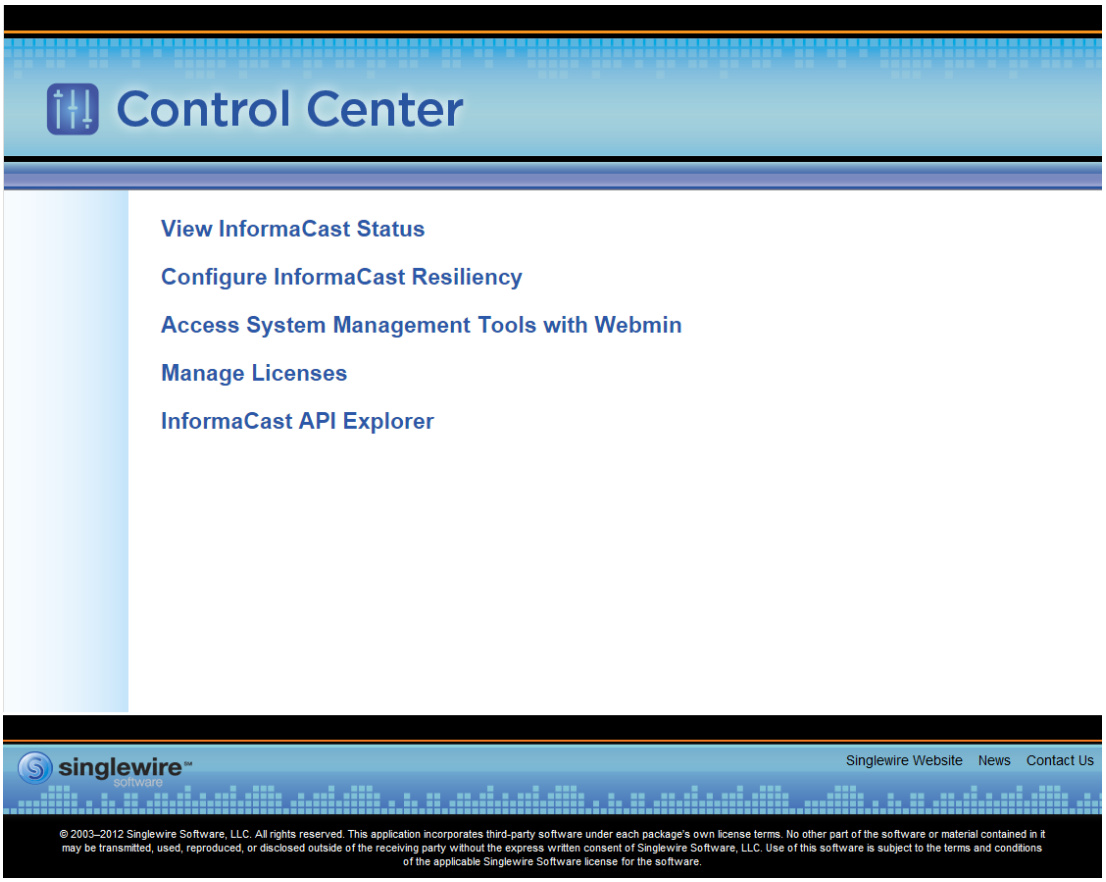
When you upgrade from Basic InformaCast to Advanced InformaCast (with the exception of your free trial of Advanced InformaCast), you will install a new license key to activate the various features of your InformaCast system. The license key will be in the form of an XML file that was sent to you by email from a Singlewire sales representative. Make sure to save this XML file to a safe location that can be accessed by the machine running your web browser.

Note If you are in participating in your free trial of Advanced InformaCast functionality, your license will already be installed for you and will be visible on InformaCast's Manage License Key page (**Admin** | **Manage License Key**). Your license will not appear on Singlewire's License Manager page until you upgrade to Advanced InformaCast on a demonstration, subscription, or perpetual license.

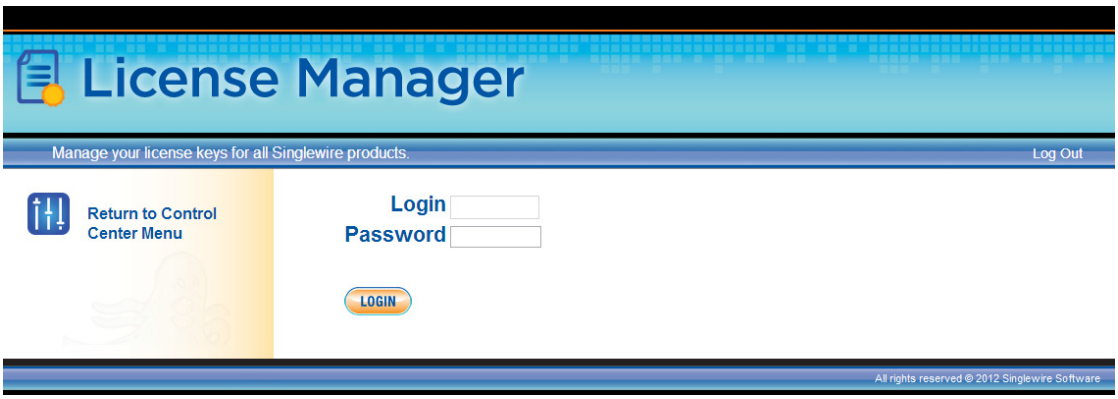
Note Bell schedules, the number of IP phones and speakers, CUCM clustering, and message confirmation are all controlled by your license key. If you are expecting certain functionality and cannot access it, contact your Singlewire salesperson.

Warning **If you are moving from Basic InformaCast to Advanced InformaCast (and you have previously had Advanced InformaCast), InformaCast will be restarted with the installation of this new license. Please plan your upgrades accordingly.**

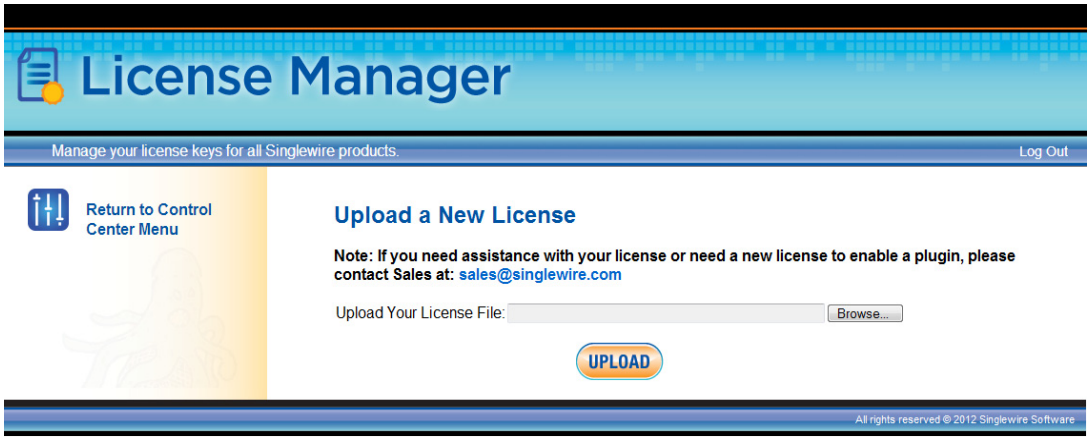
Step 1 Log into the Control Center (see "Log into the Control Center" on page 10-5 for specific steps). The Control Center menu page appears.



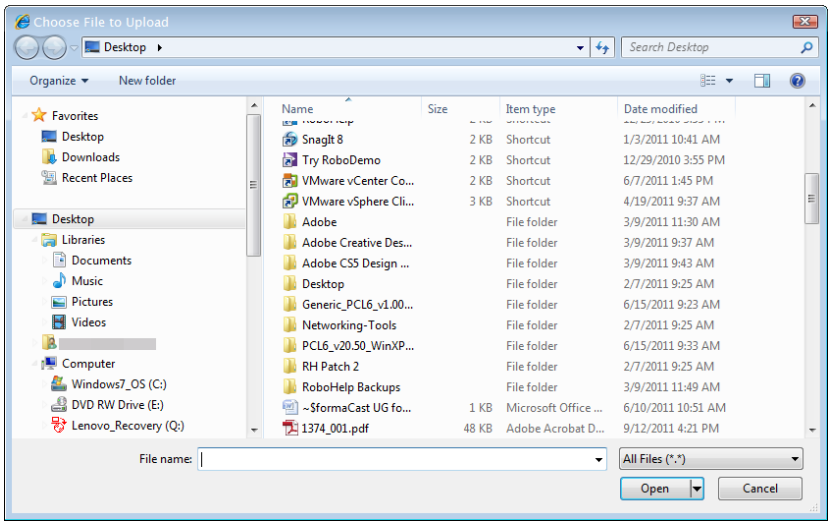
Step 2 Click the **Manage Licenses** link. The License Manager page appears.



Step 3 Enter your username and password in the **Login** and **Password** fields, respectively. By default, your username is **admin** and your password is **changeMe**. Click the **Login** button. The Upload a New License page appears.



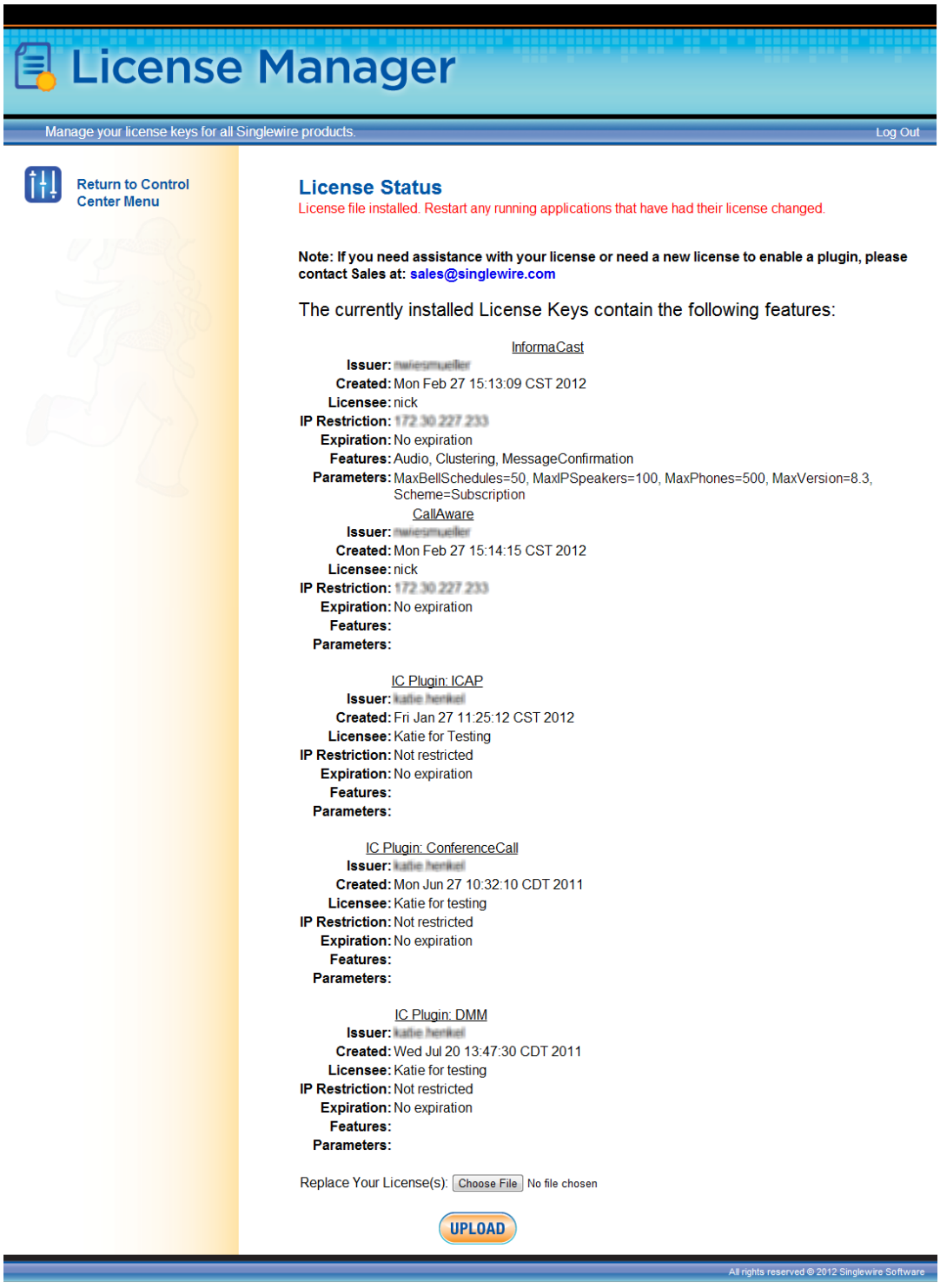
Step 4 Click the **Browse** button. The Choose File to Upload dialog box appears.



Step 5 Navigate to the license key file that was emailed to you. You can also enter the path to the license key file.

Step 6 Select your license key file and click the **Open** button.

Step 7 Click the **Upload** button on the Upload a New License page. The License Status page appears and you'll see confirmation that the license has been accepted.



The License Manager holds all of your Singlewire licenses, unless you are participating in your Advanced InformaCast trial, in which case your license will be on InformaCast's Manage License Key page (**Admin** | **Manage License Key**). Depending on the software applications you are using, you will see different licenses housed on this page.

Tip If the key is not accepted, check that you selected the proper file containing the XML key that was emailed to you, ensure that your IP address is correct, determine that your key has not expired, and ensure that the MaxVersion parameter in your license key matches or is greater than your version of InformaCast. If you're still having trouble, contact your Singlewire sales representative for assistance.

When you first register InformaCast, you will usually be emailed a temporary license key. Once you know InformaCast's permanent IP address, email that information to sales@singlewire.com so a permanent license key can be sent to you. Once you have the permanent license key, you will want to upload this key to InformaCast using the steps in this section.

Note Once you have exceeded the number of phones allowed by your license, you will receive a warning that you've attempted to broadcast to more phones than are allowed by your license key, causing some phones to be skipped. Consult the InformaCast Performance log (**Help** | **Support**) to see the phones that have been skipped and contact your Singlewire salesperson about obtaining a larger license. You can also retry your broadcast with a smaller group of phones. In Trial mode, your license limits you to 500 phones.

Frequently Asked Questions (FAQ)

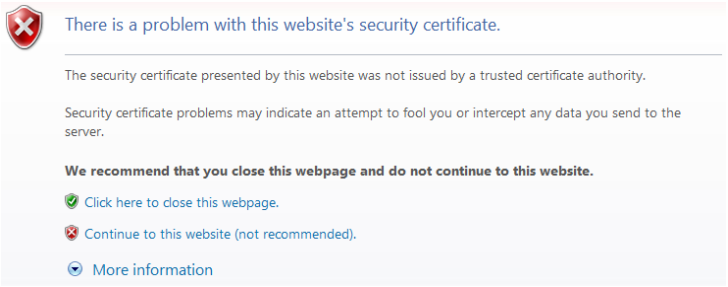
Q. I opened InformaCast for the first time and I received an HTTP Status 500 error. What's going on?

A. This is normally caused by your web browser version being out of date. Update your web browser to the latest version.

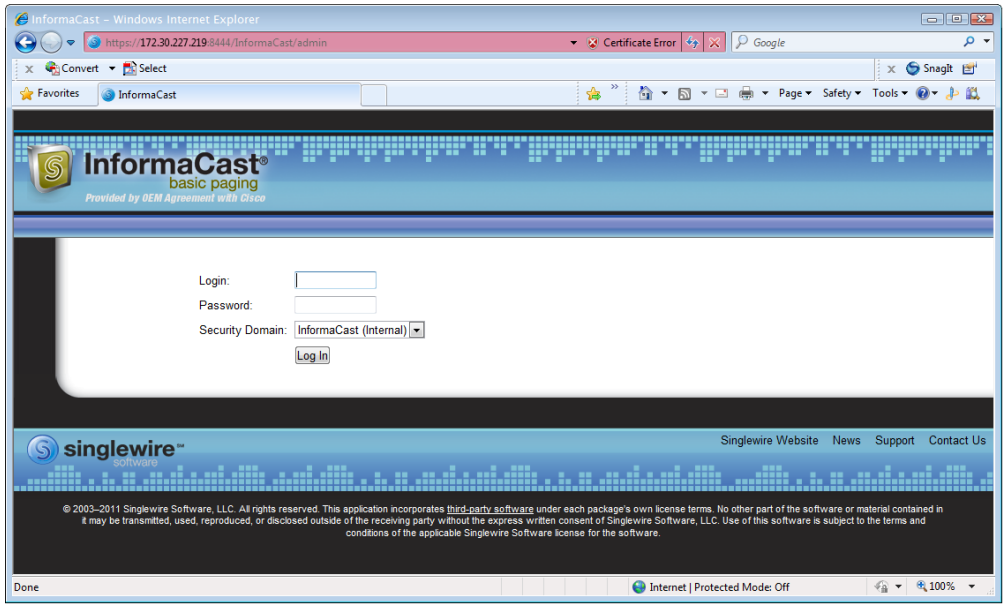
Q. Whenever I access InformaCast through Internet Explorer, I receive the error, "There is a problem with this website's security certificate." How can I get rid of this?

A. Since InformaCast, like CUCM, is a locally-installed server rather than a global, public Internet site, there is no practical way for web browsers to recognize its encryption certificate as safe. To permanently bypass this error, you can install InformaCast's SSL certificate.

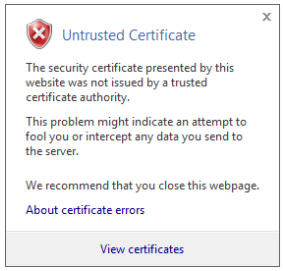
Step a. Open InformaCast in Internet Explorer. The Certification Error: Navigation Blocked page appears.



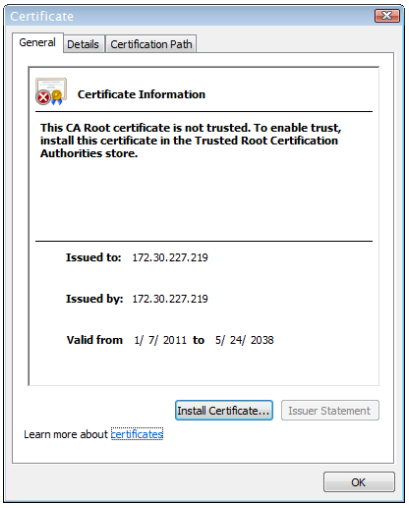
Step b. Click the **Continue to this website (not recommended)** link. The InformaCast Login page appears and your browser's address bar is highlighted in red.



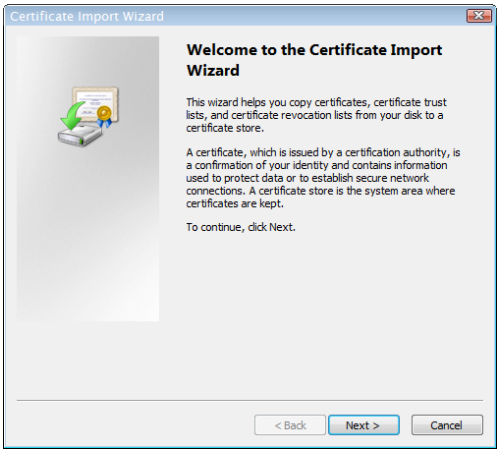
Step c. Click **Certificate Error** in your browser's address bar. The Untrusted Certificate pop-up window appears.



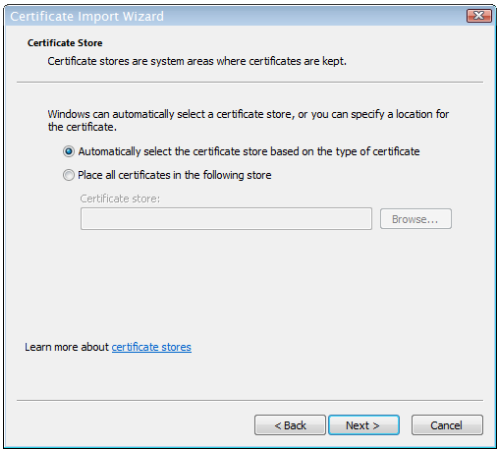
Step d. Click the **View certificates** link. The Certificate dialog box appears.



Step e. Click the **Install Certificate** button. The Certificate Import Wizard appears.



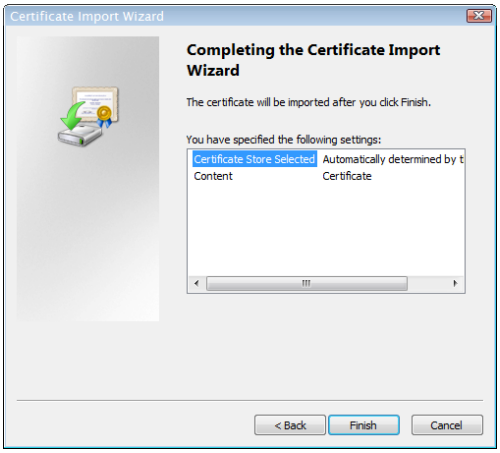
Step f. Click the **Next** button. The Certificate Import Wizard refreshes.



Step g. Select the **Automatically select the certificate store based on the type of certificate** radio button and click the **Next** button.

On Windows Server 2008, you will need to select the **Place all certificates in the following store** radio button, click the **Browse** button, select the **Trusted Root Certification Authorities** folder, and click the **OK** button.

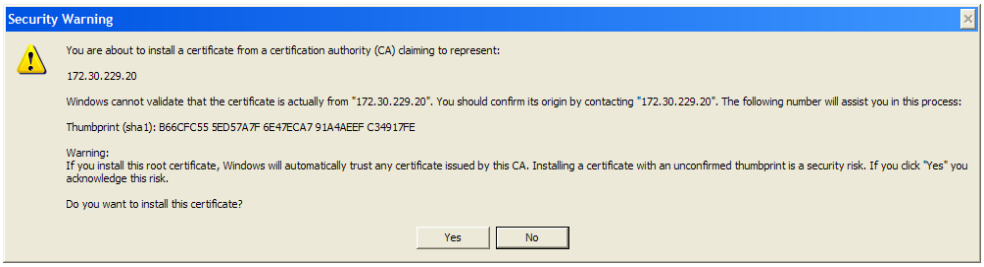
The Certificate Import Wizard refreshes.



Step h. Click the **Finish** button.

Step i. Click the **OK** button letting you know the import was successful.

You may receive a Security Warning dialog box. Click the **Yes** button.



Step j. Click the **OK** button on the Certificate dialog box.

Step k. Close your browser window and access InformaCast through Internet Explorer again. You will no longer receive the "There is a problem with this website's security certificate" error.

Q. How do I get rid of the warning about exceeding my license key?

A. As of InformaCast 8.0, the license key controls have changed. Once you have exceeded the number of phones allowed by your license, you will receive a warning that you've attempted to broadcast to more phones than are allowed by your license key, causing some phones to be skipped. You can consult the InformaCast Performance log (**Help** | **Support**) to see the phones that have been skipped. Your Performance log will include information similar to the following excerpt:

```
2010-09-08 10:44:54,209 [pool-41-thread-1] ERROR PhoneRegulator - Phone
    (SEP001AA27AFFC3,'Auto 80051') will be skipped by broadcast; need a license
    key that supports more phones

2010-09-08 10:44:54,209 [pool-41-thread-1] ERROR PhoneRegulator - Phone
    (SEP3037A616CD9E,'Auto 80059') will be skipped by broadcast; need a license
    key that supports more phones

2010-09-08 10:44:54,209 [pool-41-thread-1] ERROR PhoneRegulator - Phone
    (SEP000BBED8055C,'Whip Dev Phone 80048') will be skipped by broadcast; need
    a license key that supports more phones

2010-09-08 10:44:54,209 [pool-41-thread-1] ERROR PhoneRegulator - Phone
    (SEP0022555EF1FE,'Auto 80052') will be skipped by broadcast; need a license
    key that supports more phones
```

Stopping and restarting InformaCast will clear the warning (see"Start/Stop/Restart InformaCast and its Server" on page 9-3), but as soon as you try to send to more phones than your license covers, the warning will reappear. Contact your Singlewire salesperson to obtain a larger license.

Q. Why doesn't InformaCast work correctly on the phone?

A. Check the firmware on the phone.

Q. I followed the install guide, but I still cannot send audio broadcasts. What did I miss?

A. Maybe nothing, it could just be the phones not acting as they should and needing to be power cycled, but check these options as well:

- Were the phones reset? You can verify this on the phone viewing the authentication URL, which should point to InformaCast. The path for this information varies (e.g. **Settings** | **3-Network Configuration** | **36-Authentication URL** or **Settings** | **3-Device Configuration** | **10-Authentication URL** or **Settings** | **3-Device Configuration** | **2-HTTP Configuration** | **5-Authentication URL**).
- Did you enter the Authentication URL into CUCM's Enterprise Parameters? Please see Steps 4 and 5 on page 2-65.
- If the phone still does not work, obtain a traffic capture. Look for error messages being sent back from the phone to InformaCast.
- View the InformaCast Performance log (**Help** | **Support**). Look to the bottom of the log for the most recent entries and look for the IP address of the phone you are troubleshooting. Are there errors?

Q. Sometimes a reset of the phones is not enough. You will have to remove the phone from its power source, let it sit for a few seconds, and then plug the phone back into the power source.How do I capture traffic?

A. See "Verify Multicast with a Network Traffic Capture" on page 2-70.

Q. The group to which I want to broadcast does not have an easily definable boundary (device pool or subnet). Is there another way that I can create groups?

A. The easiest way to make flexible groups is to be creative with the description of the phones in CUCM. If you are going to be creating groups based on building location, building floor, business unit, job title, etc., you can embed that information in the description and use a regular expression or the description suffix to build the group. See "Configure Advanced Matching for Recipient Groups" on page 4-37.

Q. How do I stop calls from InformaCast from being routed to voicemail if they go unanswered?

A. Singlewire designed DialCast for this very reason. Instead of calling users to make a page, DialCast has a user call the system to create a page, eliminating broadcasts playing over voicemail. See "Manage SIP Functionality" on page 5-4 for more information.

Q. How do I change InformaCast's IP address?

A. "Change InformaCast Virtual Appliance's IP Address" on page 10-20 will walk you through the steps for changing the Virtual Appliance's IP address.

Troubleshooting

This section is intended to help track down and resolve the common problems people face when configuring and working with InformaCast. Please look it over and see if your issues are addressed. You can also check "Frequently Asked Questions (FAQ)" on page 8-1.

Server Hardening

Problem My organizational security policy requires me to perform a hardening process for my virtual machines. How can I harden my InformaCast server?

Solution Your InformaCast Virtual Appliance comes from Singlewire already configured in a hardened state. Do not attempt to apply hardening guidelines found on the Internet on your InformaCast Virtual Appliance.

Multicast

Problem The audio portion of InformaCast's broadcasts aren't reaching the phones. Some symptoms include:

- No audio is heard through the phone
- A streaming icon displays on the phone's screen, but no audio is heard through the phone
- A phone's Speaker and Mute lights illuminate
- 7900 series phones makes a "bloop" noise

Solution Multicast isn't routing properly. If you've followed the recommendations in "Prepare Your Multicast Environment" on page 2-1, but you're still unable to hear audio broadcasts through your recipients, follow the recommendations in "Review Multicast Configuration" on page 2-70.

Log Files

Problem InformaCast is acting funny concerning errors, warnings, broadcasts, and security.

Solution When trying to find out what's going wrong with InformaCast, it often helps to look at the log files. The most commonly useful log, in which error messages will be logged when something unexpectedly goes wrong, is the Performance log (go to **Help** | **Support**).

When you're trying to check that a broadcast succeeded smoothly and reached all the recipients it should have, the Summary log (go to **Help** | **Support**) provides helpful information.

If you want to keep an eye on who is using the system and view other security-related information, the Audit log (https://<InformaCast Virtual Appliance IP Address>:8444/InformaCast/logs/audit.log) is the place to look.

Two other log files generated in the InformaCast logs directory are sipStackDebug.log and sipStackServer.log (go to **Help** | **Support**). Please see "Manage the SIP Stack" on page 5-38 for more information.

Resolve EULA Error

Problem I tried to start InformaCast and got the error, "You must accept the End User License Agreement (EULA) and configure networking before you can use InformaCast. Please go to the VM console in vSphere to continue the installation." So, I went to the vSphere console and no EULA is displayed; I just see the default console with an IP address, etc.

Solution You have two options: run the **swiftstart** command or redeploy the InformaCast OVA. To run the **swiftstart** command:

- Open vSphere.
- Select your virtual machine and go to **Inventory** | **Virtual Machine** | **Open Console**.
- Press **Alt** + **F2**.
- Log into your virtual machine.
- Enter **swiftstart** and press the **Enter** key. The SwiftStart End User License Agreement (EULA) window appears.
- Click the **I Agree** button to accept the EULA.
- Continue with Step 25 on page 2-19.

To redeploy the InformaCast OVA, see "Install InformaCast Virtual Appliance" on page 2-6.

Log into InformaCast Virtual Appliance's Interfaces

Problem How do I log into InformaCast? What are the different InformaCast interfaces and what do they do?

Solution When using this guide, you will need to log into the different interfaces that InformaCast has: InformaCast, the Control Center, and Webmin. All of these interfaces are accessible through the Singlewire Start page, which is the IP address of your InformaCast Virtual Appliance. The following sections walk you through logging into InformaCast's interfaces:

- "Log into the InformaCast Virtual Appliance" on page 10-2
- "Log into InformaCast" on page 10-3
- "Log into the Control Center" on page 10-5
- "Log into Webmin" on page 10-7

Start/Stop/Restart InformaCast and its Server

Problem You need to start, stop, or restart InformaCast or reboot InformaCast's virtual machine.

Solution Backing up and restoring InformaCast and application malfunction file are all reasons you would need to start and stop InformaCast or reboot its virtual machine. The following sections walk you through starting, stopping, and restarting applications and rebooting the Virtual Appliance:

- "Stop an Application on InformaCast Virtual Appliance" on page 10-10
- "Start an Application on InformaCast Virtual Appliance" on page 10-12
- "Restart an Application on InformaCast Virtual Appliance" on page 10-14
- "Reboot the InformaCast Virtual Appliance" on page 10-16

VMware Tools

Problem vSphere has an error flag that says that my version of VMware doesn't match my version of VMware tools. Also, my CPU usage seems elevated. How do I fix this?

Solution Upgrade your VMware tools to match the level of your VMware version (see "Upgrade your VMware Tools" on page 10-24 for more information).

Authentication

Problem When attempting a broadcast, the phones do not respond (i.e. no audio is heard). The Summary log reports authentication errors for each phone attempted (go to **Help** | **Support**).

Solution Check the authentication URL. When InformaCast attempts a broadcast, the phones check whether the attempt should be permitted. Make sure that you've set up your phones to use InformaCast's built-in authentication service, and that CUCM's Enterprise System Parameters were updated to use the value displayed on InformaCast's Edit Telephony Configuration page as the URL for authentication.

On one of the phones being used with InformaCast, verify that the authentication URL shows the same value displayed on InformaCast's Edit Telephony Configuration page. The path for this information on a phone varies (e.g. **Settings** | **3-Network Configuration** | **36-Authentication URL** or **Settings** | **3-Device Configuration** | **10-Authentication URL** or **Settings** | **3-Device Configuration** | **2-HTTP Configuration** | **5-Authentication URL**).

If it does not, correct the settings in the CUCM administrative interface: in the **System** menu, select **Enterprise Parameters** and edit the **URL Authentication** and **Secured Authentication URL** fields. Once this is correct, you must reset all the phones so that they learn about the new URL.

Problem I have errors on my Edit Telephony Configuration page.

Solution If you encounter errors on the Edit Telephony Configuration page, verify that the fields have the proper information entered into them. Check the following fields' information:

- **Communications Manager AXL User.** Access CUCM's administrative interface and log in with the same username/password combination. If you are unable to log in, InformaCast will be unable to log in.

- **Communications Manager IP Address(es).** Use the same test as for the **Communications Manager Admin User** field.
- **Communications Manager Application User.** Access CUCM's administrative interface and ensure that your application user's credentials in InformaCast match those in CUCM.
- **SNMP Community Name.** Verify that the value you entered here matches the value in CUCM. Use the Multicast Testing Tool to verify SNMP functionality.

Problem I'm seeing the error, "Default configuration Not Connected," in the CUCM Versions column on the Admin Overview page.

Solution Rebuild your phone cache. This problem occurs whenever your license changes and whenever you add/update/delete a cluster. If either the license or clusters change, the phone cache must be rebuilt to reflect those changes. The phone cache is automatically rebuilt every hour, but if you want it completed sooner than that, you can click the **Update** button on the Edit Recipient Groups page to discover current IP phone information from CUCM. Once this is done, the CUCM information appears correctly on the Admin Overview page.

Phone Discovery

Problem I've added new phones to CUCM and made changes to existing ones, and these additions and changes aren't reflected in InformaCast even after I've rebuilt my phone cache.

Solution When the amount of data requested by all active InformaCast requests exceeds 16MB, AXL (which InformaCast uses to communicate with CUCM) will throttle traffic and return a 503 error. The end result is that your phone cache isn't updated and InformaCast won't "see" your changes. This is most likely to happen if you have multiple InformaCast servers. You should avoid having multiple InformaCast servers build their phone caches at the same time on a CUCM cluster. Schedule your phone caches to rebuild through the CUCM Phone Updates page (**Admin** | **Telephony** | C**UCM Phone Updates**).

Problem There are phones missing from my recipient groups.

Solution If InformaCast is unable to learn about the phones in your CUCM environment, it cannot work properly. It must do this by interacting with the CUCM server. If the Edit Recipient Groups page in InformaCast shows that the "All Recipients" group is empty, attempts to send broadcasts will result in an error message with a stack trace.

Phones are found from CUCM using SNMP and AXL. If you have phones missing from a recipient group, ensure the following:

- You have the most up-to-date recipients: click the **Update** button on the Edit Recipient Groups page.
- The CUCM Admin account has the correct username/password information. The top items on InformaCast's Edit Telephony Configuration page are used to set up an administrative password for InformaCast to interact with the CUCM server. Make sure that these are correct. Start by logging into your CUCM server's administrative interface using the same username and password, and make sure that you can use the **Device** menu's **Phone** option to list the phones in your installation. Once you're sure that the username and password are suitable, carefully re-enter them in InformaCast's Edit Telephony Configuration page to make sure they've been entered correctly.

- The Communication Manager's IP address is correct. InformaCast needs to know where to reach the CUCM server. Make sure the **Communications Manager IP Address** field on the Edit Telephony Configuration page contains the correct numeric IP address of your CUCM server.
- SNMP is properly enabled. Ensure that SNMP is enabled on the CUCM cluster node, the SNMP community strings have READ permissions on the CUCM cluster node, and that SNMP community strings are the same on the CUCM cluster node. See "Configure CUCM SNMP" on page 2-31. You can use the Multicast Testing Tool to troubleshoot SNMP further.
- You're using a supported CUCM version. You must have version 7.0 or later of CUCM in order to use InformaCast 8.2 (and later). If you're running an older version of CUCM, one of the symptoms will be InformaCast's inability to discover phone information from the server.
- Nothing is blocking UDP port 161 from InformaCast to the CUCM cluster node.
- There are usable phones registered. If everything else seems fine, it's worth double-checking, via the CUCM administrative interface, that there are actually some phones registered (they show up with IP addresses rather than "not found").

Problem I'm using Cisco's DX70, DX80, and DX650 model IP phones along with other Cisco phone models in my organization. All of my phones are registering with both CUCM and InformaCast except for my DX model phones. Why can't I add DX model phones to InformaCast's recipient groups.

Solution In order for Cisco's DX model IP phones to register with InformaCast, they need to be running the Singlewire Notification System (SNS) application. This application is not supported for Basic InformaCast. Please upgrade to Advanced InformaCast to take advantage of Cisco's DX model IP phones.

Broadcasts

Problem Many or all of my broadcasts are unsuccessful, Skip Phones in Use isn't working properly, and/or I'm seeing slow activation and deactivation times.

Solution Have you selected the **Send Commands to Phones By JTAPI** checkbox on the Broadcast Parameters page and:

- Are you working with any of the following Cisco IP phone models: 3905, 69XX, or 7905, 7910, or 7912?
- Are you using any of the following versions of CUCM: 8.6.2, 9.1.1, and 9.1.1a?

Depending on your answer, you will have different fixes:

- If you selected the **Send Commands to Phones By JTAPI** checkbox on the Broadcast Parameters page and are working with the 3905 Cisco IP phone model, you may encounter unsuccessful broadcasts and malfunctioning Skip Phones in Use behavior because the 3905 does not work with the **Send Commands to Phones By JTAPI** checkbox selected. This is a known Cisco issue (CSCtq36901). Check the Cisco Bug Toolkit for an update. As a temporary fix, you can deselect the **Send Commands to Phones By JTAPI** checkbox until Cisco resolves the issue.
- If you selected the **Send Commands to Phones By JTAPI** checkbox on the Broadcast Parameters page and are working with the 69XX Cisco IP phone model, you may encounter phones not activating or deactivating properly. This is a known Cisco issue (CSCuo79130). Check the Cisco Bug Toolkit for an update. As a temporary fix, you can deselect the **Send Commands to Phones By JTAPI** checkbox until Cisco resolves the issue.

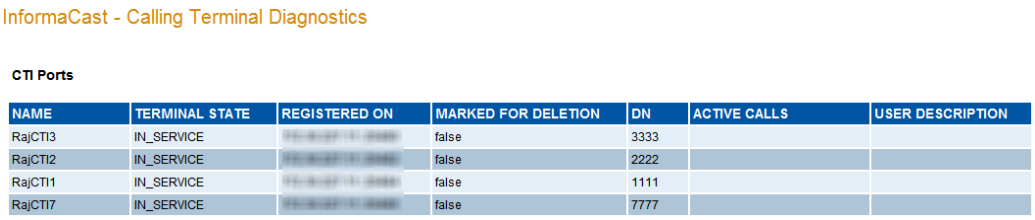
- If you selected the **Send Commands to Phones By JTAPI** checkbox on the Broadcast Parameters page and are working with the 905, 7910, or 7912 Cisco IP phone models, you will see unsuccessful broadcasts. The 905, 7910, and 7912 Cisco IP phones do not work with the **Send Commands to Phones By JTAPI** checkbox. Deselect it to resolve your problem.
- If you selected the **Send Commands to Phones By JTAPI** checkbox on the Broadcast Parameters page and you are using CUCM versions 8.6.2, 9.1.1, or 9.1.1a, you may encounter a 30-second delay when sending commands to a phone. This is a known Cisco issue (CSCug40245). To resolve it, 8.6.2 customers should upgrade to the latest service release, and 9.1 customers should upgrade to 9.1.2, or uncheck the **Send Commands to Phones By JTAPI** checkbox.

Problem There are errors on the Edit Telephony Configuration page.

Solution One or more of the following may be to blame:

- You didn't associate your CTI ports to your application user
- You upgraded CUCM, but didn't upgrade JTAPI on the Virtual Appliance
- CUCM's CTIManager service has an issue

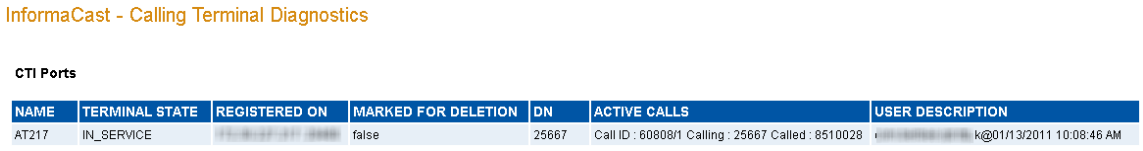
Check out Singlewire's Calling Terminal Diagnostics page (**Help** | **Support**), which shows the health of InformaCast's CTI connection to CUCM. Under normal circumstances, the Calling Terminal Diagnostics page shows you the status of your CTI ports, as shown in the following graphic.


InformaCast - Calling Terminal Diagnostics

CTI Ports

NAME	TERMINAL STATE	REGISTERED ON	MARKED FOR DELETION	DN	ACTIVE CALLS	USER DESCRIPTION
RajCTI3	IN_SERVICE	[redacted]	false	3333		
RajCTI2	IN_SERVICE	[redacted]	false	2222		
RajCTI1	IN_SERVICE	[redacted]	false	1111		
RajCTI7	IN_SERVICE	[redacted]	false	7777		

The Calling Terminal Diagnostics page can also show you the status of active calls/broadcasts, as shown in the following graphic.


InformaCast - Calling Terminal Diagnostics

CTI Ports

NAME	TERMINAL STATE	REGISTERED ON	MARKED FOR DELETION	DN	ACTIVE CALLS	USER DESCRIPTION
AT217	IN_SERVICE	[redacted]	false	25667	Call ID : 60808/1 Calling : 25667 Called : 8510028	[redacted]k@01/13/2011 10:08:46 AM

You can use the Calling Terminal Diagnostics page to verify that your CTI devices in CUCM are registered with InformaCast. It is also recommended that you have your Network Monitoring Solution (NMS) view this page to ensure all items are "In Service," and send you an alert in case of server failures.

The Calling Terminal Diagnostics page should refresh every 15 seconds. However, if you are using Internet Explorer 8.x, you will need to take some extra steps to ensure the refresh rate of the page. Firefox is unaffected and should refresh as directed.

Step 1 Open Internet Explorer.

Step 2 Go to **Tools** | **Internet Options**. The Internet Options dialog box appears.

Step 3 Click the **Security** tab and select the **Internet** zone.

Step 4 Click the **Custom level** button. The Security Settings - Internet Zone dialog box appears.

Step 5 Scroll down the Settings list until you find the **Allow META REFRESH** entry.

Step 6 Click its **Enable** radio button.

Step 7 Click the **OK** button on the Security Settings - Internet Zone dialog box.

Step 8 Click the **Yes** button on the warning that pops up.

Step 9 Click the **OK** button on the Internet Options dialog box.

Problem After a recent upgrade of InformaCast from pre-8.4 version to 8.4 or later, broadcasts sound choppy or robotic at remote sites or during times of heavy network traffic loads.

Solution In InformaCast versions prior to 8.4, applications' QoS settings were set in the code and did not match Cisco's default QoS DSCP values. On the Virtual Appliance, the QoS settings have been moved to the OS level and now match Cisco's default settings. These settings are:

- Media RTP traffic set to DSCP EF
- Call signaling traffic set to DSCP CS3 (call signaling traffic includes SIP and CTI traffic)
- HTTP traffic to IP phones set to DSCP 0
- Any other traffic set to DSCP 0

If you need to change from these default values, you will need to do so at the network level. Rewriting DSCP values is covered in the Cisco Quality of Service (QoS) Solution Reference Network Design (SRND) guide, found at http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book/QoSIntro.html and should be handled by your network administrator.

Upgrading InformaCast

Problem I want to upgrade my version of InformaCast. Where do I find the steps for that process?

Solution InformaCast is part of the larger InformaCast Virtual Appliance. If you are looking to upgrade your version of InformaCast Virtual Appliance, follow the upgrade steps in "Upgrade InformaCast Virtual Appliance" on page 10-25.

Upgrading from Basic to Advanced InformaCast

Problem I upgraded InformaCast (from Basic to Advanced trial/demonstration/subscription/perpetual) and I'm seeing some of the following problems:

- I can't log in
- My recipients/user accounts/dialing configurations, etc. are missing
- I'm sending out broadcasts that have worked in the past, but they're not going through now

Solution If you upgrade from Basic to Advanced InformaCast through either the trial, demonstration, subscription or perpetual licenses and you decide to return to Basic functionality, all additional information entered during your Advanced phase will not be saved. If you choose to upgrade back to Advanced InformaCast, that information will reappear; however, any new information you entered after you reverted to Basic functionality will be unavailable.

For the three examples cited in this problem, you have a few options:

- **I can't log in.** Did you change your administrator password while you were in Advanced InformaCast? If so, your password has reverted to what it was when you were initially in Basic InformaCast. Use that password for logging in. If you have forgotten that password, contact Singlewire Support to reset your password.
- **My recipients/user accounts/dialing configurations, etc. are missing.** If you added these recipients/user accounts/dialing configurations while you were in Advanced InformaCast, downgrading to Basic InformaCast reverts you to the information you last entered before your upgrade. You will need to enter this information again or upgrade again to Advanced InformaCast. Please note that any new information you entered in your second go-round with Basic InformaCast will not be available if you decide to upgrade again to Advanced InformaCast.
- **I'm sending out broadcasts that have worked in the past, but they're not going through now.** Did you change your IP address in Advanced InformaCast before reverting to Basic InformaCast? If so, your broadcasts will no longer work. You will need to redeploy the InformaCast OVA (see "Install InformaCast Virtual Appliance" on page 2-6) to fix this issue.

Problem I just upgraded InformaCast and I have errors on the Edit Telephony Configuration page.

Solution If you encounter errors on the Edit Telephony Configuration page, verify that the fields have the proper information entered into them. Check the following fields' information:

- **Communications Manager AXL User.** Access CUCM's administrative interface and log in with the same username/password combination. If you are unable to log in, InformaCast will be unable to log in.
- **Communications Manager IP Address(es).** Use the same test as for the **Communications Manager Admin User** field.
- **Communications Manager Application User.** Access CUCM's administrative interface and ensure that your application user's credentials in InformaCast match those in CUCM.
- **SNMP Community Name.** Verify that the value you entered here matches the value in CUCM. Use the Multicast Testing Tool to verify SNMP functionality.

Problem I just upgraded/downgraded InformaCast and I'm seeing the error, "Default configuration Not Connected," in the Communications Manager Versions column on the Admin Overview page.

Solution Rebuild your phone cache. This problem occurs whenever your license changes and whenever you add/update/delete a cluster. If either the license or clusters change, the phone cache must be rebuilt to reflect those changes. The phone cache is automatically rebuilt every hour, but if you want it completed sooner than that, you can click the **Update** button on the Edit Recipient Groups page to discover current IP phone info from CUCM. Once this is done, the CUCM information appears correctly on the Admin Overview page.

Problem I just upgraded InformaCast and there are phones missing from my recipient groups.

Solution Phones are found from CUCM using SNMP and AXL. If you have phones missing from a recipient group, ensure the following:

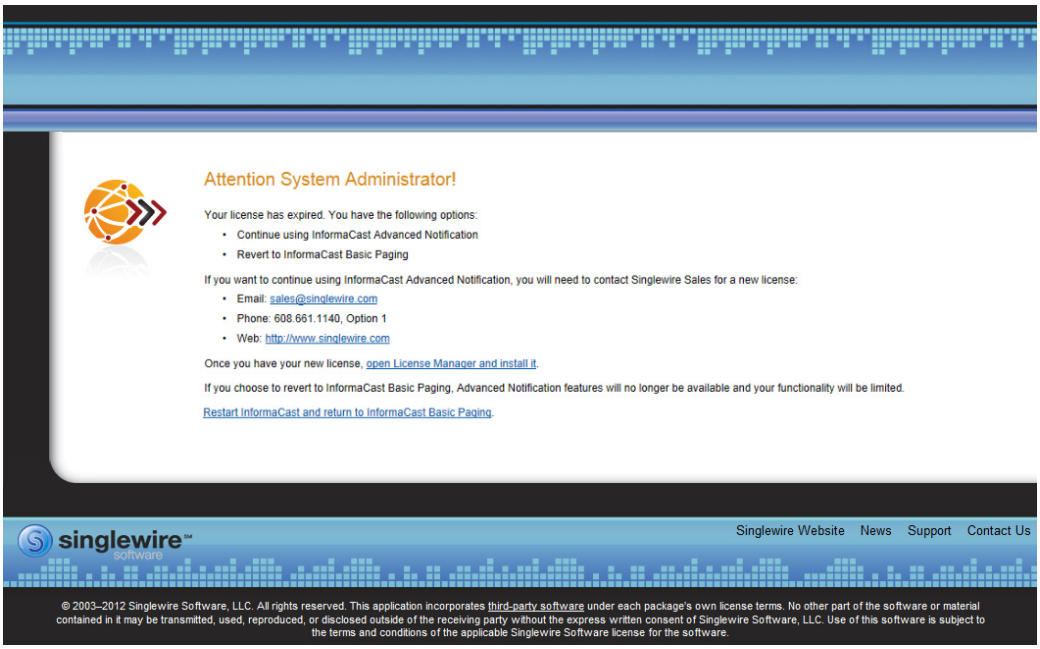
- The CUCM Admin account has the correct username/password information
- SNMP is enabled on all CUCM cluster nodes
- SNMP community strings have READ permissions on all CUCM cluster nodes
- SNMP community strings are the same on all CUCM cluster nodes
- Nothing is blocking UDP port 161 from InformaCast to all CUCM cluster nodes

You can use the Multicast Testing Tool to troubleshoot SNMP further.

Problem I upgraded from Basic to Advanced InformaCast, but then returned to Basic functionality. Now, I'm seeing some empty recipient groups and my broadcasts aren't successful.

Solution If you upgrade from Basic to Advanced InformaCast through either the trial, demonstration, subscription, or perpetual licenses and you decide to return to Basic functionality, the phones you see on the Edit Recipient Groups and Add/Edit Recipient Group pages may not reflect the current telephony configuration, leading to empty recipient groups and unsuccessful broadcasts. Ensure that you have the most up-to-date recipients by clicking the **Update** button on the Edit Recipient Groups page.

Problem I just logged into InformaCast and I'm getting a message that my license has expired.



Solution Advanced Notification trial, demonstration, and subscription licenses all have expiration limits. If you want to continue using Advanced Notification, you will need to contact Singlewire to obtain a new license. If you decide to revert to Basic Paging by clicking the **Restart InformaCast and return to InformaCast Basic Paging** link, InformaCast will restart, you will lose Advanced

Notification functionality and all additional data entered during your Advanced Notification phase will be unavailable (e.g. when you revert to Basic Paging from Advanced Notification, any data you entered after you upgraded initially—dialing configurations, users, recipient groups, etc.—will not be available once you downgrade to Basic Paging). If you choose to upgrade back to Advanced Notification, that data will be restored; however, any new data you entered after you reverted to Basic Paging functionality will be unavailable.

Manage InformaCast Virtual Appliance

The following sections detail how to manage InformaCast Virtual Appliance from the server side.

Log into InformaCast Virtual Appliance's Interfaces

When using InformaCast Virtual Appliance, you will need to log into it and its different interfaces: InformaCast, PushToTalk, the Control Center, and Webmin. All of these interfaces are accessible through the Singlewire Start page, which is the IP address of the InformaCast Virtual Appliance.

Note PushToTalk is not supported by InformaCast Basic Paging. Please contact Singlewire for an upgrade to Advanced Notification.

Log into the InformaCast Virtual Appliance

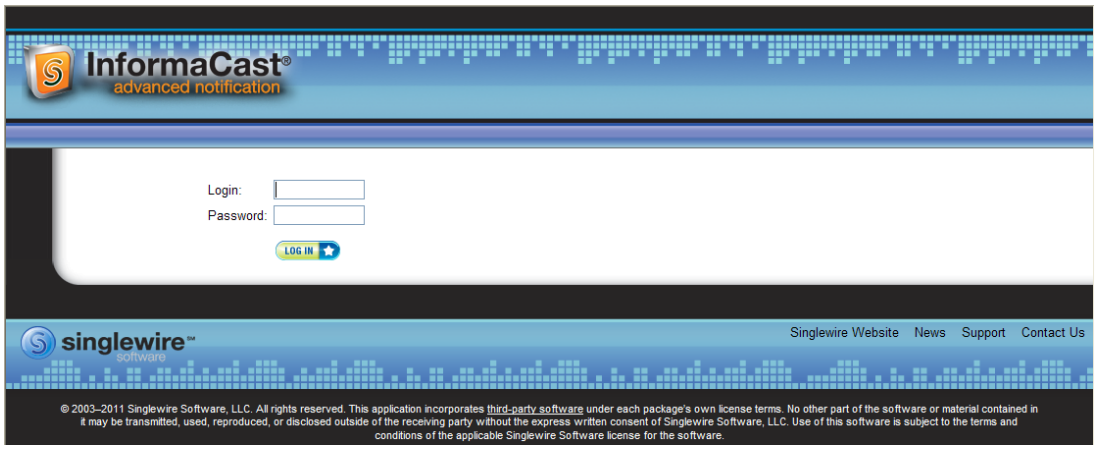
Open a web browser, enter the IP address of the InformaCast Virtual Appliance, and press the **Enter** key. The Singlewire Start page appears.

Log into InformaCast

InformaCast's web interface is where you will set up your InformaCast environment, e.g. recipient groups, DialCasts, etc.

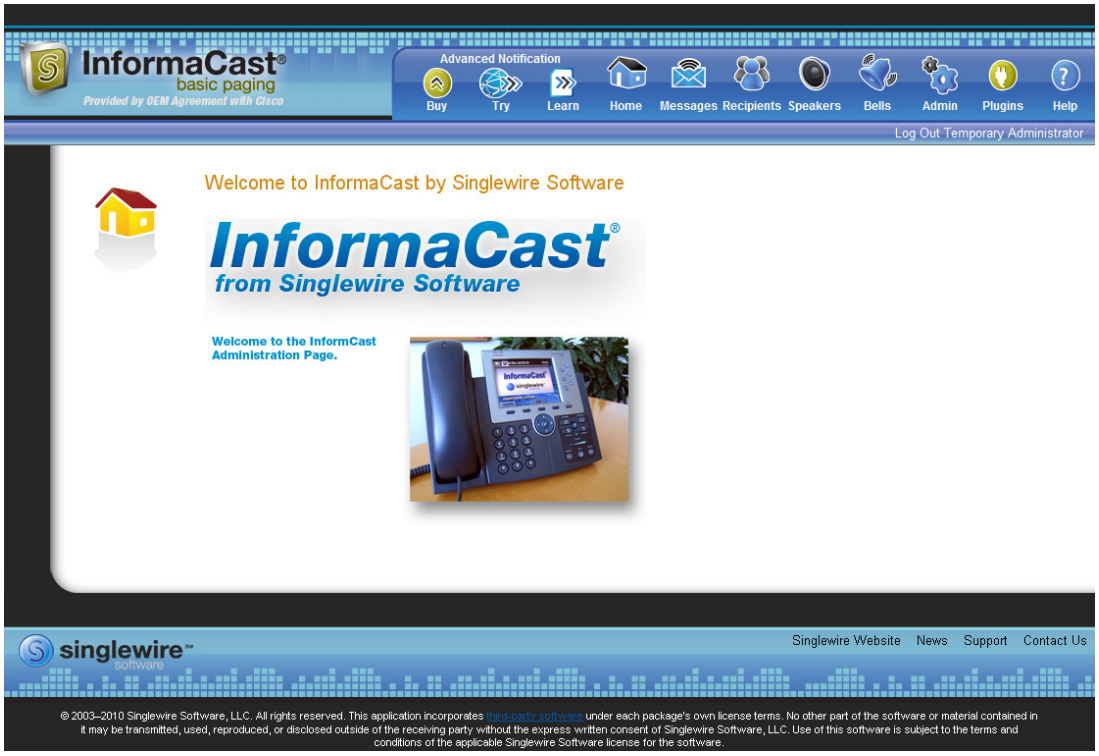
Step 1 Open a web browser, enter the IP address of the InformaCast Virtual Appliance, and press the **Enter** key. The Singlewire Start page appears.

Step 2 Click the **InformaCast** link. A separate tab/window opens to InformaCast's Login page.



Step 3 Enter your username and password in the **Login** and **Password** fields, respectively. By default, these are **admin** and **changeMe**.

Step 4 Click the **Log In** button. InformaCast's homepage appears.



From InformaCast's homepage, you can access any of its web features through the icons at the top of the page.

Log into PushToTalk

PushToTalk is designed to facilitate easy and immediate communication between multiple parties or on a one-to-one basis through talk/listen or intercom functionality. From the **Services** button on any designated phone or the side button of the 7921G wireless IP phone, you can pick from a list of phone groups and initiate a PushToTalk "session." For sessions with greater than two participants, parties can either talk or listen and switch between the two (i.e. talk/listen functionality). For one-to-one sessions, both parties can talk and listen at the same time (i.e. intercom functionality).

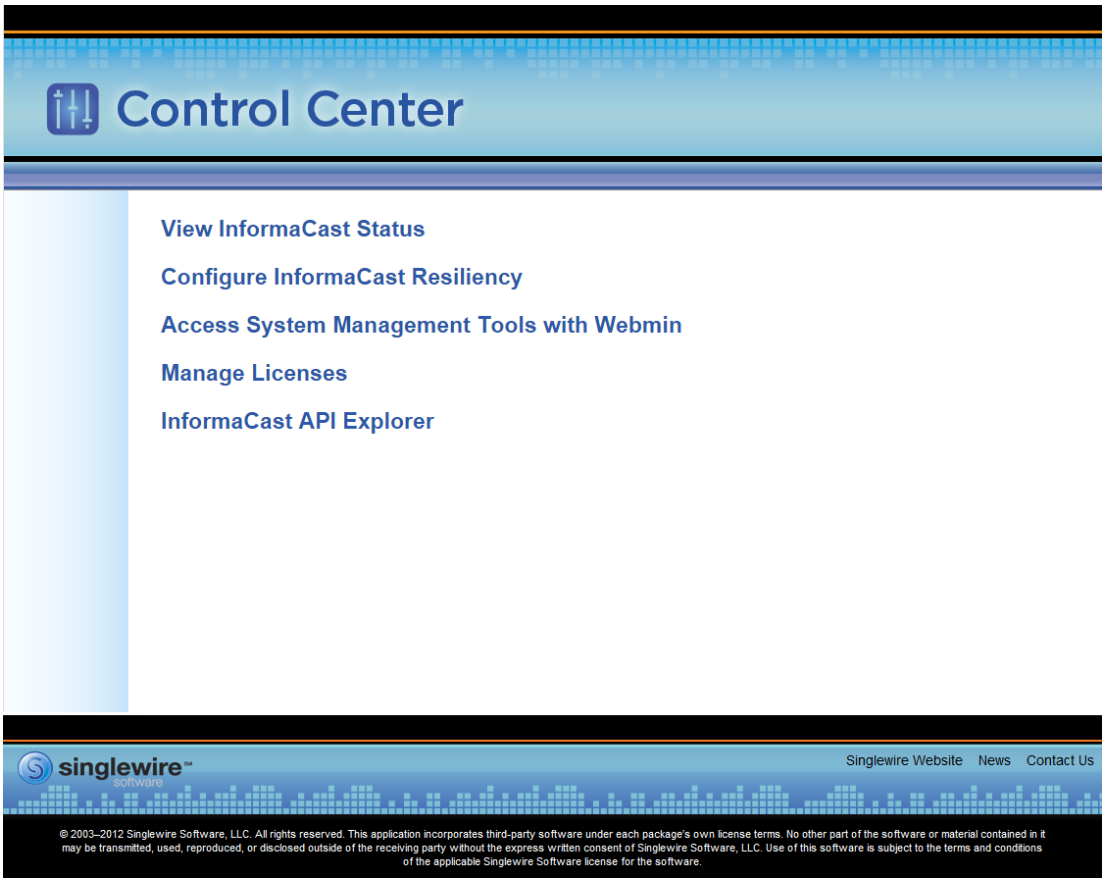
Note PushToTalk is not supported by InformaCast Basic Paging. Please contact Singlewire for an upgrade to Advanced Notification.

Log into the Control Center

The Control Center is your destination for Virtual Appliance accessory actions, e.g. viewing InformaCast's status, accessing Webmin, upgrading licensing, etc.

Step 1 Open a web browser, enter the IP address of the InformaCast Virtual Appliance, and press the **Enter** key. The Singlewire Start page appears.

Step 2 Click the **Access Application Management Tools with Control Center** link. A separate tab/window opens to the Control Center menu page.



Note You may have to accept a warning from your web browser about the security of this page's content.

Note The **Configure InformaCast Resiliency** link is dependent upon your license containing resiliency functionality: if your license doesn't include resiliency, you won't see the link.

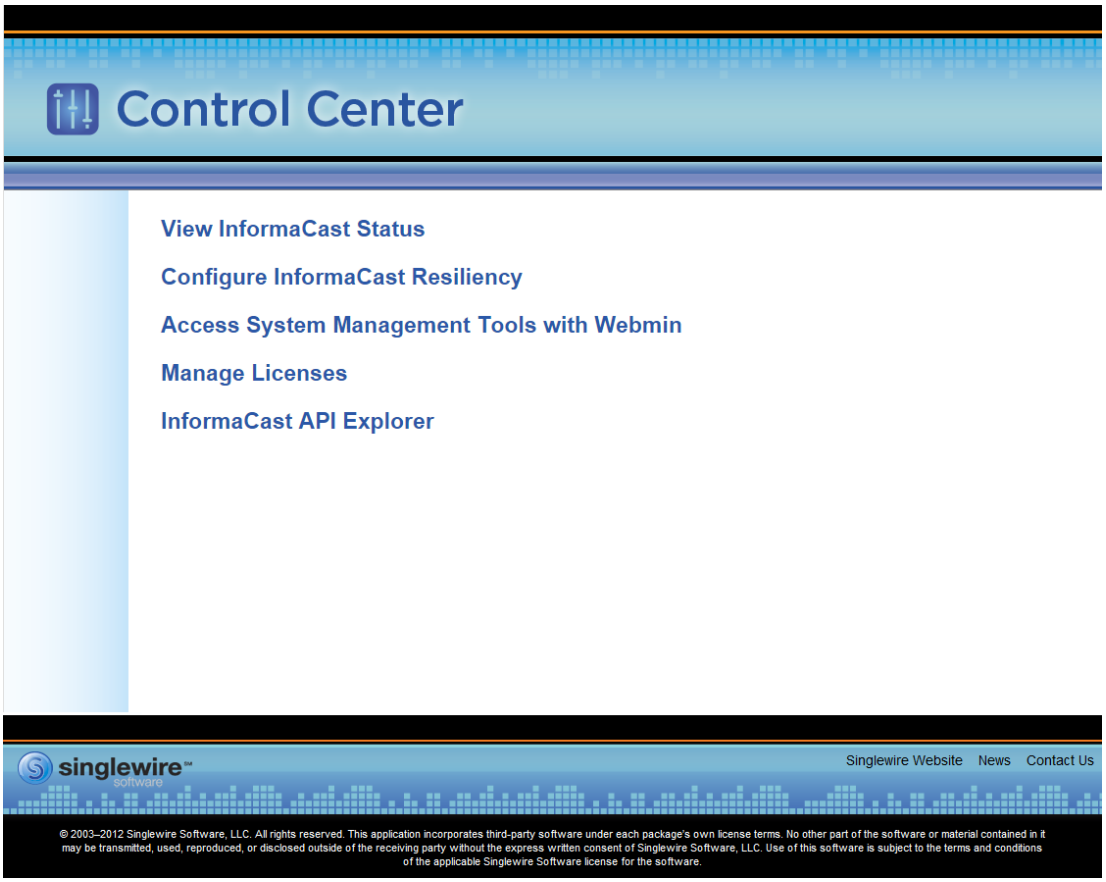
From the Control Center menu page, you can access Singlewire's accessory tools.

Log into Webmin

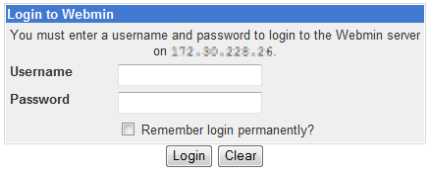
Webmin's interface is used primarily for installing new software packages, starting/stopping/restarting Singlewire's applications, and rebooting the InformaCast Virtual Appliance virtual machine.

Step 1 Open a web browser, enter the IP address of the InformaCast Virtual Appliance, and press the **Enter** key. The Singlewire Start page appears.

Step 2 Click the **Access Application Management Tools with Control Center** link. A separate tab/window opens to the Control Center menu page.

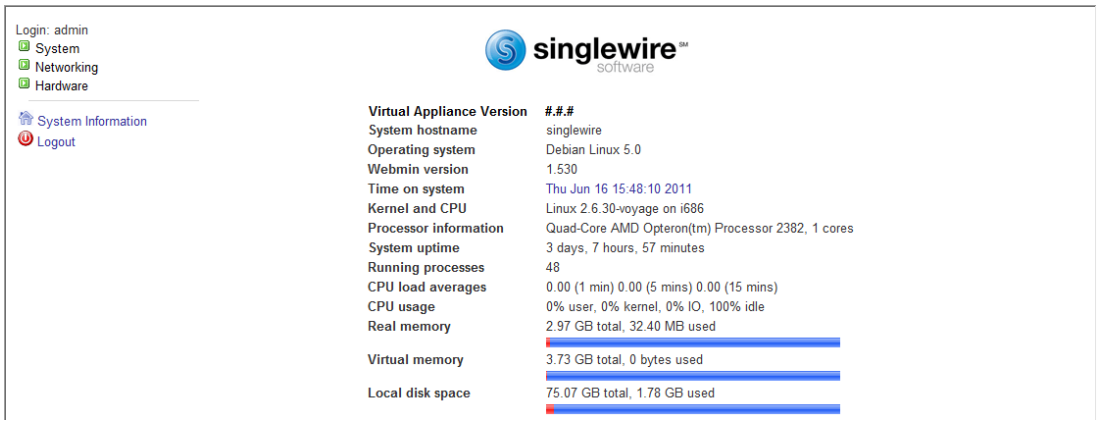


Step 3 Click the **Access System Management Tools with Webmin** link. A separate tab/window opens to the Login to Webmin page.



Note You may have to accept a warning from your web browser about the security of this page's content.

Step 4 Enter your login credentials and click the **Login** button. By default, your username is **admin** and your password is **changeMe**. The Webmin homepage appears.



The Webmin homepage displays versioning information and statistics about the Virtual Appliance.

From the Webmin homepage, you can install a new software package (see "Install a New Software Package" on page 10-27), start/stop/restart Singlewire's applications, and reboot the InformaCast virtual machine (see the sections on stopping/starting/rebooting starting with "Manage Virtual Appliance Actions" on page 10-10 for more information).

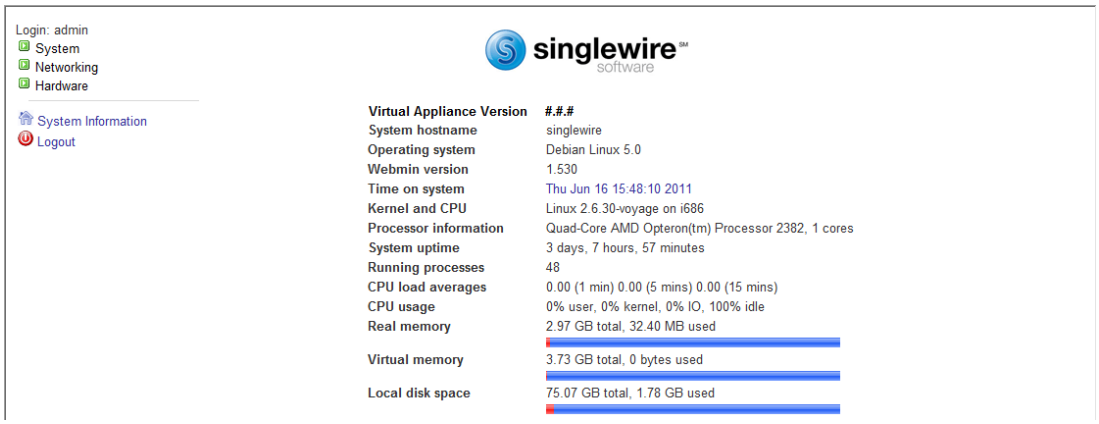
Manage Virtual Appliance Actions

Starting, stopping, and restarting applications and rebooting the Virtual Appliance are all management actions you can perform through Webmin.

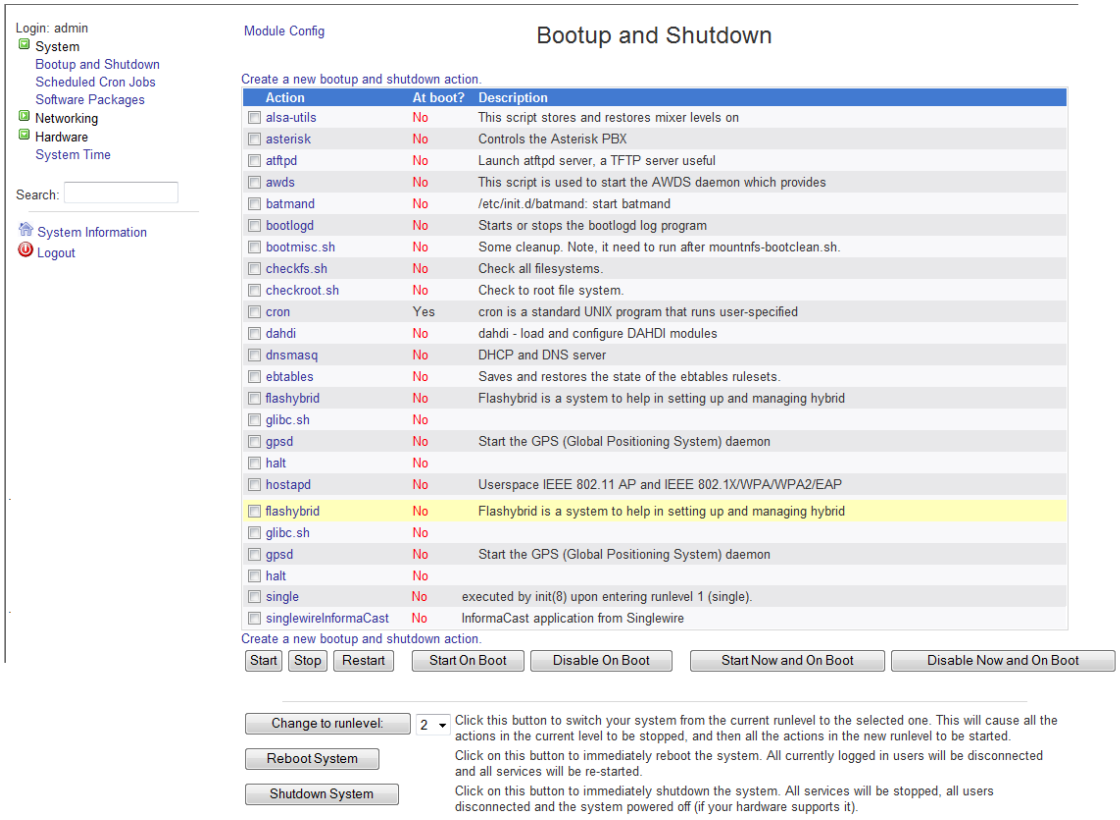
Stop an Application on InformaCast Virtual Appliance

Follow these steps to stop individual applications on InformaCast Virtual Appliance.

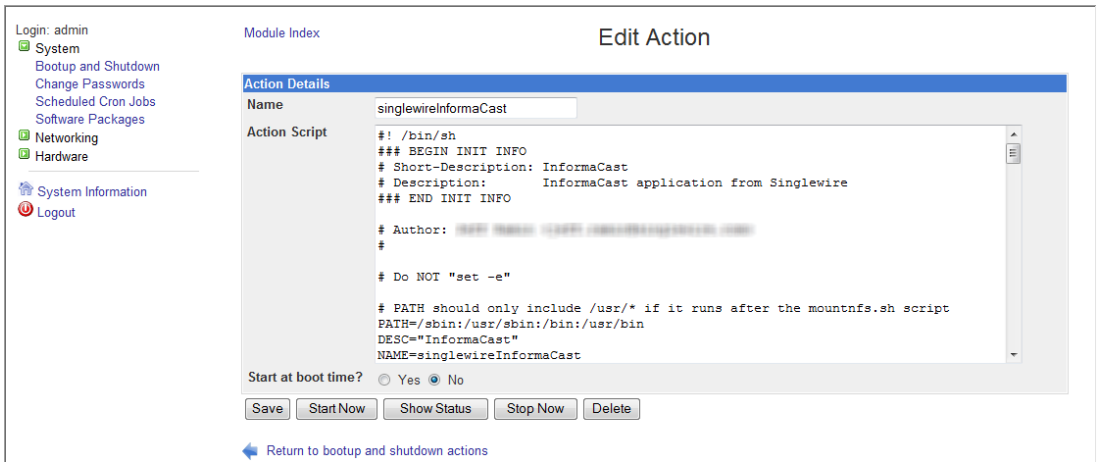
Step 1 Log into Webmin (see "Log into Webmin" on page 10-7 for specific steps). The Webmin homepage appears.



Step 2 Go to **System | Bootup and Shutdown**. The Bootup and Shutdown page appears.



Step 3 Scroll down the list of actions until you come to your application's name (e.g. **singlewireInformaCast**). Click its link. The Edit Action page appears.

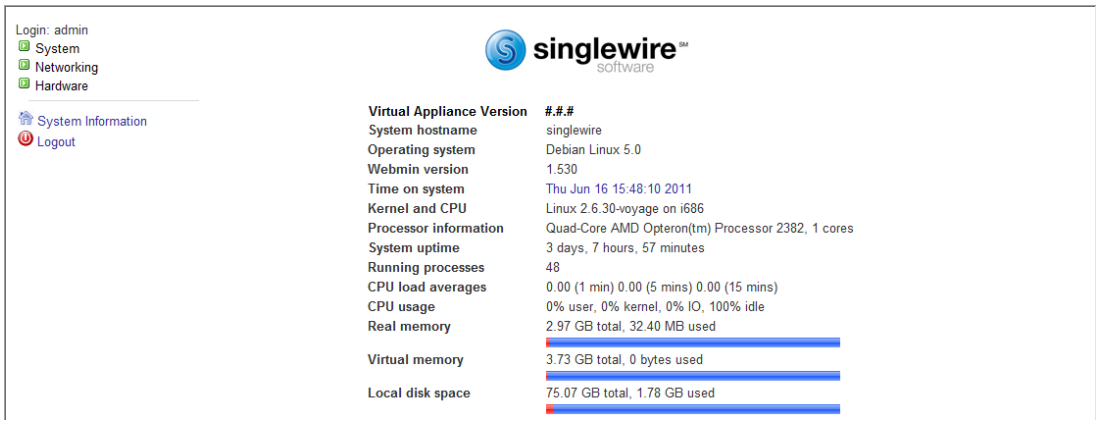


Step 4 Click the **Stop Now** button. It will take a minute or so for the application to stop.

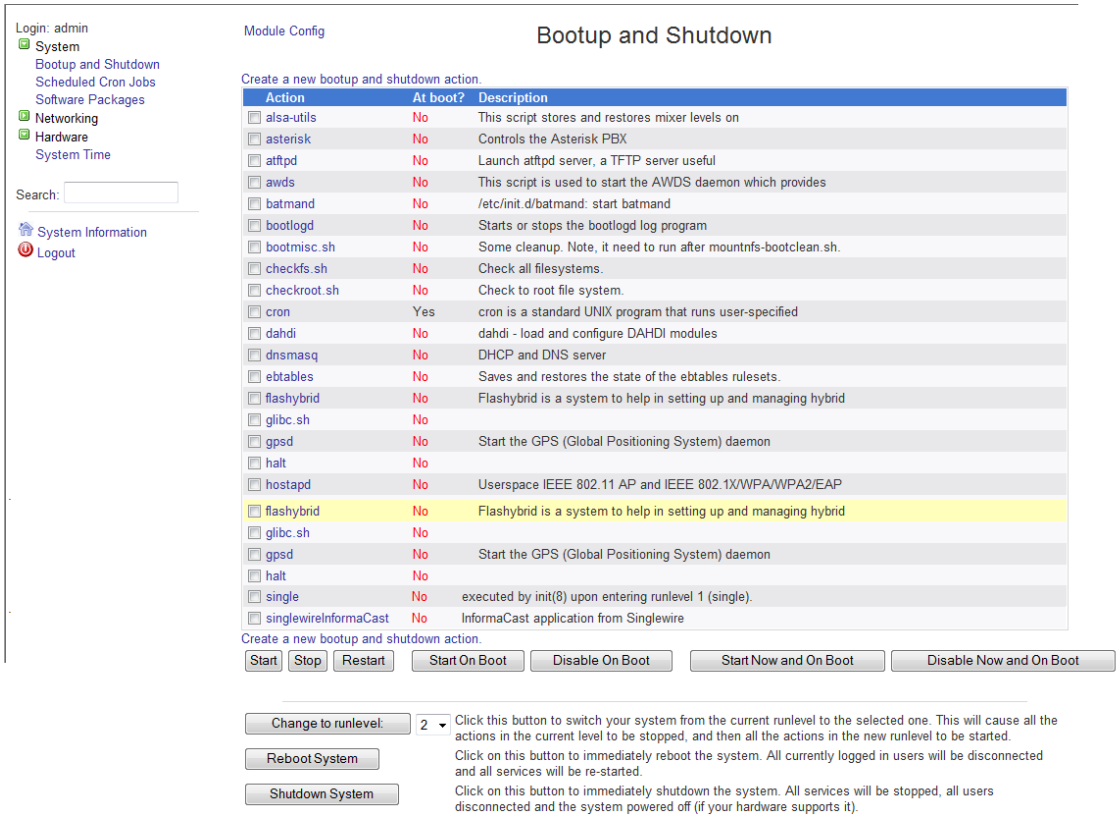
Start an Application on InformaCast Virtual Appliance

Follow these steps to start individual applications on InformaCast Virtual Appliance.

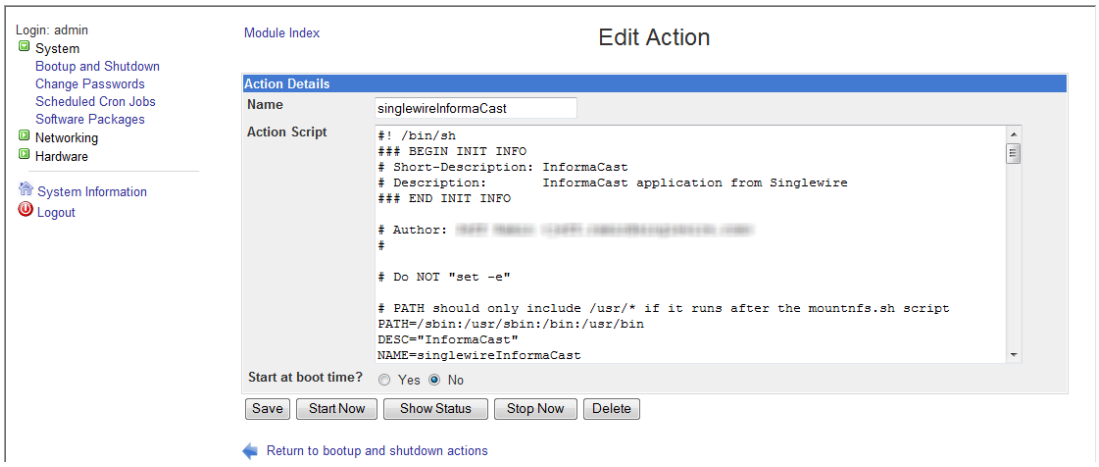
Step 1 Log into Webmin (see "Log into Webmin" on page 10-7 for specific steps). The Webmin homepage appears.



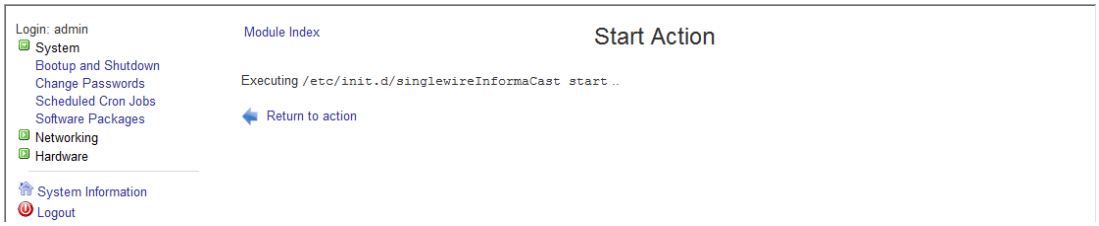
Step 2 Go to **System | Bootup and Shutdown**. The Bootup and Shutdown page appears.



Step 3 Scroll down the list of actions until you come to your application's name (e.g. **singlewireInformaCast**). Click its link. The Edit Action page appears.



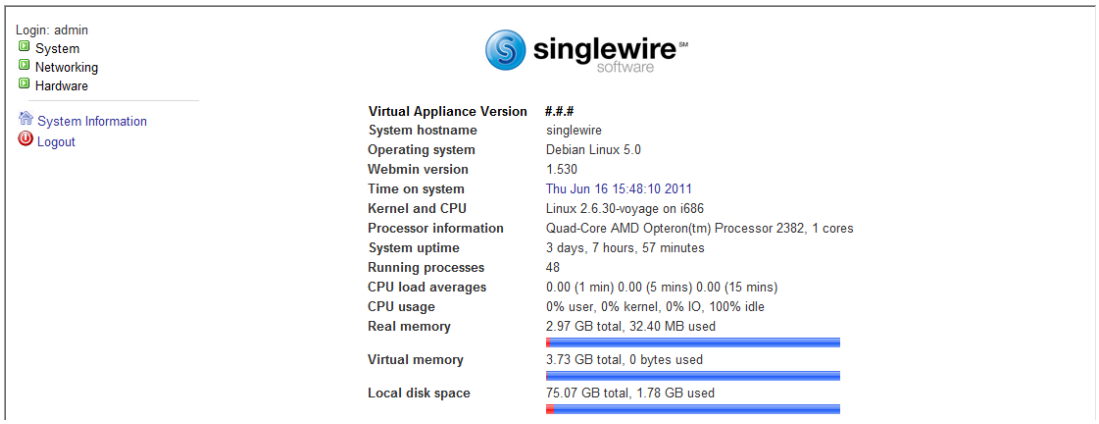
Step 4 Click the **Start Now** button. It will take a minute or so for the application to start.



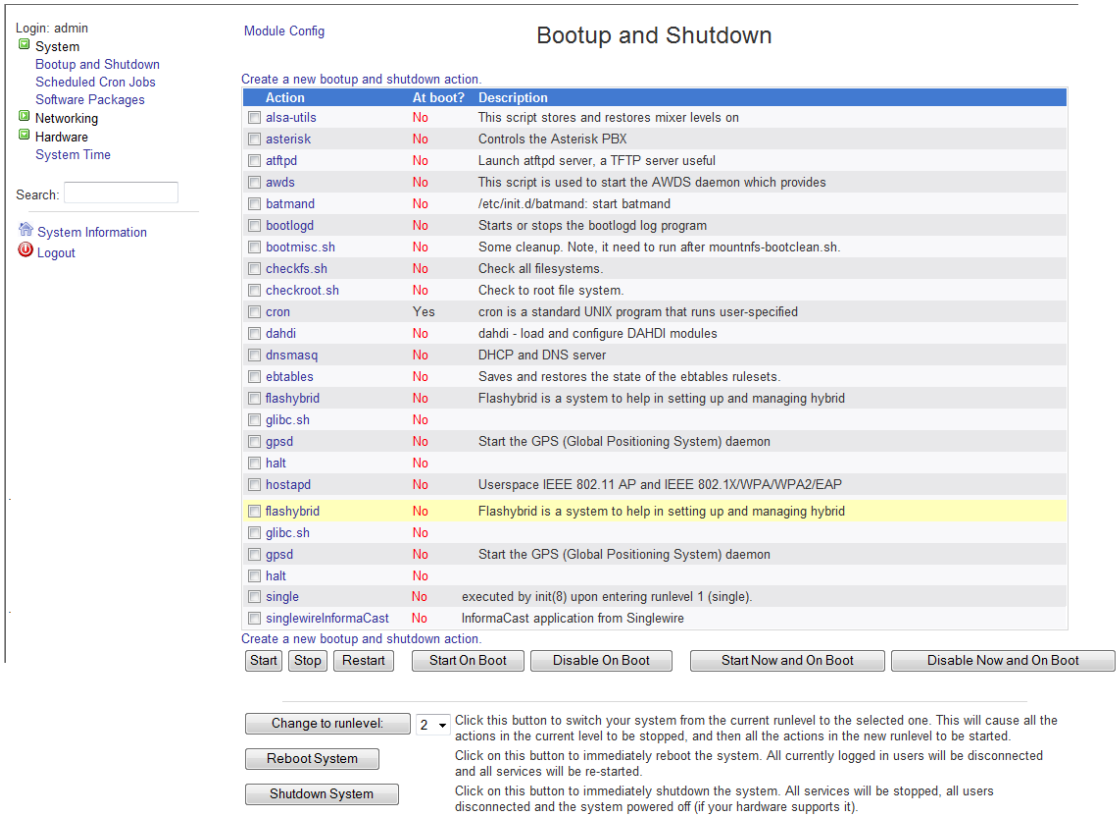
Restart an Application on InformaCast Virtual Appliance

Follow these steps to restart individual applications on InformaCast Virtual Appliance.

Step 1 Log into Webmin (see "Log into Webmin" on page 10-7 for specific steps). The Webmin homepage appears.



Step 2 Go to **System | Bootup and Shutdown**. The Bootup and Shutdown page appears.



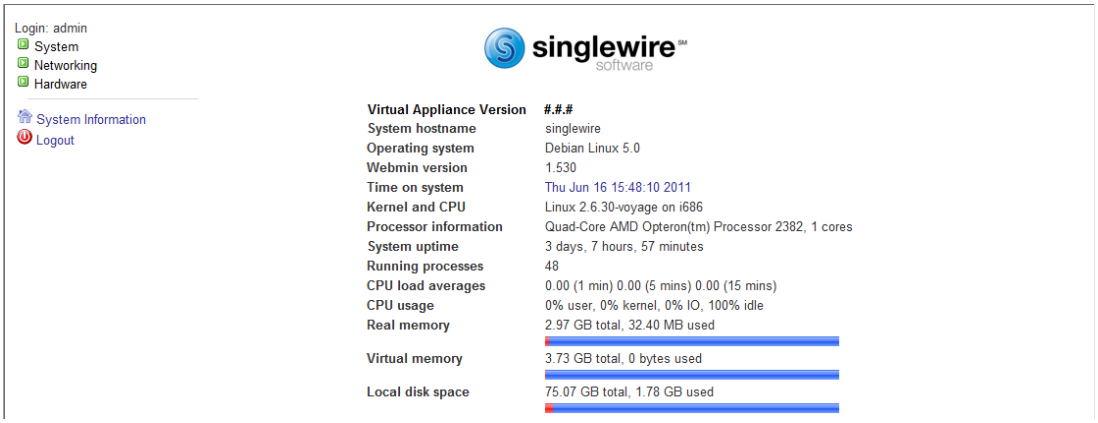
Step 3 Scroll down the list of actions until you come to your application's name (e.g. **singlewireInformaCast**). Select it by placing a checkmark in its Action column and click the **Restart** button. The Restarting Actions page appears.

It will take a minute for your application to restart.

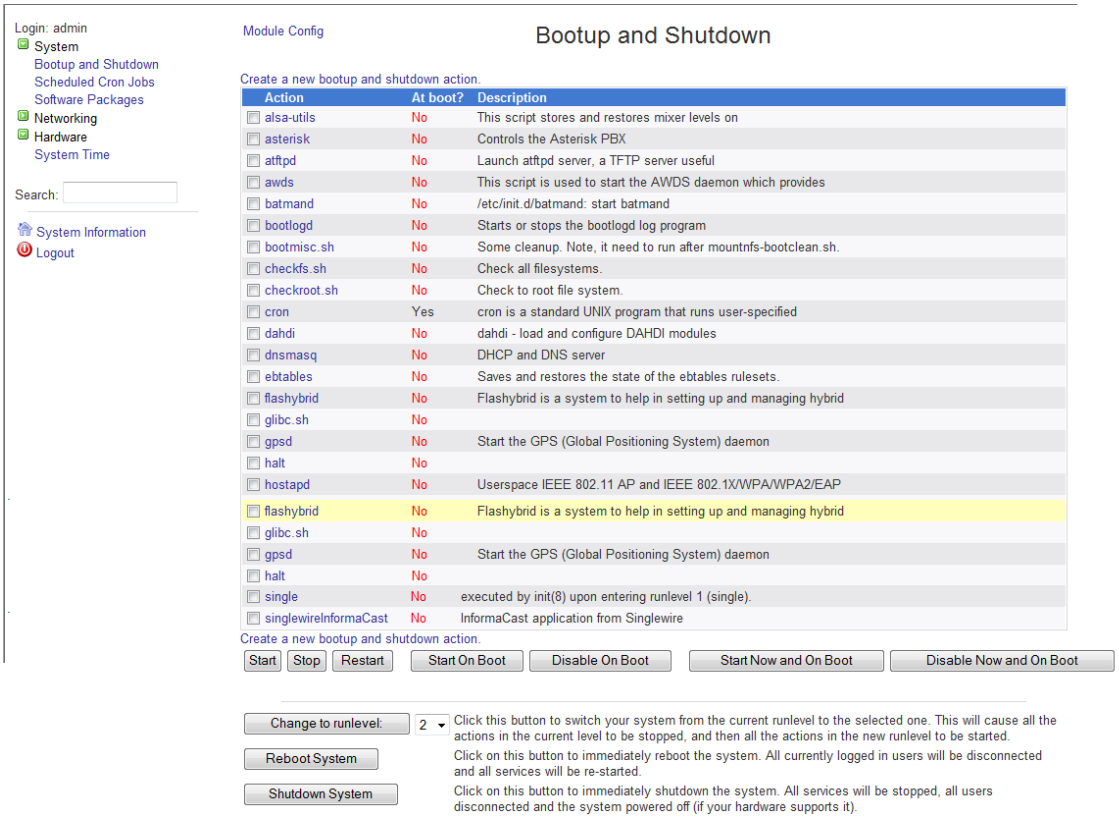
Reboot the InformaCast Virtual Appliance

Follow these steps to reboot the InformaCast Virtual Appliance.

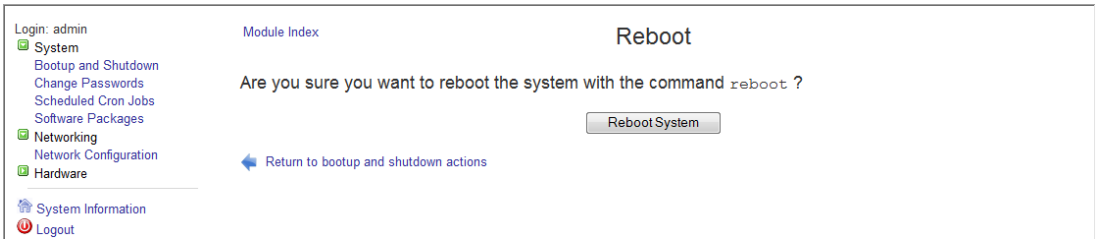
Step 1 Log into Webmin (see "Log into Webmin" on page 10-7 for specific steps). The Webmin homepage appears.



Step 2 Go to **System** | **Bootup and Shutdown**. The Bootup and Shutdown page appears.



Step 3 Scroll to the bottom of the page and click the **Reboot System** button. The Reboot page appears.

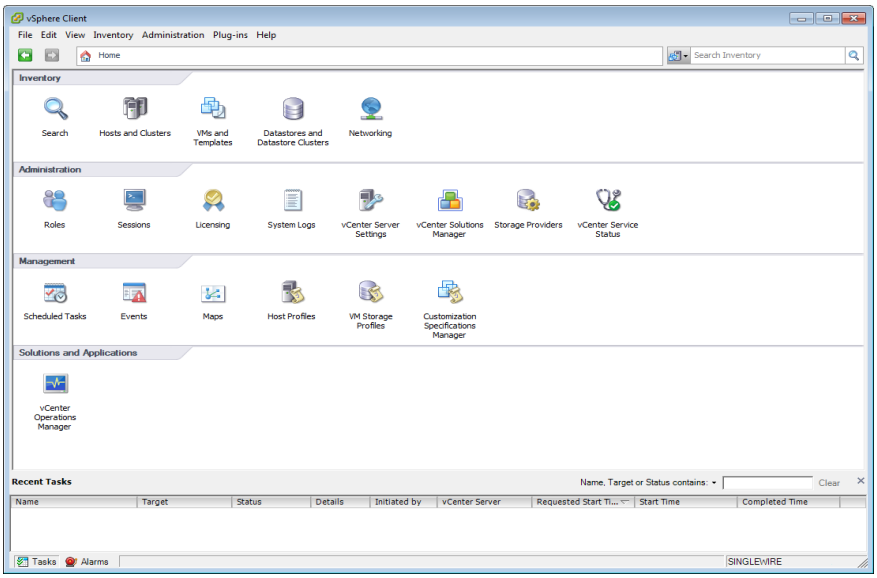


Step 4 Click the **Reboot System** button. The server will shutdown, then restart.

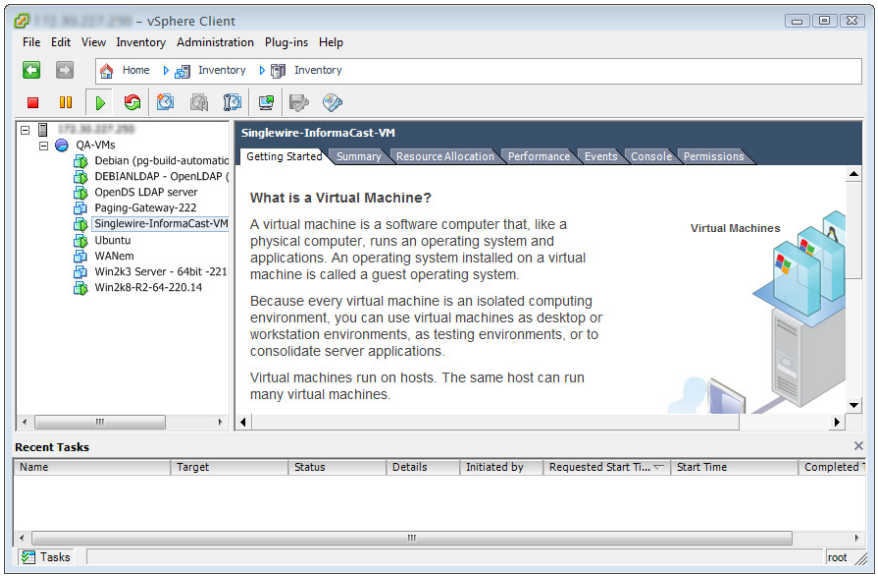
Change the InformaCast Virtual Appliance's Password

For tighter security, you may want to change the InformaCast Virtual Appliance's default password.

Step 1 Open and log into the vSphere client. The vSphere Client window appears.

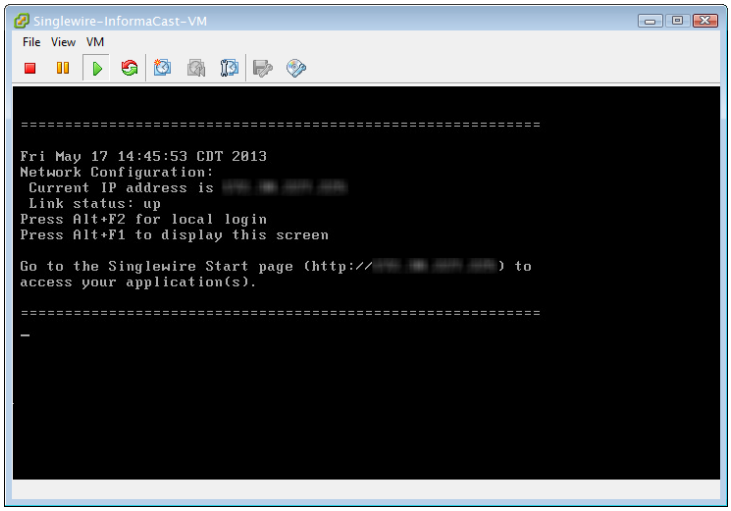


Step 2 Click the **Inventory** icon ( ) on the vSphere Client window. The vSphere Client window refreshes.

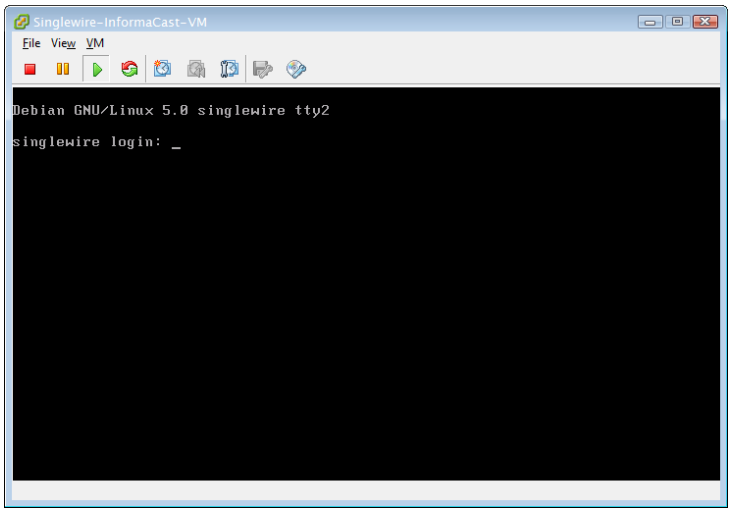


Step 3 Select your virtual machine (by default, this is Singlewire InformaCast VM).

Step 4 Go to **Inventory** | **Virtual Machine** | **Open Console**. The Singlewire InformaCast VM console window appears.

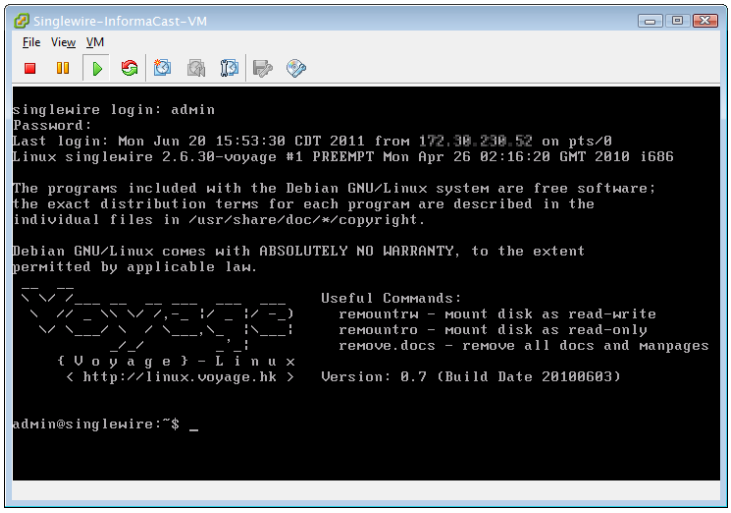


Step 5 Press **Alt + F2** in the Singlewire InformaCast VM console window. The Singlewire InformaCast VM console window refreshes.



Step 6 Enter **admin** at the **singlewire login** prompt and press the **Enter** key.

Step 7 Enter **changeMe** at the **Password** prompt and press the **Enter** key. The Singlewire InformaCast VM console window refreshes.



Step 8 Enter **sudo changePassword** at the command prompt and press the **Enter** key.

Step 9 Enter your new password at the **Enter new UNIX password** prompt and press the **Enter** key.

Step 10 Confirm your new password by entering it again at the **Retype new UNIX password** prompt and press the **Enter** key. Your password is changed and you will see, "passwd: password updated successfully".

Note Your new password needs to be used for both the administrative web and command interfaces.

Change InformaCast Virtual Appliance's IP Address

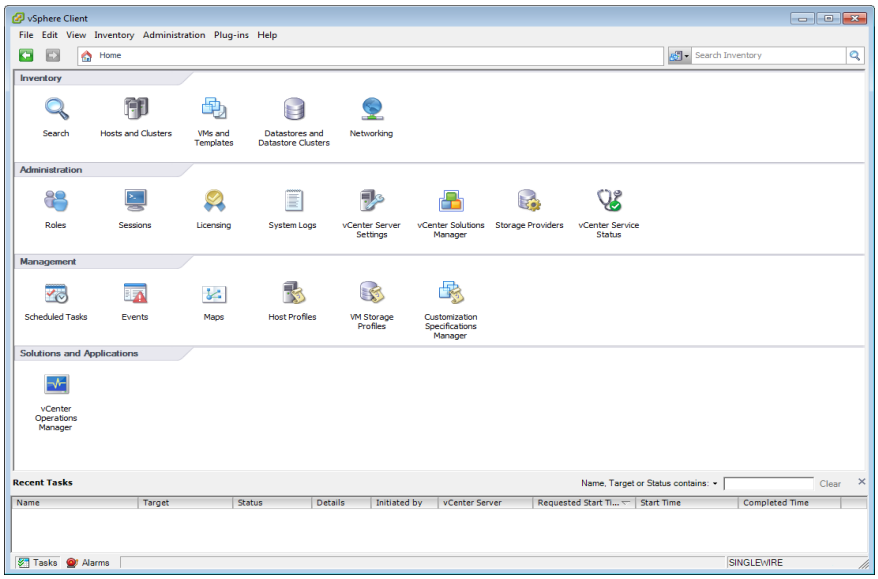
When changing the IP address of the InformaCast Virtual Appliance, use the following steps.

Note Performing these steps will set all of your Singlewire applications to start when the server boots.

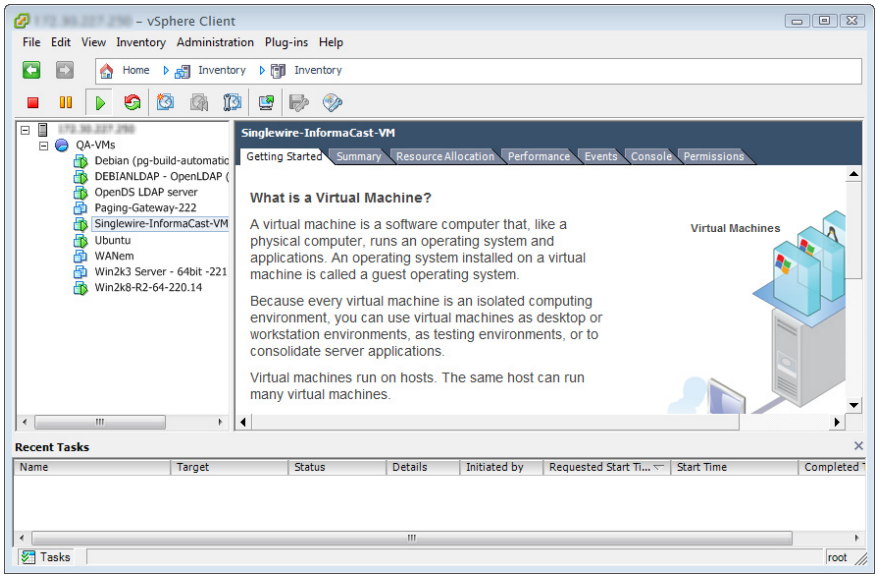
Warning **If you plan to switch between Basic and Advanced InformaCast and you change your IP address, you will need to redeploy the InformaCast OVA (see "Install InformaCast Virtual Appliance" on page 2-6).**

Step 1 Stop your Singlewire applications (see "Stop an Application on InformaCast Virtual Appliance" on page 10-10).

Step 2 Open and log into the vSphere client. The vSphere Client window appears.

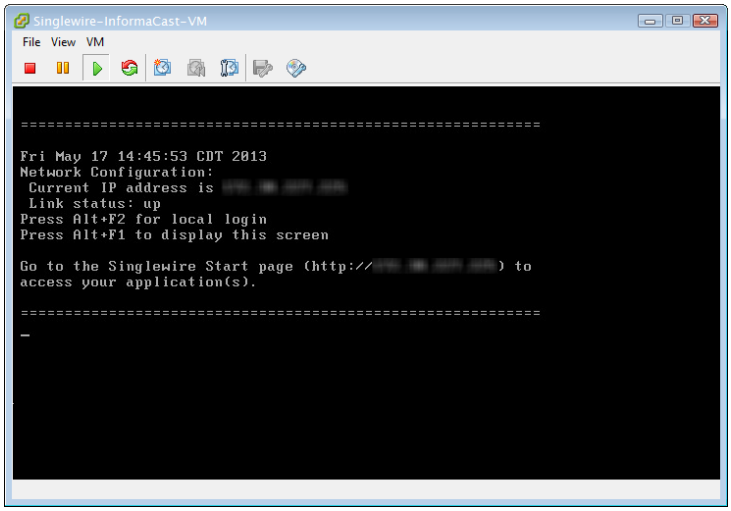


Step 3 Click the **Inventory** icon ( ) on the vSphere Client window. The vSphere Client window refreshes.

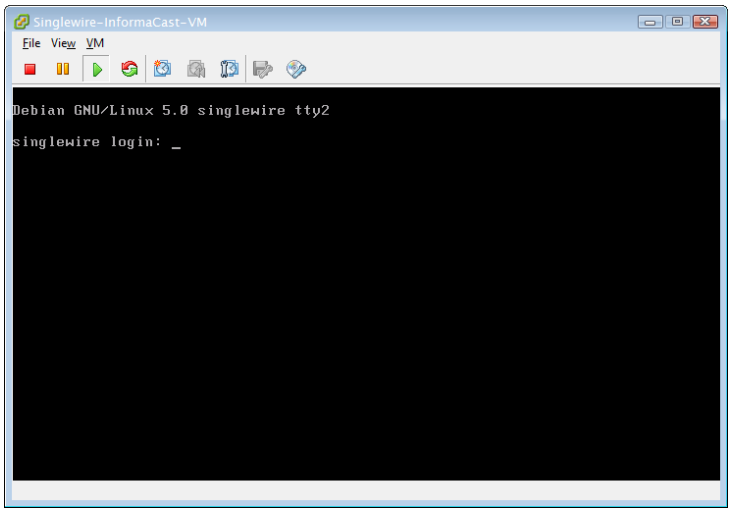


Step 4 Select your virtual machine (by default, this is Singlewire InformaCast VM).

Step 5 Go to **Inventory** | **Virtual Machine** | **Open Console**. The Singlewire InformaCast VM console window appears.

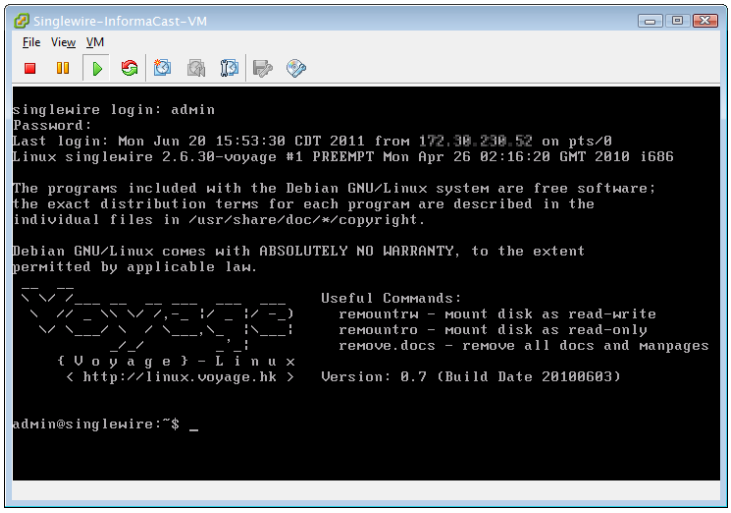


Step 6 Press **Alt** + **F2** in the Singlewire InformaCast VM console window. The Singlewire InformaCast VM console window refreshes.

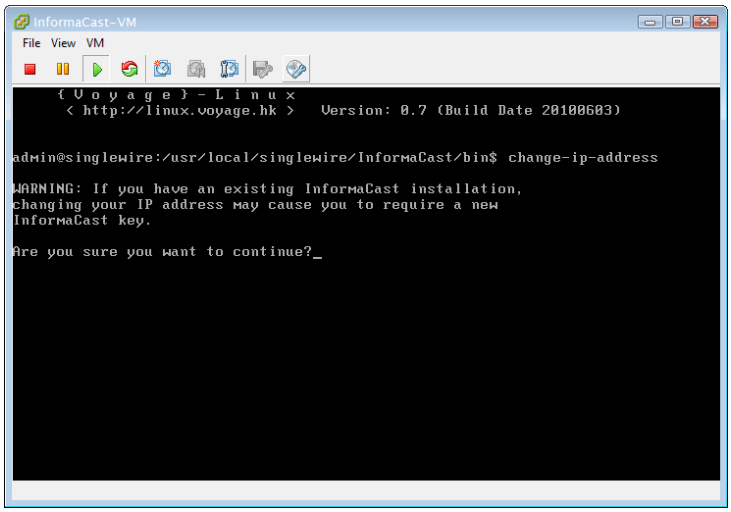


Step 7 Enter **admin** at the **singlewire login** prompt and press the **Enter** key.

Step 8 Enter **changeMe** at the **Password** prompt and press the **Enter** key. The Singlewire InformaCast VM console window refreshes.



Step 9 Enter **change-ip-address** and press the **Enter** key. The Singlewire InformaCast VM console window refreshes.



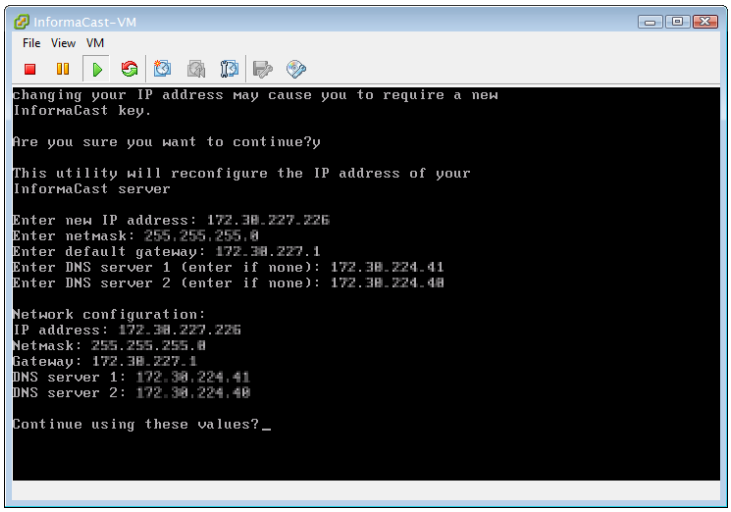
Step 10 Enter **Y** and press the **Enter** key.

Step 11 Enter a routable IP address on your network that's not currently in use and press the **Enter** key.

Step 12 Enter a valid netmask for that IP address and press the **Enter** key.

Step 13 Enter the default gateway for your specified IP address and press the **Enter** key.

Step 14 Enter the IP address(es) of a DNS server(s) on your network and press the **Enter** key.



Step 15 Enter **Y** and press the **Enter** key.

Step 16 Enter **Exit** and press the **Enter** key.

Step 17 For InformaCast, log into CUCM, go to **System** | **Enterprise Parameters**, and change the **URL Authentication** and **Secured Authentication URL** fields field reflect your new IP address.

Also, go to **Device** | **Device Settings** | **Phone Services**, and change the IP address for any InformaCast service URLs you have created.

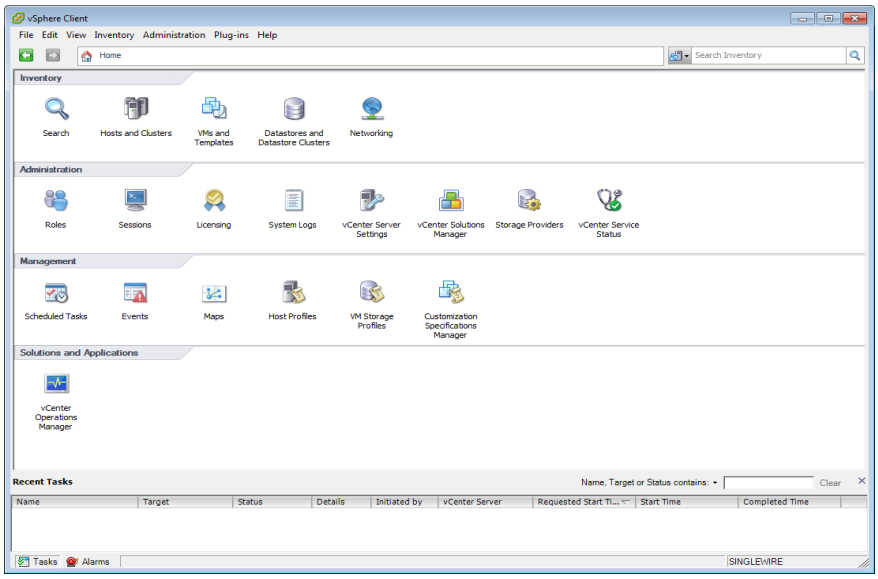
Note InformaCast SIP certificates are regenerated whenever InformaCast is installed or its IP address is changed, so if you are using TLS protocol with SIP, you will need to install the InformaCast SIP certificate on all CUCMs in your InformaCast environment (see "Install the InformaCast SIP Certificate on a SIP Device" in the "InformaCast Installation and User Guide."

Step 18 Reset all of your phones.

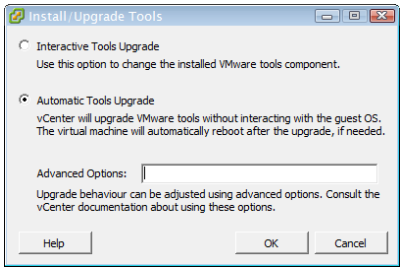
Upgrade your VMware Tools

If vSphere has an error flag that says that your version of VMware doesn't match your version of VMware tools, or if your CPU usage seems elevated, you should upgrade your VMware tools to match the level of your VMware version.

Step 1 Open and log into the vSphere client. The vSphere Client window appears.



Step 2 Select your virtual machine, and go to **Inventory** | **Virtual Machine** | **Guest** | **Install/Upgrade VMware Tools**. The Install/Upgrade Tools window appears.



Step 3 Select the **Automatic Tools** radio button and click the **OK** button. Your VMware tools are upgraded.

Upgrade InformaCast Virtual Appliance

Prior to upgrading InformaCast Virtual Appliance, create a snapshot of the Virtual Appliance in case you need to perform disaster recovery.

Note the Differences

If you are upgrading from an earlier version of InformaCast Virtual Appliance, please review "Release Notes" on page 11-1 for a list of new features.

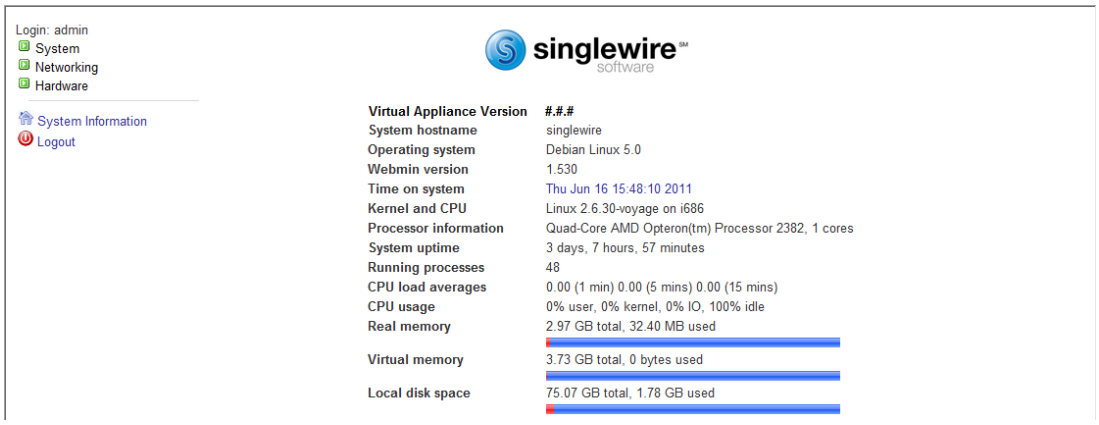
Determine Your Current Version

Depending on the version of InformaCast Virtual Appliance from which you are starting, you will follow different steps when upgrading. It is important to know your originating InformaCast version.

Step 1 Log into InformaCast (see "Log into InformaCast" on page 10-3 for specific steps).

Step 2 Look at the upper right corner of the InformaCast homepage. If your version of InformaCast is 8.4 or earlier, you will see your version number. Continue with "Obtain InformaCast Virtual Appliance Software Package" on page 10-26. If your version of InformaCast is 8.5.1 or later, continue with the following steps.

Step 3 Log into Webmin (see "Log into Webmin" on page 10-7 for specific steps). The Webmin homepage appears.



Step 4 Look at the top line of the Webmin homepage, e.g. Virtual Appliance Version. That is your current version of InformaCast.

Step 5 Make note of your version number and continue with "Obtain InformaCast Virtual Appliance Software Package" on page 10-26.

Obtain InformaCast Virtual Appliance Software Package

You can download the latest version of InformaCast Virtual Appliance from the Cisco website. Contact Cisco if you need help.

Depending on the version of InformaCast Virtual Appliance from which you are starting, you will follow different steps:

- **8.3 or 8.4 Virtual Appliance to Current Version.** Your download should include three package files:
  - CiscoPagingServer_8.5.1.deb
  - CiscoPagingServer_9.1.1.deb
  - CiscoPagingServer_11.0.2.deb

  The upload process is detailed in the next section.
- **8.5.1, 9.0.1, or 9.0.2 Virtual Appliance to Current Version.** Your download will include two package files: CiscoPagingServer_9.1.1.deb and CiscoPagingServer_11.0.2.deb.

  The upload process is detailed in the next section.
- **9.1.1 or 11.0.1 Virtual Appliance to Current Version.** Your download will include one package file: CiscoPagingServer_11.0.2.deb.

  The upload process is detailed in the next section.

Install a New Software Package

Once you've obtained your package file(s), you can install them and update your version of InformaCast Virtual Appliance:

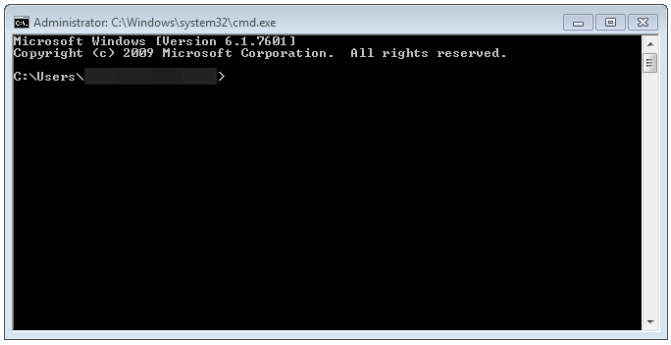
- Upgrading from an 8.3 or 8.4 version to the current version calls for three files (CiscoPagingServer_8.5.1.deb, CiscoPagingServer_9.1.1.deb, and CiscoPagingServer_11.0.2.deb) to be uploaded
- Upgrading from 8.5.1, 9.0.1, or 9.0.2 to the current version calls for two files (CiscoPagingServer_9.1.1.deb and CiscoPagingServer_11.0.2.deb) to be uploaded
- Upgrading from 9.1.1 or 11.0.1 to the current version only calls for one file (CiscoPagingServer_11.0.2.deb) to be uploaded

Please follow these steps carefully to ensure a successful InformaCast Virtual Appliance upgrade.

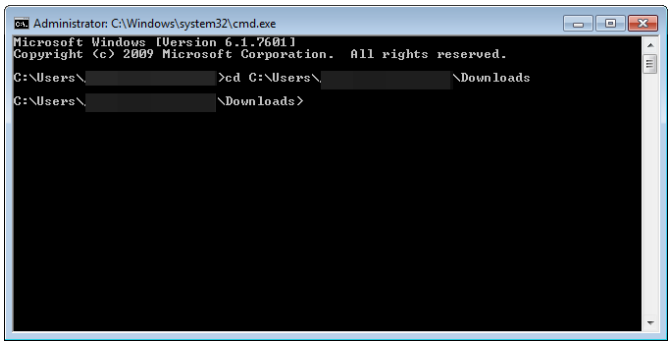
Step 1 Create a snapshot of your current InformaCast Virtual Appliance installation.

Step 2 Use PuTTY's to PSCP functionality to transfer your .deb file(s) to your Virtual Appliance. PuTTY is available as a free download from http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html and it should be installed on the machine from which you'll transfer files to the Virtual Appliance.

Step a. Open a command window on the machine on which you've saved your .deb file(s). A command window appears.

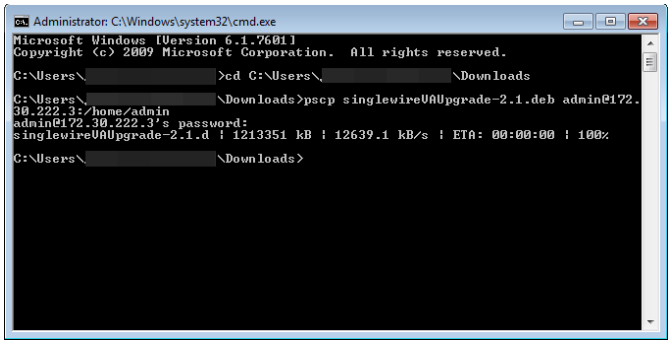


Step b. Enter **cd <directory>** and press the **Enter** key, where <directory> is the location of your .deb file(s). The command window refreshes to the location of your directory.



Step c. Enter **pscp <file name> admin@<InformaCast Virtual Appliance IP Address>:/home/admin** at the prompt and press the **Enter** key, where <file name> is the name of your .deb file and <InformaCast Virtual Appliance IP Address> is your actual Virtual Appliance's IP address, e.g. pscp CiscoPagingServer_9.1.1.deb admin@111.22.333.4:/home/admin.

Step d. Enter your Virtual Appliance password at the prompt and press the **Enter** key. The file will be transferred.

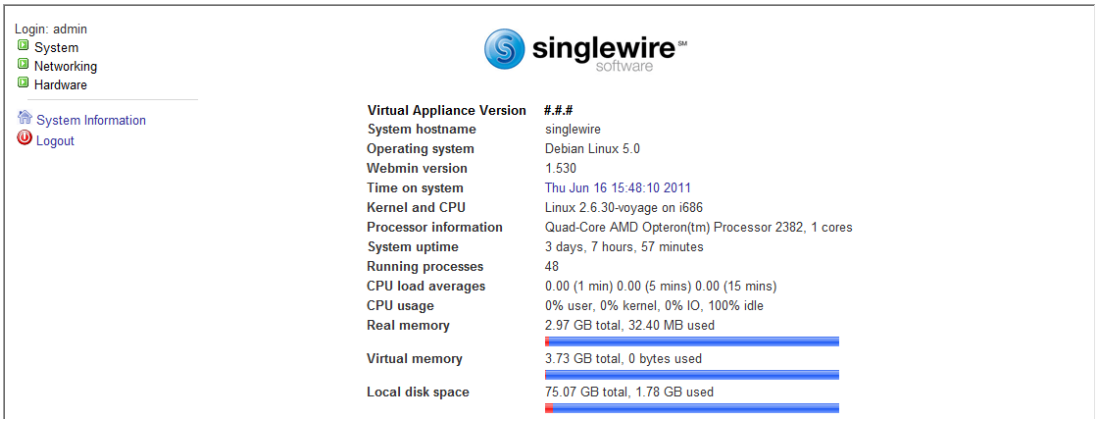


Step e. Repeat Steps a through d until you've copied all of your .deb files to the Virtual Appliance.

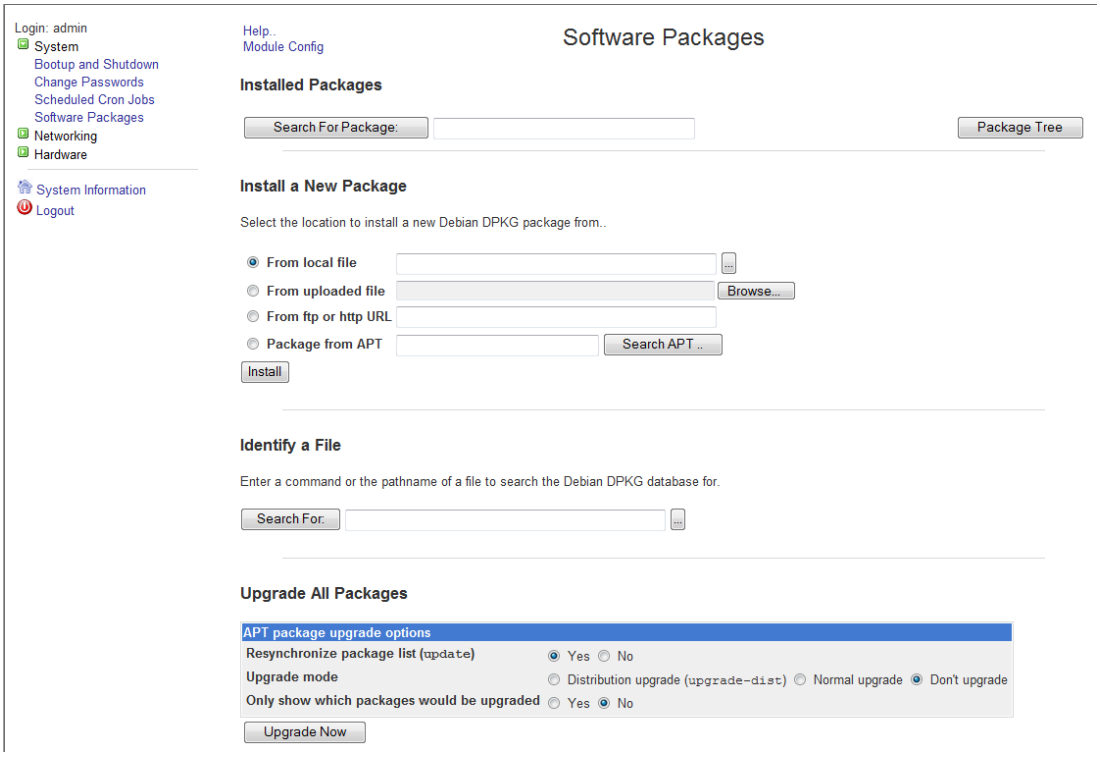
Step 3 Log into Webmin (see "Log into Webmin" on page 10-7 for specific steps).

Note For versions of InformaCast Virtual Appliance prior to 8.4, you will need to go to https://<InformaCast Virtual Appliance IP Address>:10000, where <InformaCast Virtual Appliance IP Address> is InformaCast Virtual Appliance's statically configured IP address.

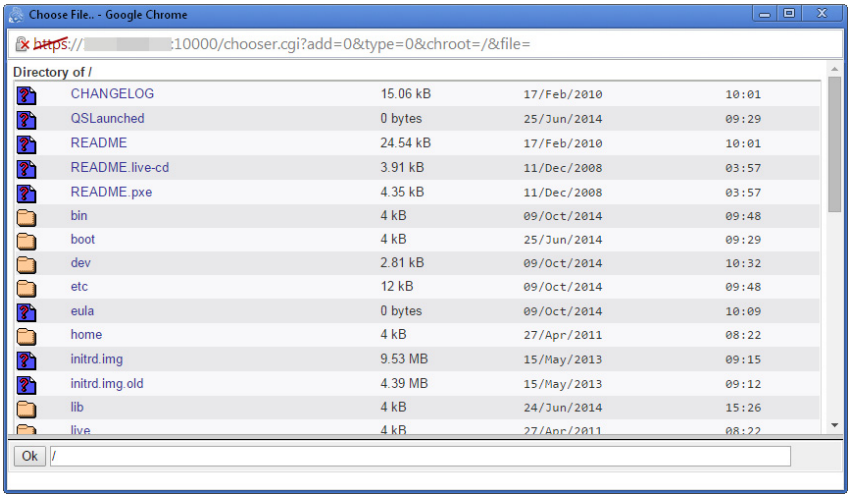
The Webmin homepage appears.



Step 4 Go to **System** | **Software Packages**. The Software Packages page appears.



Step 5 Select the **From local file** radio button in the *Install a New Package* area and click its **Browse** button. The Choose File window appears.

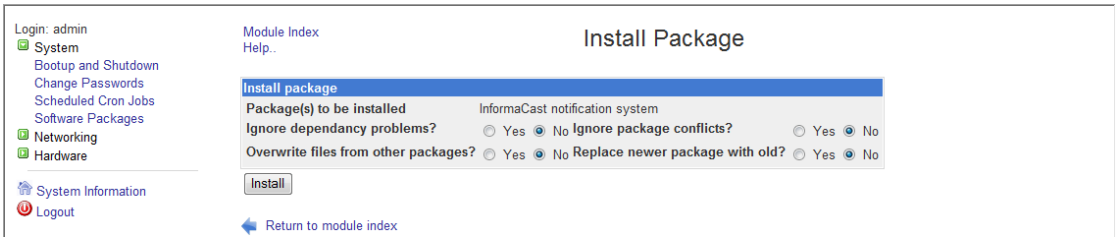


Step 6 Navigate to where you saved the InformaCast Virtual Appliance software package(s) you downloaded earlier (/home/admin in the example). Depending on the version of InformaCast Virtual Appliance from which you are upgrading, you will select one of the following:

- 8.3 or 8.4 versions of InformaCast Virtual Appliance: CiscoPagingServer_8.5.1.deb
- 8.5.1, 9.0.1, or 9.0.2 version of InformaCast Virtual Appliance: CiscoPagingServer_9.1.1.deb

- 9.1.1 or 11.0.1 version of InformaCast Virtual Appliance: CiscoPagingServer_11.0.2.deb

Step 7 Click the **Install** button in the *Install a New Package* area. The Install Package page appears.



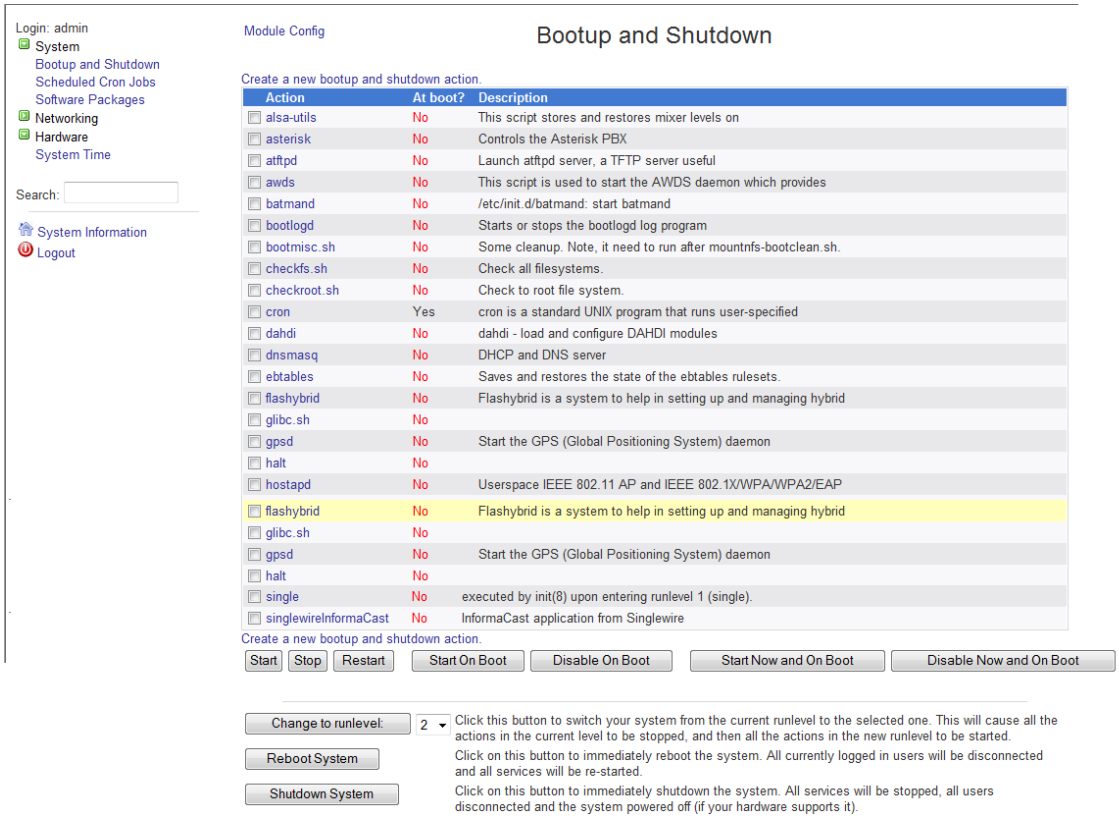
Step 8 Leave the default selections as they are and click the **Install** button. Your software package is installed.

Note The Install Package page should display a list of files that were correctly installed. If you see, "...process completed:" with no listing of files, your upgrade has failed and you should contact Cisco.

Step 9 Determine your next steps depending on the version of Virtual Appliance from which you are upgrading:

- If you are upgrading from the 9.1.1 or 11.0.1 version of InformaCast Virtual Appliance and later, proceed with Step 10
- If you are upgrading from the 8.5.1, 9.0.1, or 9.0.2 version of InformaCast Virtual Appliance:
  - Reboot the Virtual Appliance (see "Reboot the InformaCast Virtual Appliance" on page 10-16)
  - Go to **System** | **Software Packages** and follow Steps 5 through 8 one more time, selecting the CiscoPagingServer_11.0.2.deb file
  - Proceed with Step 10
- If you are upgrading from the 8.3 or 8.4 version of InformaCast Virtual Appliance:
  - Reboot the Virtual Appliance (see "Reboot the InformaCast Virtual Appliance" on page 10-16)
  - Go to **System** | **Software Packages** and follow Steps 5 through 8, selecting the CiscoPagingServer_9.1.1.deb file
  - Reboot the Virtual Appliance (see "Reboot the InformaCast Virtual Appliance" on page 10-16)
  - Go to **System** | **Software Packages** and follow Steps 5 through 8 one more time, selecting the CiscoPagingServer_11.0.2.deb file
  - Proceed with Step 10

Step 10 Go to **System** | **Bootup and Shutdown**. The Bootup and Shutdown page appears.



Step 11 Scroll down to the bottom of the page and click the **Reboot System** button. It will take a minute or so for the InformaCast Virtual Appliance to reboot.

Note Leave this window open. You will come back to it in the next section.

Step 12 Create a new snapshot of your Virtual Appliance.

Step 13 Clear your web browser's cache.

Step 14 Remove your already installed .deb files by following Steps a and b on page 10-27 and entering **rm <.deb filename>** for each .deb file you've copied over.

Upload a New License

Note You only need to upload a new license if you are upgrading from Basic to Advanced (e.g. perpetual or subscription). If you are only upgrading between versions of Basic InformaCast, you can skip this section.

The Control Center holds your InformaCast Virtual Appliance license key, which contains your designated functionality for InformaCast (e.g. Basic vs. Advanced, the number of phones to which you can broadcast, trial vs. demonstration vs. subscription vs. perpetual, etc.).

If you upgrade from Basic InformaCast to Advanced InformaCast (with the exception of your free trial of Advanced InformaCast) or upgrade your version of the Virtual Appliance, you will install a new license key.

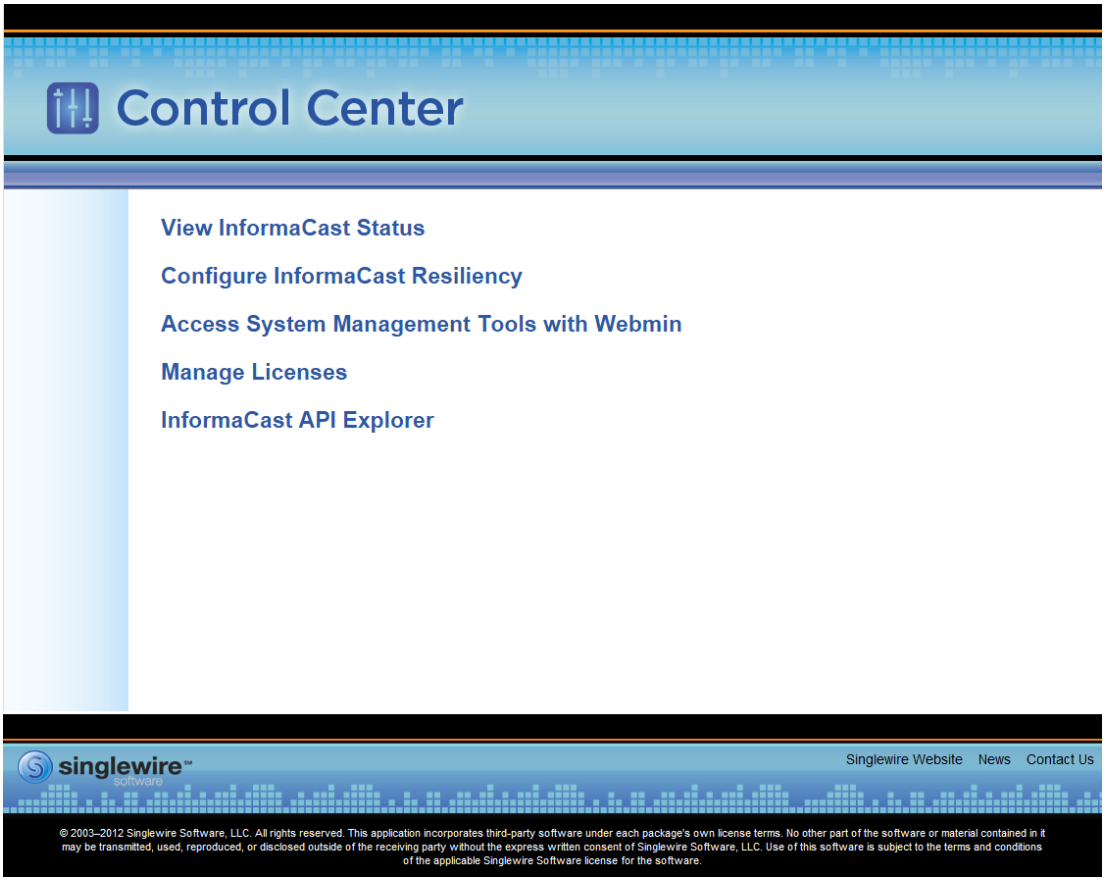
Before you can perform these steps, you must have an InformaCast Virtual Appliance license, which will be in the form of an XML file that was sent to you by email from a Singlewire sales representative. If your salesperson has not already provided one to you, contact Singlewire and request that a license be emailed to you.

Tip Make sure to save your XML license key file to a safe location that can be accessed by the machine running your web browser.

Step 1 Log into the Control Center (see "Log into the Control Center" on page 10-5 for specific steps).

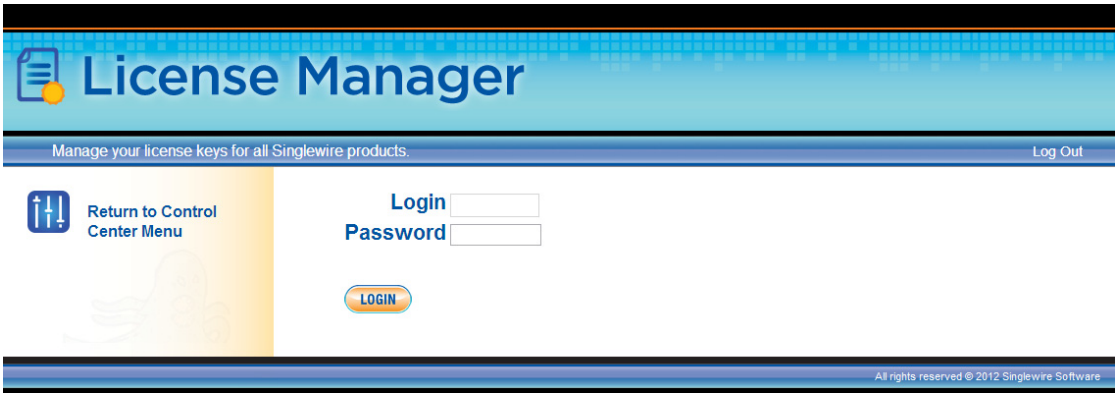
Note For versions of InformaCast Virtual Appliance prior to 8.4, you will need to go to https://<InformaCast Virtual Appliance IP Address>:8463/LicenseManager, where <InformaCast Virtual Appliance IP Address> is InformaCast Virtual Appliance's statically configured IP address. Skip to Step 3 on page 10-34.

A separate tab/window opens to the Control Center page.

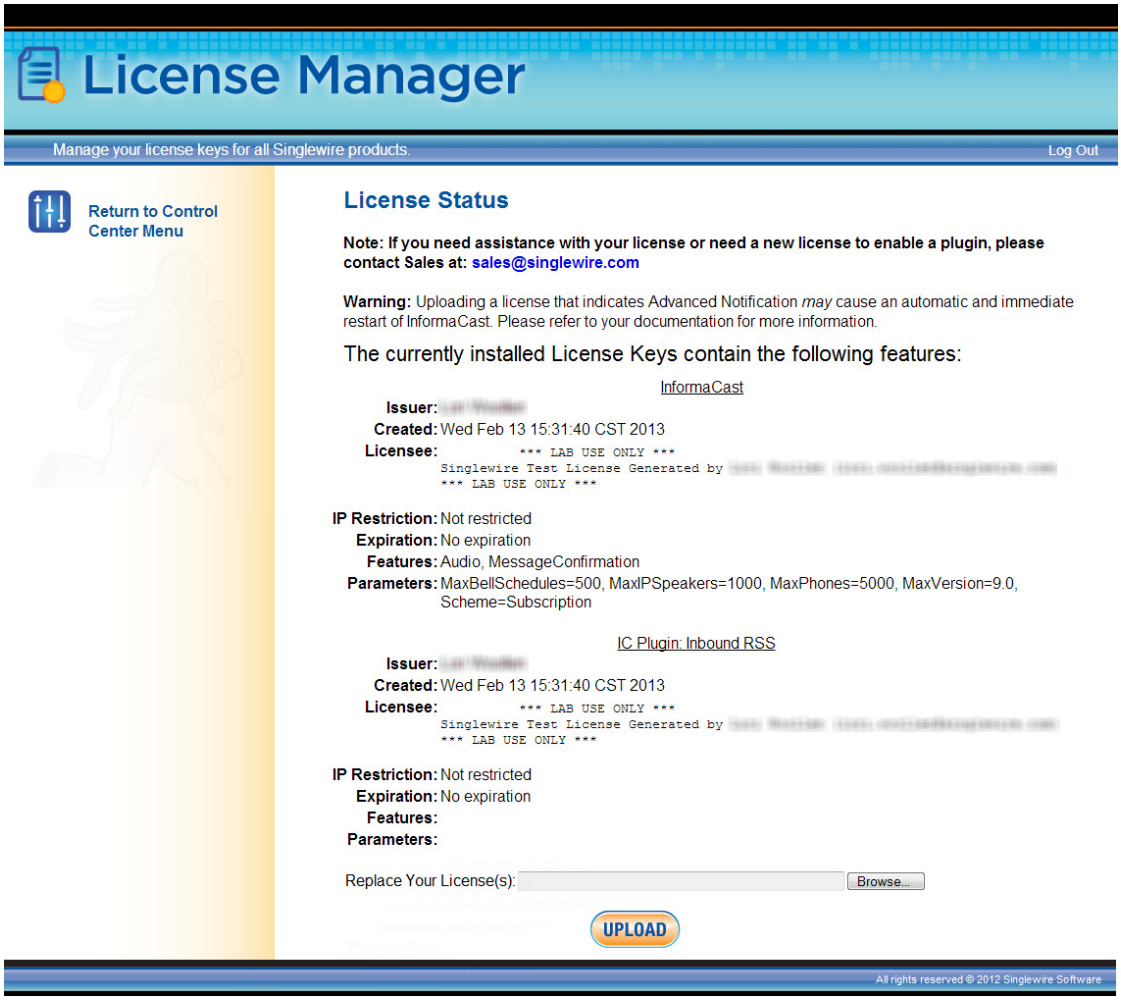


Note You may have to accept a warning from your web browser about the security of this page's content.

Step 2 Click the **Manage Licenses** link. The License Manager page appears.

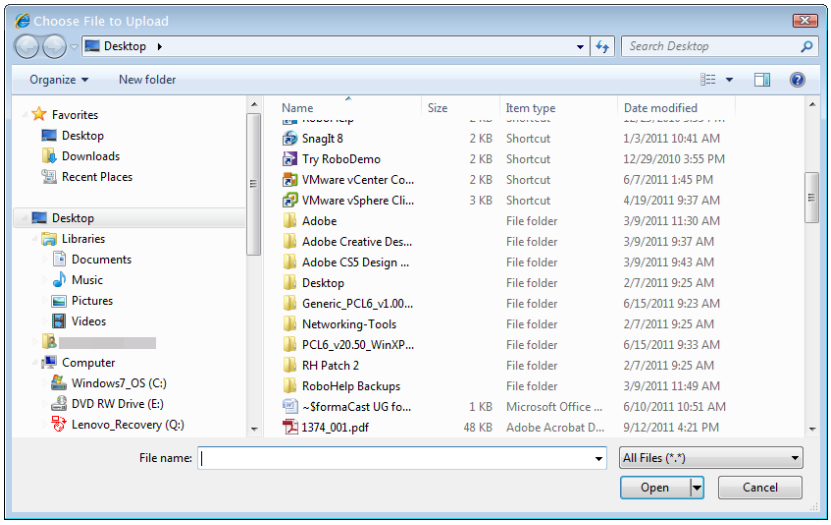


Step 3 Enter your username and password in the **Login** and **Password** fields, respectively. By default, your username is **admin** and your password is **changeMe**. Click the **Login** button. The License Status page appears.



The License Manager holds all of your Singlewire licenses. Depending on the software applications you are using, you will see different licenses housed on this page.

Step 4 Click the **Browse** button. The Choose File to Upload window appears.



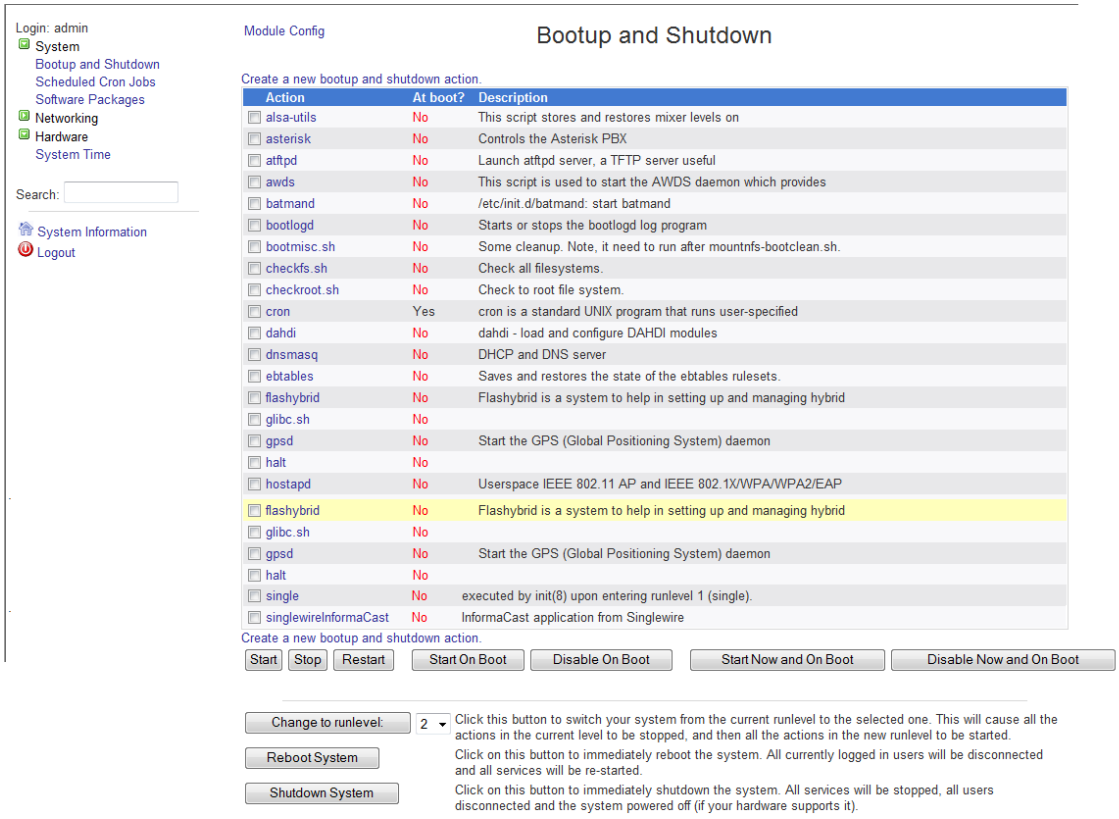
Step 5 Navigate to where you saved your new license file, select it, and click the **Open** button.

Step 6 Click the **Upload** button on the License Status page. Your page refreshes with a confirmation that the license has been uploaded.

Note If your new license key contains less functionality than your previous key, you will be presented with a warning to that effect, a comparison of your two licenses, and the request to click the **Apply** button to confirm the change.

Tip If the key is not accepted, check that you selected the proper file containing the XML key that was emailed to you, ensure that your IP address is correct, determine that your key has not expired, and ensure that the MaxVersion parameter in your license key matches or is greater than your version of InformaCast. If you're still having trouble, contact Singlewire for assistance.

Step 7 Return to your Webmin tab/window and click the **Bootup and Shutdown** link. The Bootup and Shutdown page appears.



Step 8 Select all of your Singlewire applications that were affected by your new license and click the **Restart** button. The Restarting Actions page appears.

It may take a moment for the application(s) to restart.

Release Notes

The following sections contain the release notes for InformaCast from version 8.3 (Basic Paging's inception) through the current version.

InformaCast 11.0.2

Compatibility

InformaCast is compatible with the following versions of Cisco Unified Communications Manager server (including Business Edition 6000): 8.5.1, 8.6.2, 9.0.1, 9.1.2, 10.0.1, 10.5.2, or 11.0.1.

New Features

New Upgrade File. A new file (CiscoPagingServer_11.0.2.deb) has been added to the upgrade process. Depending on the version of InformaCast Virtual Appliance from which you are starting, you will install different package files:

- For 8.3 or 8.4 versions to the current version, you will install three package files (CiscoPagingServer_8.5.1.deb, CiscoPagingServer_9.1.1.deb, and CiscoPagingServer_11.0.2.deb)
- For 8.5.1, 9.0.1, or 9.0.2 to the current version, you will install two package files (CiscoPagingServer_9.1.1.deb and CiscoPagingServer_11.0.2.deb)
- For 9.1.1 or 11.0.1 to the current version, you will install one package file (CiscoPagingServer_11.0.2.deb)

InformaCast Virtual Appliance 8.5.1 and 9.1.1 are waypoints in the upgrade process. For 8.0.2 through 8.4 versions of the Virtual Appliance, you must upgrade to 8.5.1, reboot the Virtual Appliance, upgrade to 9.1.1, reboot the Virtual Appliance, and then continue to upgrade to 11.0.1. For 8.5.1, 9.0.1, or 9.0.2 versions of the Virtual Appliance, you must upgrade to 9.1.1, reboot the Virtual Appliance, and then continue to upgrade to 11.0.1. For the 11.0.1 version of the Virtual Appliance, you can upgrade directly to 11.0.2.

Announcements

- **Streamlined Support for CUCM.** Releases of InformaCast subsequent to 11.0.2 will not support CUCM 8.5 or 8.6 due to its "end of software maintenance" status with Cisco (see http://www.cisco.com/c/en/us/products/unified-communications/unified-communications-manager-callmanager/eos-eol-notice-listing.html)
- **New Standardized Name.** Coming soon: Cisco Unified Communications Manager will no longer be abbreviated as CUCM and will instead appear as Unified Communications Manager after its first mention as Cisco Unified Communications Manager. This will affect all documentation as well as InformaCast's user interface. Stay tuned.

Resolved Caveats

CDETs ID	Title
CSCuu82554	June 2015 SSL Vulnerabilities

InformaCast 11.0.1.a

Compatibility

InformaCast is compatible with the following versions of Cisco Unified Communications Manager server (including Business Edition 6000): 8.5.1, 8.6.2, 9.0.1, 9.1.2, 10.0.1, 10.5.2, or 11.0.1.

Updated Information

9.0.1 and 9.0.2 Upgrade Information. References to upgrading from 9.0.1 or 9.0.2 to the current version had been inadvertently omitted. Follow the same steps as noted for upgrading from 8.5.1, installing two package files (CiscoPagingServer_9.1.1.deb and CiscoPagingServer_11.0.1.deb).

For 9.0.1 or 9.0.2 versions of the Virtual Appliance, you must upgrade to 9.1.1, reboot the Virtual Appliance, and then continue to upgrade to 11.0.1.

InformaCast 11.0.1

Compatibility

InformaCast is compatible with the following versions of Cisco Unified Communications Manager server (including Business Edition 6000): 8.5.1, 8.6.2, 9.0.1, 9.1.2, 10.0.1, 10.5.2, or 11.0.1.

New Features

- **Newly Supported Phones.** InformaCast now supports the 7811, 8845, and 8865 Cisco IP phone models.
- **Added UTF-8 Support.** The following pages in InformaCast 11.0.1 now support UTF-8 character encoding: Edit Recipient Groups and Delete Recipient Group. The View Recipients dialog box (accessible through the **View** button on the Edit Recipient Group page) also offers UTF-8 support.
- **New Upgrade File.** A new file (CiscoPagingServer_11.0.1.deb) has been added to the upgrade process. Depending on the version of InformaCast Virtual Appliance from which you are starting, you will install different package files:
  - For 8.3 or 8.4 versions to the current version, you will install three package files (CiscoPagingServer_8.5.1.deb, CiscoPagingServer_9.1.1.deb, and CiscoPagingServer_11.0.1.deb)
  - For 8.5.1, 9.0.1, or 9.0.2 to the current version, you will install two package files (CiscoPagingServer_9.1.1.deb and CiscoPagingServer_11.0.1.deb)
  - For 9.1.1 to the current version, you will install one package file (CiscoPagingServer_11.0.1.deb)

InformaCast Virtual Appliance 8.5.1 and 9.1.1 are waypoints in the upgrade process. For 8.3 through 8.4 versions of the Virtual Appliance, you must upgrade to 8.5.1, reboot the Virtual Appliance, upgrade to 9.1.1, reboot the Virtual Appliance, and then continue to upgrade to 11.0.1. For 8.5.1, 9.0.1, or 9.0.2 versions of the Virtual Appliance, you must upgrade to 9.1.1, reboot the Virtual Appliance, and then continue to upgrade to 11.0.1.

Resolved Issues

DSA Private Keys and the Upgrade Process. Some versions of Chrome, Firefox, and Internet Explorer reject connections to websites with DSA private keys, and some older versions of InformaCast defaulted to using DSA keys for self-signed certificates. If you are using an older version of InformaCast with DSA private keys and you upgrade the 11.0.1, the upgrade process will automatically regenerate your DSA private key as an RSA key; it will not automatically regenerate DSA keys with signed certificates. You must regenerate them manually.

Announcement

- **Streamlined Support for CUCM.** Releases of InformaCast subsequent to 11.0.1 will not support CUCM 8.5 or 8.6 due to its "end of maintenance" status with Cisco (see http://www.cisco.com/c/en/us/products/unified-communications/unified-communications-manager-callmanager/eos-eol-notice-listing.html)
- **New Standardized Name.** Coming soon: Cisco Unified Communications Manager will no longer be abbreviated as CUCM and will instead appear as Unified Communications Manager after its first mention as Cisco Unified Communications Manager. This will affect all documentation as well as InformaCast's user interface. Stay tuned.

Resolved Caveats

CDETs ID	Title
CSCus31451	October 2014; OpenSSL Vulnerabilities
CSCus42905	January 2015; OpenSSL Vulnerabilities
CSCus69788	Evaluation of glibc GHOST vulnerability - CVE-2015-0235
CSCut46607	March 2015; OpenSSL Vulnerabilities
CSCut77657	April 2015; NTPd Vulnerabilities
CSCut91894	Connections from FF37 and Chrome to InformaCast fail after FF/Chrome updt

New Caveats

CDETs ID	Title
CSCuh28628	Provide a more user-friendly interface/functions on the Start Page

InformaCast 9.1.1

Compatibility

InformaCast is compatible with the following versions of Cisco Unified Communications Manager server (including Business Edition 6000): 8.5, 8.6, 9.0, 9.1, 9.12, 10.0, 10.5, and 10.5.2.

New Features

The following features have been added to enhance functionality and improve user experience:

- **Newly Supported Phone.** InformaCast now supports the 8811 Cisco IP phone model.
- **New IVRs.** Anytime you pick up a phone to use InformaCast's DialCast functionality, you come in contact with InformaCast's Interactive Voice Response (IVR). These IVRs have been upgraded in sound and quality, providing a more consistent phone user experience.
- **New Upgrade File.** A new file (CiscoPagingServer_9.1.1.deb) has been added to the upgrade process. Depending on the version of InformaCast Virtual Appliance from which you are starting, you will install different package files:
  - For 8.3 or 8.4 versions to the current version, you will install two package files (CiscoPagingServer_8.5.1.deb and CiscoPagingServer_9.1.1.deb)
  - For 8.5.1, 9.0.1, or 9.0.2 to the current version, you will install one package file (CiscoPagingServer_9.1.1.deb)

  InformaCast Virtual Appliance 8.5.1 is a waypoint in the upgrade process. For 8.3 through 8.4 versions of the Virtual Appliance, you must upgrade to 8.5.1, reboot the Virtual Appliance, and then continue to upgrade to 9.1.1.

Resolved Caveats

CDETs ID	Title
CSCur73771	Cisco Paging Server vulnerability to POODLE CVE-2014-3566
CSCur21692	Voice traffic not properly marked
CSCur04834	InformaCast and Shellshock vulnerability CVE-2014-6271/CVE-2014-7169
CSCuq31086	change-ip-address fails, referencing /usr/local/singlewire/PushToTalk

New Caveats

CDETs ID	Title
CSCuh28628	Provide a more user-friendly interface/functions on the Start Page
CSCul53228	No phones brought into InformaCast via SNMP

InformaCast 9.0.2

Compatibility

InformaCast is compatible with the following versions of Cisco Unified Communications Manager server (including Business Edition 6000): 8.5, 8.6, 9.0, 9.1, 9.12, 10.0, and 10.5.

New Feature

New Upgrade File. A new file (singlewireVAUpgrade-2.0.2.deb) has been added to the upgrade process. Depending on the version of InformaCast Virtual Appliance from which you are starting, you will install different package files:

- For the 8.3 or 8.4 version to the current version, you will install two package files (singlewireVAUpgrade-1.4.deb and singlewireVAUpgrade-2.0.2.deb)
- For 8.5.1 or 9.0.1 to the current version, you will install one package file (singlewireVAUpgrade-2.0.2.deb)

InformaCast Virtual Appliance 8.5.1 is a waypoint in the upgrade process. For the 8.3 or 8.4 version of the Virtual Appliance, you must upgrade to 8.5.1, reboot the Virtual Appliance, and then continue to upgrade to 9.0.2.

Known Issues

Broadcasts Fail Using JTAPI with 7905 and 7912 Model IP Phones. The 7905 and 7912 model phones (running firmware 8.0.3, and 8.0.4 respectively) will fail to broadcast and remain in an Activated state if the **Send Commands to Phones By JTAPI** checkbox is selected on the Broadcast Parameters page. Continue to use HTTP requests for broadcasts to these phones (i.e. do not select the **Send Commands to Phones By JTAPI** checkbox). This is a known and outstanding issue.

Resolved Issues

The following issues have been resolved for this version:

- **Bug Affected Upgrade Process for 8.4 Priority Patch Installations.** If you used the Priority Patch supplied to InformaCast 8.4 users, upgrading to InformaCast 9.0.1 from InformaCast 8.5.1 would fail. You can resolve this issue by reverting to your 8.5.1 snapshot of the Virtual Appliance and then upgrading to 9.0.2. This issue has been resolved.
- **Documentation Change.** The file name for a backup of InformaCast had been listed erroneously in InformaCast 9.0.1. It has been corrected for 9.0.2: InformaCastBackup.zip. This issue has been resolved.

Resolved Caveats

CDETs ID	Title
CSCuh30601	Phone caches were persisting after transitioning back to Basic mode. Ensure that you have the most up-to-date recipients by clicking the **Update** button on the Edit Recipient Groups page.

New Caveats

CDETs ID	Title
CSCtq36901	The 3905 model IP phone does not support CTI; it will not receive commands from InformaCast when using JTAPI transport and busy monitoring via CTI does not work. If you are using the 3905, run InformaCast in HTTP mode only.

InformaCast 9.0.1

Compatibility

InformaCast is compatible with the following versions of Cisco Unified Communications Manager server (including Business Edition 6000): 8.5, 8.6, 9.0, 9.1, 9.12, 10.0, and 10.5.

New Features

- **Added Documentation.** The documentation for the server-side aspect of the Virtual Appliance has been added to provide a more robust experience for users.
- **New Upgrade File.** A new file (singlewireVAUpgrade-2.0.deb) has been added to the upgrade process. Depending on the version of InformaCast Virtual Appliance from which you are starting, you will install different package files:
  - For the 8.3 or 8.4 version to the current version, you will install two package files (singlewireVAUpgrade-1.4.deb and singlewireVAUpgrade-2.0.deb)
  - For 8.5.1 to the current version, you will install one package file (singlewireVAUpgrade-2.0.deb)

  InformaCast Virtual Appliance 8.5.1 is a waypoint in the upgrade process. For the 8.3 or 8.4 version of the Virtual Appliance, you must upgrade to 8.5.1, reboot the Virtual Appliance, and then continue to upgrade to 9.0.1.
- **New Application Architecture.** Before this version of Virtual Appliance, InformaCast was a web application provided by a Tomcat servlet container. As of 9.0.1, Tomcat is embedded within the InformaCast application and is started from within the Java Virtual Machine (JVM). You should not notice a difference in functionality.
- **New Supported ESXi Version.** VMware ESXi 5.5 is now supported by the Virtual Appliance.
- **Newly Supported Phone Communication.** You can now use JTAPI between InformaCast and your phones by selecting the **Standard CTI Allow Control of All Devices** checkbox when configuring your application user in CUCM and the **Send Commands to Phones By JTAPI** checkbox on the Broadcast Parameters page in InformaCast.
- **Newly Supported Phones.** InformaCast now supports the 8841, 8851, and 8861 Cisco IP phone models.
- **Upgraded Java Version.** Java was upgraded from version 1.6. to 1.7.
- **Reorganized Communications Manager Integration Section.** The section of this user guide dealing with integrating CUCM with the Virtual Appliance has been reorganized. In correlation, DialCast users are urged to update their configurations to use SIP instead of route points as that configuration is now discouraged and has been removed from the documentation.
- **Added Documentation for Setting System Time.** The InformaCast Virtual Appliance's system time is automatically set for you using the pool.ntp.org server, but if your Virtual Appliance does not have Internet access or if you want to use your own NTP server, you can do so.
- **Removed SIP Stack Fields.** Two fields, **UDP/TCP Port** and **TLS Port**, were removed from InformaCast's SIP Stack page to prevent you from disabling DialCast functionality.

Known/Resolved Issues

- **Broadcasts Fail Using JTAPI with 7905 and 7912 Model IP Phones.** The 7905 and 7912 model phones (running firmware 8.0.3, and 8.0.4 respectively) will fail to broadcast and remain in an Activated state if the **Send Commands to Phones By JTAPI** checkbox is selected on the Broadcast Parameters page. Continue to use HTTP requests for broadcasts to these phones (i.e. do not select the **Send Commands to Phones By JTAPI** checkbox). This is a known and outstanding issue.

- **Fixed Backlight Display.** Broadcast text and images on Cisco's 7945 and 7965 model IP phones weren't displaying because InformaCast was not turning on the phone's backlight display. InformaCast was modified to turn on the phone's backlight display when sending text to these models of IP phones. This issue is resolved.
- **Fixed Leading Spaces with DialCast.** DialCast calls were not completing when you entered a leading space as the first character in a DialCast dialing configuration. Leading spaces with DialCast phone exceptions also caused the calling phone to not match its exception. InformaCast was modified to remove leading and trailing spaces from dialing patterns and phone exceptions. This issue is resolved.
- **Fixed CTI Connection with CUCM.** In the past, if CUCM was unavailable and InformaCast was unable to establish a CTI connection with it when starting, InformaCast would never make another CTI connection attempt and would need to be restarted. InformaCast was modified to continue trying to establish a CTI connection if the first attempt fails. This issue is resolved.

Resolved Caveats

CDETs ID	Title
CSCui86392	The InformaCast web interface no longer incorrectly accepts spaces as characters in DialCast dialing patterns.

New Caveat

CDETs ID	Title
None	

InformaCast 8.5.1

Compatibility

InformaCast Basic Paging is compatible with the following versions of Cisco Unified Communications Manager server (including Business Edition 6000): 8.5, 8.6, 9.0, 9.1, 9.12, and 10.0.

New Features

- **Newly Supported Phones.** The following Cisco IP phone models are now supported by InformaCast: 3905, 7821, 7841, 7861, and 8831.
- **Newly Supported CUCM.** Cisco's Unified Communications Manager 10.0 is now supported by InformaCast.

Known/Resolved Issues

None

Resolved Caveats

None

New Caveat

CDETs ID	Title
CSCui86392	Leading spaces on DialCast configuration. The InformaCast web interface incorrectly accepts spaces as characters in DialCast dialing patterns. Workaround: remove spaces from these configurations.

InformaCast 8.4.a

Compatibility

InformaCast Basic Paging is compatible with the following versions of Cisco Unified Communications Manager server (including Business Edition 6000): 8.5, 8.6, 9.0, 9.1, and 9.12.

New Features

- **Added Content to the Support Page.** The InformaCast Support page (**Help** | **Support**) now includes links to both SIP stack logs and a link to the Singlewire Plugins page on the Singlewire website. These links were added to increase your ease of access to InformaCast content.
- **Improved SIP Logging.** New parameters (called DN and callID) have been added to the Performance log. By logging the SIP call ID along with the calling DN and called DN, you can more easily track calls in the Performance log (e.g. when the call started, ended, various modes, etc.).
- **Improved Recipient Group Display.** When sending a message from the InformaCast web interface, recipient groups are now displayed alphabetically by name on the Send Message page instead of randomly, which is now consistent with how recipient groups display on the Edit Recipient Groups page.
- **Enhanced DialCast Usability.** Due to customer requests, the initial DialCast welcome prompt ("Welcome to the Singlewire InformaCast...") has been removed.
- **Upgraded Tomcat Version.** Tomcat was upgraded from version 7.0.16 to 7.0.35. This should have no effect on your user experience.
- **Updated QoS Settings.** In InformaCast versions prior to 8.4.a, the QoS settings were set in the code and did not match Cisco's default QoS DSCP values. On the Virtual Appliance, the QoS settings have been moved to the OS level and now match Cisco's default settings. These settings are:
  - Media RTP traffic set to DSCP EF
  - Call signaling traffic set to DSCP CS3 (call signaling traffic includes SIP and CTI traffic)
  - HTTP traffic to IP phones set to DSCP 0
  - Any other traffic set to DSCP 0

  If you need to change from these default values, you will need to do so at the network level. Rewriting DSCP values is covered in the Cisco Quality of Service (QoS) Solution Reference Network Design (SRND) guide, found at http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book/QoSIntro.html and should be handled by your network administrator.

Resolved Issues

- **Fixed DN Retrieval from AXL (Mantis ID #4154).** Under certain circumstances (e.g. with CUCM 6.1.3, if there were more than 26,300 DNs, or if there were multiple DNs per phone), InformaCast was not always retrieving all the necessary DNs from AXL when building the phone cache. This issue has been resolved.
- **Fixed Broadcast Jitter (Mantis ID #4300).** Previously, sending as-available messages to a large number of devices could result in degraded audio quality (jitter). This issue has been resolved.
- **Fixed Webmin Access through Internet Explorer (Mantis ID #4066).** Previously, accessing Webmin through Internet Explorer was prevented due to an out-of-date SSL certificate. This issue has been resolved.
- **Fixed Release Notes; Changed Version Number.** The release notes have been separated into Basic and Advanced categories, which necessitated a version number change from 8.4 to 8.4.a.
- **Fixed Spelling Inconsistencies, Hover Text, and Display Issues.** Many pages received new hover text, standardized hover text, and standardized word spellings to improve overall user experience.

Resolved Caveats

CDETs ID	Title
CSCuh28590	Voice prompt changed for Basic Paging
CSCuh28557	Standardize all tooltips
CSCuh28540	Missing the “please complete...” hover text on the Basic sign-in form
CSCuh28521	Phone license limit warning text incorrectly refers to Adv mode license
CSCuh22651	Webmin - Unable to get beyond the security cert error page with IE

New Caveats

CDETs ID	Title
CSCuh28628	Provide a more user-friendly interface/functions on the Start Page
CSCuh28601	IP endpoints labeled as required but isn’t on Basic sign-in form
CSCuh28499	Learn More about InformaCast links don't hold focus
CSCuh30592	change-ip-address script for backed up databases
CSCuh30601	Phone caches persists after transitioning back to Basic mode

InformaCast 8.3.a

Compatibility

InformaCast Basic Paging is compatible with the following versions of Cisco Unified Communications Manager server (including Business Edition 6000): 8.5, 8.6, 9.0, and 9.1

Known Issues

- **Updated Graphics.** Black and white graphics in the documentation were changed to color on request.
- **Incorrect Error Message.** In Basic Paging, when you exceed the limit of the number of phones to which you can broadcast in a recipient group, the error message you receive is wrong (i.e. "There are more phones associated with your CUCM server than your InformaCast license key supports. Broadcast messages will be limited to 50 total phones. The number of phones in the list that will participate in a broadcast depends on how many other phones have been broadcast participants. For example, if 50 other phones have been broadcast participants, then no phones in the list can participate. Otherwise, either all or some of the phones can participate. Please contact Singlewire at www.singlewire.com for support or to upgrade your key."). In actuality, each recipient group is limited to 50 phones, and you can send to another separate recipient group of 50 phones. This differs from Advanced Notification where if you exceed your license limit of recipients in one recipient group, you will be unable to send to another separate group of additional phones.

InformaCast 8.3

Compatibility

InformaCast Basic Paging is compatible with the following versions of Cisco Unified Communications Manager server (including Business Edition 6000): 8.5, 8.6, 9.0, and 9.1

New Features

- **New Functionality.** InformaCast 8.3 now comes in two new versions: Basic and Advanced. Basic functionality includes live paging only. Advanced functionality contains the full-featured version of InformaCast: the ability to send a number of different types of broadcasts (e.g. live audio, pre-recorded audio, pre-recorded audio and text, etc.) using your Cisco IP phone's interface and/or InformaCast's web interface, interact with InformaCast's plugins (e.g. conduct conference calls, trigger contact closures, post to Facebook and Twitter, send broadcasts to email addresses, etc.), customize scripts that can be attached to broadcasts, and receive confirmation when broadcasts are sent, among other features. Basic functionality comes automatically installed on the Cisco Unified Communications Manager Business Edition 6000, and you have the option to upgrade to Advanced functionality.
- **New InformaCast Licensing.** Advanced InformaCast can be obtained through a limited, free trial, purchased as a subscription service, or purchased outright (perpetual) with a maintenance contract (which is how InformaCast has traditionally been purchased). The InformaCast trial and subscription licenses allow you to try InformaCast's full functionality without committing to a long-term contract (subscription) or without a contract at all (free, limited-time trial).
- **New Backup Location.** The default backup location setting in previous versions of InformaCast could produce unusable backups. As such, a new backup location was created: /usr/local/singlewire/InformaCast/backup. You should examine the InformaCast backup location that you are currently using and consider changing it to the new recommended location.
- **New License Parameter.** The MaxVersion parameter, a new license parameter, must be present in all 8.3 and later releases of InformaCast and its number must match or be greater than your version of InformaCast in order for you to access any of InformaCast's functionality.

- **Disk Performance Increase.** VMware and storage vendors recommend that virtual machines align on 64Kb boundaries to minimize disk reads, and InformaCast's partitions are now in line with this recommendation. Fewer reads with the same result means better performance, and if you are running VA/EX on SAN disks, you may notice lower IOPS (I/O operations per second) as a result of this change.

Known Issues

- **Unable to Access Webmin with Internet Explorer 9 After Installing Microsoft Security Update KB2661254.** If you've installed Microsoft Security Update KB2661254 and use Internet Explorer 9 to access Webmin (https://<InformaCast Server IP Address:10000), the site will fail. To avoid this issue, use Google, Chrome, or Firefox to access Webmin or use the solutions described by Microsoft at http://support.microsoft.com/?kbid=2661254.
- **InformaCast Not Functioning Correctly After Changing its IP Address in Advanced Notification and Switching Back to Basic Paging.** Changing InformaCast's IP address while using Advanced Notification and switching back to Basic Paging can make broadcasts unavailable to phones. There is currently a warning that occurs when executing the script that changes InformaCast's IP address; users can elect to abort or continue.
- **Phone Cache Becomes Unavailable with a License Change.** Whenever you change InformaCast's license or add/update/delete a cluster, "Default configuration Not Connected" appears for the **Communications Manager Versions** field on the Overview page. If either the license or clusters change, the phone cache must be rebuilt to reflect those changes. The phone cache is automatically rebuilt every hour, but if you want it completed sooner than that, you can click the **Update** button on the Edit Recipient Groups page to discover current IP phone info from CUCM. Once this is done, the CUCM information appears correctly on the Overview page.

Glossary

In order to fully understand your InformaCast environment, you should familiarize yourself with the terms in this section.

API

Application Programming Interface. A language and message format used by an application program to communicate with the operating system or some other control program such as a database management system (DBMS) or communications protocol.

Application User

A user within Cisco Unified Communications Manager (CUCM) that has been granted privileges to work with CTI resources. InformaCast needs to know the username and password of an application user that has been associated with the CTI ports it will be using to place calls for recording messages and integrating with legacy paging systems. This is set up in the CUCM Administration interface.

Audio Stream RTP Packets

Packets capable of conducting real-time voice data over connectionless networks such as IP. See also "RTP" on page 12-8.

Authentication

The process of determining the identity of a user attempting to access a system.

AVVID

Cisco Architecture for Voice, Video, and Integrated Data. Cisco AVVID provides the framework for today's Internet business solutions. As the industry's only enterprise-wide, standards-based network architecture, Cisco AVVID provides the roadmap for combining your business and technology strategies into one cohesive model.

Cisco AVVID provides the baseline infrastructure that enables enterprises to design networks that scale to meet Internet business demands. Cisco AVVID delivers the eBusiness infrastructure and intelligent network services that are essential for rapid deployment of emerging technologies and new Internet business solutions.

AXL

AVVID XML Layer (AXL). A Cisco API and web service designed to give applications access to CUCM configuration and provisioning services. AXL is implemented as a Simple Object Access Protocol (SOAP) over HTTP web service in which requests in the form of extensible markup language (XML) documents are sent from the application to the Cisco CUCM's web server, which responds with an XML-formatted response. InformaCast uses AXL to gather phone information from CUCM.

BAT

Bulk Administration Tool. A web-based application for CUCM that enables bulk system modifications, including adding and deleting phones, modifying phones, and adding users and mailboxes.

Break Key

The key on a phone you press to signal InformaCast that you do not want to hear the remainder of any message.

Broadcast

An audio message sent to a group of phones, made up of one or more recipient groups. A message that is sent to a group of devices, made up of one or more recipient groups and/or dial codes.

Browser

A GUI-based hypertext client application, such as Internet Explorer, Firefox, and Netscape Navigator, used to access the InformaCast administrative interface, as well as hypertext documents and other services located on innumerable remote servers throughout the World Wide Web and Internet. See also "GUI" on page 12-5.

Calling Search Space

Determines which partitions a calling device searches when attempting to complete a call. One of the ways in which InformaCast recipient groups can be defined.

Cisco IP Phone

A full-feature telephone that provides voice communication over an IP network while functioning much like a traditional analog phone. Allows you to place and receive telephone calls, and supports features such as call forwarding, redial, speed dialing, call transfer, and conference calling. Also allows you to access voicemail, providing connectivity to Cisco IP Telephony Solutions.

Cisco Unified Communications Manager

Software-based call processing component of the Cisco IP telephony solution, which extends enterprise telephony features and functions to packet telephony network devices such as IP phones, media processing devices, voice-over-IP (VoIP) gateways, and multimedia applications. See also "Cisco Unified Communications Manager Administration."

Cisco Unified Communications Manager Administration

The web interface used to administer a CUCM's configuration settings and operation.

Client

Node or software program (front-end device) that requests services from a server. The Cisco IP Phone is an example of a client.

Codec

Coder-decoder:

- A device that typically uses pulse code modulation to transform analog signals into a digital bit stream, and digital signals back to analog. See also "G.711" on page 12-5.
- In Voice over IP, Voice over Frame Relay, and Voice over ATM, a software algorithm used to compress/decompress speech or audio signals.

Control Center

The Control Center is designed to be an inclusive destination for application-level accessories.

CTI

Computer Telephony Integration or Computer Telephony Interface. An interface exported by CUCM that allows application developers to create programs that work with the telephone system.

CTI Port

Computer Telephony Interface ports. Virtual devices that are used by Cisco CUCM applications and InformaCast to create virtual lines. CTI ports are configured through the same Cisco CUCM Administration area as phones, but require different configuration settings.

Device Association

A link that allows a specific CUCM user to control a device (such as a CTI port) within the CUCM environment. InformaCast will take control of all CTI ports that are associated with its application user, and make them available for recording.

Device Description

A free-form text entry within the CUCM Administration interface that is intended for the user to describe and identify a specific telephony device (such as a physical phone or CTI port). Because this field is entirely under the administrator's control, it provides the best opportunity for organizing phones into recipient groups to meet an organization's paging needs. Also, a popular method of defining InformaCast recipient groups.

Device Loads

Files that contain updated application software for phones or gateways. Provided automatically during installation or upgrades.

Device Name

The logical name by which a specific telephony device (such as a physical phone or CTI port) is known within the CUCM Administration interface.

Device Pool

In CUCM, a collection of commonly configured devices (such as phones, computers and gateways) that belong to a common database, cluster, and group. Use device pools to define common characteristics for devices, including region, date/time group, CUCM group, and calling search space for automatic definition. One of the ways in which InformaCast recipient groups can be defined.

DialCast

A broadcast triggered by dialing a SIP number configured with dialing pattern that determines which InformaCast message should be sent and which recipient groups should receive it.

Dial Pad

Buttons on a phone that are used to dial a phone number. The dial pad on a Cisco IP phone operates like the dial pad on a traditional telephone.

Directory Number (DN)

Directory Number. The telephone number or internal extension assigned to a Cisco IP phone. The directory number is assigned to the phone itself, not a location or a user, so if the phone is moved, it still retains the same directory number. Also called subscriber number. One of the ways in which InformaCast recipient groups can be defined.

DN Not Recognized Audio

When you pick up a phone and dial your set pattern for a DialCast broadcast, if that pattern doesn't match a configuration you've set, you hear this message.

DSCP

Differentiated Services Code Point, or DiffServe CodePoint. A marker in the header of each IP packet that prompts network routers to apply differentiated grades of service to various packet streams, forwarding them according to different Per-Hop Behaviors (PHBs). Part of DiffServe, a set of technologies proposed by the IETF that allows Internet and other IP-based network service providers to offer differentiated levels of service to customers and their information streams. InformaCast tags its voice traffic to facilitate assured delivery in network environments where this is important.

Dynamic Host Configuration Protocol (DHCP)

A TCP/IP protocol that enables PCs and workstations to get temporary or permanent IP addresses out of a pool from centrally-administered servers. Like its predecessor, BOOTP, DHCP provides a mechanism for allocating IP addresses manually, automatically, and dynamically, so that addresses can be reused when hosts no longer need them. The DHCP server provides Cisco IP phones and InformaCast IP speakers with an IP address, subnet mask, default gateway, and DNS server.

ESXi

VMware ESXi is an enterprise-level computer virtualization product offered by VMware, Inc. ESXi is a component of VMware's larger offering, VMware Infrastructure, and adds management and reliability services to the core server product. VMware ESXi is a bare-metal embedded hypervisor that is VMware's enterprise software hypervisors for servers that run directly on server hardware without requiring an additional underlying operating system.

Ethernet

Baseband LAN specification invented by Xerox Corporation and developed jointly by Xerox, Intel, and Digital Equipment Corporation. Used to connect computers, workstations, terminals, printers, and other devices located in the same building or campus.

Filter

The term "filter" is used to select a defined subset (e.g. matching constructs that select devices to be placed in a recipient group).

G.711

An audio compression standard used for digital telephones on a digital PBX/ISDN. In G.711, encoded voice is already in the correct format for digital voice delivery in the PSTN or through PBXs. G.711 uses a bandwidth of 64 Kbps. G.711-compliant devices can communicate with other G.711 devices, but not with G.723 devices. Described in the ITU-T standard in its G-series recommendations. InformaCast audio broadcasts through phones must use G.711 encoding.

Go Tone

The tone you hear through a phone when InformaCast has finished activating devices in your recipient group in preparation for a live broadcast.

GUI

Graphical User Interface. User environment that uses pictorial as well as textual representations of the input and output of applications and the hierarchical or other data structure in which information is stored. Conventions such as buttons, icons, and windows are typical, and many actions are performed using a pointing device (such as a mouse).

Handset

The portion of a telephone set containing the transmitter and receiver, usually designed to be hand-held when the telephone is in use.

HTTP

HyperText Transfer Protocol. Used by the web server and the client browser to communicate over the Internet. InformaCast also uses HTTP to communicate with CUCM and Cisco IP phones.

Humoctopus

A genetic experiment gone horribly awry.

InformaCast Virtual Appliance

Singlewire's bundled package for virtualized environments. It contains an operating system and InformaCast.

Invalid License Audio

When you pick up a phone and dial your set pattern for a DialCast broadcast, if that pattern matches a configuration you've set and the SIP trunk used, and InformaCast has an invalid license, you hear this message.

IOS

The Cisco Internetworking Operating System (IOS) is a sophisticated operating system optimized for internetworking. Cisco IOS provides the unifying principles around which an internetwork can be maintained cost-effectively over time. It is a software architecture, disassociated from hardware, that can be dynamically upgraded to adapt to changing technologies (hardware and software) as they evolve within a networking infrastructure. Cisco IOS can be thought of as an internetworking brain, a highly intelligent administrator that manages and controls complex, distributed network resources and functions.

IP Address

Internet Protocol Address. A 32-bit address assigned to hosts using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as four octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, while the host number is used to address an individual host within the network or subnetwork. A subnet mask is used to extract network and subnetwork information from the IP address. Also known as an Internet address. See also "Subnet Mask" on page 12-9.

IP Phone

See "Cisco IP Phone" on page 12-2.

Java

Programming language and runtime environment from Sun Microsystems in which InformaCast is implemented.

Jitter

A type of distortion caused by the variation of a signal from its reference that can cause data transmission errors, particularly at high speeds.

JTAPI

Java Telephony Application Programming Interface. The mechanism by which InformaCast is able to place and control calls in a CUCM environment.

Login

A word or string of characters recognized by automatic means, generally paired with a password, that identifies a user and permits specific access to a place or to protected storage, files, or input/output devices.

MAC Address

Standardized data link layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are six bytes long and are controlled by the IEEE. Also known as a hardware address, MAC-layer address, and physical address. Compare with Network Address.

Message

The basis of any InformaCast broadcast, a message predefines the characteristics of the broadcast.

µLaw

(mu-law) North American companding standard used in conversion between analog and digital signals in PCM systems. This is the kind of audio encoding used in G.711.

Multicast

Single packets copied by the network and sent to a specific subset of network addresses. A process of transmitting messages from one source to many destinations. Used by InformaCast to allow scalable paging to thousands of devices. Contrast with "Unicast" on page 12-10.

Multicast Address

Single address that refers to multiple network devices. These use a special numbering scheme distinct from ordinary unicast IP addresses.

Network Address

Network layer address referring to a logical, rather than a physical, network device. Also called a protocol address. Compare with MAC Address.

NIC

- Network Interface Card. Board that provides network communication capabilities to and from a computer system. Also called an adapter.
- Network Interface Controller. An intelligent device that connects a workstation to a network.

No Active Devices Audio

The tone you hear through a phone if there are no active devices in the recipient group for your live broadcast.

Password

A word or string of characters recognized by automatic means, generally paired with a login, that permits a user access to a place or protected storage, files, input/output devices, or other system resources.

PBX

A PBX (private branch exchange) is a telephone system within an enterprise that switches calls between enterprise users on local lines while allowing all users to share a certain number of external phone lines. The main purpose of a PBX is to save the cost of requiring a line for each user to the telephone company's central office.

Phone Loads

See "Device Loads" on page 12-3.

Protocol

A set of rules or conventions that govern the format and relative timing of data in a communications network. There are three basic types of protocols: character-oriented, byte-oriented, and bit-oriented. The protocols for data communications cover such things as framing, error handling, transparency, and line control. Ethernet is an example of a LAN protocol.

Proxy

A device that relays network connections for other devices that usually lack their own network access.

Recipient

An endpoint capable of receiving an InformaCast broadcast. Currently, these can include Cisco IP phones.

Recipient Group

A logical, pre-defined group of recipients that can receive InformaCast broadcasts. One recipient can be part of one or more recipient groups.

Recipient Group Tags

Recipient group tags allow you finer control over the display results for recipient groups.

RTP

Real-Time Transport Protocol. A network protocol used to carry packetized audio and video traffic over an IP network. The audio portions of InformaCast broadcasts are sent as a multicast RTP stream.

Scalable

Indicates that a software application or a hardware device has the ability to migrate from small operations to large operations.

Server

Node or software program that provides services to clients. In an InformaCast environment, the computer on which InformaCast is running is a server. If you are in a telephony environment, there will be at least one separate CUCM server as well.

Singlewire Start Page

The Singlewire Start page is accessible through a web browser addressed with the IP address of the Virtual Appliance, and it contains links to your applications' user interfaces, the Control Center, and Webmin.

SIP

Session Initiation Protocol is an IETF-defined signaling protocol used for controlling communication sessions such as voice and video calls over Internet Protocol (IP). The protocol can be used for creating, modifying, and terminating two-party (unicast) or multi-party (multicast) sessions. Sessions may consist of one or several media streams.

SNMP

Simple Network Management Protocol. Forms part of the Internet protocol suite as defined by the Internet Engineering Task Force. The protocol is used by network management systems for monitoring network-attached devices for conditions that warrant administrative attention. Starting with CUCM 5, Cisco requires InformaCast to use SNMP rather than the previous DeviceListX mechanism for obtaining dynamic information about registered phones (such as their IP address) needed for sending broadcasts.

Stall Tone

The tones you hear through a phone while waiting for InformaCast to activate the recipients in your recipient group during a live broadcast.

Subnet Mask

A 32-bit address mask used in IP to indicate the bits of an IP address that are being used for the subnet address. See also "IP Address" on page 12-6. One of the ways in which InformaCast recipient groups can be defined.

TFTP

Trivial File Transfer Protocol. A simplified version of the FTP protocol, TFTP servers generally provide configuration information and firmware files to Cisco IP phones.

TLS

Transport Layer Security (TLS) is a cryptographic protocol that provides communication security over the Internet. TLS encrypts the segments of network connections above the Transport layer, using asymmetric cryptography for key exchange, symmetric encryption for privacy, and message authentication codes for message integrity. Several versions of the protocol is in widespread use in applications such as web browsing, electronic mail, Internet faxing, instant messaging, and voice-over-IP (VoIP).

UDP

The User Datagram Protocol (UDP) is one of the core members of the Internet Protocol Suite, the set of network protocols used for the Internet. With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network without requiring prior communications to set up special transmission channels or data paths.

Unicast

A process of transmitting messages from one source to one destination. Compare with "Multicast" on page 12-7.

Unicast Address

Address specifying a single network device. See also "Unicast." The IP addresses that you encounter in ordinary use of the Internet are generally unicast addresses.

User

A person who will use InformaCast. He/she will be assigned an individual login and password, which can be used to configure the roles and filters that determine the features and resources available to him/her.

Via Header

With SIP, the Via header indicates the path taken by a SIP request so far.Via headers can be used to prevent request looping and ensure replies take the same path as the requests.

Virtual Appliance

A virtual appliance is a virtual machine image designed to run on a virtualization platform (e.g., VirtualBox, Xen, VMware Workstation, Parallels Workstation).

Virtual Machine

A virtual machine (VM) is a software implementation of a machine (i.e. a computer) that executes programs like a physical machine.

VMware

A company providing virtualization software. VMware's desktop software runs on Microsoft Windows, Linux, and Mac OS X, while VMware's enterprise software hypervisors for servers, VMware ESX and VMware ESXi, are bare-metal embedded hypervisors that run directly on server hardware without requiring an additional underlying operating system.

VoIP

Voice over Internet Protocol. Enables users to transfer voice communications over a data network using IP.

Web Interface

A software application that runs on the World Wide Web and is usually accessed through a web browser running on a computer workstation. InformaCast and CUCM Administration use web interfaces.

Webmin

The virtual machine administrative web interface is used for administering the underlying operating system of the virtual machine, e.g. configuring the network interface, stopping and starting InformaCast and shutting down the virtual machine. You can access it at https://<InformaCast Virtual Appliance IP Address>:10000.

XML

eXtensible Markup Language. A general-purpose specification for creating custom markup languages. It is classified as an extensible language because it allows its users to define their own elements. Its primary purpose is to help information systems share structured data, particularly via the Internet, and it is used both to encode documents and to serialize data.

Acknowledgments

Without the following products and software, InformaCast wouldn't be the revolutionary broadcast system that it is.

Apache Axis2

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at
http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Apache Software

This product includes software developed by the Apache Software Foundation (http://www.apache.org/) including Jakarta Tomcat, Jakarta Commons, Jakarta log4j, Jakarta ORO, Apache Xerces, and Apache XML-RPC.

Copyright 2004, The Apache Software Foundation.

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at
http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

CSVToXML

This product contains CSVToXML, a library for converting CSV files to XML. The code is available here: http://www.dpawson.co.uk/java/csv2xml.html

Hibernate

This product uses Hibernate for object persistence. Hibernate is distributed under the GNU Lesser General Public License version 2.1. The source code can be found in the directory, /usr/local/singlewire/InformaCast/web/doc, within your InformaCast installation.

hsqldb

This product contains the HSQL database engine.

Copyright 2001-2002 The HSQL Development Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer, including earlier license statements (above) and comply with all above license conditions.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution, including earlier license statements (above) and comply with all above license conditions.
- Neither the name of the HSQL Development Group nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL HSQL DEVELOPMENT GROUP, HSQLDB.ORG, OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Hypersonic SQL

This product contains Hypersonic SQL.

Copyright 1995-2000 by the Hypersonic SQL Group. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Hypersonic SQL Group nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

This software is provided "as is" and any expressed or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the Hypersonic SQL Group or its contributors be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption). However caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

This software consists of voluntary contributions made by many individuals on behalf of the Hypersonic SQL Group.

Java Platform

This product relies on the Java platform and includes code licensed from RSA Security, Inc.

Some portions licensed from IBM are available at http://www.ibm.com/developerworks/opensource/.

Java, Sun, and Sun Microsystems are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. IBM is a registered trademark of International Business Machines Corporation in the United States and other countries.

JAXB

This product contains JAXB, whose code is available from: http://jaxb.java.net/

COMMON DEVELOPMENT AND DISTRIBUTION LICENSE (CDDL) Version 1.0

1. Definitions.

1.1. Contributor means each individual or entity that creates or contributes to the creation of Modifications.

1.2. Contributor Version means the combination of the Original Software, prior Modifications used by a Contributor (if any), and the Modifications made by that particular Contributor.

1.3. Covered Software means (a) the Original Software, or (b) Modifications, or (c) the combination of files containing Original Software with files containing Modifications, in each case including portions thereof.

1.4. Executable means the Covered Software in any form other than Source Code.

1.5. Initial Developer means the individual or entity that first makes Original Software available under this License.

1.6. Larger Work means a work which combines Covered Software or portions thereof with code not governed by the terms of this License.

1.7. License means this document.

1.8. Licensable means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9. Modifications means the Source Code and Executable form of any of the following:

A. Any file that results from an addition to, deletion from or modification of the contents of a file containing Original Software or previous Modifications;

B. Any new file that contains any part of the Original Software or previous Modification; or

C. Any new file that is contributed or otherwise made available under the terms of this License.

1.10. Original Software means the Source Code and Executable form of computer software code that is originally released under this License.

1.11. Patent Claims means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1.12. Source Code means (a) the common form of computer software code in which modifications are made and (b) associated documentation included in or with such code.

1.13. You (or Your) means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License. For legal entities, You includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, control means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. License Grants.

2.1. The Initial Developer Grant.

Conditioned upon Your compliance with Section 3.1 below and subject to third party intellectual property claims, the Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license:

(a) Under intellectual property rights (other than patent or trademark) Licensable by Initial Developer, to use, reproduce, modify, display, perform, sublicense and distribute the Original Software (or portions thereof), with or without Modifications, and/or as part of a Larger Work; and

(b) Under Patent Claims infringed by the making, using or selling of Original Software, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Software (or portions thereof).

(c) The licenses granted in Sections 2.1(a) and (b) are effective on the date Initial Developer first distributes or otherwise makes the Original Software available to a third party under the terms of this License.

(d) Notwithstanding Section 2.1(b) above, no patent license is granted: (1) for code that You delete from the Original Software, or (2) for infringements caused by: (i) the modification of the Original Software, or (ii) the combination of the Original Software with other software or devices.

2.2. Contributor Grant.

Conditioned upon Your compliance with Section 3.1 below and subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license:

(a) Under intellectual property rights (other than patent or trademark) Licensable by Contributor to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof), either on an unmodified basis, with other Modifications, as Covered Software and/or as part of a Larger Work; and

(b) Under Patent Claims infringed by the making, using, or selling of Modifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale, have made, and/or otherwise dispose of: (1) Modifications made by that Contributor (or portions thereof); and (2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination).

(c) The licenses granted in Sections 2.2(a) and 2.2(b) are effective on the date Contributor first distributes or otherwise makes the Modifications available to a third party.

(d) Notwithstanding Section 2.2(b) above, no patent license is granted: (1) for any code that Contributor has deleted from the Contributor Version; (2) for infringements caused by: (i) third party modifications of Contributor Version, or (ii) the combination of Modifications made by that Contributor with other software (except as part of the Contributor Version) or other devices; or (3) under Patent Claims infringed by Covered Software in the absence of Modifications made by that Contributor.

3. Distribution Obligations.

3.1. Availability of Source Code.

Any Covered Software that You distribute or otherwise make available in Executable form must also be made available in Source Code form and that Source Code form must be distributed only under the terms of this License. You must include a copy of this License with every copy of the Source Code form of the Covered Software You distribute or otherwise make available. You must inform recipients of any such Covered Software in Executable form as to how they can obtain such Covered Software in Source Code form in a reasonable manner on or through a medium customarily used for software exchange.

3.2. Modifications.

The Modifications that You create or to which You contribute are governed by the terms of this License. You represent that You believe Your Modifications are Your original creation(s) and/or You have sufficient rights to grant the rights conveyed by this License.

3.3. Required Notices.

You must include a notice in each of Your Modifications that identifies You as the Contributor of the Modification. You may not remove or alter any copyright, patent or trademark notices contained within the Covered Software, or any notices of licensing or any descriptive text giving attribution to any Contributor or the Initial Developer.

3.4. Application of Additional Terms.

You may not offer or impose any terms on any Covered Software in Source Code form that alters or restricts the applicable version of this License or the recipients rights hereunder. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Software. However, you may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear that any such warranty, support, indemnity or liability obligation is offered by You alone, and You

hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

3.5. Distribution of Executable Versions.

You may distribute the Executable form of the Covered Software under the terms of this License or under the terms of a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable form does not attempt to limit or alter the recipients rights in the Source Code form from the rights set forth in this License. If You distribute the Covered Software in Executable form under a different license, You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

3.6. Larger Works.

You may create a Larger Work by combining Covered Software with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Software.

4. Versions of the License.

4.1. New Versions.

Sun Microsystems, Inc. is the initial license steward and may publish revised and/or new versions of this License from time to time. Each version will be given a distinguishing version number. Except as provided in Section 4.3, no one other than the license steward has the right to modify this License.

4.2. Effect of New Versions.

You may always continue to use, distribute or otherwise make the Covered Software available under the terms of the version of the License under which You originally received the Covered Software. If the Initial Developer includes a notice in the Original Software prohibiting it from being distributed or otherwise made available under any subsequent version of the License, You must distribute and make the Covered Software available under the terms of the version of the License under which You originally received the Covered Software. Otherwise, You may also choose to use, distribute or otherwise make the Covered Software available under the terms of any subsequent version of the License published by the license steward.

4.3. Modified Versions.

When You are an Initial Developer and You want to create a new license for Your Original Software, You may create and use a modified version of this License if You: (a) rename the license and remove any references to the name of the license steward (except to note that the license differs from this License); and (b) otherwise make it clear that the license contains terms which differ from this License.

5. DISCLAIMER OF WARRANTY.

COVERED SOFTWARE IS PROVIDED UNDER THIS LICENSE ON AN AS IS BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE COVERED SOFTWARE IS FREE OF DEFECTS, MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE OR NON-INFRINGING.

THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE COVERED SOFTWARE IS WITH YOU. SHOULD ANY COVERED SOFTWARE PROVE DEFECTIVE IN ANY RESPECT, YOU (NOT THE INITIAL DEVELOPER OR ANY OTHER CONTRIBUTOR) ASSUME THE COST OF ANY NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED SOFTWARE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

6. TERMINATION.

6.1. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

6.2. If You assert a patent infringement claim (excluding declaratory judgment actions) against Initial Developer or a Contributor (the Initial Developer or Contributor against whom You assert such claim is referred to as Participant) alleging that the Participant Software (meaning the Contributor Version where the Participant is a Contributor or the Original Software where the Participant is the Initial Developer) directly or indirectly infringes any patent, then any and all rights granted directly or indirectly to You by such Participant, the Initial Developer (if the Initial Developer is not the Participant) and all Contributors under Sections 2.1 and/or 2.2 of this License shall, upon 60 days notice from Participant terminate prospectively and automatically at the expiration of such 60 day notice period, unless if within such 60 day period You withdraw Your claim with respect to the Participant Software against such Participant either unilaterally or pursuant to a written agreement with Participant.

6.3. In the event of termination under Sections 6.1 or 6.2 above, all end user licenses that have been validly granted by You or any distributor hereunder prior to termination (excluding licenses granted to You by any distributor) shall survive termination.

7. LIMITATION OF LIABILITY.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU, THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF COVERED SOFTWARE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOST PROFITS, LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTYS NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

8. U.S. GOVERNMENT END USERS.

The Covered Software is a commercial item, as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of commercial computer software (as that term is defined at 48 C.F.R. 252.227-7014(a)(1)) and commercial computer software documentation as such terms are used in 48 C.F.R. 12.212 (Sept. 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire Covered Software with only those rights set forth herein. This U.S. Government Rights clause is in lieu of, and supersedes, any other FAR, DFAR, or other clause or provision that addresses Government rights in computer software under this License.

9. MISCELLANEOUS.

This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by the law of the jurisdiction specified in a notice contained within the Original Software (except to the extent applicable law, if any, provides otherwise), excluding such jurisdictions conflict-of-law provisions. Any litigation relating to this License shall be subject to the jurisdiction of the courts located in the jurisdiction and venue specified in a notice contained within the Original Software, with the losing party responsible for costs, including, without limitation, court costs and reasonable attorneys fees and expenses. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License. You agree that You alone are responsible for compliance with the United States export administration regulations (and the export control laws and regulation of any other countries) when You use, distribute or otherwise make available any Covered Software.

10. RESPONSIBILITY FOR CLAIMS.

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

JDOM

This product includes software developed by the JDOM Project (http://www.jdom.org/).

Copyright 2000-2002 Brett McLaughlin & Jason Hunter. All rights reserved.

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at
http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

jTDS

This product contains the jTDS JDBC driver, http://jtds.sourceforge.net/.

This product includes software developed by CDS Networks, Inc.

Copyright 1998, 1999 CDS Networks, Inc., Medford Oregon. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes software developed by CDS Networks, Inc."
- The name of CDS Networks, Inc. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY CDS NETWORKS, INC. "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL CDS NETWORKS, INC. BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Linux/Voyage

This product from Singlewire Software runs on a Linux kernel and the Voyage Linux distribution.

The Linux kernel and Voyage Linux are distributed under the following license:

- This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation.
- This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.
- To see a copy of the GNU public license, see this URL: http://www.gnu.org/licenses/gpl-2.0.html.
- You may also write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.
- Modifications Singlewire Software has made to the Voyage Linux distribution can be found here: http://www.singlewire.com/pgl.

Quartz

This product includes the Quartz Enterprise Job Scheduler, http://www.quartz-scheduler.org/.

Copyright James House 2001-2003, PartNET Inc. 2002. All rights reserved.

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

SLP Mesh Enhancement, Customization, and Global Attributes

Copyright 2001-2005, Columbia University. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Columbia University; nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

SNMP4J

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

Terms and Conditions for Use, Reproduction, and Distribution

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination

of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

   You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.
9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

Index

A

Access
- InformaCast 1-1
- InformaCast Virtual Appliance 1-21
- License Manager 1-22
- Singlewire Start Page 1-21
- Webmin 1-27

Access InformaCast 1-2, 1-3, 1-7
Acknowledgments 1-1
- Apache Axis2 1-1
- Apache Software 1-1
- CSVToXML 1-1
- Hibernate 1-2
- hsqldb 1-2
- Hypersonic SQL 1-2
- Java Platform 1-3
- JAXB 1-3
- JDOM 1-8
- jTDS 1-8
- Linux/Voyage 1-9
- Quartz 1-10
- SLP Mesh Enhancement 1-10
- SNMP4J 1-10

Active Broadcasts 1-47
Add
- Broadcast Dialing Configuration 1-41
- Recipient Group Exclusion 1-21
- Recipient Group with Existing Recipient Groups 1-15
- Recipient Group with Individual Recipients 1-13
- Recipient Group with Rules 1-18
- Recipient Groups 1-11
- Route Pattern 1-25
- SIP Access Exception 1-28
- SIP Trunk Security Profile 1-5
- SIP User Credentials 1-34
- TLS SIP Trunk 1-17
- TLS SIP Trunk Security Profile 1-15

Administer
- Installation 1-70
- Recipients 1-37

Advanced Functionality Definition 1-5, 1-1
Advanced InformaCast 1-1
API 1-1, 1-9
Authentication URL 1-64
AXL Credentials 1-2, 1-9

B

Backup
- Configure InformaCast 1-2
- InformaCast 1-2
- Move ZIP File to a Safe Location 1-3

Basic Functionality Definition 1-5, 1-1
Basic InformaCast Upgrade 1-1
Basic License Definition 1-5
Broadcast
- Cancel 1-46
- Send a Broadcast 1-45

Broadcast Dialing Configuration
- Add 1-41
- Delete 1-44
- Edit 1-42

Broadcasts
- Parameters 1-44
- Troubleshooting 1-7

Buy Advanced Notification 1-8

C

Calling Terminal Diagnostics 1-6
Cancel
- Audio Broadcast 1-46

Change
- Virtual Appliance Password 1-17

Change IP Address 1-6, 1-20
Command Line Interface 1-10
Configure
- Default CUCM Cluster 1-2
- InformaCast Backups 1-2
- Messages and Broadcasts 1-1
- Recipients 1-1
- Session Timeouts 1-15
- SIP Trunk 1-4
- SNMP Monitoring 1-14
- Update JTAPI 1-22

Copy
- Recipient Group 1-29

Create
- SIP Trunk 1-7

CTI Credentials 1-2, 1-9
CUCM
- Add User Group 1-49
- Application User 1-53
- Authentication URL 1-64
- Calling Search Space 1-43
- Configure SNMP 1-31
- Create a Community String 1-33
- Create CTI Ports 1-44
- Create Route Partition 1-42
- Device Pool 1-40
- Enable SNMP 1-31
- G.711 Codec 1-36
- G.711 Codec for Virtual Appliance, 9.x CUCM or later 1-38
- G.711 Codec for Virtual Appliance, pre-9.x CUCM 1-36
- Integrate 1-30

JTAPI and Phones' Busy States 1-41
Reboot Phones 1-65
Test Phones 1-67
Web Access for Phones 1-56
CUCM Clusters
Default 1-2, 1-9

D

Defunct Phones 1-31
Delete
Broadcast Dialing Configuration 1-44
Defunct Phones from InformaCast 1-31
Recipient Group 1-33
SIP User Credentials 1-37
Demonstration License Definition 1-5, 1-6
Determine Phones' Busy States 1-41
DialCast
Manage SIP Functionality 1-4
DialCasts
Add Broadcast Dialing Configuration 1-41
Cancel 1-46
Delete Broadcast Dialing Configuration 1-44
Edit Broadcast Dialing Configuration 1-42
Manage 1-40
Send 1-45

E

Edit
Broadcast Dialing Configuration 1-42
Default CUCM Cluster 1-9
Recipient Group 1-25
SIP User Credentials 1-36
Enable
Web Access for Individual Phones 1-60
Web Access for Multiple Phones 1-57, 1-58
Web Access for Phones 1-56
ESXi 1-6
EULA Error 1-2

F

FAQ 1-1
Capture Traffic 1-6
Create Recipient Groups 1-6
Exceeded License Key 1-5
HTTP Status 500 Error 1-1
IP Address 1-6, 1-20
New IP Address 1-6, 1-20
No Text or Audio Broadcasts 1-6
SSL Certificate 1-1
Voicemail 1-6
Free Trial 1-4
Frequently Asked Questions, see FAQ 1-1

H

Help 1-11

I

InformaCast
Access 1-1
Configure Messages and Broadcasts 1-1
Configure Recipients 1-1
DSCP Quality of Service Policies 1-4
Log In Initially 1-2
Maintain 1-1
Manage Telephony 1-2
Reboot Phones 1-65
Set Authentication URL 1-64
Set G.711 Codec for 9.x or later CUCM 1-38
Set G.711 Codec for pre-9.x CUCM 1-36
Test Phones 1-67
Upgrade from Basic to Advanced 1-1
InformaCast IP Address 1-2, 1-3, 1-7
InformaCast Virtual Appliance
Access 1-21
Administrator Password 1-6
API 1-1, 1-9
Change Password 1-17
Command Line Interface 1-10
Configure Backups 1-2
Control Center Interface 1-9
Definition of 1-1
Documentation 1-11
Embedded SNMP Agent 1-14
Hardware Requirements 1-2
Help 1-11
Icons, Description of 1-8
Illustrations 1-6
Install 1-1, 1-6
Install CUCM Certificates 1-20
Install SIP Certificate 1-12
Intended Audience 1-1
Interface Orientation 1-6
License 1-7
Licensing 1-5
Log in 1-2
Manage Backups 1-2
Multicast 1-2, 1-70, 1-76, 1-77, 1-78
Notification Boxes Explained 1-2
Open 1-2, 1-3, 1-7
Plan your Multicast Environment 1-1
Port Configuration 1-3
Prepare your Multicast Environment 1-1
Prerequisites 1-2
Remove Defunct Phones 1-31
Restore from Backup 1-7
Set the System Time 1-27
Singlewire Start Page 1-7
Support 1-11
Test Multicast 1-2
Troubleshooting 1-11
Update JTAPI 1-22
Upgrade 1-25
Upgrade License 1-9
Upgrade, Determine Version 1-25
Upgrade, Upload New License 1-31
User Guide Standards 1-1
Versions 1-25
Web Interface 1-8
Webmin 1-10
InformaCast Virtual Appliance Version 1-9
InformaCastBackup.ZIP 1-3
Install
Administration 1-70
Configure CUCM SNMP 1-31

Create a Calling Search Space 1-43
Create Application User 1-53
Create AXL User Group 1-49
Create CTI Ports 1-44
Create Device Pool 1-40
Create Route Partition 1-42
CUCM 1-30
CUCM Certificates on InformaCast 1-20
CUCM SNMP 1-33
Enable CUCM SNMP 1-31
Enable Web Access for Phones 1-56
InformaCast SIP Certificate 1-12
InformaCast Virtual Appliance 1-6
Reboot Phones 1-65
Set Authentication URL 1-64
Set G.711 Codec 1-36
Set G.711 Codec for 9.x or later CUCM 1-38
Set G.711 Codec for pre-9.x CUCM 1-36
Test Phones 1-67
Install InformaCast 1-1
Interface Orientation 1-6
IP Address, Change 1-6, 1-20

J

JTAPI 1-22, 1-41, 1-44

L

License
Demonstration, Definition of 1-6
Perpetual, Definition of 1-6
Subscription, Definition of 1-6
Trial, Definition of 1-5
License Definitions 1-5
License Key 1-5, 1-7, 1-9
Exceed 1-7, 1-13, 1-5
Upload New 1-31
License Key, Dependent Features 1-9
License Manager, Access 1-22
Live Audio Broadcast 1-45
Log into InformaCast 1-2, 1-1, 1-3
Log into InformaCast Initially 1-2
Log into InformaCast Virtual Appliance 1-2
Log into PushToTalk 1-4
Log into the Control Center 1-5
Log into Webmin 1-7
Logs
Performance 1-7, 1-13, 1-5, 1-6, 1-1
Summary 1-1, 1-3

M

Maintain InformaCast 1-1
Manage
Broadcast Parameters 1-44
DialCasts 1-40
Digest Authentication with SIP User Credentials 1-34
InformaCast Administrator Password 1-6
InformaCast Backups 1-2
InformaCast Telephony 1-2
Installation Administration 1-70
Messages 1-1
New License 1-31
New License Key 1-9
Phone Updates 1-39, 1-12
Recipient Administration 1-37
Recipient Groups 1-11
SIP Access to InformaCast 1-27
SIP Authentication for InformaCast 1-30
SIP Certificates 1-9
SIP Functionality 1-4
SIP Stack 1-38
Management Information Base 1-14
message URL http
//www.singlewire.com/compatibility-matrix.html 1-2
Messages
Ad-hoc Audio, Description of 1-2
Live Audio, Description of 1-2
Manage 1-1
Pre-recorded Audio, Description of 1-2
Talk and Listen, Description of 1-2
Text and Ad-hoc Audio, Description of 1-2
Text and Live Audio, Description of 1-1
Text and Pre-recorded Audio, Description of 1-1
Text, Description of 1-1
Multicast 1-44
IGMP Snooping 1-78
IGMPv3 1-78
MPLS Provider 1-77
Network Capture 1-71, 1-74
PIM 1-76
Plan your environment 1-1
Review Configuration 1-70
Test Configuration 1-2
Testing Tool 1-2
Traffic Capture 1-70
Troubleshooting 1-70, 1-1
Multicast Environment Preparation
InformaCast Virtual Appliance 1-1

N

Network DSCP QoS 1-4, 1-7
Network Management Software 1-14
Network Traffic Capture
Obtain 1-71
Read 1-74
Notification Box
Caution 1-2
Note 1-2
Tip 1-2
Warning 1-2

P

Performance Log 1-7, 1-13, 1-5, 1-6, 1-1
Perpetual InformaCast 1-8
Perpetual License Definition 1-5, 1-6
Phones, Reboot 1-65
Phones, Test 1-67
Port Configuration 1-3

R

Reboot
Phones 1-65
Reboot InformaCast Virtual Machine 1-3, 1-16

Recipient Group Tags
Add 1-34
Delete 1-36
Description of 1-34
Edit 1-35
Recipient Groups
Add 1-11
Add Exclusions 1-21
Add with Existing Recipient Groups 1-15
Add with Individual Recipients 1-13
Add with Rules 1-18
Advanced Matching 1-37
Copy 1-29
Delete 1-33
Edit 1-25
Manage 1-11
Regular Expressions 1-38
Remove Defunct Phones 1-31
Remove Rules 1-21
Subnet Matching 1-37
Tag 1-34, 1-35, 1-36
View Recipients 1-27
Recipients
Administration 1-37
Configure 1-1
Regular Expressions
Group Recipients 1-38
Release Notes 1-1
11.0.1 1-2
11.0.1.a 1-2
11.0.2 1-1
8.3 1-10
8.3.a 1-9
8.4.a 1-8
8.5.1 1-7
9.0.1 1-5
9.0.2 1-4
9.1.1 1-3
Remove
Defunct Phones 1-31
Recipient Group Rules 1-21
Restart
SIP 1-39
Restart InformaCast 1-3, 1-14
Restore InformaCast from Backup 1-7

S

Send
DialCast 1-45
Live Audio Broadcast 1-45
Send Commands to Phones by JTAPI, Troubleshooting 1-5
Server Hardening
Troubleshooting 1-1
Session Timeouts, Configure 1-15
Set Authentication URL 1-64
Set System Time 1-27
Singlewire Start Page 1-7
Singlewire Start Page, Access 1-21
SIP 1-4
Add a Route Pattern 1-25
Add a SIP Trunk Security Profile 1-5
Add a TLS SIP Trunk 1-17
Add a TLS SIP Trunk Security Profile 1-15
Add Access Exception 1-28
Add User Credentials 1-34
Allow/Deny Access to InformaCast 1-27
Configure a SIP Trunk 1-4
Create a SIP Trunk 1-7
Delete SIP User Credentials 1-37
Edit User Credentials 1-36
Enable Authentication for InformaCast 1-30
Enable Digest Authentication with SIP User Credentials 1-34
Install CUCM Certificates on InformaCast 1-20
Install InformaCast SIP Certificate 1-12
Manage SIP Certificates 1-9
Manage SIP Stack 1-38
Restart 1-39
View InformaCast SIP Certificate 1-10
SIP Functionality
Manage 1-4
SNMP, Configure Monitoring 1-14
Start InformaCast 1-12
Start Page 1-21, 1-2, 1-3, 1-7
Start/Stop InformaCast 1-3
Stop InformaCast 1-10
Subnet Matching 1-37
Subscription InformaCast 1-8
Subscription License Definition 1-5, 1-6
Summary Log 1-1, 1-3
Support 1-11

T

Test
Phones 1-67
Test Multicast 1-2
TLS
Add a SIP Trunk 1-17
Add a SIP Trunk Security Profile 1-15
Definition 1-9
Install CUCM Certificates on InformaCast 1-20
Install the InformaCast SIP Certificate 1-12
Manage SIP Certificates 1-9
Trial License Definition 1-5
Troubleshooting 1-11, 1-1
Authentication 1-3
Broadcasts 1-5
EULA Error 1-2
Log Files 1-1
Log into InformaCast 1-2, 1-1
Multicast 1-1
Phone Discovery 1-4
Server Hardening 1-1
Start/Stop/Restart and Reboot InformaCast 1-3
Upgrade from Basic to Advanced 1-7
Upgrade InformaCast Virtual Appliance 1-7
VMware Tools 1-3, 1-24
Try Advanced Notification 1-4

U

Update InformaCast's Phone Information 1-39, 1-12
Upgrade
How To Steps 1-7
Upgrade InformaCast 1-1

Basic to Advanced 1-1
Buy Advanced Notification 1-8
Differences Between Versions 1-25
Enter New License Key 1-9
Errors on Telephony Configuration 1-8
Install a Software Package 1-27
Missing CUCM Information 1-8
Missing Phones 1-9
Note the Differences 1-2
Try Advanced Notification 1-4
Upgrade InformaCast EX
Obtain Software Package 1-26
Upgrade InformaCast Virtual Appliance 1-25
Determine Your Current Version 1-25
Upload New License 1-31

V

Version, InformaCast Virtual Appliance 1-9, 1-25
View
Active Broadcasts 1-47
InformaCast SIP Certificate 1-10
License Key 1-7
Recipients in a Recipient Group 1-27
Virtual Appliance 1-6
Webmin 1-10
Virtual Machine 1-6
Virtual Machine Control Center Interface 1-9
VMware 1-6
VMware Tools 1-3, 1-24

W

Web Access, Individual Phones 1-60
Web Access, Multiple Phones 1-57, 1-58
Web Access, Phones 1-56
Web Interface 1-8
Webmin 1-10
Webmin, Access 1-27