



InformaCast Virtual Appliance Basic Paging[®]

Version 11.5.2

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

August 31, 2016

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.

© 2016 Cisco Systems, Inc. All rights reserved.

© 2016 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.

Singlewire Software products would not be what they are without the use of open source software. Singlewire takes its open source compliance obligations seriously, and towards this end, the open source information for each product release is published [here](#).

Last Updated: August 31, 2016



CONTENTS

- InformaCast Virtual Appliance Basic Paging Overview 1-1
 - Intended Audience 1-1
 - User Guide Standards 1-1
 - Prerequisites 1-2
 - Hardware Requirements 1-3
 - Port Configuration 1-3
 - DSCP Quality of Service Policies 1-5
 - Licensing Information 1-5
 - InformaCast Illustrations 1-7
 - Virtual Appliance Interface Orientation 1-7
 - Troubleshooting 1-12
 - Getting Help 1-12
 - Technical Support 1-13
- Install InformaCast 2-1
 - Prepare Your Multicast Environment 2-1
 - Install InformaCast Virtual Appliance 2-6
 - Log into InformaCast Virtual Appliance’s Interfaces 2-21
 - Update JTAPI 2-30
 - Set the System Time 2-35
 - Create and Install a Signed Certificate 2-38
 - Integrate Unified Communications Manager 2-45
 - Manage Installation Administration 2-88
- Access InformaCast 3-1
 - Log into InformaCast for the First Time 3-2
 - View Your License Key 3-6
- Configure Recipients 4-1
 - Manage InformaCast’s Telephony 4-2
 - Manage Recipient Groups 4-11
 - Manage Recipient Administration 4-38
- Configure Messages and Broadcasts 5-1
 - Manage Messages 5-1
 - Manage SIP Functionality 5-4
 - Manage DialCasts 5-46
 - Send a DialCast/Broadcast 5-51
 - Cancel a DialCast/Broadcast 5-52

Manage Call Detail Records	5-53
Maintain InformaCast	6-1
Change the Application Administrator's Password	6-2
Manage InformaCast Backups	6-3
Manage Phone Updates	6-14
Configure SNMP Monitoring	6-16
Configure Session Timeout	6-18
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	9-5
VMware Tools	9-5
Authentication	9-6
Phone Discovery	9-7
Broadcasts	9-8
Backups	9-11
Upgrading InformaCast	9-12
Upgrading from Basic to Advanced InformaCast	9-12
Manage InformaCast Virtual Appliance	10-1
Manage Virtual Appliance Actions	10-1
Change the OS Administrator's Password	10-8
Change InformaCast Virtual Appliance's IP Address	10-9
Upgrade your VMware Tools	10-14
Upgrade InformaCast Virtual Appliance	10-15
Release Notes	11-1
InformaCast 11.5.2	11-1
InformaCast 11.5.1	11-2
InformaCast 11.0.5	11-3
InformaCast 11.0.2	11-5
InformaCast 11.0.1.a	11-6
InformaCast 11.0.1	11-6

InformaCast 9.1.1	11-8
InformaCast 9.0.2	11-9
InformaCast 9.0.1	11-10
InformaCast 8.5.1	11-12
InformaCast 8.4.a	11-12
InformaCast 8.3.a	11-14
InformaCast 8.3	11-15
Glossary	12-1
Index	13-1



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 <https://www.singlewire.com/help/InformaCastAPI/v11.5.1/index.html> 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, 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 1-3)
- 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 47, Chrome 52, 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 server (including Business Edition 6000); the following versions are supported: 9.0.1, 9.1.2, 10.0.1, 10.5.2, 11.0.1, and 11.5.1



Note If you are running Unified Communications Manager in mixed mode and you want calls to and from InformaCast to use encrypted media, you must configure SRTP support (see “Enable SIP Call Security” on page 5-36).

- Web access enabled on any Cisco IP phones working with InformaCast
- SNMP enabled on all servers in a Unified Communications Manager cluster
- The AXL service running on at least one server in the Unified Communications Manager 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 **Server Platforms** 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
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	Unified Communications Manager SNMP phone data
427	UDP and TCP	InformaCast SLP
443	TCP	Secure web interface for: <ul style="list-style-type: none"> webservices.singlewire.com Unified Communications Manager AXL web services
2748	TCP	Unified Communications Manager'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 subscribe to InformaCast Advanced Notification on an annual basis rather than purchasing perpetual licensing; 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)

Singlewire Start Page

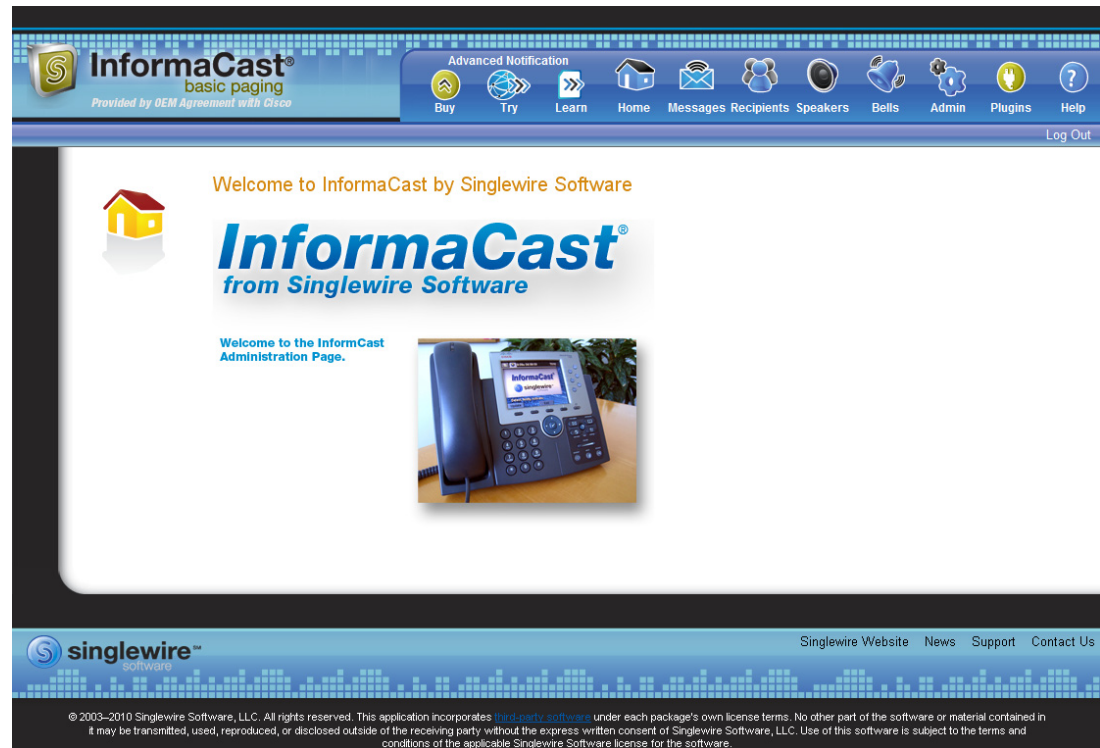
The Singlewire Start page is accessible through a web browser addressed with the IP address of your Virtual Appliance, and it contains links to InformaCast and the Control Center.



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.



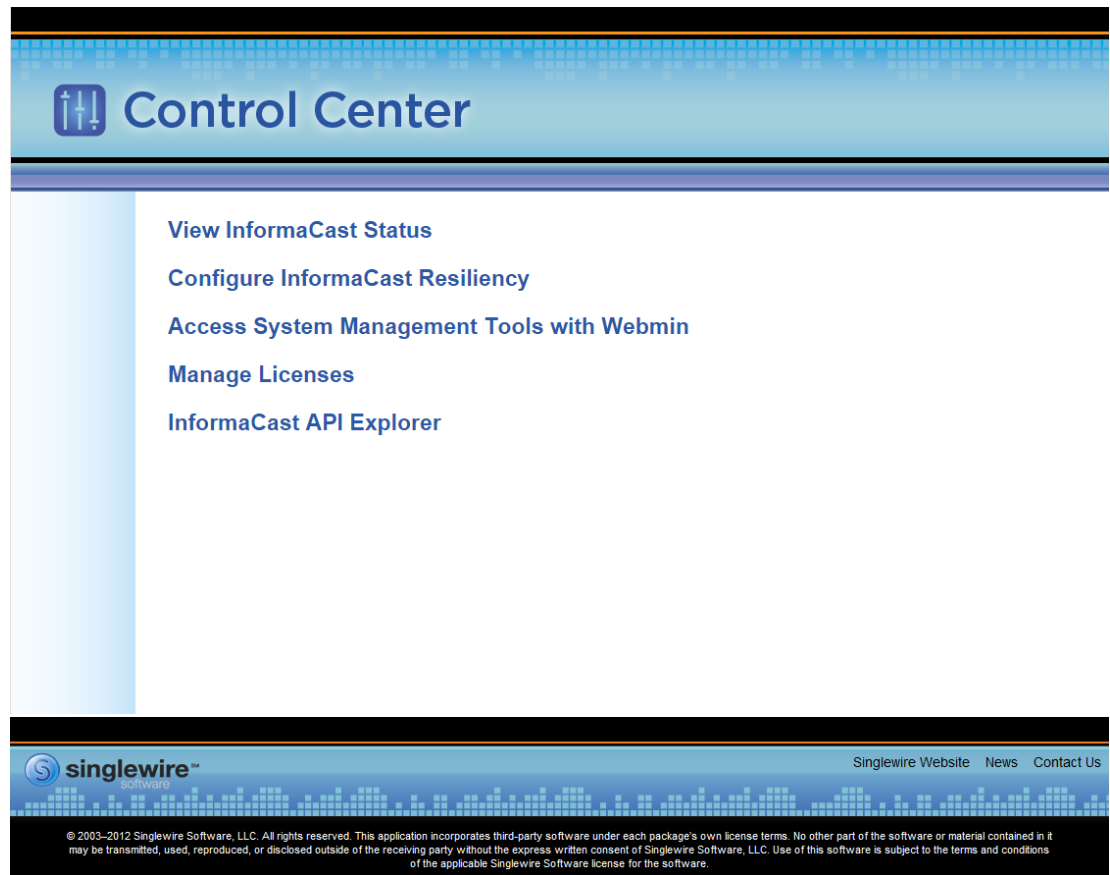
Note

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 10-25). 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

<https://www.singlewire.com/help/InformaCastAPI/v11.5.1/index.html> 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.

The screenshot displays the Singlewire Webmin interface. On the left, there is a navigation menu with options: System, Networking, Hardware, System Information (selected), and Logout. The main content area shows the Singlewire logo and a list of system statistics:

Virtual Appliance Version	###
System hostname	singlewire
Operating system	Debian Linux 5.0
Webmin version	1.530
Time on system	Thu Jun 16 15:48:10 2011
Kernel and CPU	Linux 2.6.30-voyage on i686
Processor information	Quad-Core AMD Opteron(tm) Processor 2382, 1 cores
System uptime	3 days, 7 hours, 57 minutes
Running processes	48
CPU load averages	0.00 (1 min) 0.00 (5 mins) 0.00 (15 mins)
CPU usage	0% user, 0% kernel, 0% IO, 100% idle
Real memory	2.97 GB total, 32.40 MB used
Virtual memory	3.73 GB total, 0 bytes used
Local disk space	75.07 GB total, 1.78 GB used

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.

```

Singlewire-InformaCast-VM
File View VM
singlewire login: admin
Password:
Last login: Mon Jun 20 15:53:30 CDT 2011 from 172.30.230.52 on pts/0
Linux singlewire 2.6.30-voyage #1 PREEMPT Mon Apr 26 02:16:20 GMT 2010 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

      _   _
     / \ / \
    / _ \_ / \
   / ___\/___\
  /_____/_____\

 { U o y a g e } - L i n u x
 < http://linux.voyage.hk >

Useful Commands:
remountm - mount disk as read-write
remountro - mount disk as read-only
remove.docs - remove all docs and manpages
Version: 0.7 (Build Date 20100603)

admin@singlewire:~$ _

```



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, call detail records, InformaCast's Performance, Summary, and SIP logs, and the log collection tool.

InformaCast®
basic paging
Provided by OEM Agreement with Cisco

Advanced Notification
Buy Try Learn Home Messages Recipients Speakers Bells Admin Plugins Help
Log Out

Help | Support

Your version of help is dependent on your version of Cisco Unified Communications Manager. InformaCast Basic Paging requires that your version of Cisco Unified Communications Manager be 9.0 or later.

If you have Unified Communications Manager 9.0 or later, you can contact Cisco directly for help: <http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html> or view InformaCast's installation and user guide.

If you have a version of Unified Communications Manager previous to 9.0, you have the following options:

- Click the **Try** icon to start your 60-day free trial of InformaCast Advanced Notification
- Click the **Buy** icon to obtain a demonstration, subscription, or purchased license for InformaCast Advanced Notification

Documentation

- [InformaCast User Guide](#)
- [Frequently Asked Questions](#)
- [Troubleshooting Guide](#)
- [API Documentation](#)
- [API Quick Start Guide](#)
- [End User License Agreement](#)

Tools

These links help carry out steps mentioned in the documentation, or suggested by technical support.

- [API Log](#) Shows requests made to the InformaCast REST API.
- [Calling Terminal Diagnostics](#) Shows the CTI ports and route points registered with InformaCast.
- [Call Detail Records Directory](#) Shows the directory containing the call detail records.
- [InformaCast Logs Directory](#) Shows the directory containing the InformaCast logs.
- [Log Tool](#) Collects and analyzes Singlewire log files for errors.
- [Performance Log](#) Contains information logged by InformaCast.
- [SIP Stack Log](#) Contains information logged by the SIP stack.
- [Summary Log](#) Contains a summary of broadcasts sent by InformaCast.

singlewire® software

Singlewire Website News Support Contact Us

© 2003–2016 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software.

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 Unified Communications Manager.

The general steps to install InformaCast are:

- “Prepare Your Multicast Environment” on page 2-1
- “Install InformaCast Virtual Appliance” on page 2-6
- “Log into InformaCast Virtual Appliance’s Interfaces” on page 2-21
- “Update JTAPI” on page 2-30
- “Set the System Time” on page 2-35
- “Create and Install a Signed Certificate” on page 2-38
- “Integrate Unified Communications Manager” on page 2-45
- “Manage Installation Administration” on page 2-88

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)
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 www.singlewire.com/tools/multicast-testing-tool.

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.

```

Administrator: Singlewire Software: IC Tester - Multicast
Singlewire Software

[1] Multicast Server (transmit packets)
[2] Multicast Client (receive packets)
[3] Two Phone Send & Receive
[9] Exit

Menu Choice-> _
  
```

- 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.

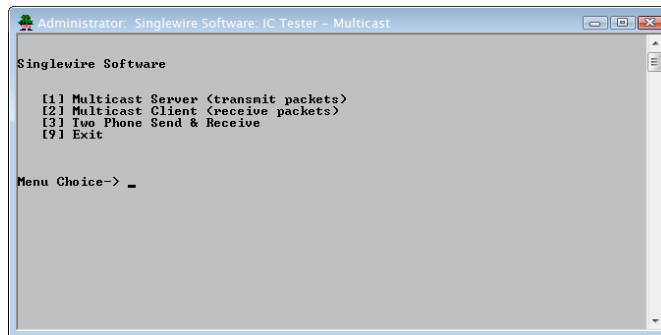
```

Administrator: Singlewire Software: IC Tester - Multicast - Server
Singlewire Software

[1] Multicast Server (transmit packets)
[2] Multicast Client (receive packets)
[3] Two Phone Send & Receive
[9] Exit

Menu Choice-> 1
Singlewire Software Packet 0    239.0.1.2:20400  TTL: 16
Singlewire Software Packet 1    239.0.1.2:20400  TTL: 16
Singlewire Software Packet 2    239.0.1.2:20400  TTL: 16
Singlewire Software Packet 3    239.0.1.2:20400  TTL: 16
  
```

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



```

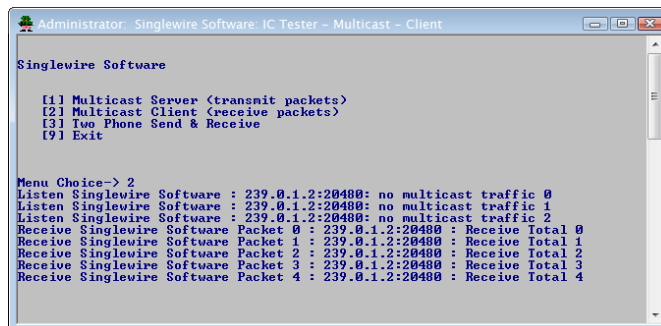
Administrator: Singlewire Software: IC Tester - Multicast

Singlewire Software

[1] Multicast Server <transmit packets>
[2] Multicast Client <receive packets>
[3] Two Phone Send & Receive
[9] Exit

Menu Choice-> _
  
```

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.



```

Administrator: Singlewire Software: IC Tester - Multicast - Client

Singlewire Software

[1] Multicast Server <transmit packets>
[2] Multicast Client <receive packets>
[3] Two Phone Send & Receive
[9] Exit

Menu Choice-> 2
Listen Singlewire Software : 239.0.1.2:20480: no multicast traffic 0
Listen Singlewire Software : 239.0.1.2:20480: no multicast traffic 1
Listen Singlewire Software : 239.0.1.2:20480: no multicast traffic 2
Receive Singlewire Software Packet 0 : 239.0.1.2:20480 : Receive Total 0
Receive Singlewire Software Packet 1 : 239.0.1.2:20480 : Receive Total 1
Receive Singlewire Software Packet 2 : 239.0.1.2:20480 : Receive Total 2
Receive Singlewire Software Packet 3 : 239.0.1.2:20480 : Receive Total 3
Receive Singlewire Software Packet 4 : 239.0.1.2:20480 : Receive Total 4
  
```

If you receive a “no multicast traffic” result, you can try Option 3, follow the recommendations in “Review Multicast Configuration” on page 2-88, or see “Multicast” on page 9-1.

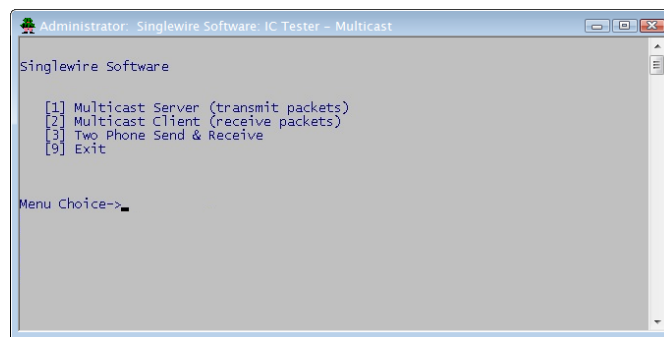
Use Option 3

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 Unified Communications Manager 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.

```
Administrator: Singlewire Software: IC Tester - Multicast
Singlewire Software

[1] Multicast Server (transmit packets)
[2] Multicast Client (receive packets)
[3] Two Phone Send & Receive
[9] Exit

Menu Choice-> 3
User Name.....: p1
User Password.....: p1
Phone IP of Sender...: 172.30.236.230
Phone IP of Receiver.: 172.30.236.233
HTTP/1.1 200 OK
Cache-Control: no-cache
Date: Wed, 12 Jan 2011 16:34:34 GMT
Server: Allegro-Software-RomPager/4.34
Content-Length: 162
Content-Type: text/xml; charset="utf-8"
Expires: Thu, 26 Oct 1995 00:00:00 GMT
Client-Date: Wed, 12 Jan 2011 16:34:38 GMT
Client-Peer: 172.30.236.230:80
Client-Response-Num: 1

<?xml version="1.0" encoding="utf-8"?>
<CiscoIPPhoneResponse>
<ResponseItem URL="RTPMTx:239.0.1.2:20480" Data="Success" Status="0" />
</CiscoIPPhoneResponse>
HTTP/1.1 303 See Other
Location: http://172.30.236.233/FS/PUSH_RESP_6_4
Server: Allegro-Software-RomPager/3.12
Content-Length: 0
Client-Date: Wed, 12 Jan 2011 16:34:52 GMT
Client-Peer: 172.30.236.233:80
Client-Response-Num: 1

Press Enter to Stop Two Phone Test_
```

- 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 2-88 or see "Multicast" on page 9-1.

Install InformaCast Virtual Appliance

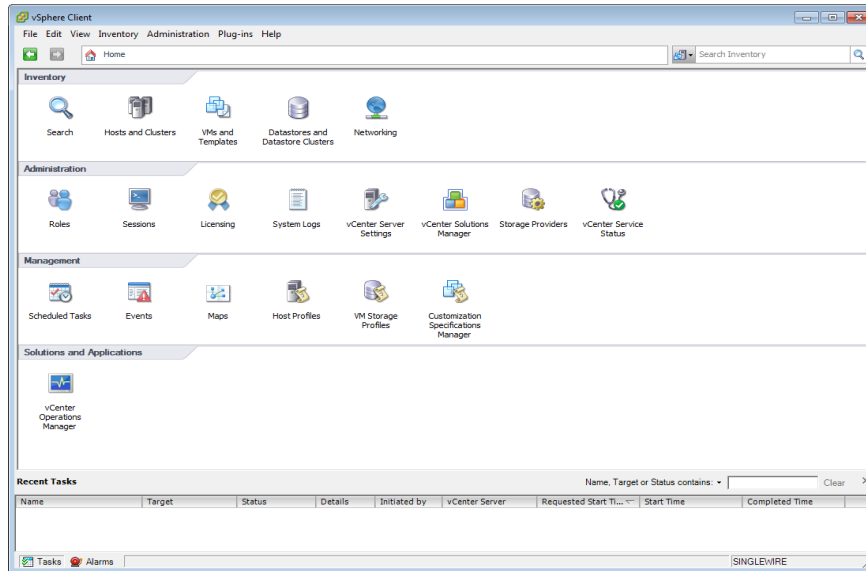
Singlewire supports InformaCast Virtual Appliance on the VMware ESXi platform, which is managed through the vSphere client. This section describes how to import InformaCast Virtual Appliance using the vSphere client. Your client can be downloaded from your VMware server.

- Step 1** Download the OVA file from [Cisco's website](#).

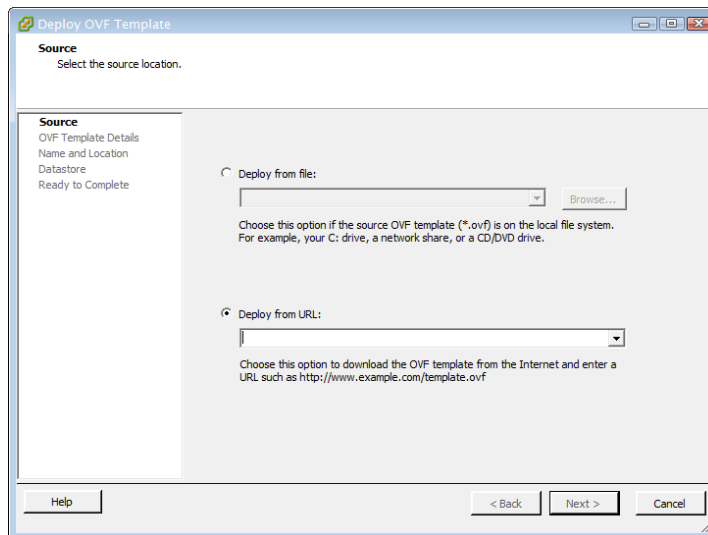


Note If you are using InformaCast on the Unified Communications Manager Business Edition 6000, you will be supplied with a DVD in a package with an OVA on it (physical media).

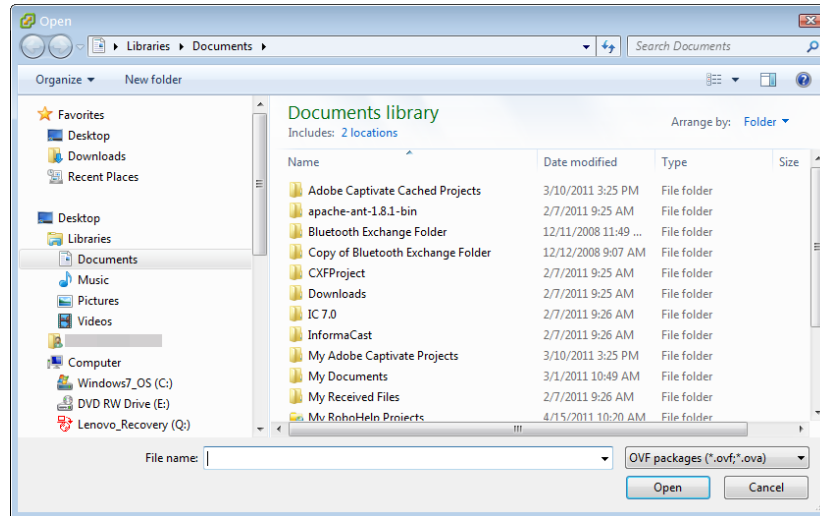
Step 2 Open and log into the vSphere client. The vSphere Client window appears.



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

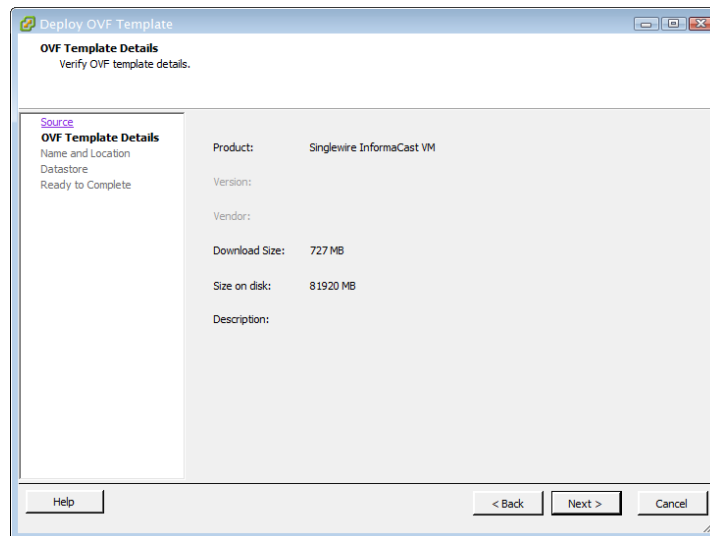


Step 4 Click the **Deploy from File** radio button and click its **Browse** button. The Open dialog box appears.

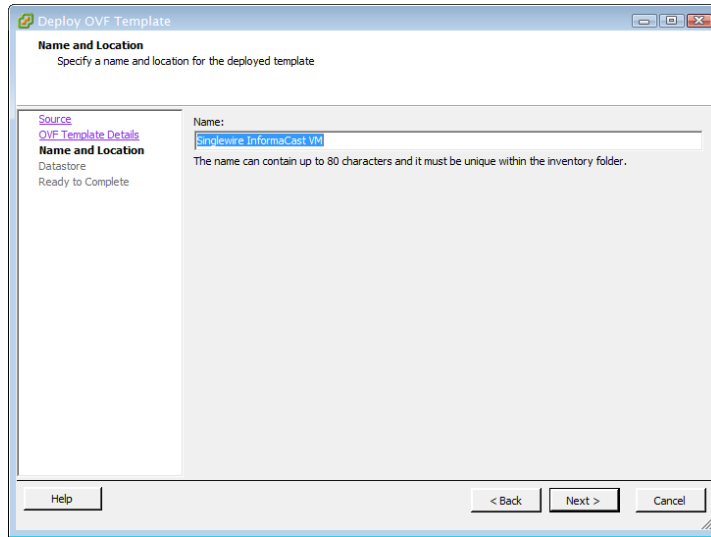


Step 5 Navigate to where you saved the OVA file (or to the OVA file on the supplied DVD), select it, and click the **Open** button.

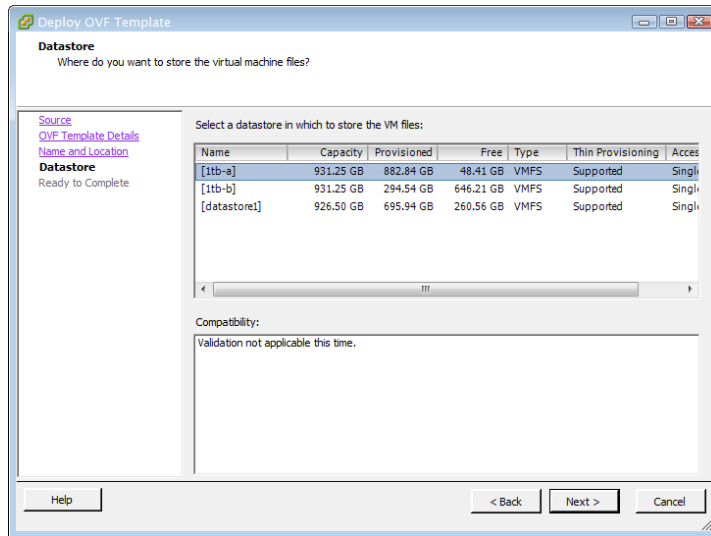
Step 6 Click the **Next** button. The Deploy OVF Template dialog box refreshes.



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.

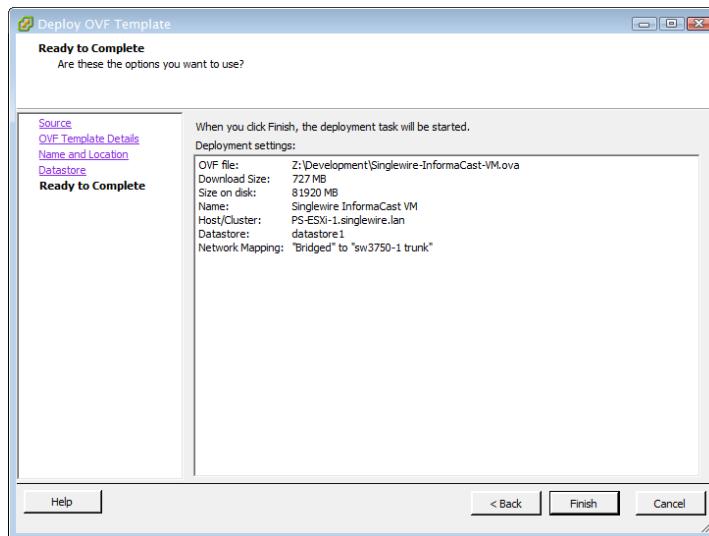


Step 9 Select the network on which the new virtual machine will reside and click the **Next** button.

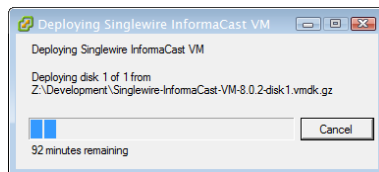


Tip It is good practice to place the Virtual Appliance on the same VLAN as your Unified Communications Manager.

The Deploy OVF template dialog box refreshes.

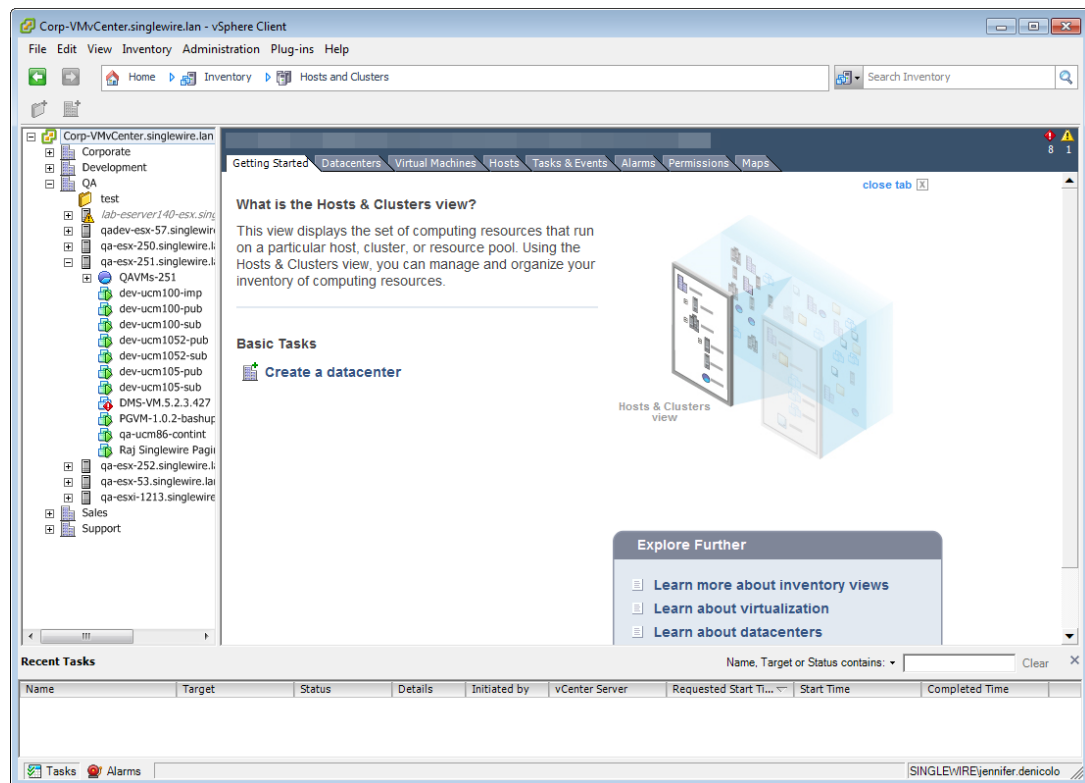


Step 10 Click the **Finish** button. InformaCast Virtual Appliance will begin importing.

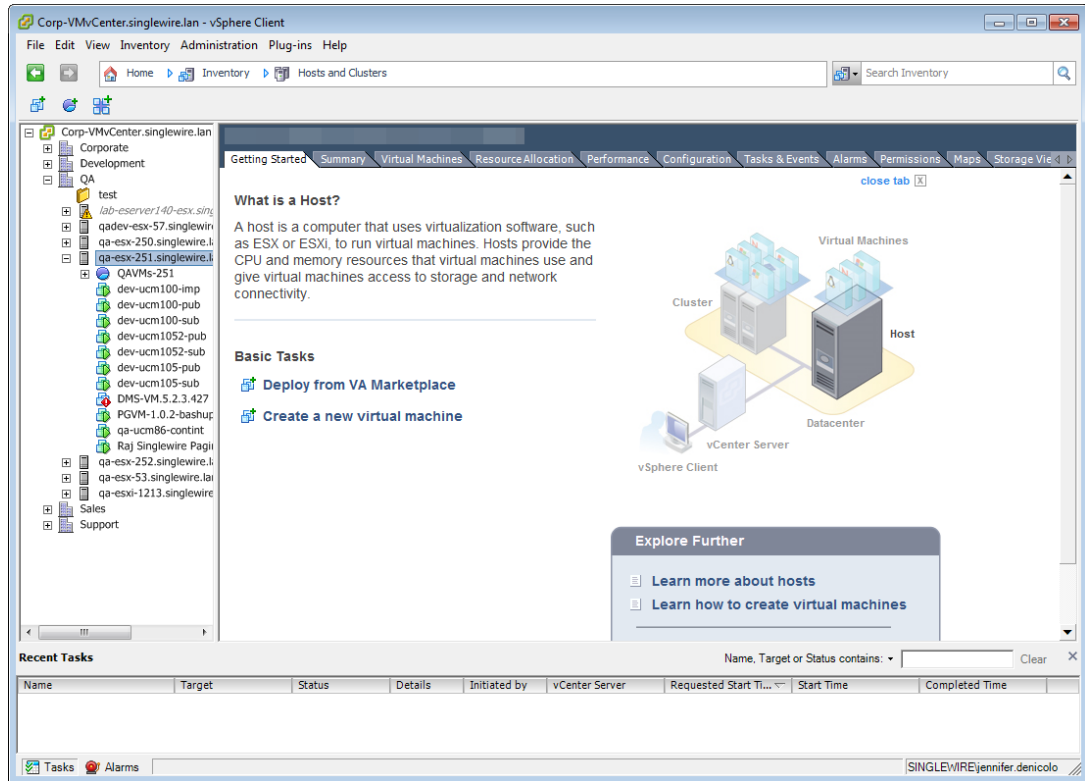


When it's finished, click the **Close** button.

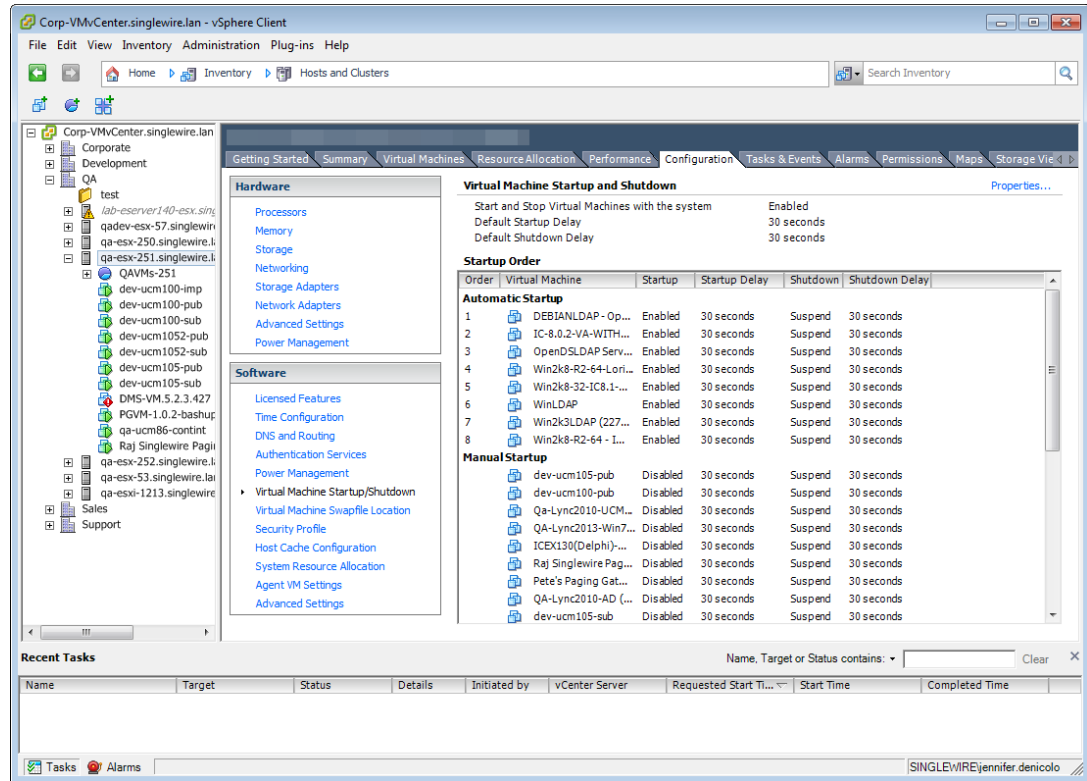
Step 11 Go back to your vSphere Client window and click the **Hosts and Clusters** icon (🏠). The vSphere Client window refreshes.



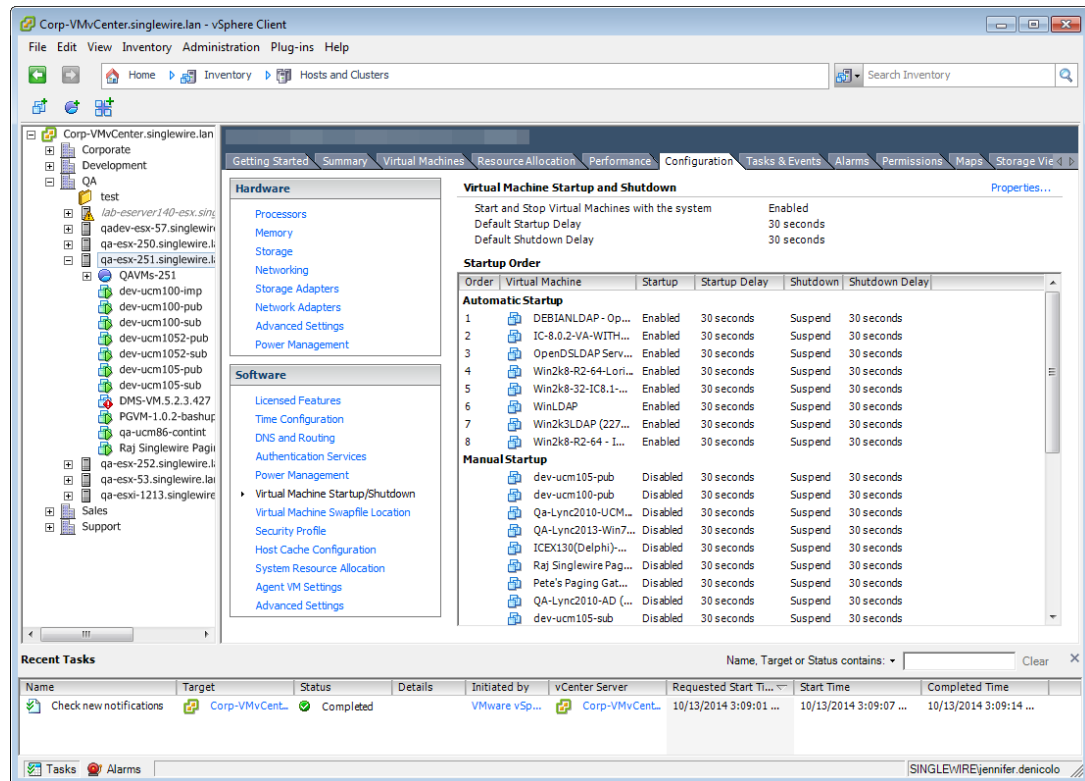
Step 12 Select your host server. The vSphere Client window refreshes.



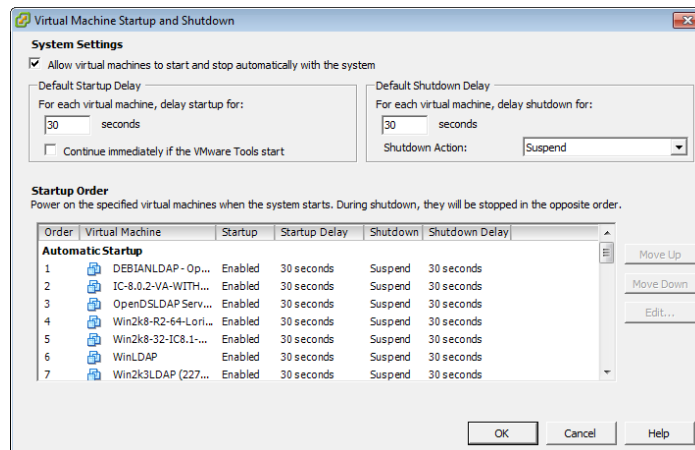
Step 13 Click the **Configuration** tab. The vSphere Client window refreshes.



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

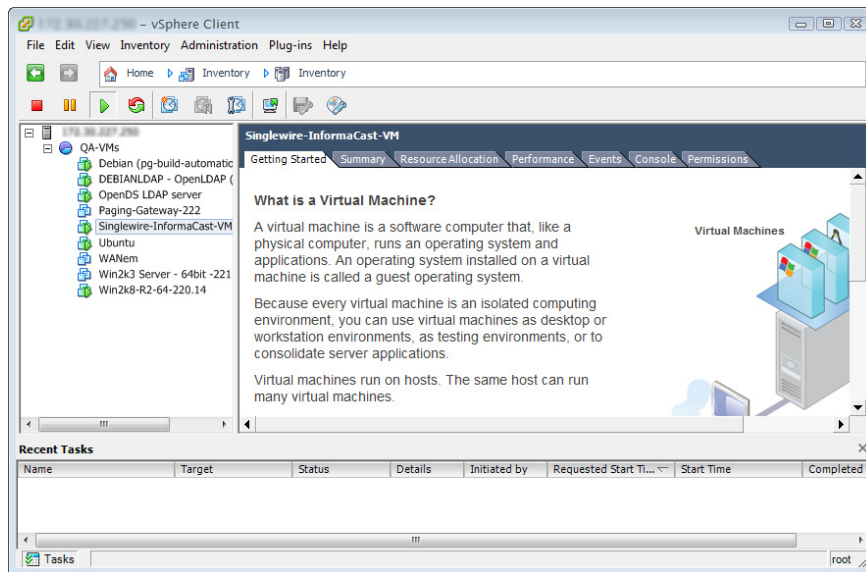


Step 15 Click the **Properties** link in the upper right corner. The Virtual Machine Startup and Shutdown dialog box appears.

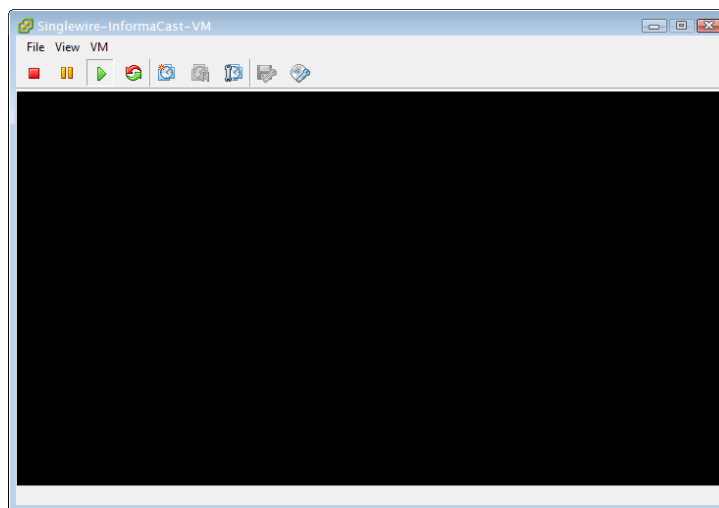



Step 16 Select the **Allow virtual machines to start and stop automatically with the system** checkbox in the *System Settings* area.

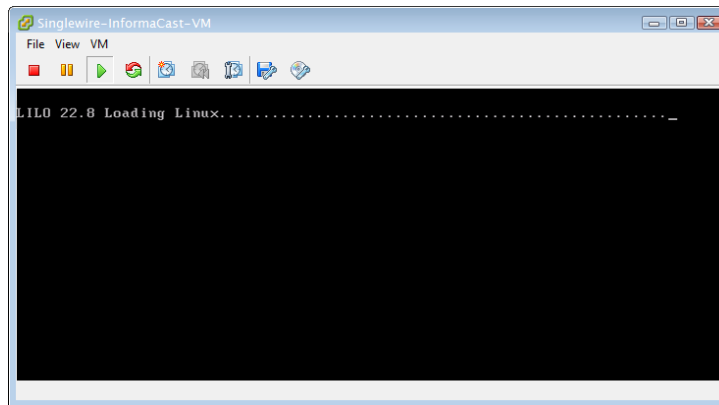
- Step 17** Scroll to the **Manual Startup** section of the **Startup Order** field, select your virtual machine (by default, this is Singlewire InformaCast VM), and move it from the **Manual Startup** section to the **Automatic Startup** section using the **Move Up** button.
- Step 18** Click the **OK** 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.

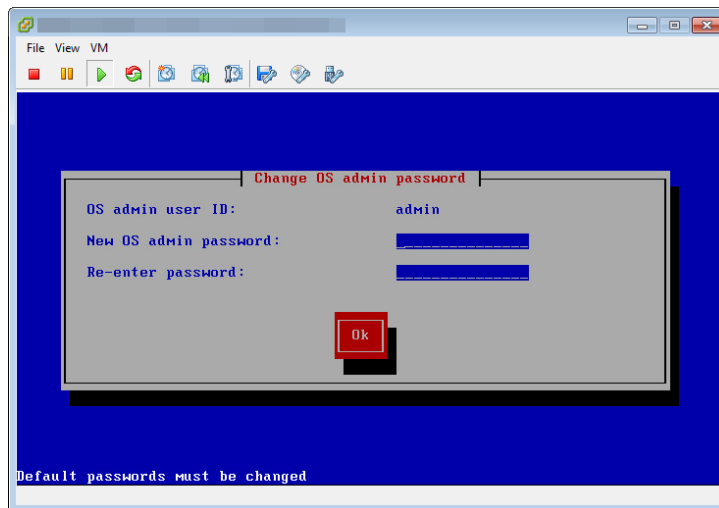


Step 22 Click the green arrow button () to turn on the virtual machine. The Singlewire InformaCast VM console window begins booting the virtual machine.



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, you will be prompted to change the OS Administrator's password.

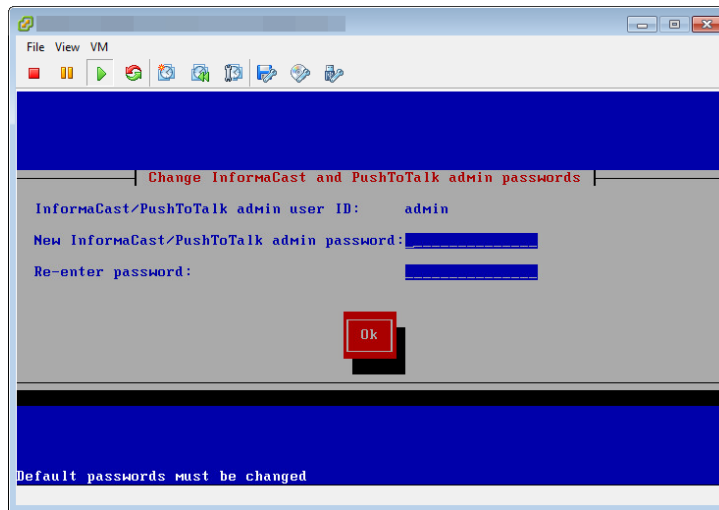


Step 23 Enter a new password in the **New OS admin password** field, press the **Tab** key, and enter the password again in the **Re-enter password** field. Your OS credentials are used to enter Webmin and Control Center and when using SSH to access the Virtual Appliance.



Note When setting your password, you cannot use "changeMe."

Step 24 Press the **Enter** key three times to advance to the next screen in the console window where you will be prompted to change the Application Administrator's password.



Step 25 Enter a new password in the **New InformaCast/PushToTalk admin password** field, press the **Tab** key, and enter the password again in the **Re-enter password** field. Your application credentials are used to enter InformaCast and PushToTalk.



Note When setting your password, you cannot use “changeMe.”



Note PushToTalk is only available for Advanced InformaCast users.

- Step 26** Press the **Enter** key three times. The Virtual Appliance will finish its boot process. SwiftStart will then start automatically, and you will see the End User License Agreement (EULA) page.



SwiftStart

End User License Agreement

I AGREE ✓

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. IT IS VERY IMPORTANT THAT YOU CHECK THAT YOU ARE PURCHASING CISCO SOFTWARE OR EQUIPMENT FROM AN APPROVED SOURCE AND THAT YOU, OR THE ENTITY YOU REPRESENT (COLLECTIVELY, THE "CUSTOMER") HAVE BEEN REGISTERED AS THE END USER FOR THE PURPOSES OF THIS CISCO END USER LICENSE AGREEMENT. IF YOU ARE NOT REGISTERED AS THE END USER YOU HAVE NO LICENSE TO USE THE SOFTWARE AND THE LIMITED WARRANTY IN THIS END USER LICENSE AGREEMENT DOES NOT APPLY. ASSUMING YOU HAVE PURCHASED FROM AN APPROVED SOURCE, DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

....

For all countries referred to above, the parties specifically disclaim the application of the UN Convention on Contracts for the International Sale of Goods. Notwithstanding the foregoing, either party may seek interim injunctive relief in any court of appropriate jurisdiction with respect to any alleged breach of such party's intellectual property or proprietary rights. If any portion hereof is found to be void or unenforceable, the remaining provisions of the Agreement and Warranties shall remain in full force and effect. Except as expressly provided herein, the Agreement constitutes the entire agreement between the parties with respect to the license of the Software and Documentation and supersedes any conflicting or additional terms contained in any Purchase Order or elsewhere, all of which terms are excluded. The Agreement has been written in the English language, and the parties agree that the English version will govern.

Product warranty terms and other information applicable to Cisco products are available at the following URL: <http://www.cisco.com/go/warranty>

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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.

All Rights Reserved © 2012 Singlewire Software




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

- Step 27** 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 28 Determine if you will use DHCP or manual entry to set the static IP address of InformaCast:

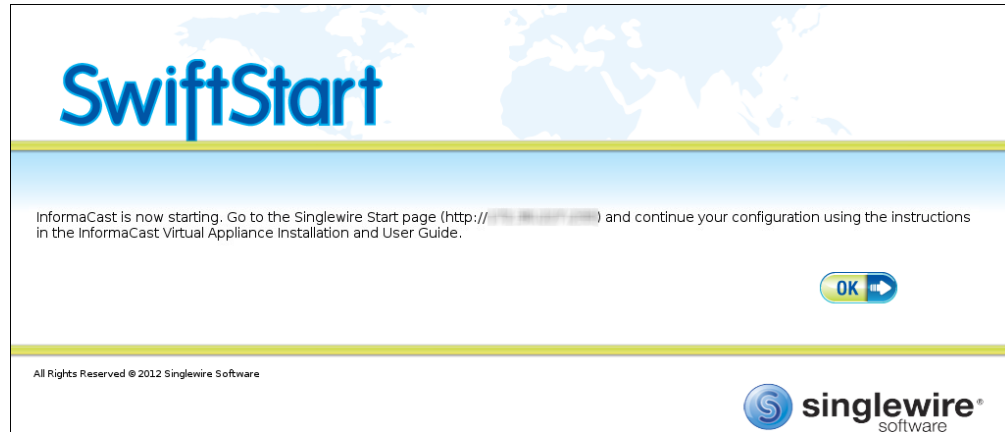
- Selecting the **Use DHCP Parameters** radio button will allow SwiftStart to make static the IP address it has detected, pull the relevant network configuration information from this IP address, and configure your network to work with InformaCast.
- Selecting the **Enter Manually** radio button will 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 29 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 30 Click the **Finish** button. The SwiftStart window appears with a note about starting InformaCast.



Step 31 Click the **OK** button and close your open console window.

Log into InformaCast Virtual Appliance's Interfaces

When using InformaCast Virtual Appliance, you will access it and log into 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.

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 28 on page 2-20), and press the **Enter** key. The Singlewire Start page appears.



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.



Note

When you access the Virtual Appliance (or any of its interfaces), you may receive a warning from your web browser about the safety of the website you are about to visit. This is normal. InformaCast Virtual Appliance 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 a signed certificate (see “Create and Install a Signed Certificate” on page 2-38).

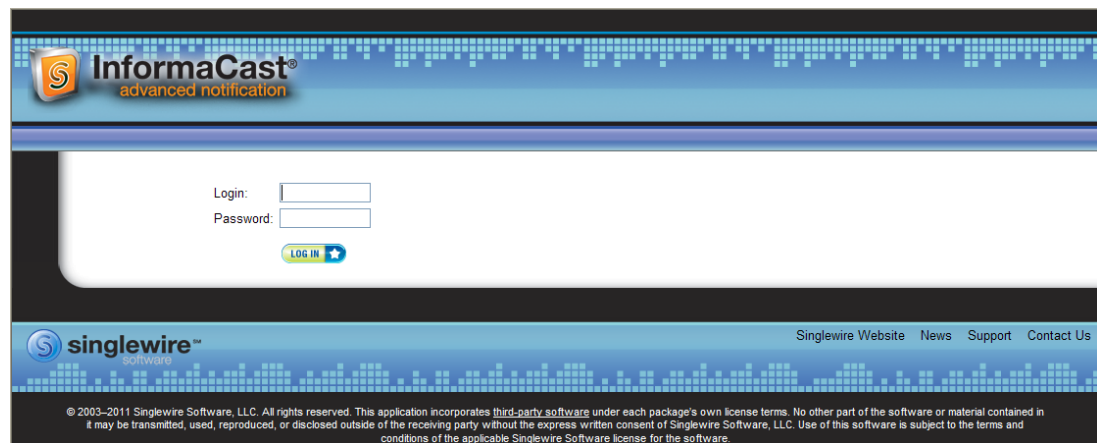
Log into InformaCast

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.

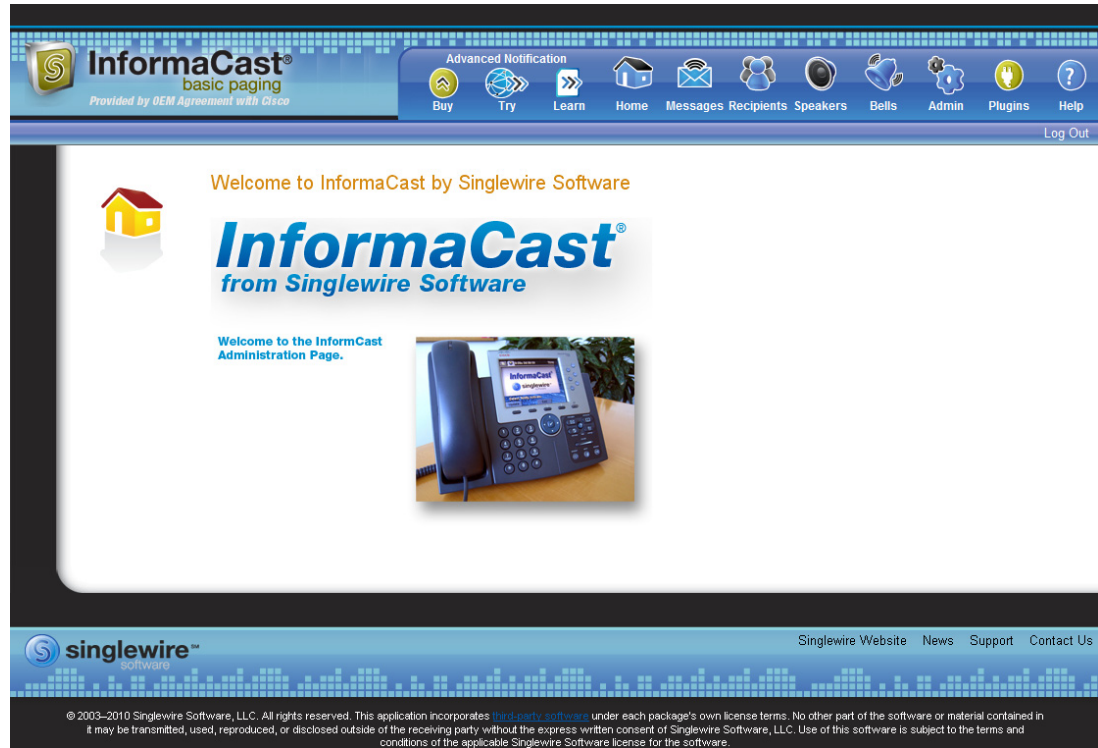


- Step 2** Click the **InformaCast** link. A separate tab/window opens to InformaCast's Login page.



- Step 3** Enter your application credentials in the **Login** and **Password** fields.

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.

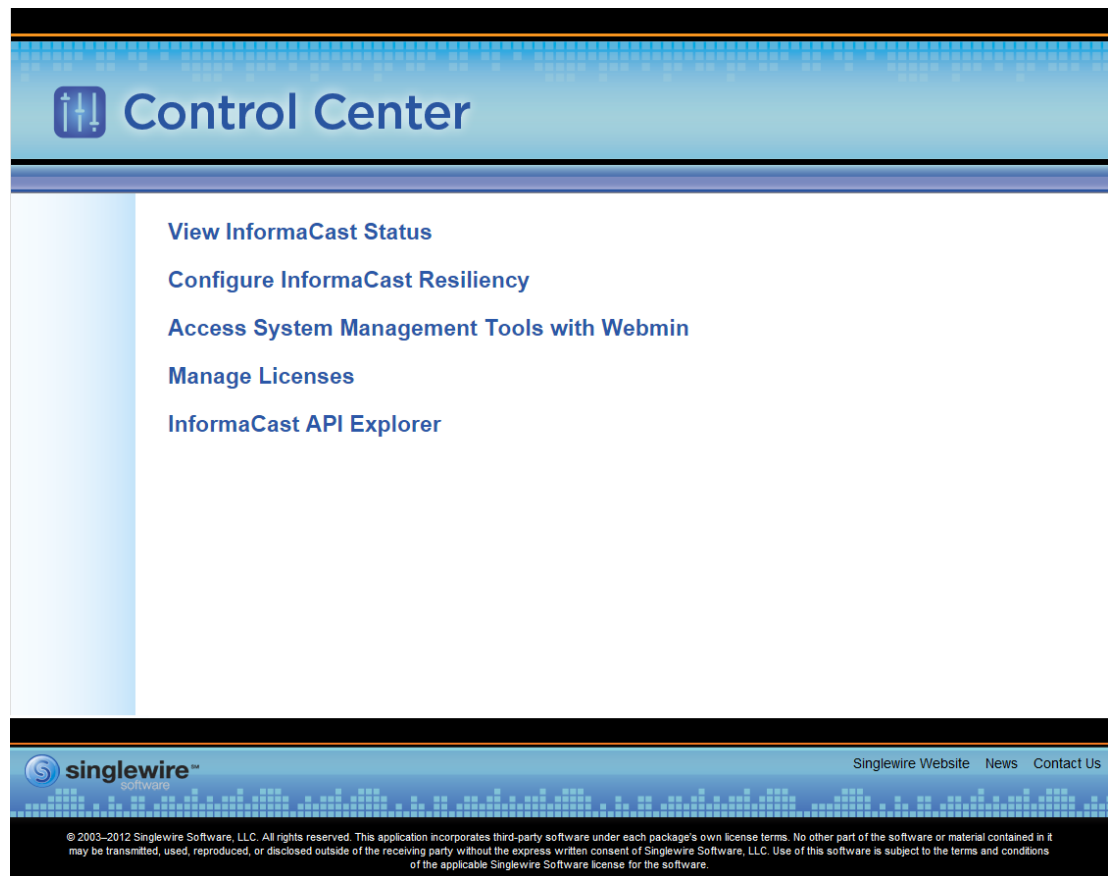
Log into the Control Center

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.

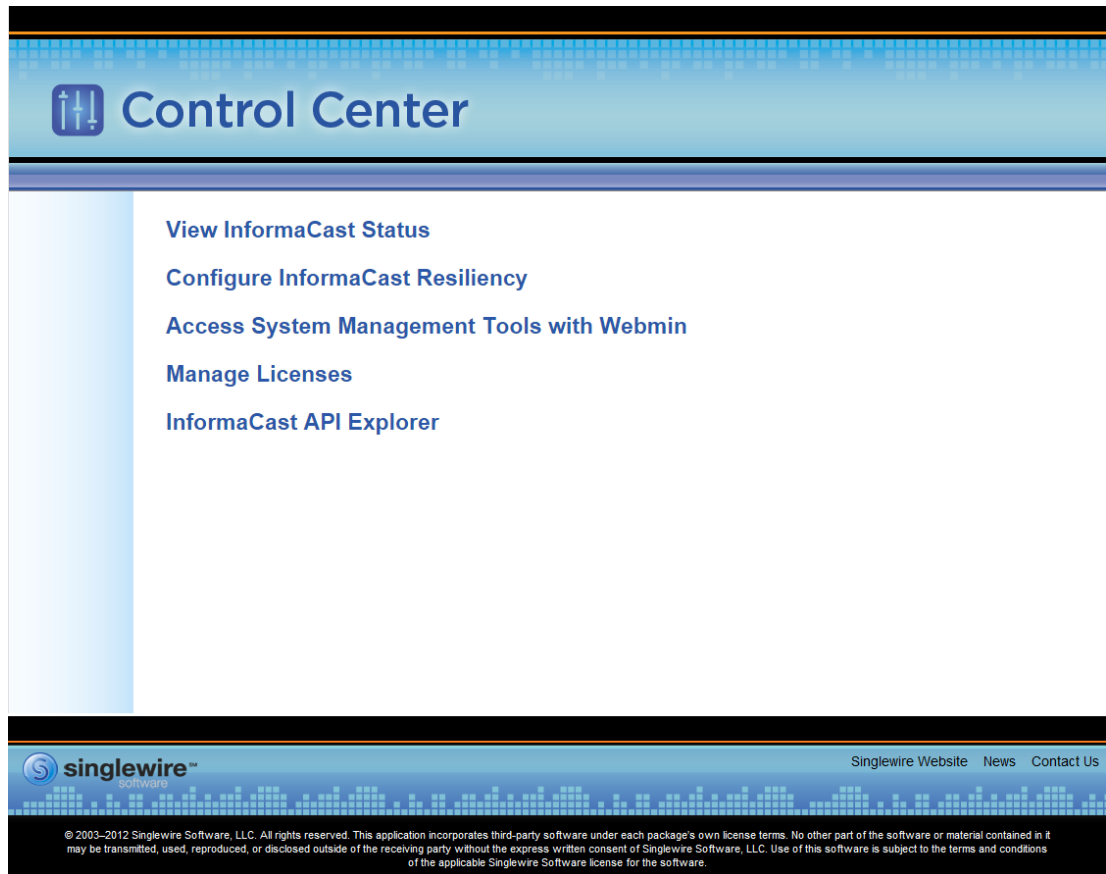
Log into Webmin

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.

The screenshot shows the "Login to Webmin" page. It has a blue header with the text "Login to Webmin". Below the header, there is a message: "You must enter a username and password to login to the Webmin server on [hostname]". There are two input fields: "Username" and "Password". Below the input fields, there is a checkbox labeled "Remember login permanently?". At the bottom, there are two buttons: "Login" and "Clear".**Note**

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

Step 4 Enter your OS credentials and click the **Login** button. The Webmin homepage appears.

The screenshot shows the Webmin homepage for a Singlewire virtual appliance. The page features a navigation menu on the left with options like System, Networking, Hardware, System Information, and Logout. The main content area displays system information and statistics, including system hostname, operating system, Webmin version, time on system, kernel and CPU, processor information, system uptime, running processes, CPU load averages, CPU usage, real memory, virtual memory, and local disk space. The Singlewire logo is prominently displayed at the top right.

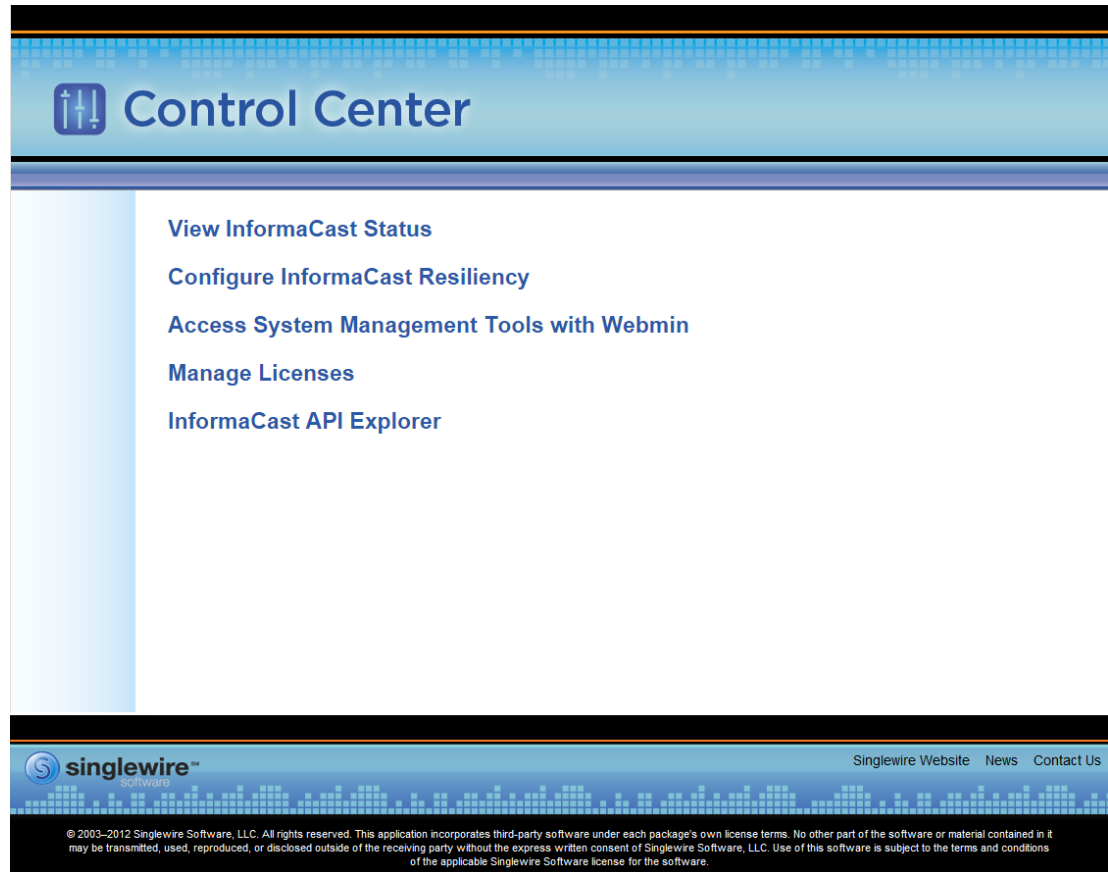
Virtual Appliance Version	###
System hostname	singlewire
Operating system	Debian Linux 5.0
Webmin version	1.530
Time on system	Thu Jun 16 15:48:10 2011
Kernel and CPU	Linux 2.6.30-voyage on i686
Processor information	Quad-Core AMD Opteron(tm) Processor 2382, 1 cores
System uptime	3 days, 7 hours, 57 minutes
Running processes	48
CPU load averages	0.00 (1 min) 0.00 (5 mins) 0.00 (15 mins)
CPU usage	0% user, 0% kernel, 0% IO, 100% idle
Real memory	2.97 GB total, 32.40 MB used
Virtual memory	3.73 GB total, 0 bytes used
Local disk space	75.07 GB total, 1.78 GB used

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 10-16), 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 10-1 for more information).

Update JTAPI

When you initially install InformaCast Virtual Appliance or whenever you change versions of Unified Communications Manager, you need to update the JTAPI library used by InformaCast Virtual Appliance to the same version used by your Unified Communications Manager 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. The Webmin homepage appears.

The screenshot shows the Singlewire Webmin interface. On the left is a navigation menu with 'System Information' selected. The main content area displays system details:

Virtual Appliance Version	###
System hostname	singlewire
Operating system	Debian Linux 5.0
Webmin version	1.530
Time on system	Thu Jun 16 15:48:10 2011
Kernel and CPU	Linux 2.6.30-voyage on i686
Processor information	Quad-Core AMD Opteron(tm) Processor 2382, 1 cores
System uptime	3 days, 7 hours, 57 minutes
Running processes	48
CPU load averages	0.00 (1 min) 0.00 (5 mins) 0.00 (15 mins)
CPU usage	0% user, 0% kernel, 0% IO, 100% idle
Real memory	2.97 GB total, 32.40 MB used
Virtual memory	3.73 GB total, 0 bytes used
Local disk space	75.07 GB total, 1.78 GB used

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

The screenshot shows the 'Bootup and Shutdown' configuration page in Webmin. The left sidebar has 'System Time' selected. The main area contains a table of system services with checkboxes to enable or disable them at boot.

Action	At boot?	Description
<input type="checkbox"/> alsa-utils	No	This script stores and restores mixer levels on
<input type="checkbox"/> asterisk	No	Controls the Asterisk PBX
<input type="checkbox"/> atftpd	No	Launch atftpd server, a TFTP server useful
<input type="checkbox"/> awds	No	This script is used to start the AWDS daemon which provides
<input type="checkbox"/> batmand	No	/etc/init.d/batmand: start batmand
<input type="checkbox"/> bootlogd	No	Starts or stops the bootlogd log program
<input type="checkbox"/> bootmisc.sh	No	Some cleanup. Note, it need to run after mountnfs-bootclean.sh.
<input type="checkbox"/> checkfs.sh	No	Check all filesystems.
<input type="checkbox"/> checkroot.sh	No	Check to root file system.
<input type="checkbox"/> cron	Yes	cron is a standard UNIX program that runs user-specified
<input type="checkbox"/> dahdi	No	dahdi - load and configure DAHDI modules
<input type="checkbox"/> dnsmasq	No	DHCP and DNS server
<input type="checkbox"/> ebttables	No	Saves and restores the state of the ebttables rulesets.
<input type="checkbox"/> flashybrid	No	Flashybrid is a system to help in setting up and managing hybrid
<input type="checkbox"/> glibc.sh	No	
<input type="checkbox"/> gpsd	No	Start the GPS (Global Positioning System) daemon
<input type="checkbox"/> halt	No	
<input type="checkbox"/> hostapd	No	Userspace IEEE 802.11 AP and IEEE 802.1X/WPA/WPA2/EAP
<input type="checkbox"/> flashybrid	No	Flashybrid is a system to help in setting up and managing hybrid
<input type="checkbox"/> glibc.sh	No	
<input type="checkbox"/> gpsd	No	Start the GPS (Global Positioning System) daemon
<input type="checkbox"/> halt	No	
<input type="checkbox"/> single	No	executed by init(8) upon entering runlevel 1 (single).
<input type="checkbox"/> singlewireInformaCast	No	InformaCast application from Singlewire

Below the table are buttons for 'Start', 'Stop', 'Restart', 'Start On Boot', 'Disable On Boot', 'Start Now and On Boot', and 'Disable Now and On Boot'. At the bottom, there are controls for 'Change to runlevel:' (set to 2), 'Reboot System', and 'Shutdown System', each with a descriptive tooltip.

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

The screenshot shows the 'Edit Action' page for 'singlewireInformaCast'. The left sidebar contains a navigation menu with categories like System, Bootup and Shutdown, Change Passwords, Scheduled Cron Jobs, Software Packages, Networking, Hardware, System Information, and Logout. The main content area is titled 'Edit Action' and includes a 'Module Index' link. Below this is the 'Action Details' section, which contains a text area for the 'Action Script'. The script is as follows:

```
#!/bin/sh
### BEGIN INIT INFO
# Short-Description: InformaCast
# Description: InformaCast application from Singlewire
### END INIT INFO

# Author: [REDACTED]
#

# Do NOT "set -e"

# PATH should only include /usr/* if it runs after the mountnfs.sh script
PATH=/sbin:/usr/sbin:/bin:/usr/bin
DESC="InformaCast"
NAME=singlewireInformaCast
```

Below the script is a 'Start at boot time?' section with radio buttons for 'Yes' and 'No' (selected). At the bottom are buttons for 'Save', 'Start Now', 'Show Status', 'Stop Now', and 'Delete'. A link 'Return to bootup and shutdown actions' is also present.

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

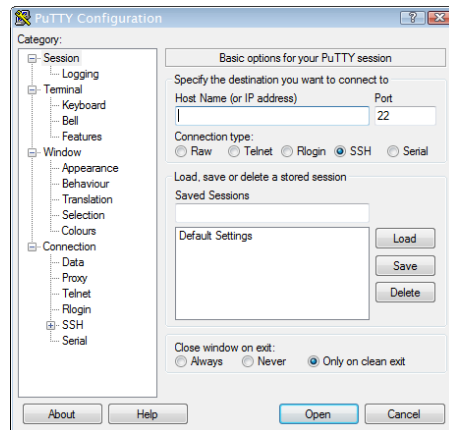
The screenshot shows the 'Stop Action' page. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Stop Action' and shows the status 'Executing /etc/init.d/singlewireInformaCast stop ..'.



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.

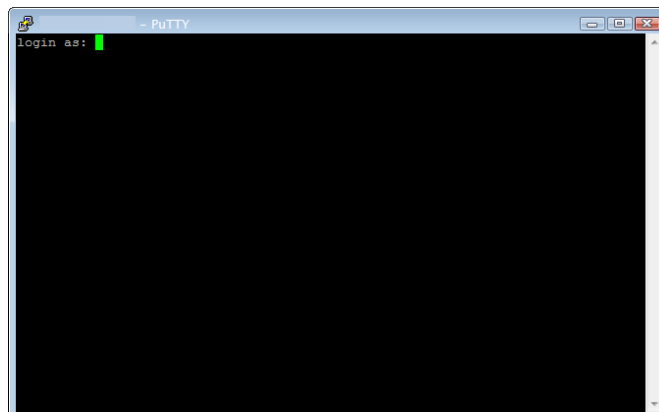


Step 9 Enter InformaCast's IP address in the **Host Name (or IP address)** field.

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.

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.

Control Center

- [View InformaCast Status](#)
- [Configure InformaCast Resiliency](#)
- [Access System Management Tools with Webmin](#)
- [Manage Licenses](#)
- [InformaCast API Explorer](#)

singlewire™
software

Singlewire Website News Contact Us

© 2003–2012 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software.

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. 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.

The screenshot shows the 'System Time' configuration page with the 'Time server sync' tab selected. The page includes a navigation menu on the left with 'System Time' highlighted. The main content area has tabs for 'Set time', 'Change timezone', and 'Time server sync'. Below the tabs is a text input field for 'Timeserver hostnames or addresses' containing 'pool.ntp.org'. There is a checked checkbox for 'Set hardware time too' and a radio button for 'Synchronize on schedule?' set to 'Yes, at times below...'. Below this are five columns of radio buttons for 'Minutes', 'Hours', 'Days', 'Months', and 'Weekdays', each with a grid of options. A 'Sync and Apply' button is at the bottom.

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.

The screenshot shows the 'System Time' configuration page with the 'Change timezone' tab selected. The page includes the same navigation menu. The main content area has tabs for 'Set time', 'Change timezone', and 'Time server sync'. Below the tabs is a text input field for 'Change timezone to' containing 'America/Chicago (Central Time)'. A 'Save' button is at the bottom.

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.

Create and Install a Signed Certificate


Note

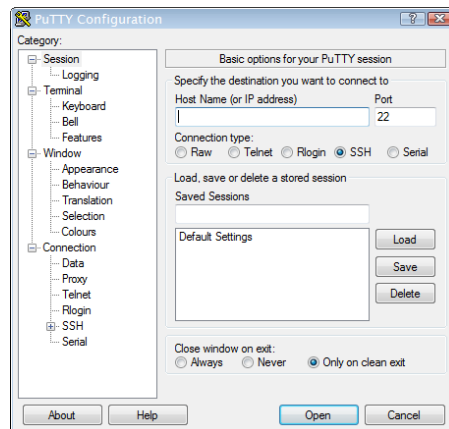
This section is optional.

Whenever you access of the Virtual Appliance's interfaces (e.g. the Singlewire Start page, InformaCast's homepage, Webmin, etc.), your browser warns you of a problem with the website's certificate. You know InformaCast is a trusted resource, but your web browser does not.

By installing a signed certificate, you can avoid this warning and protect yourself against Man-in-the-Middle (MITM) attacks, where a malicious entity can insert itself between you and the Virtual Appliance, impersonating one and manipulating your communication. A signed certificate is an electronic document that proves ownership of a public key; it includes information about the key, its owner's identity, and the digital signature of a certificate authority (CA).

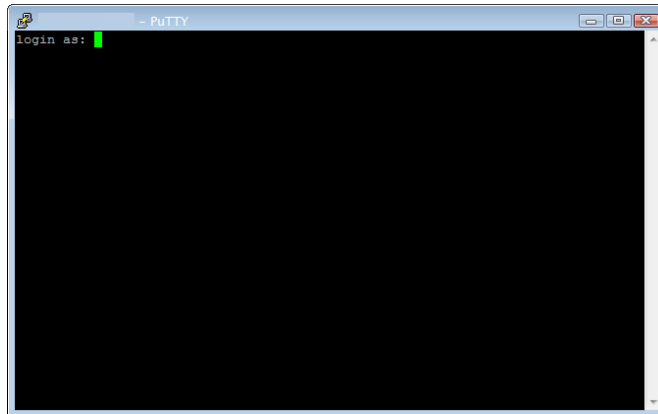
SSLMGR is a command contained within the Virtual Appliance that allows you to regenerate a public key and certificate, produce a certificate-signing request, and import a certificate signed by your CA.

- Step 1** Use an SSH client to access InformaCast's command line interface (Singlewire recommends PuTTY: <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>).
- Step 2** Open PuTTY. The PuTTY Configuration window appears.



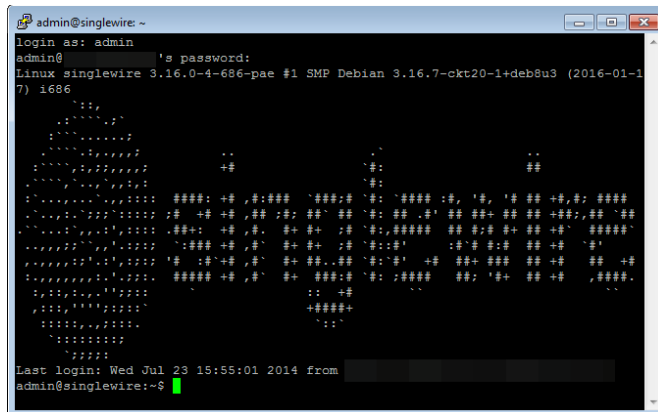
- Step 3** Enter the Virtual Appliance's IP address in the **Host Name (or IP address)** field.
- Step 4** Leave the **Port** field at its default of 22.
- Step 5** Click the **SSH** radio button.

Step 6 Click the **Open** button. The command-line interface for the Virtual Appliance appears.

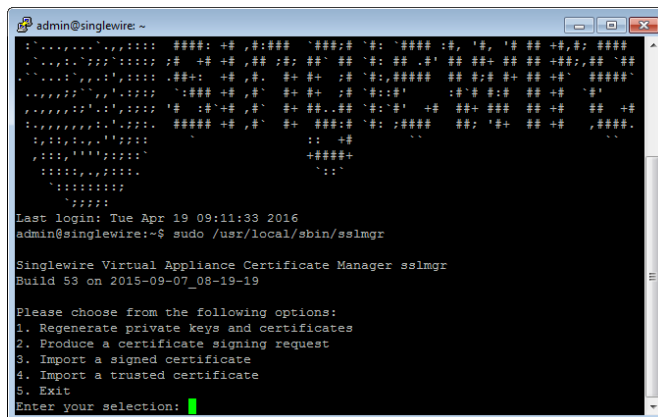


Step 7 Enter **admin** at the prompt and press the **Enter** key.

Step 8 Enter your OS password at the prompt and press the **Enter** key. The command-line interface refreshes, showing you that you're logged in.



Step 9 Enter **sudo /usr/local/sbin/sslmgr** at the prompt and press the **Enter** key. The command-line interface refreshes with some choices.



- Step 15** Enter your organization's name at the prompt (e.g. Example Company) and press the **Enter** key.
- Step 16** Enter the name of your organizational unit at the prompt (e.g. Security) and press the **Enter** key.
- Step 17** Enter the fully qualified hostname of your server at the prompt (e.g. informacast.example.com) and press the **Enter** key.



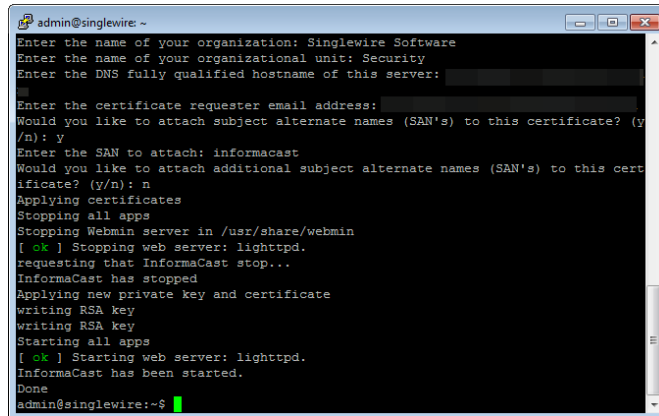
Note This must be a domain or common name—it cannot be an IP address—and it must match the record on your DNS server.

- Step 18** Enter your email address at the prompt (e.g. user@example.com) and press the **Enter** key.
- Step 19** Determine whether you want to add Subject Alternate Names (SANs) to your server (SANs allow you to secure multiple domain names with one certificate, e.g. www.example.com, www.exchange.example.com, and www.example.net can all be secured through SANs):
- If yes, enter **Y** at the prompt and press the **Enter** key. Enter your SAN at the prompt and press the **Enter** key. You will continue to be prompted for a new SAN until you enter **N** at the prompt asking if you'd like to attach more SANs.
 - If no, enter **N** at the prompt and press the **Enter** key.

Once you enter **N** and press the **Enter** key, SSLMGR will stop all of the applications running on the Virtual Appliance.

```
admin@singlewire: ~
Please wait for PTT to start...
All apps are running
Generating new private key
Generating new self signed certificate
Enter your country code: us
Enter your state or province: wi
Enter your city: madison
Enter the name of your organization: Singlewire Software
Enter the name of your organizational unit: Security
Enter the DNS fully qualified hostname of this server:
Enter the certificate requester email address:
Would you like to attach subject alternate names (SAN's) to this certificate? (y/n): y
Enter the SAN to attach: informacast
Would you like to attach additional subject alternate names (SAN's) to this certificate? (y/n): n
Applying certificates
Stopping all apps
Stopping Webmin server in /usr/share/webmin
[ ok ] Stopping web server: lighttpd.
requesting that InformaCast stop...
InformaCast has stopped
```

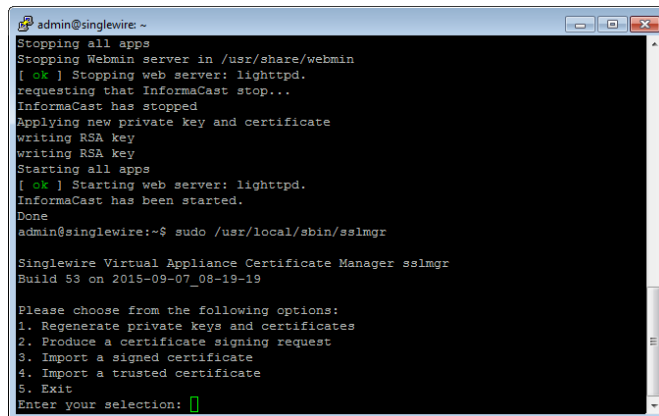
It will then write a new RSA key and start all of the Virtual Appliance's applications.



```
admin@singlewire:~$
Enter the name of your organization: Singlewire Software
Enter the name of your organizational unit: Security
Enter the DNS fully qualified hostname of this server:
Enter the certificate requester email address:
Would you like to attach subject alternate names (SAN's) to this certificate? (y/n): y
Enter the SAN to attach: informacast
Would you like to attach additional subject alternate names (SAN's) to this certificate? (y/n): n
Applying certificates
Stopping all apps
Stopping Webmin server in /usr/share/webmin
[ ok ] Stopping web server: lighttpd.
requesting that InformaCast stop...
InformaCast has stopped
Applying new private key and certificate
writing RSA key
writing RSA key
Starting all apps
[ ok ] Starting web server: lighttpd.
InformaCast has been started.
Done
admin@singlewire:~$
```

Now, you will create a new certificate-signing request.

Step 20 Enter `sudo /usr/local/sbin/sslmgr` at the prompt and press the **Enter** key. The command-line interface refreshes with some choices.



```
admin@singlewire:~$
Stopping all apps
Stopping Webmin server in /usr/share/webmin
[ ok ] Stopping web server: lighttpd.
requesting that InformaCast stop...
InformaCast has stopped
Applying new private key and certificate
writing RSA key
writing RSA key
Starting all apps
[ ok ] Starting web server: lighttpd.
InformaCast has been started.
Done
admin@singlewire:~$ sudo /usr/local/sbin/sslmgr
Singlewire Virtual Appliance Certificate Manager sslmgr
Build 53 on 2015-09-07_08-19-19

Please choose from the following options:
1. Regenerate private keys and certificates
2. Produce a certificate signing request
3. Import a signed certificate
4. Import a trusted certificate
5. Exit
Enter your selection: 
```



```
-----END CERTIFICATE-----
```



Note Certificates commonly come in two file types: PEM and DER. SSLMGR only handles PEM-formatted files. If your CA provides you with a DER-formatted file, contact them and request a PEM-formatted file.

You will now import the signed certificate to InformaCast. Again, this import will require starting and stopping all interfaces of the Virtual Appliance, which will cause service interruptions. Before continuing, make sure that you are performing this import during a time when you are least likely to inconvenience your users.

- Step 25** Re-establish your PuTTY connection to the Virtual Appliance (see Steps 1 through 8 beginning on page 38).
- Step 26** Enter `sudo /usr/local/sbin/sslmgr` at the prompt and press the **Enter** key. The command-line interface refreshes with some choices.

```
admin@singlewire: ~
Last login: Tue Apr 19 09:11:33 2016
admin@singlewire:~$ sudo /usr/local/sbin/sslmgr
Singlewire Virtual Appliance Certificate Manager sslmgr
Build 53 on 2015-09-07_08-19-19

Please choose from the following options:
1. Regenerate private keys and certificates
2. Produce a certificate signing request
3. Import a signed certificate
4. Import a trusted certificate
5. Exit
Enter your selection: █
```

- Step 27** Enter **3** at the prompt and press the **Enter** key. SSLMGR will ensure all of the applications on the Virtual Appliance are started and then prompt you to paste in your signed certificate text.

```
admin@singlewire: ~
Last login: Tue Apr 19 10:35:17 2016 from [REDACTED]
admin@singlewire:~$ sudo /usr/local/sbin/sslmgr
Singlewire Virtual Appliance Certificate Manager sslmgr
Build 53 on 2015-09-07_08-19-19

Please choose from the following options:
1. Regenerate private keys and certificates
2. Produce a certificate signing request
3. Import a signed certificate
4. Import a trusted certificate
5. Exit
Enter your selection: 3
All applications must be in a started state. Starting any applications that are
n't already running.
All apps are running
Loading private key
Paste in the signed certificate. Ensure that you include the --- BEGIN --- and
--- END --- lines.
Press enter on a line by itself when done.
█
```

Step 28 Copy the text of your signed certificate and paste it into your command-line interface.



Tip Right clicking your mouse will immediately paste whatever is in your clipboard into the command-line interface.

Step 29 Press the **Enter** key twice. SSLMGR will stop all applications running on the Virtual Appliance, apply your signed certificate, and start the Virtual Appliance's applications.

Step 30 Enter **exit** at the prompt and press the **Enter** key. You have finished installing your signed certificate. When you next log into any of the Virtual Appliance's interfaces, you should not receive any warning about a security risk in continuing to your destination.



Note Typically, signed certificates last for five years, but this is at the discretion of your CA. It is your responsibility to ask your CA for your certificate's expiration date and perform these steps again in the future as your expiration date nears.



Tip If you encounter any errors in the SSLMGR process, [contact Singlewire Support](#).

Integrate Unified Communications Manager

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

- “Configure Unified Communications Manager SNMP” on page 2-46
- “Set the Default Codec to G.711” on page 2-54
- “Create a Device Pool” on page 2-56
- “Create a Route Partition” on page 2-58
- “Create a Calling Search Space” on page 2-59
- “Create CTI Ports” on page 2-61
- “Create an Access Control Group” on page 2-66
- “Create an Application User” on page 2-70
- “Enable Web Access for Cisco IP Phones” on page 2-73
- “Set Your Authentication URL” on page 2-80
- “Set the Authentication Method for API Browser Access” on page 2-82
- “Reboot Your Phones” on page 2-83
- “Test Your Phones” on page 2-85

**Tip**

When naming your Unified Communications Manager 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 5-46 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 Unified Communications Manager SNMP

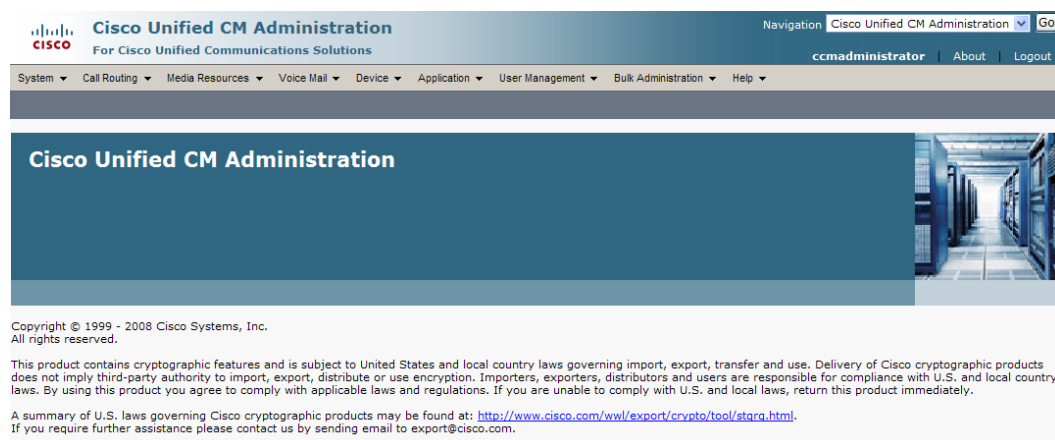
InformaCast uses SNMP to gather phone information from Unified Communications Manager. Depending on whether you are using SNMP v2 or v3, you will follow different steps:

- **SNMP v2.** Follow the steps in “Enable SNMP on Unified Communications Manager Cluster Nodes” on page 2-46 and “Create an InformaCast SNMP v2 Community String” on page 2-49.
- **SNMP v3.** Follow the steps in “Enable SNMP on Unified Communications Manager Cluster Nodes” on page 2-46 and “Create an SNMP v3 User” on page 2-51.

Enable SNMP on Unified Communications Manager Cluster Nodes

You must enable SNMP on Unified Communications Manager cluster nodes that will function with InformaCast.

- Step 1** Open a web browser and log into the administration interface of the Unified Communications Manager server (the address will be similar to `https://<Unified Communications Manager 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.

Service Activation Related Links: [Control Center - Feature Services](#) Go

Save Set to Default Refresh

Status
Status : Ready

Select Server
Server* IPTCUCM613 Go
 Check All Services

CM Services		
	Service Name	Activation Status
<input checked="" type="checkbox"/>	Cisco CallManager	Activated
<input checked="" type="checkbox"/>	Cisco Tftp	Activated
<input type="checkbox"/>	Cisco Messaging Interface	Deactivated
<input type="checkbox"/>	Cisco Unified Mobile Voice Access Service	Deactivated
<input type="checkbox"/>	Cisco IP Voice Media Streaming App	Deactivated
<input checked="" type="checkbox"/>	Cisco CTIManager	Activated
<input checked="" type="checkbox"/>	Cisco Extension Mobility	Activated
<input type="checkbox"/>	Cisco Extended Functions	Deactivated
<input type="checkbox"/>	Cisco Dialed Number Analyzer	Deactivated
<input type="checkbox"/>	Cisco DHCP Monitor Service	Deactivated

CTI Services		
	Service Name	Activation Status
<input type="checkbox"/>	Cisco CallManager Attendant Console Server	Deactivated
<input type="checkbox"/>	Cisco IP Manager Assistant	Deactivated
<input type="checkbox"/>	Cisco WebDialer Web Service	Deactivated

CDR Services		
	Service Name	Activation Status
<input type="checkbox"/>	Cisco SOAP - CDRonDemand Service	Deactivated
<input type="checkbox"/>	Cisco CAR Web Service	Deactivated

Database and Admin Services		
	Service Name	Activation Status
<input checked="" type="checkbox"/>	Cisco AXL Web Service	Activated
<input type="checkbox"/>	Cisco UXL Web Service	Deactivated
<input checked="" type="checkbox"/>	Cisco Bulk Provisioning Service	Activated
<input type="checkbox"/>	Cisco TAPS Service	Deactivated

Performance and Monitoring Services		
	Service Name	Activation Status
<input type="checkbox"/>	Cisco Serviceability Reporter	Deactivated
<input checked="" type="checkbox"/>	Cisco CallManager SNMP Service	Activated

Security Services		
	Service Name	Activation Status
<input type="checkbox"/>	Cisco CTL Provider	Deactivated
<input type="checkbox"/>	Cisco Certificate Authority Proxy Function	Deactivated

Directory Services		
	Service Name	Activation Status
<input type="checkbox"/>	Cisco DirSync	Deactivated

Save Set to Default Refresh

i *- indicates required item.

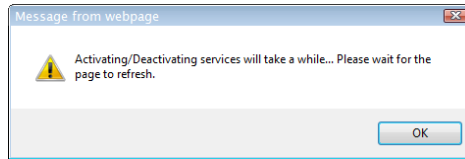


Note If you have more than one server, you'll have to select your server from the **Server** dropdown menu and click the **Go** button. The Service Activation page for that server will then appear.

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**, **Cisco 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 v2 Community String

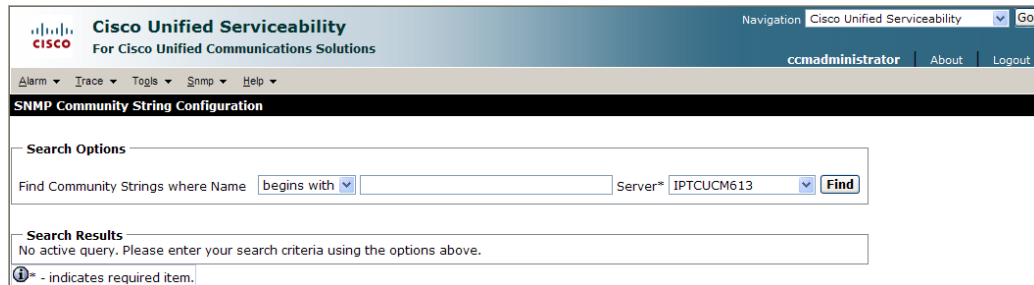
Follow these steps to create an SNMP v2 InformaCast SNMP community string.



Note

Skip this section if you're using SNMP v3 and go to "Create an SNMP v3 User" on page 2-51.

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.

The screenshot shows the Cisco Unified Serviceability interface for SNMP Community String Configuration. The page title is "SNMP Community String Configuration". The status bar indicates "1 records found". The search options section shows "Find Community Strings where Name begins with" and "Server*" set to "CUCM7". The search results table is as follows:

<input type="checkbox"/>	Community String Name	Access Privileges
<input type="checkbox"/>	InformaCast	ReadNotifyOnly

Below the table are buttons for "Add New" and "Delete Selected". A help box at the bottom provides instructions: "Click on the Add New button to add a new Community String", "Click on the corresponding Community String Name to Update the Community String Information", "Select corresponding Checkbox and click on Delete Selected button to Delete Community String", and "* - indicates required item."

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

The screenshot shows the "Add New" form for creating a community string. The status bar indicates "Status : Ready". The "Server*" dropdown is set to "IPTCUCM613". The "Community String Information" section has a "Community String Name*" field. The "Host IP Addresses Information" section has radio buttons for "Accept SNMP Packets from any host" (selected) and "Accept SNMP Packets only from these hosts". Below are fields for "Host IP Address" and "Host IP Addresses" with "Insert" and "Remove" buttons. The "Access Privileges" section has a dropdown for "Access Privileges*" set to "-- Select Access Privilege --" and a note: "Notify access privilege is required in order to configure Notification Destinations." At the bottom are "Save", "Clear All", and "Cancel" buttons. A help box at the bottom states "* - indicates required item."

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 Unified Communications Manager Cluster" on page 4-2.

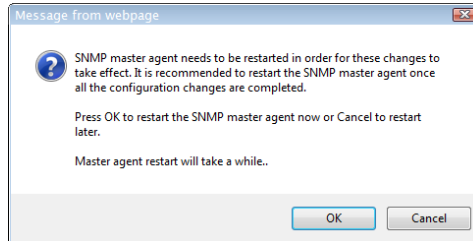


Note For additional security, click the **Accept SNMP packets only from these hosts** radio button and enter the Virtual Appliance's IP address in the **Host IP Address** field.

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.



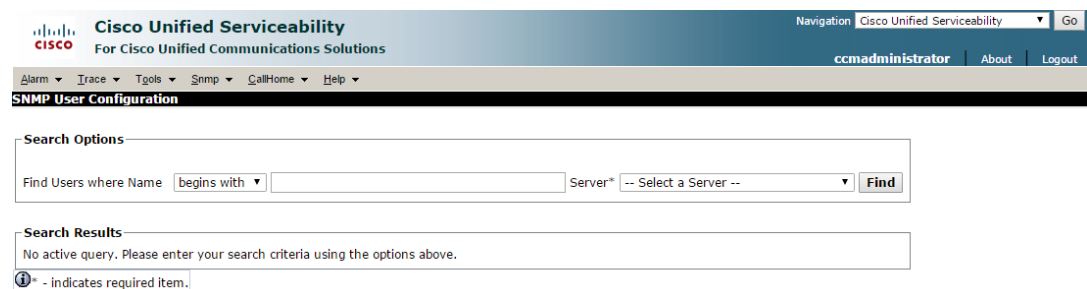
Create an SNMP v3 User

Follow these steps to create an SNMP v3 user.



Note Skip this section if you're using SNMP v2.

Step 1 Go to **SNMP | V3 | User**. The SNMP User Configuration page appears.



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

Search Results

<input type="checkbox"/>	User Name	Authentication Required	Authentication Protocol	Privacy Required	Privacy Protocol	Access Privileges
<input type="checkbox"/>	ICVA	true	SHA	true	AES128	ReadOnly
<input type="checkbox"/>	snmpUser	true	SHA	true	AES128	ReadOnly
<input type="checkbox"/>		true	SHA	true	AES128	ReadOnly
<input type="checkbox"/>		true	SHA	true	AES128	ReadOnly
<input type="checkbox"/>		false	None	false	None	ReadOnly

Apply To All Nodes

Click on the Add New button to add a new User
 Click on the corresponding User Name to Update the User Information
 Select corresponding Checkbox and click on Delete Selected button to Delete User
 * - indicates required item.

Step 3 Click the **Add New** button to create a new user. The SNMP User Configuration page refreshes.

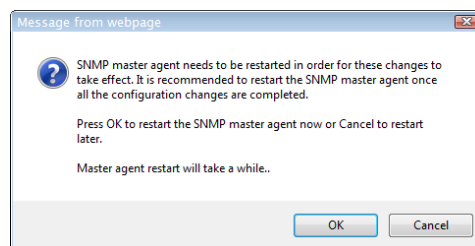
Step 4 Enter a name for your user in the **User Name** field, e.g. ICVA. Your username can contain up to 32 characters and any combination of alphanumeric characters, hyphens (-), and underscore characters (_).



Note

You will need to remember this name and its associated passwords when you edit InformaCast's SNMP configuration in "Configure Your Default Unified Communications Manager Cluster" on page 5-3.

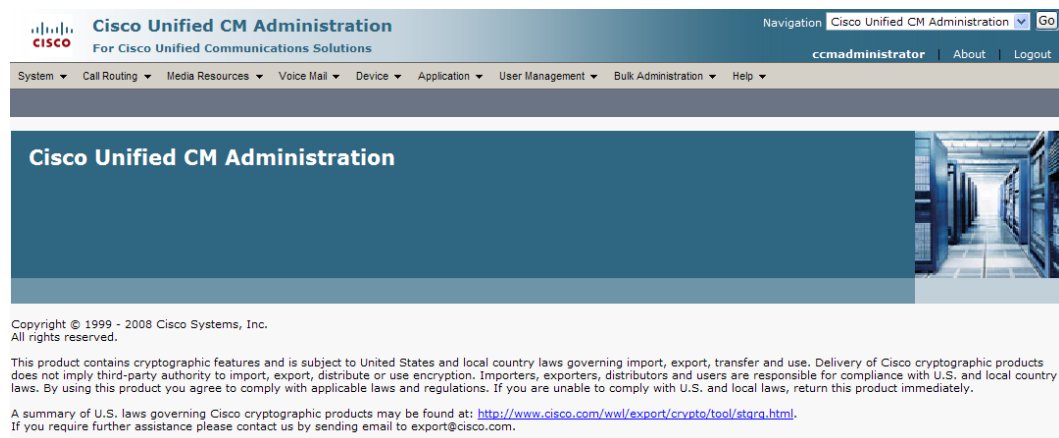
- Step 5** Select the **Authentication Required** checkbox.
- Step 6** Enter an authentication password for your user in the **Password** and **Reenter Password** fields. The password must contain at least eight characters.
- Step 7** Select the **SHA** radio button.
- Step 8** Select the **Privacy Required** checkbox.
- Step 9** Enter a privacy password for your user in the **Password** and **Reenter Password** fields. The password must contain at least eight characters.
- Step 10** Select the **AES128** radio button.
- Step 11** Select **ReadOnly** from the **Access Privileges** dropdown menu.
- Step 12** Select the **Apply To All Nodes** checkbox.
- Step 13** 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 μ Law format. Because most Unified Communications Manager 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.

- 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.

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration Go
ccadministrator About Logout

System Call Routing Media Resources Voice Mail Device Application User Management Bulk Administration Help

Find and List Regions

+ Add New

Regions

Find Regions where Name begins with Find Clear Filter + -

No active query. Please enter your search criteria using the options above.

Add New

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

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration Go
ccadministrator About Logout

System Call Routing Media Resources Voice Mail Device Application User Management Bulk Administration Help

Region Configuration Related Links: Back To Find/List Go

Save

Region Information

Name* |

Save

*- indicates required item.
**The Audio Codec selection determines bandwidth only. The G.711 and G.722 codecs both result in a maximum bandwidth of 64 Kbps between regions and can be used interchangeably.

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

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration Go
ccadministrator About Logout

System Call Routing Media Resources Voice Mail Device Application User Management Bulk Administration Help

Region Configuration Related Links: Back To Find/List Go

Save Delete Reset Add New

Status

Add successful
Click on the Reset button to have the changes take effect.

Region Information

Name* ICVA

Region Relationships

Region	Audio Codec	Video Call Bandwidth	Link Loss Type
NOTE: Region(s) not displayed	Use System Default	Use System Default	Use System Default

Modify Relationship to other Regions

Regions	Audio Codec	Video Call Bandwidth	Link Loss Type
ICVA InformaCast	Keep Current Setting	<input checked="" type="radio"/> Keep Current Setting <input type="radio"/> Use System Default <input type="radio"/> None <input type="text"/> kbps	Keep Current Setting

Save Delete Reset Add New

*- indicates required item.
**The Audio Codec selection determines bandwidth only. The G.711 and G.722 codecs both result in a maximum bandwidth of 64 Kbps between regions and can be used interchangeably.

- 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 Unified Communications Manager. In order to have those components use the newly created G.711 μ Law region, you must first create a device pool.

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

The screenshot shows the Cisco Unified CM Administration web interface. At the top, there is a navigation bar with the Cisco logo and the text 'Cisco Unified CM Administration For Cisco Unified Communications Solutions'. Below this is a navigation menu with options like System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. The main content area is titled 'Find and List Device Pools' and contains an 'Add New' button. Below this is a search section for 'Device Pool' with a dropdown menu for 'Device Pool Name', a 'begins with' dropdown, and search buttons labeled 'Find', 'Clear Filter', and a plus/minus icon. A message below the search bar reads: 'No active query. Please enter your search criteria using the options above.' There is also an 'Add New' button at the bottom of the search section.

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

The screenshot displays the Cisco Unified CM Administration interface for configuring a new Device Pool. The page is titled "Device Pool Configuration" and includes a navigation bar with "Cisco Unified CM Administration" and "Go" buttons. The user is logged in as "ccmadministrator".

Status: Ready

Device Pool Information: Device Pool: New

Device Pool Settings:

- Device Pool Name* (text input)
- Cisco Unified Communications Manager Group* (dropdown: -- Not Selected --)
- Calling Search Space for Auto-registration (dropdown: < None >)
- Reverted Call Focus Priority (dropdown: Default)
- Local Route Group (dropdown: < None >)

Roaming Sensitive Settings:

- Date/Time Group* (dropdown: -- Not Selected --)
- Region* (dropdown: -- Not Selected --)
- Media Resource Group List (dropdown: < None >)
- Location (dropdown: < None >)
- Network Locale (dropdown: < None >)
- SRST Reference* (dropdown: -- Not Selected --)
- Connection Monitor Duration*** (text input)
- Single Button Barge* (dropdown: Default)
- Join Across Lines* (dropdown: Default)
- Physical Location (dropdown: < None >)
- Device Mobility Group (dropdown: < None >)

Device Mobility Related Information**:**

- Device Mobility Calling Search Space (dropdown: < None >)
- AAR Calling Search Space (dropdown: < None >)
- AAR Group (dropdown: < None >)
- Calling Party Transformation CSS (dropdown: < None >)
- Called Party Transformation CSS (dropdown: < None >)

Incoming Calling Party Settings:

If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned.

Buttons: **Clear Prefix Settings** | **Default Prefix Settings**

- Incoming Calling Party National Number Prefix (text input: Default)
- Incoming Calling Party International Number Prefix (text input: Default)
- Incoming Calling Party Unknown Number Prefix (text input: Default)
- Incoming Calling Party Subscriber Number Prefix (text input: Default)

Save button is located at the bottom left.

Footnote:

- *- indicates required item.
- **Number of devices that have to be reset when this device pool is updated. To see a detailed list of these devices and other dependencies, click on Dependency Records.
- ***leave blank to use default.
- ****These five parameters will overwrite device level settings when device is roaming and in the same device mobility group.

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



Tip

Make sure that the Unified Communications Manager group you choose contains the Unified Communications Manager 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 2-54.
- 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.

The screenshot shows the Cisco Unified CM Administration interface. The top navigation bar includes the Cisco logo, the title "Cisco Unified CM Administration For Cisco Unified Communications Solutions", and a navigation dropdown menu set to "Cisco Unified CM Administration" with a "Go" button. Below the navigation bar is a menu with items: System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. The main content area is titled "Find and List Partitions" and features an "Add New" button with a plus icon. Below this is a search section titled "Partition" with a form containing "Find Partition where" followed by two dropdown menus (one set to "Name" and the other to "begins with"), a "Find" button, a "Clear Filter" button, and a refresh icon. A message below the search form reads: "No active query. Please enter your search criteria using the options above." At the bottom of the search section is another "Add New" button.

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

Partition Configuration

Status: Ready

Partition Information

To enter multiple partitions, use one line for each partition entry. You can enter up to 75 partitions; the names and descriptions can have up to a total of 1475 characters. The partition name cannot exceed 50 characters. Use a comma (',') to separate the partition name and description on each line. If a description is not entered, Cisco Unified Communications Manager uses the partition name as the description. For example:
 << partitionName >> , << description >>
 CiscoPartition, Cisco employee partition
 DallasPartition

Name*

Save

*- indicates required item.

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 Unified Communications Manager'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.

Find and List Calling Search Spaces

Add New

Calling Search Space

Find Calling Search Space where CSS Name begins with Find Clear Filter

No active query. Please enter your search criteria using the options above.

Add New

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

The screenshot shows the Cisco Unified CM Administration interface for the 'Calling Search Space Configuration' page. The page title is 'Calling Search Space Configuration' and it includes a 'Save' button. The 'Status' section shows 'Status: Ready'. The 'Calling Search Space Information' section has two input fields: 'Name*' and 'Description'. The 'Route Partitions for this Calling Search Space' section contains two lists: 'Available Partitions**' and 'Selected Partitions'. The 'Available Partitions**' list includes: Global Learned Enterprise Patterns, ICVA Park Page, ICVA-CTIOutbound, ICVA-Redirect1-CA, and InformaCast. The 'Selected Partitions' list is currently empty. A 'Save' button is located below the lists. At the bottom, there are two informational icons: one indicating that '*' denotes a required item, and another indicating that '**Selected Partitions are ordered by highest priority'.

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 2-58
- 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.

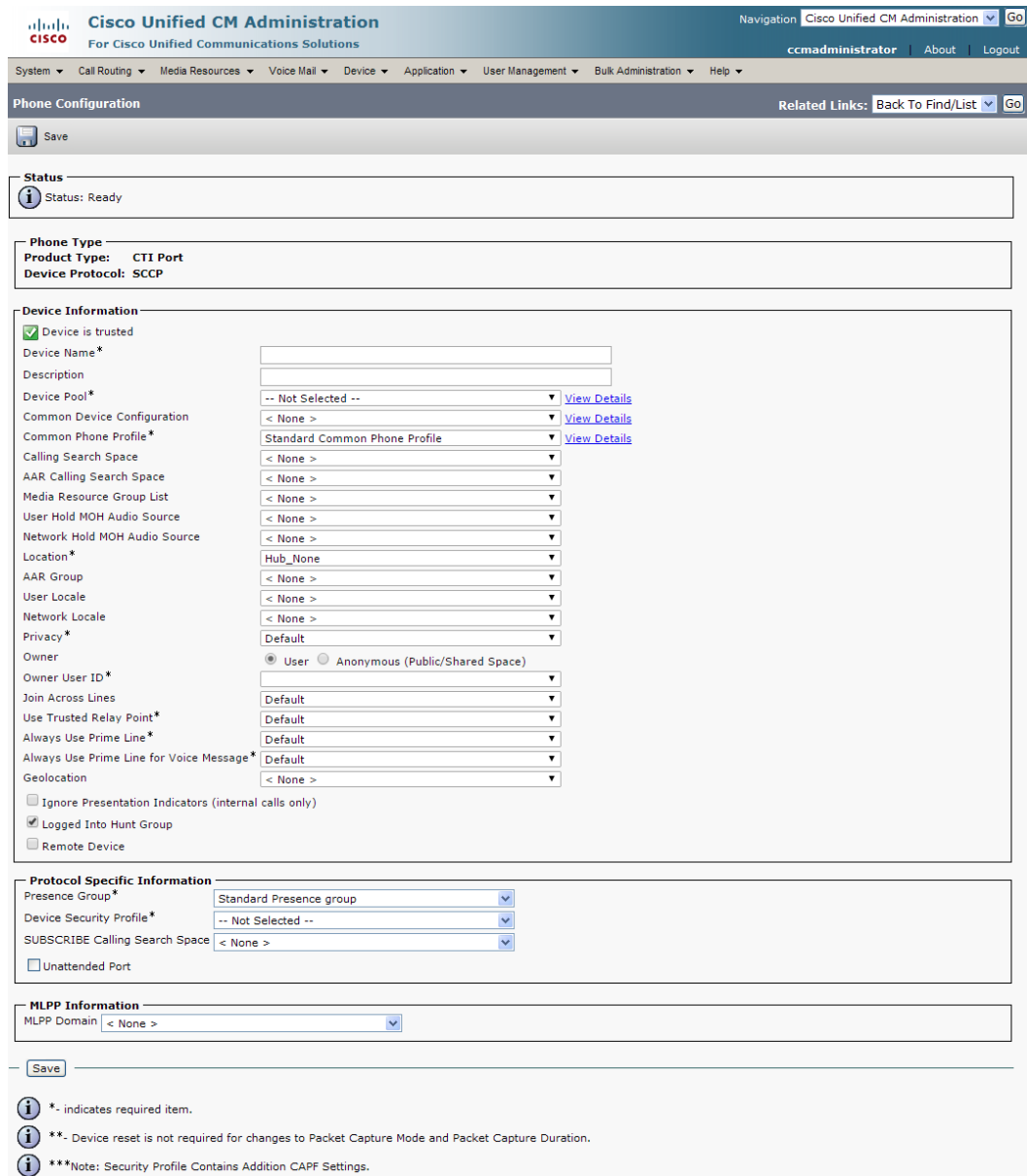
Step 1 Go to **Device | Phone**. The Find and List Phones page appears.

The screenshot shows the Cisco Unified CM Administration interface. The page title is "Find and List Phones". The navigation menu includes System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. The user is logged in as "ccadministrator". The page features a search bar with a dropdown menu for "Device Name" and a "begins with" filter. There are buttons for "Find", "Clear Filter", and "Add New". A message at the bottom of the search area states: "No active query. Please enter your search criteria using the options above." There is also a "Go" button next to the search bar.

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

The screenshot shows the Cisco Unified CM Administration interface for the "Add a New Phone" page. The navigation menu is the same as in the previous screenshot. The page title is "Add a New Phone". There is a "Next" button with a green arrow. The "Status" section shows "Status: Ready". The "Select the type of phone you would like to create" section has a dropdown menu for "Phone Type*" with "-- Not Selected --" selected. There is a "Next" button at the bottom. A note at the bottom left states: "i *- indicates required item."

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



Phone Configuration

Save

Status
Status: Ready

Phone Type
Product Type: CTI Port
Device Protocol: SCCP

Device Information

Device is trusted

Device Name*

Description

Device Pool* -- Not Selected -- [View Details](#)

Common Device Configuration < None > [View Details](#)

Common Phone Profile* Standard Common Phone Profile [View Details](#)

Calling Search Space < None >

AAR Calling Search Space < None >

Media Resource Group List < None >

User Hold MOH Audio Source < None >

Network Hold MOH Audio Source < None >

Location* Hub_None

AAR Group < None >

User Locale < None >

Network Locale < None >

Privacy* Default

Owner User Anonymous (Public/Shared Space)

Owner User ID*

Join Across Lines Default

Use Trusted Relay Point* Default

Always Use Prime Line* Default

Always Use Prime Line for Voice Message* Default

Geolocation < None >

Ignore Presentation Indicators (internal calls only)

Logged Into Hunt Group

Remote Device

Protocol Specific Information

Presence Group* Standard Presence group

Device Security Profile* -- Not Selected --

SUBSCRIBE Calling Search Space < None >

Unattended Port

MLPP Information

MLPP Domain < None >

Save

Info *- indicates required item.

Info **: Device reset is not required for changes to Packet Capture Mode and Packet Capture Duration.

Info ***Note: Security Profile Contains Addition CAPF Settings.

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.

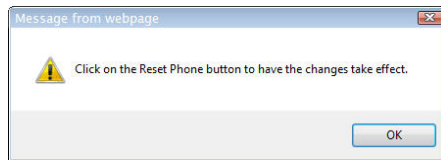
Step 5 Enter a description in the **Description** field, e.g. InformaCast Port.

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



Note The device pool must use a region that will allow a G.711 μ Law 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.
- Step 8** Select the **Anonymous/Public Shared Space** radio button above the **Owner User ID** field, which will remove the required setting from the **Owner User ID** field.
- Step 9** 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 10** Click the **Save** button. A warning dialog box appears.



Step 11 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.

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration Go
ccadministrator About Logout

System Call Routing Media Resources Voice Mail Device Application User Management Bulk Administration Help

Phone Configuration Related Links: Back To Find/List Go

Save Delete Copy Reset Add New

Status
Add successful

Association Information

- 7775 Line [1] - Add a new DN
- 7775 Intercom [1] - Add a new Intercom

Phone Type
Product Type: CTI Port
Device Protocol: SCCP

Device Information

Registration: Unknown
IP Address: Unknown
 Device is Active
 Device is trusted
 Device Name*: ICVA-IC-1
 Description: InformaCast Recording Port
 Device Pool*: ICVA [View Details](#)
 Common Device Configuration: < None > [View Details](#)
 Common Phone Profile*: Standard Common Phone Profile
 Calling Search Space: ICVA
 AAR Calling Search Space: < None >
 Media Resource Group List: < None >
 User Hold MOH Audio Source: < None >
 Network Hold MOH Audio Source: < None >
 Location*: Hub_None
 AAR Group: < None >
 Owner User ID: < None >
 Join Across Lines: Default
 Use Trusted Relay Point*: Default
 Always Use Prime Line*: Default
 Always Use Prime Line for Voice Message*: Default
 Calling Party Transformation CSS: < None >
 Geolocation: < None >
 Use Device Pool Calling Party Transformation CSS
 Ignore Presentation Indicators (internal calls only)
 Logged Into Hunt Group
 Remote Device

Protocol Specific Information

Presence Group*: Standard Presence group
 Device Security Profile*: Cisco CTI Port - Standard SCCP Non-Secure Profil
 SUBSCRIBE Calling Search Space: < None >
 Unattended Port

Save Delete Copy Reset Add New

Legend:
 i *- indicates required item.
 i ** - Device reset is not required for changes to Packet Capture Mode and Packet Capture Duration.
 i ***Note: Security Profile Contains Addition CAPF Settings.

Step 12 Click the **Line[1] - Add an New DN** link. The Directory Number Configuration page appears.

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration

System | Call Routing | Media Resources | Voice Mail | Device | Application | User Management | Bulk Administration | Help

ccmadministrator | About | Logout

Directory Number Configuration Related Links: [Configure Device \(ICVA-IC-1\)](#)

Status
Status: Ready

Directory Number Information

Directory Number*

Route Partition

Description

Alerting Name

ASCII Alerting Name

Active

Directory Number Settings

Voice Mail Profile (Choose <None> to use system default)

Calling Search Space

Presence Group*

User Hold MOH Audio Source

Network Hold MOH Audio Source

AAR Settings

AAR	Voice Mail	AAR Destination Mask	AAR Group
<input type="checkbox"/>	<input type="checkbox"/> or	<input type="text"/>	<input style="border: none;" type="text" value=" < None > "/>

Retain this destination in the call forwarding history

MLPP Alternate Party Settings

Target (Destination)

MLPP Calling Search Space

MLPP No Answer Ring Duration (seconds)

Line Settings for All Devices

Hold Reversion Ring Duration (seconds) Setting the Hold Reversion Ring Duration to zero will disable the feature

Hold Reversion Notification Interval (seconds) Setting the Hold Reversion Notification Interval to zero will disable the feature

Line 1 on Device ICVA-IC-1

Display (Internal Caller ID) Display text for a line appearance is intended for displaying text such as a name instead of a directory number for internal calls. If you specify a number, the person receiving a call may not see the proper identity of the caller.

ASCII Display (Internal Caller ID)

External Phone Number Mask

Multiple Call/Call Waiting Settings on Device InformaCast

Note: The range to select the Max Number of calls is: 1-10000

Maximum Number of Calls*

Busy Trigger* (Less than or equal to Max. Calls)

Forwarded Call Information Display on Device InformaCast

Caller Name

Caller Number

Redirected Number

Dialed Number

i * - indicates required item.

i ** - Changes to Line or Directory Number settings require restart.

Step 13 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 14 Select **ICVA-CTIOutbound** from the **Route Partition** dropdown menu.

Step 15 Scroll to the *Line 1 on Device ICVA-IC-001* area and enter **InformaCast** in the **Display (Internal Caller ID)** field.

- Step 16** 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 17** Click the **Save** button to add the directory number.
- Step 18** Repeat Steps 1 through 17 as many times as needed to create the number of CTI ports that you need (minimum two).

Create an Access Control Group

In “Create an Application User” on page 2-70, 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.

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

The screenshot shows the Cisco Unified CM Administration interface. The main heading is "Find and List Access Control Groups". Below the heading is a search bar with a dropdown menu set to "begins with", a text input field, and buttons for "Find", "Clear Filter", and a search icon. Below the search bar, a message states "No active query. Please enter your search criteria using the options above." and there is an "Add New" button.

- Step 2** Click the **Add New** button. The Access Control Group Configuration page appears.

The screenshot shows the Cisco Unified CM Administration interface for "Access Control Group Configuration". The page includes a "Save" button, a status message "0 records found", and a "User Group Information" section with a "Name*" field. Below the field is a "Save" button. A note at the bottom indicates that an asterisk (*) indicates a required item.

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

The screenshot shows the Cisco Unified CM Administration interface. At the top, the navigation bar includes 'Cisco Unified CM Administration' and 'Go'. Below the navigation bar, there are several tabs: 'System', 'Call Routing', 'Media Resources', 'Voice Mail', 'Device', 'Application', 'User Management', 'Bulk Administration', and 'Help'. The main content area is titled 'Access Control Group Configuration'. On the right side of this area, there is a 'Related Links' dropdown menu set to 'Back To Find/List' and a 'Go' button. Below the title bar, there are icons for 'Save', 'Delete', 'Copy', and 'Add New'. A 'Status' section shows '0 records found'. The 'User Group Information' section has a 'Name*' field containing 'ICVA User Group'. Below this is a 'User' section with search filters for 'User ID' and 'begins with', and buttons for 'Find', 'Clear Filter', and navigation arrows. A message states 'No active query. Please enter your search criteria using the options above.' Below the search filters are buttons for 'Add End Users to Group', 'Add App Users to Group', 'Select All', 'Clear All', and 'Delete Selected'. At the bottom of the 'User' section are buttons for 'Save', 'Delete', 'Copy', and 'Add New'. A note at the bottom indicates '* - indicates required item.'

- 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 Access Control Groups page appears.

The screenshot shows the Cisco Unified CM Administration interface. At the top, the navigation bar includes 'Cisco Unified CM Administration' and 'Go'. Below the navigation bar, there are several tabs: 'System', 'Call Routing', 'Media Resources', 'Voice Mail', 'Device', 'Application', 'User Management', 'Bulk Administration', and 'Help'. The main content area is titled 'Find and List Access Control Groups'. Below the title bar is an 'Add New' button. The 'User Group' section has search filters for 'Name' and 'begins with', and buttons for 'Find', 'Clear Filter', and navigation arrows. A message states 'No active query. Please enter your search criteria using the options above.' Below the search filters is an 'Add New' button.

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

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration **ccmadministrator** | About | Logout

System | Call Routing | Media Resources | Voice Mail | Device | Application | User Management | Bulk Administration | Help

Find and List Access Control Groups

Status
23 records found

User Group (1 - 23 of 23) Rows per Page: 50

Find User Group where Name begins with

<input type="checkbox"/>	Name ^	Roles	Copy
<input type="checkbox"/>	ICVA User Group		
<input type="checkbox"/>	MarkUserGroup		
<input type="checkbox"/>	Standard_CAR_Admin_Users		
	Standard_CCM_Admin_Users		
	Standard_CCM_End_Users		
	Standard_CCM_Gateway_Administration		
	Standard_CCM_Phone_Administration		
	Standard_CCM_Read_Only		
	Standard_CCM_Server_Maintenance		
	Standard_CCM_Server_Monitoring		
	Standard_CCM_Super_Users		
	Standard_CTI_Allow_Call_Monitoring		
	Standard_CTI_Allow_Call_Park_Monitoring		
	Standard_CTI_Allow_Call_Recording		
	Standard_CTI_Allow_Calling_Number_Modification		
	Standard_CTI_Allow_Control_of_All_Devices		
	Standard_CTI_Allow_Reception_of_SRTP_Key_Material		
	Standard_CTI_Enabled		
	Standard_CTI_Secure_Connection		
	Standard_EM_Authentication_Proxy_Rights		
	Standard_Packet_Sniffer_Users		
	Standard_RealtimeAndTraceCollection		
	Standard_TabSync_User		

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

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration **ccmadministrator** | About | Logout

System | Call Routing | Media Resources | Voice Mail | Device | Application | User Management | Bulk Administration | Help

Access Control Group Configuration Related Links: [Back To Find/List](#)

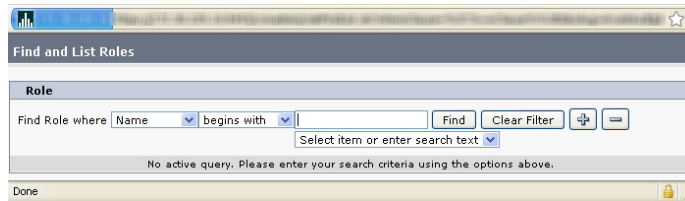
Status
 Status: Ready

User Group Information
Name* ICVA User Group

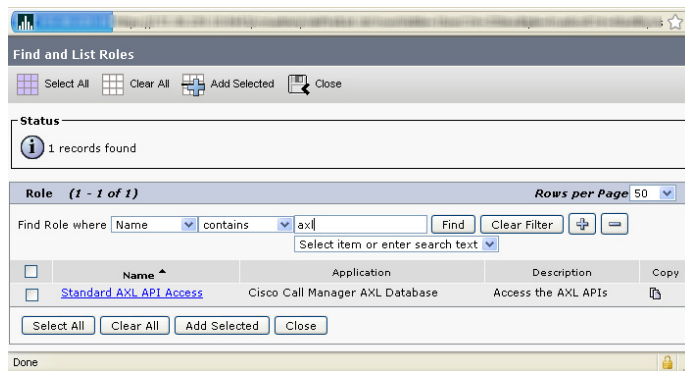
Role Assignment
Role

* - indicates required item.
 **The role Standard CCM Admin Users must be assigned to a user group to enable its members to logon to CCMAdmin web site
 ***The role Standard CCM End Users must be assigned to a user group to enable its members to logon to CCMUser web site

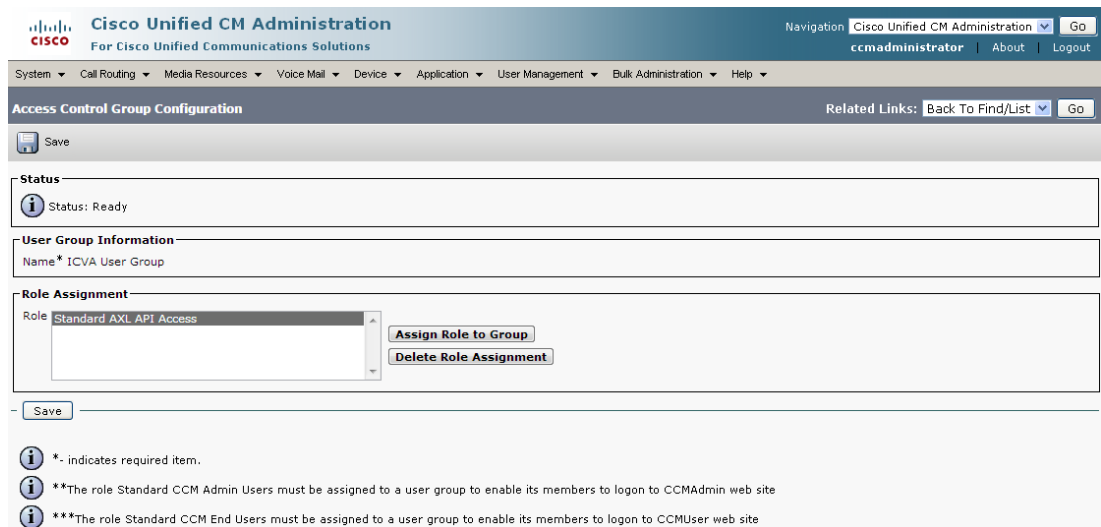
Step 7 Click the **Assign Role to Group** button. The Find and List Roles window appears.



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 Access Control Group Configuration page refreshes.



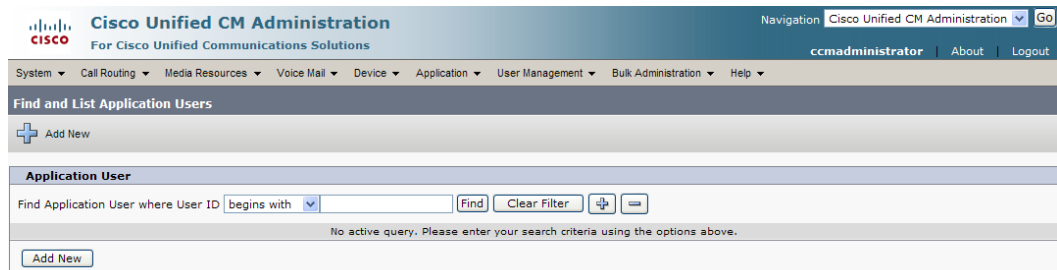
Step 10 Click the **Save** button.

Create an Application User

InformaCast needs an application user set in Unified Communications Manager so that it can establish a CTI connection and gain access to the telephony features Unified Communications Manager 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 Access Control Group” on page 2-66.
- **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 4-45).
- **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.

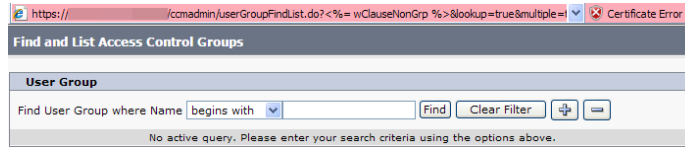
Step 3 Enter an appropriate user ID in the **User ID** field, e.g. ICVA InformaCast.

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

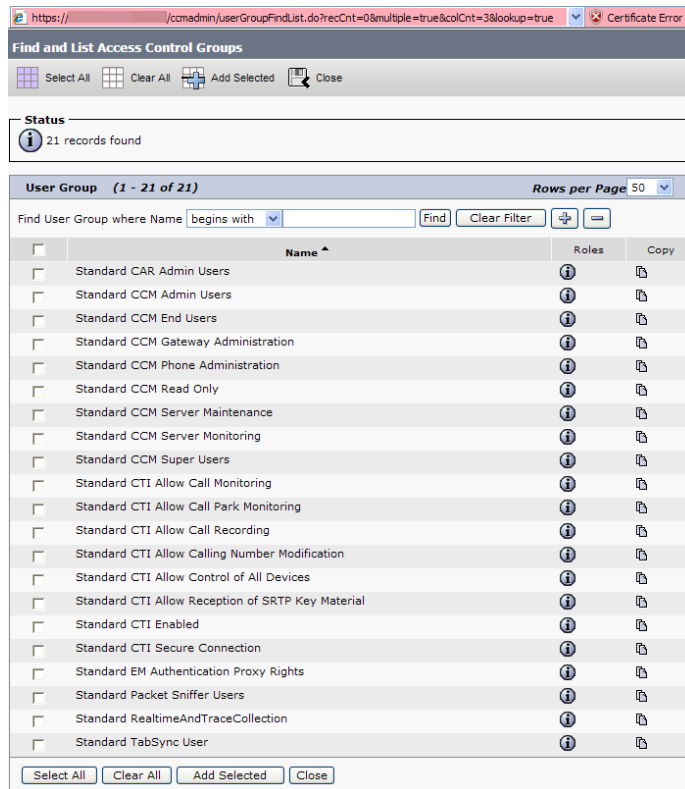
You will need to remember the user ID and password values because you will enter them into InformaCast's own Edit Telephony Configuration page once you install InformaCast (see "Configure Your Default Unified Communications Manager Cluster" on page 4-2).

Step 5 Select the CTI ports (created in "Create CTI Ports" on page 2-61) 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 Access Control Group** button. The Find and List Access Control Groups pop-up window appears.



Step 7 Click the **Find** button. The Find and List Access Control Groups pop-up 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 Unified Communications Manager 9.x or later.

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

Parameter	Parameter Value	Override Common Settings
<input type="checkbox"/> Disable USB	Enabled	<input type="checkbox"/>
Back USB Port*	Enabled	<input type="checkbox"/>
Side USB Port*	Mass Storage	<input type="checkbox"/>
Enable/Disable USB Classes	Human Interface Device	<input type="checkbox"/>
	Audio Class	<input type="checkbox"/>
SDIO*	Disabled	<input type="checkbox"/>
Bluetooth*	Enabled	<input type="checkbox"/>
Bluetooth Profiles*	Handsfree	<input type="checkbox"/>
	Human Interface Device	<input type="checkbox"/>
Lock Device During Audio Call*	Disabled	<input type="checkbox"/>
Kerberos Server		<input type="checkbox"/>
Kerberos Realm		<input type="checkbox"/>
TLS Resumption Timer*	3600	<input type="checkbox"/>
Detect Unified CM Connection Failure*	Normal	<input type="checkbox"/>
Time to Wait for Seamless Reconnect After TCP Drop or Roaming (seconds)	5	<input type="checkbox"/>
Load Server		<input type="checkbox"/>
IPv6 Load Server		<input type="checkbox"/>
Peer Firmware Sharing*	Enabled	<input type="checkbox"/>
Log Server		<input type="checkbox"/>
HTTPS Server*	http and https Enabled	<input type="checkbox"/>

Save

*- indicates required item.

- 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 2-80. 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 2-83.

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.

The screenshot shows the Cisco Unified CM Administration interface. The main heading is "Find and List Common Phone Profiles". Below the heading, there is a search bar with the text "Find Common Phone Profile where Name" and a "begins with" dropdown. To the right of the search bar are "Find", "Clear Filter", and navigation icons. Below the search bar, a message states "No active query. Please enter your search criteria using the options above." and there is an "Add New" button.

- Step 2** Click the **Find** button to display all the phone profiles of which Unified Communications Manager 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.

The screenshot shows the Cisco Unified CM Administration interface after a search. The main heading is "Find and List Common Phone Profiles". Below the heading, there are buttons for "Add New", "Select All", "Clear All", and "Delete Selected". A status bar indicates "1 records found". Below the status bar, there is a table with the following data:

Common Phone Profile (1 - 1 of 1)			Rows per Page 50
Name ^	Description	Copy	
<input type="checkbox"/> Standard Common Phone Profile	Standard Common Phone Profile		

Below the table, there are buttons for "Add New", "Select All", "Clear All", and "Delete Selected".

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.

Common Phone Profile Configuration

Navigation: Cisco Unified CM Administration | Go

System | Call Routing | Media Resources | Voice Mail | Device | Application | User Management | Bulk Administration | Help

Related Links: Back To Find/List | Go

Save | Delete | Copy | Reset | Apply Config | Add New

Status
Status: Ready

Common Phone Profile Information

Name*: Standard Common Phone Profile
 Description: Standard Common Phone Profile
 Local Phone Unlock Password:
 DND Option*: Ringer Off
 DND Incoming Call Alert*: Beep Only
 Feature Control Policy: < None >
 Enable End User Access to Phone Background Image Setting

Secure Shell Information

Secure Shell User:
 Secure Shell Password:

Phone Personalization Information

Phone Personalization*: Default
 Always Use Prime Line*: Default
 Always Use Prime Line for Voice Message*: Default
 Services Provisioning*: Default

Product Specific Configuration Layout

	Param	Override Common Settings
Back USB Port*	Enabled	<input type="checkbox"/>
Side USB Port*	Enabled	<input type="checkbox"/>
Cisco Camera*	Disabled	<input type="checkbox"/>
Enable/Disable USB Classes	Mass Storage Human Interface Device Audio Class	<input type="checkbox"/>
SDIO *	Disabled	<input type="checkbox"/>
Bluetooth *	Enabled	<input type="checkbox"/>
Wifi *	Enabled	<input type="checkbox"/>
Bluetooth Profiles*	Headset Human Interface Device	<input type="checkbox"/>
Join And Direct Transfer Policy*	Same line, across line enable	<input type="checkbox"/>
Settings Access*	Enabled	<input type="checkbox"/>
Video Capabilities*	Disabled	<input type="checkbox"/>
Web Access*	Enabled	<input checked="" type="checkbox"/>
Load Server	<input type="text"/>	<input type="checkbox"/>
RTCP*	Disabled	<input type="checkbox"/>
Peer Firmware Sharing*	Disabled	<input type="checkbox"/>
Cisco Discovery Protocol (CDP): Switch Port*	Enabled	<input type="checkbox"/>
Cisco Discovery Protocol (CDP): PC Port*	Enabled	<input type="checkbox"/>
Link Layer Discovery Protocol - Media Endpoint Discover (LLDP-MED): Switch Port*	Enabled	<input type="checkbox"/>
Link Layer Discovery Protocol (LLDP): PC Port*	Enabled	<input type="checkbox"/>
IPv6 Load Server	<input type="text"/>	<input type="checkbox"/>
802.1x Authentication*	User Controlled	<input type="checkbox"/>
Days Display Not Active	Sunday Monday Tuesday	<input type="checkbox"/>
Display On Time	07:30	<input type="checkbox"/>
Display On Duration	10:30	<input type="checkbox"/>
Display Idle Timeout	01:00	<input type="checkbox"/>
HTTPS Server*	http and https Enabled	<input type="checkbox"/>

Save | Delete | Copy | Reset | Apply Config | Add New

* - indicates required item.

- 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 2-80. 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 2-83.

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.

The screenshot shows the Cisco Unified CM Administration interface. The main heading is "Find and List Phones". Below the heading, there is a search bar with the following elements:

- A dropdown menu for "Find Phone where" set to "Device Name".
- A dropdown menu for "begins with" set to "begins with".
- A text input field for search criteria.
- Buttons for "Find", "Clear Filter", and a plus/minus icon.
- A dropdown menu for "Select item or enter search text".

Below the search bar, there is a message: "No active query. Please enter your search criteria using the options above." and an "Add New" button.

Step 2 Click the **Find** button to display all phones of which Unified Communications Manager 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.

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration **Go**

ccadministrator | About | Logout

System | Call Routing | Media Resources | Voice Mail | Device | Application | User Management | Bulk Administration | Help

Find and List Phones Related Links: [Actively Logged In Device Report](#) **Go**

+ Add New | Select All | Clear All | Delete Selected | Reset Selected

Status
75 records found

Phone (1 - 25 of 75) Rows per Page: 25

Find Phone where Device Name begins with **Find** **Clear Filter**

<input type="checkbox"/>	Device Name(Line) ^	Description	Device Pool	Device Protocol	Status	IP Address	Copy	Super Copy
<input type="checkbox"/>	AT211		Default	SCCP	Registered with iptapps-ccm61pub	172.30.227.211		
<input type="checkbox"/>	ATA0023EBC6AB6A	Auto 60018	Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	ATA23EBC6AB6A01	Auto 60019	Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	CTIFORNICK		Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	ICNick1	ICNick1	Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	ICNick2	ICNick2	Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	ICNick3	ICNick3	Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	ICNick4	ICNick4	Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	ICNick5	ICNick5	Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	ICNick6	ICNick6	Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	JessCTI1	JessCTI1	Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	JessCTI2	JessCTI2	Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	JessRCCTI		Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	KatieLC1		Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	KatieLC2		Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	KatieLC3		Default	SCCP	Unregistered	172.30.227.200		
<input type="checkbox"/>	KatieLC4		Default	SCCP	Unregistered	172.30.227.200		
<input type="checkbox"/>	PeteCTI1	PeteCTI1	Default	SCCP	Registered with iptapps-ccm61pub	172.30.227.211		
<input type="checkbox"/>	PeteCTI2	PeteCTI2	Default	SCCP	Registered with iptapps-ccm61pub	172.30.227.211		
<input type="checkbox"/>	RajCallAlert	RajCallAlert	RajInformaCast	SCCP	Unknown	Unknown		
<input type="checkbox"/>	RajCTIPort	RajCTIPort	RajInformaCast	SCCP	Unknown	Unknown		
<input type="checkbox"/>	RajCTIPort2	RajCTIPort2	RajInformaCast	SCCP	Unknown	Unknown		
<input type="checkbox"/>	RajCTIPort3	RajCTIPort3	RajInformaCast	SCCP	Unknown	Unknown		
<input type="checkbox"/>	RajCTIPort4	RajCTIPort4	RajInformaCast	SCCP	Unknown	Unknown		
<input type="checkbox"/>	SEP0004F2E67F44	Auto 60037	Default	SCCP	Unknown	Unknown		

+ Add New | Select All | Clear All | Delete Selected | Reset Selected

Go 1 of 3

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.

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration

ccmadministrator | About | Logout

System | Call Routing | Media Resources | Voice Mail | Device | Application | User Management | Bulk Administration | Help

Phone Configuration Related Links: [Back To Find/List](#)

Status
Status: Ready

Association Information

1	Line [1] - 60028 (no partition)
2	None
3	Add a new SD
4	Add a new SD
5	Add a new SD
6	Add a new SD
7	Add a new SD
8	Add a new SD
9	Add a new SD
10	Add a new SD
11	Add a new SD
12	Add a new SD
----- Unassigned Associated Items -----	
13	Line [2] - Add a new DN
14	Add a new SD
15	Privacy
16	None

Phone Type
Product Type: Cisco 7937
Device Protocol: SCCP

Device Information

Registration	Unknown
IP Address	Unknown
MAC Address*	0004F2E67F44
Description	Auto 60028
Device Pool*	Default View Details
Common Device Configuration	< None > View Details
Phone Button Template*	-- Not Selected --
Softkey Template	< None >
Common Phone Profile*	Standard Common Phone Profile
Calling Search Space	Phones
Media Resource Group List	< None >
User Hold MOH Audio Source	< None >
Network Hold MOH Audio Source	< None >
Location*	Hub_None
User Locale	< None >
Network Locale	< None >
Built In Bridge*	Default
Privacy*	Default
Device Mobility Mode*	Default View Current Device Mobility Settings
Owner User ID	< None >
Phone Load Name	

Ignore Presentation Indicators (internal calls only)
 Allow Control of Device from CTI
 Logged Into Hunt Group
 Remote Device

Product Specific Configuration Layout

Settings Access*	Enabled
Gratuitous ARP*	Enabled
PC Voice VLAN Access*	Enabled
Web Access*	Enabled
Load Server	
SSH Access*	Disabled

Legend:
 * - indicates required item.
 ** - Device reset is not required for changes to Packet Capture Mode and Packet Capture Duration.
 ***Note: Security Profile Contains Addition CAPF Settings.

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 2-80. 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 2-83.

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 Unified Communications Manager's Authentication URL to InformaCast.

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

The screenshot displays the 'Enterprise Parameters Configuration' page in the Cisco Unified CM Administration interface. The page is organized into several sections, each containing a list of parameters with their current values and suggested values. The 'URL Authentication' parameter under the 'Phone URL Parameters' section is highlighted with a red box.

Parameter Name	Parameter Value	Suggested Value
Synchronization Between Auto Device Profile and Phone Configuration *	True	True
Max Number of Device Level Trace *	12	12
DSCP for Phone-based Services *	default DSCP (000000)	default DSCP (000000)
DSCP for Phone Configuration *	CS3(precedence 3) DSCP (011000)	CS3(precedence 3) DSCP (011000)
DSCP for Cisco CallManager to Device Interface *	CS3(precedence 3) DSCP (011000)	CS3(precedence 3) DSCP (011000)
Connection Monitor Duration *	120	120
Auto Registration Phone Protocol *	SCCP	SCCP
BLF For Call Lists *	Disabled	Disabled
Advertise G.722 Codec *	Enabled	Enabled
Phone Personalization *	0	0
CCAdmin Parameters		
Max List Box Items *	250	250
Max Lookup Items *	1000	1000
Enable Dependency Records *	False	False
Security Parameters		
Cluster Security Mode *	0	
CAPF Phone Port *	3804	3804
Authentication Method for API Browser Access *	Basic	Basic
Enable Caching *	False	False
Phone URL Parameters		
URL Authentication	http://172.30.224.20/auth.asp	
URL Directories	http://IPTAPPS-CCM60-PUB:8080/ccmcp/xmldirectory.js	
URL Idle		
URL Idle Time	0	0
URL Information	http://IPTAPPS-CCM60-PUB:8080/ccmcp/GetTelecasterH	
URL Messages		
IP Phone Proxy Address		
URL Services	http://IPTAPPS-CCM60-PUB:8080/ccmcp/getservicesmen	
User Search Parameters		
Enable All User Search *	True	True
User Search Limit *	64	64

Buttons: Save, Set to Default, Reset

Legend:
 * indicates required item.
 **Set-to-Default button only applies to the modifiable parameters.



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 11 on page 4-7.
- 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 2-83.

Set the Authentication Method for API Browser Access



Note

You only need to perform the steps in this section if you are using Unified Communications Manager 11.5.1 or later

InformaCast uses API services in its communication with Unified Communication Manager. In order for this communication to work properly, you need to set your authentication method for API browser access to **Basic**.

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

The screenshot shows the Cisco Unified CM Administration interface. The main content area is titled "Enterprise Parameters Configuration". It contains several sections of parameters, each with a table of "Parameter Name", "Parameter Value", and "Suggested Value".

Parameter Name	Parameter Value	Suggested Value
Synchronization Between Auto Device Profile and Phone Configuration *	True	True
Max Number of Device Level Trace *	12	12
DSCP for Phone-based Services *	default DSCP (000000)	default DSCP (000000)
DSCP for Phone Configuration *	CS3(precedence 3) DSCP (011000)	CS3(precedence 3) DSCP (011000)
DSCP for Cisco CallManager to Device Interface *	CS3(precedence 3) DSCP (011000)	CS3(precedence 3) DSCP (011000)
Connection Monitor Duration *	120	120
Auto Registration Phone Protocol *	SCCP	SCCP
BLF For Call Lists *	Disabled	Disabled
Advertise G.722 Codec *	Enabled	Enabled
Phone Personalization *	0	0

CCAdmin Parameters		
Max List Box Items *	250	250
Max Lookup Items *	1000	1000
Enable Dependency Records *	False	False

Security Parameters		
Cluster Security Mode *	0	3804
CAPF Phone Port *	3804	3804
Authentication Method for API Browser Access *	Basic	Basic
Enable Caching *	False	False

Phone URL Parameters		
URL Authentication	http://172.30.224.20/auth.asp	
URL Directories	http://IPTAPPS-CCM60-PUB:8080/ccmcp/xmldirectory.js	
URL Idle		
URL Idle Time	0	0
URL Information	http://IPTAPPS-CCM60-PUB:8080/ccmcp/GetTelecasterH	
URL Messages		
IP Phone Proxy Address	.	
URL Services	http://IPTAPPS-CCM60-PUB:8080/ccmcp/getservicesmen	

User Search Parameters		
Enable All User Search *	True	True
User Search Limit *	64	64

At the bottom of the page, there are buttons for "Save", "Set to Default", and "Reset". Below these buttons are two informational icons: one with an asterisk indicating required items, and another with two asterisks indicating that the "Set-to-Default" button only applies to modifiable parameters.

Step 2 Scroll down the page to the *Security Parameters* area.

- Step 3** Select **Basic** from the **Authentication Method for API Browser Access** dropdown menu.
- Step 4** Click the **Save** button.

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.

Find and List Phones Related Links: [Actively Logged In Device Report](#)

155 records found

Phone (1 - 25 of 155) Rows per Page: 25

Find Phone where Device Pool begins with icva Find Clear Filter

Device Name(Line)	Description	Device Pool	Device Protocol	Status	IPv4 Address	Copy	Super Copy
LonAicCTI04	InformaCast CTI port	ICVA	SCCP	Registered with qa-ucm105-pub	172.30.227.226		
SEP00115C979921	Auto 105030	ICVA	SCCP	Registered with qa-ucm105-pub	172.30.223.7		
LonAccCTI12	Conference Call CTI port	ICVA	SCCP	Registered with qa-ucm105-pub	172.30.227.226		
LonBcaCTI01	CallAware CTI port	ICVA	SCCP	None	None		
LonBccCTI09	Conference Call CTI port	ICVA	SCCP	Unregistered	172.30.223.3		
JenkCccConf01	Conference Call CTI port (Jenkins C)	ICVA	SCCP	None	None		
LonAccCTI15	Conference Call CTI port	ICVA	SCCP	Registered with qa-ucm105-pub	172.30.227.226		
SEP0026085BE26A	Auto 105190	ICVA	SCCP	Registered with qa-ucm105-pub	172.30.227.74		
LonBicCTI01	InformaCast CTI port	ICVA	SCCP	Registered with qa-ucm105-pub	172.30.223.3		
LonBccCTI12	Conference Call CTI port	ICVA	SCCP	Unregistered	172.30.223.3		
SEP001E138C7D81	Auto 105032	ICVA	SCCP	Registered with qa-ucm105-pub	172.30.227.22		
SEP04FE7F6911B9	Auto 105015	ICVA	SCCP	Registered with qa-ucm105-pub	172.30.227.81		
LonBccCTI11	Conference Call CTI port	ICVA	SCCP	Unregistered	172.30.223.3		
SEP001D45E95D12	Auto 105040	ICVA	SIP	Registered with qa-ucm105-pub	172.30.227.27		
SEP9CAFCAFE72CA	Auto 105035	ICVA	SCCP	Registered with qa-ucm105-pub	172.30.223.5		
LonAccCTI11	Conference Call CTI port	ICVA	SCCP	Registered with qa-ucm105-pub	172.30.227.226		
LonAccCTI14	Conference Call CTI port	ICVA	SCCP	Registered with qa-ucm105-pub	172.30.227.226		
LonBicCTI02	InformaCast CTI port	ICVA	SCCP	Registered with qa-ucm105-pub	172.30.223.3		

Add New Select All Clear All Delete Selected Reset Selected Apply Config to Selected

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.

Device Reset

Reset Restart

Status: Ready

Reset Information

Selected Device: 1 devices selected

If a device is not registered with Cisco Unified Communications Manager, you cannot reset or restart it. If a device is registered, to restart a device without shutting it down, click the **Restart** button. To shut down a device and bring it back up, click the **Reset** button. To return to the previous window without resetting/restarting the device, click **Close**.

Note:
Resetting a gateway/trunk/media devices **drops** any calls in progress that are using that gateway/trunk/media devices. Restarting a gateway/media devices tries to preserve the calls in progress that are using that gateway/media devices, if possible. Other devices wait until calls are complete before restarting or resetting. Resetting/restarting a H323 device does not physically reset/restart the hardware; it only reinitializes the configuration loaded by Cisco Unified Communications Manager.

Reset Restart Close

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.

The screenshot shows the Cisco Unified CM Administration interface. The main heading is 'Find and List Phones'. Below the heading, there is a search bar with a dropdown menu for 'Device Name' and another dropdown for 'begins with'. There are 'Find' and 'Clear Filter' buttons. Below the search bar, a message states: 'No active query. Please enter your search criteria using the options above.' There is also an 'Add New' button.

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.

The screenshot shows the same Cisco Unified CM Administration interface, but now with search results. The search criteria are 'Directory Number' and 'begins with' 105030. The 'Find' button has been clicked. Below the search bar, there is a 'Status' section indicating '1 records found'. There is also a 'Query Information' section with a message: 'Searching on a directory number may show the same device name multiple times depending on the number of lines configured per device.' Below this, there is a table of search results.

Device Name(Line)	Description	Device Pool	Extension	Partition	Device Protocol	Status	IPv4 Address	Copy	Super Copy
SEP00115C979921(1)	Auto 105030	ICVA	105030	ICVA-CTIOoutbound	SCCP	Registered with qa-ucm105-pub			

At the bottom of the table, there are buttons for 'Add New', 'Select All', 'Clear All', 'Delete Selected', 'Reset Selected', and 'Apply Config to Selected'.

- Step 4** Click the **IP address** link in the IPv4 Address column. The Device Information page should open in a new window/tab. If None appears in that column or 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 2-73 for more information).

		Device Information Cisco Systems, Inc. IP Phone CP-7960G (SEP00115C979921)	
Device Information	MAC Address	00115C979921	
Network Configuration	Host Name	SEP00115C979921	
Network Statistics	Phone DN	105030	
Ethernet	App Load ID	P0030801SR02	
Port 1 (Network)	Boot Load ID	PC0303010100	
Port 2 (Access)	Version	8.1(SR.2)	
Port 3 (Phone)	DSP	4.0(5.0)[A0]	
Device Logs	Expansion Module 1		
Debug Display	Expansion Module 2		
Stack Statistics	Hardware Revision	4.3	
Status Messages	Serial Number	INM08241GDV	
Streaming Statistics	Model Number	CP-7960G	
Stream 1	Codec	ADLCodec	
Stream 2	Amps	5V Amp	
	C3PO Revision	2	
	Message Waiting	NO	

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

Cisco Systems, Inc. IP Phone CP-7960G (SEP00115C979921)	
DHCP Server	
BOOTP Server	No
MAC Address	00115C979921
Host Name	SEP00115C979921
Domain Name	singlewire.lan
IP Address	
Subnet Mask	
TFTP Server 1	
Default Router 1	
Default Router 2	
Default Router 3	
Default Router 4	
Default Router 5	
DNS Server 1	
DNS Server 2	
DNS Server 3	
DNS Server 4	
DNS Server 5	
Operational VLAN Id	
Admin. VLAN Id	
CallManager 1	qa-ucm105-pub Active
CallManager 2	
CallManager 3	
CallManager 4	
CallManager 5	
Information URL	http://:8080/ccmcip/GetTelecasterHelpText.jsp
Directories URL	http://:8080/ccmcip/xmlldirectory.jsp
Messages URL	
Services URL	http://:8080/ccmcip/getservicesmenu.jsp
DHCP Enabled	Yes
DHCP Address Released	No
Alternate TFTP	Yes
Erase Configuration	NO
Idle URL	
Idle URL Time	0
Authentication URL	http://:8081/InformaCast/phone/auth
Proxy Server URL	
PC Port Disabled	NO
Web Access	Enabled
Connection Monitor Duration	120
PC VLAN	0
Reverting Focus Priority	Higher

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 2-81. If it does not, see “Set Your Authentication URL” on page 2-80.

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

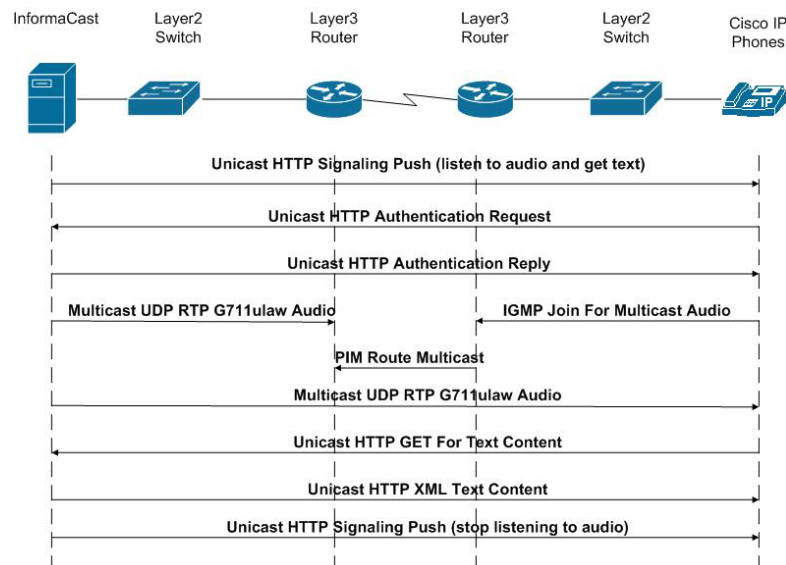
Multicast must be configured in order for InformaCast broadcasts to properly play on your recipients. The following recommendations can also apply:

- 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.

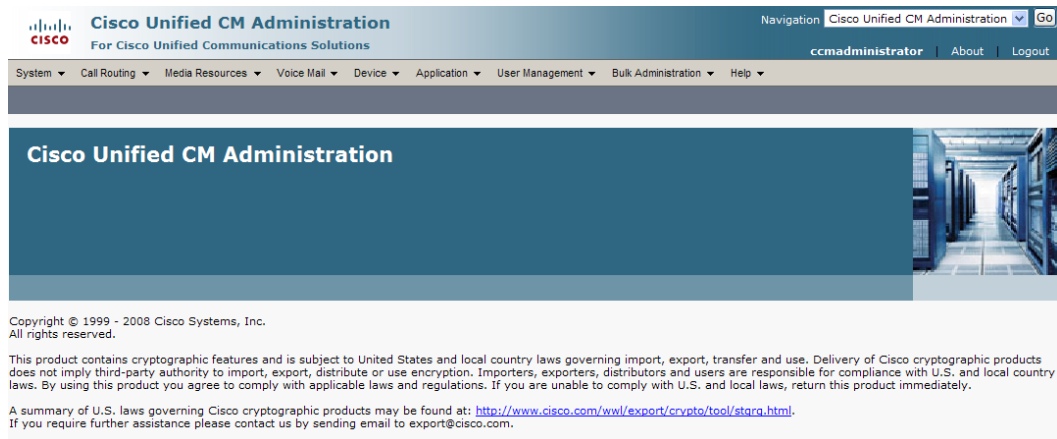


Now that you are familiar with the traffic flow created by InformaCast, you can use a protocol analyzer, such as Wireshark, to sniff the traffic on the network to see that multicast is enabled.

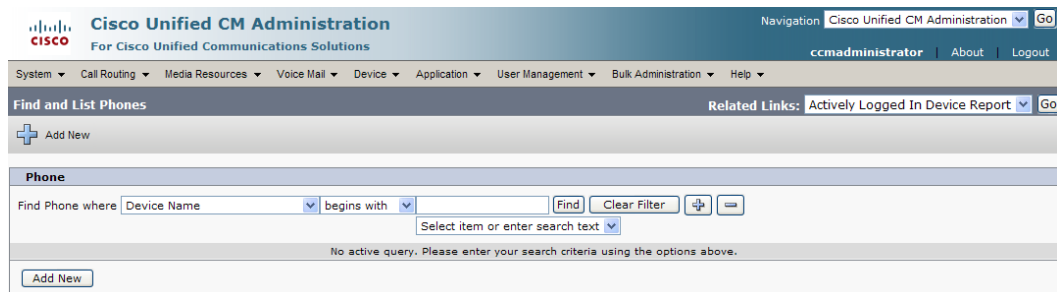
Obtain a Network Traffic Capture

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 Unified Communications Manager'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.

The screenshot shows the Cisco Unified CM Administration interface. At the top, there's a navigation bar with 'Cisco Unified CM Administration' and 'Go' button. Below it, a menu bar includes 'System', 'Call Routing', 'Media Resources', 'Voice Mail', 'Device', 'Application', 'User Management', 'Bulk Administration', and 'Help'. The main header area contains 'Find and List Phones' and 'Related Links: Actively Logged In Device Report'. Below this, there are buttons for 'Add New', 'Select All', 'Clear All', 'Delete Selected', and 'Reset Selected'. A status bar indicates '75 records found'. The main content area is titled 'Phone (1 - 25 of 75)' and shows a search filter for 'Device Name' with 'begins with' selected. A table of phone records is displayed with columns for checkboxes, Device Name, Description, Device Pool, Device Protocol, Status, IP Address, Copy, and Super Copy. The table lists 25 phone records, including models like AT211, ICNick1-6, JessCTI1-2, KatieLC1-4, and RajCTIPort1-4. At the bottom, there are buttons for 'Add New', 'Select All', 'Clear All', 'Delete Selected', and 'Reset Selected', along with a pagination control showing 'Go 1 of 3'.

<input type="checkbox"/>	Device Name(Line) ^	Description	Device Pool	Device Protocol	Status	IP Address	Copy	Super Copy
<input type="checkbox"/>	AT211		Default	SCCP	Registered with iptapps-ccm61pub	172.30.227.211		
<input type="checkbox"/>	ATA0023EBC6AB6A	Auto 60018	Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	ATA23EBC6AB6A01	Auto 60019	Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	CTIFORNICK		Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	ICNick1	ICNick1	Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	ICNick2	ICNick2	Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	ICNick3	ICNick3	Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	ICNick4	ICNick4	Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	ICNick5	ICNick5	Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	ICNick6	ICNick6	Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	JessCTI1	JessCTI1	Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	JessCTI2	JessCTI2	Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	JessRCCCTI		Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	KatieLC1		Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	KatieLC2		Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	KatieLC3		Default	SCCP	Unregistered	172.30.227.200		
<input type="checkbox"/>	KatieLC4		Default	SCCP	Unregistered	172.30.227.200		
<input type="checkbox"/>	PeteCTI1	PeteCTI1	Default	SCCP	Registered with iptapps-ccm61pub	172.30.227.211		
<input type="checkbox"/>	PeteCTI2	PeteCTI2	Default	SCCP	Registered with iptapps-ccm61pub	172.30.227.211		
<input type="checkbox"/>	RajCallAlert	RajCallAlert	RajInformaCast	SCCP	Unknown	Unknown		
<input type="checkbox"/>	RajCTIPort	RajCTIPort	RajInformaCast	SCCP	Unknown	Unknown		
<input type="checkbox"/>	RajCTIPort2	RajCTIPort2	RajInformaCast	SCCP	Unknown	Unknown		
<input type="checkbox"/>	RajCTIPort3	RajCTIPort3	RajInformaCast	SCCP	Unknown	Unknown		
<input type="checkbox"/>	RajCTIPort4	RajCTIPort4	RajInformaCast	SCCP	Unknown	Unknown		
<input type="checkbox"/>	SEP0004F2E67F44	Auto 60037	Default	SCCP	Unknown	Unknown		

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

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration

ccmadministrator | About | Logout

System | Call Routing | Media Resources | Voice Mail | Device | Application | User Management | Bulk Administration | Help

Phone Configuration Related Links: [Back To Find/List](#)

Status
Status: Ready

Association Information

1	Line [1] - 60028 (no partition)
2	None
3	Add a new SD
4	Add a new SD
5	Add a new SD
6	Add a new SD
7	Add a new SD
8	Add a new SD
9	Add a new SD
10	Add a new SD
11	Add a new SD
12	Add a new SD
----- Unassigned Associated Items -----	
13	Line [2] - Add a new DN
14	Add a new SD
15	Privacy
16	None

Phone Type
Product Type: Cisco 7937
Device Protocol: SCCP

Device Information

Registration	Unknown
IP Address	Unknown
MAC Address*	0004F2E67F44
Description	Auto 60028
Device Pool*	Default View Details
Common Device Configuration	< None > View Details
Phone Button Template*	-- Not Selected --
Softkey Template	< None >
Common Phone Profile*	Standard Common Phone Profile
Calling Search Space	Phones
Media Resource Group List	< None >
User Hold MOH Audio Source	< None >
Network Hold MOH Audio Source	< None >
Location*	Hub_None
User Locale	< None >
Network Locale	< None >
Built In Bridge*	Default
Privacy*	Default
Device Mobility Mode*	Default View Current Device Mobility Settings
Owner User ID	< None >
Phone Load Name	

Ignore Presentation Indicators (internal calls only)
 Allow Control of Device from CTI
 Logged Into Hunt Group
 Remote Device

Product Specific Configuration Layout ?

Settings Access*	Enabled
Gratuitous ARP*	Enabled
PC Voice VLAN Access*	Enabled
Web Access*	Enabled
Load Server	
SSH Access*	Disabled

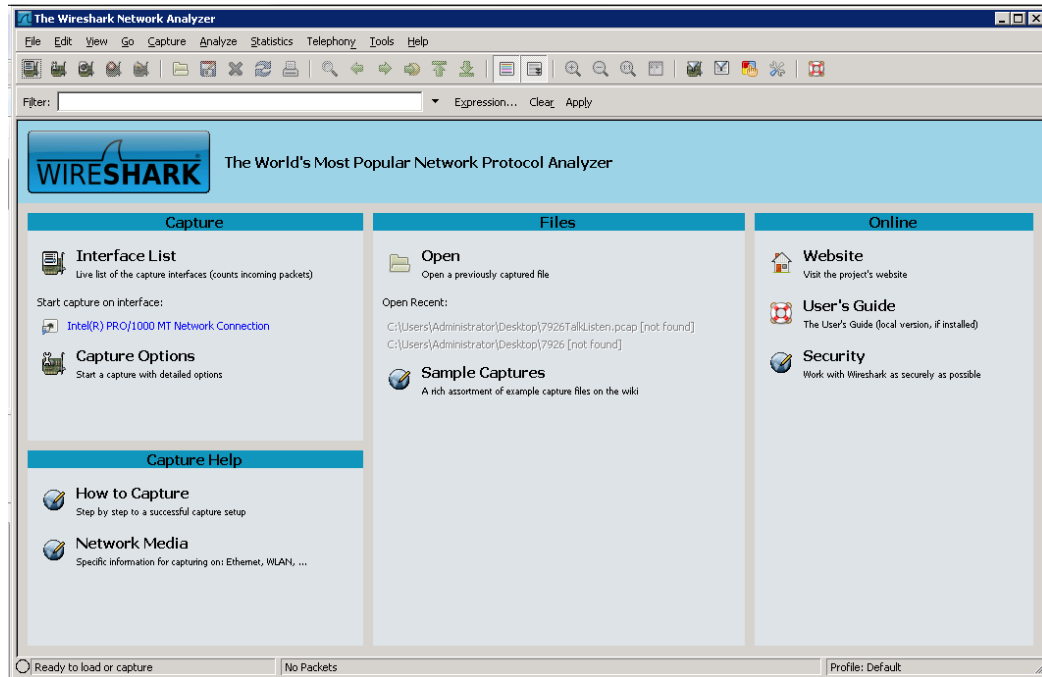
Info *- indicates required item.
Info ** - Device reset is not required for changes to Packet Capture Mode and Packet Capture Duration.
Info ***Note: Security Profile Contains Addition CAPF Settings.

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:

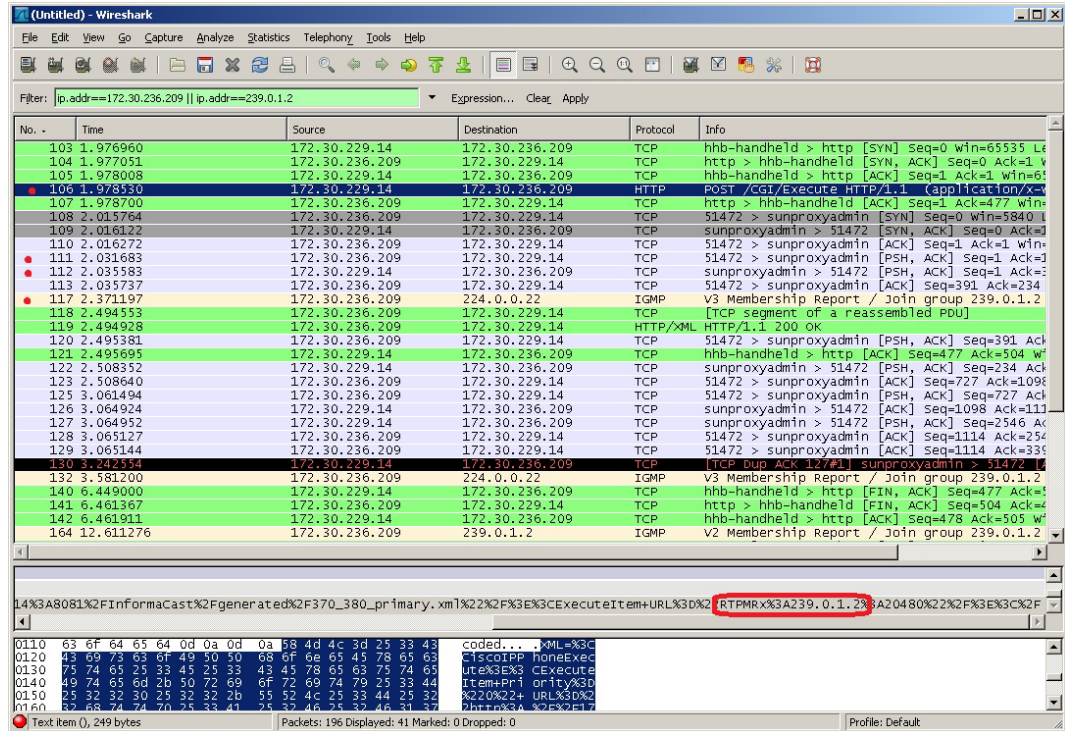
- A unicast HTTP command from InformaCast to the recipient to join the multicast group
- Successful authentication
- An IGMP join from the recipient to the multicast group
- A multicast audio stream

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.

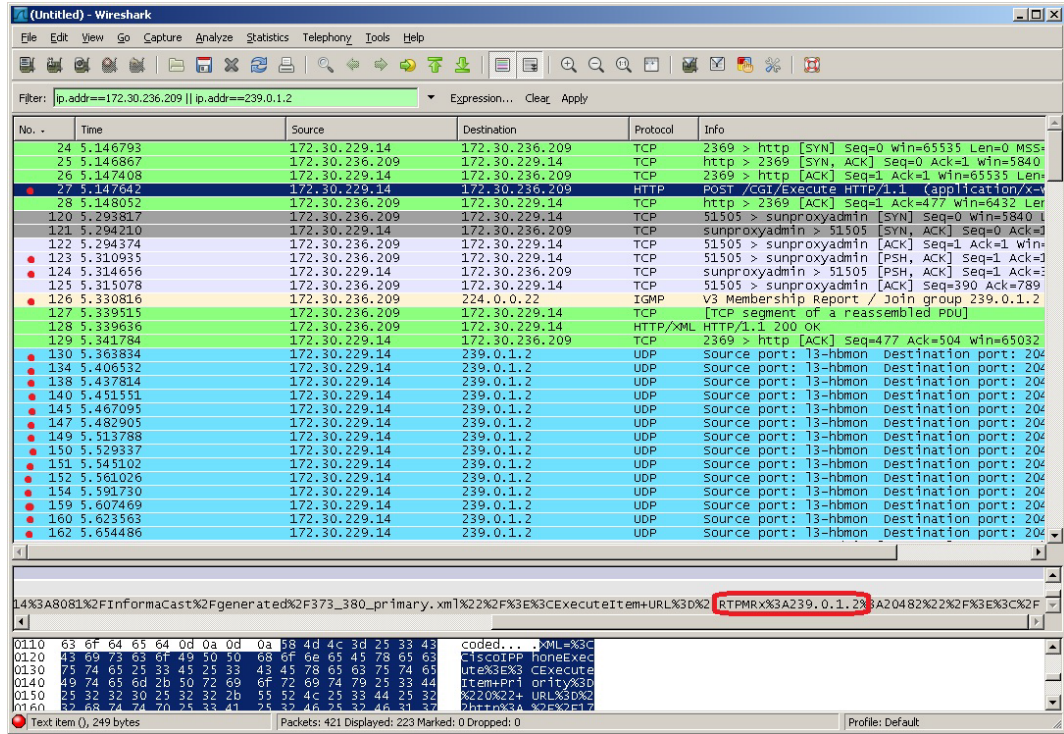
Each of the things to look for are marked with red in the following graphic.



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.

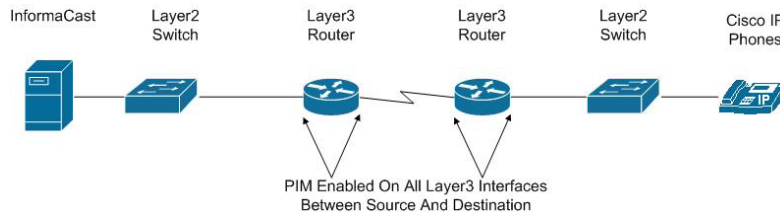


If multicast isn't working, troubleshoot the problems singly by frame(s). Work with your network administrator to configure multicast appropriately.

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.

```

Tera Term Web 3.1 - 172.30.224.1 VT
File Edit Setup Web Control Window Help
IPTAPPS-SW3560-2#
IPTAPPS-SW3560-2#sh run int vlan 236
Building configuration...
Current configuration : 156 bytes
!
interface Vlan236
 description Voice VLAN - Cisco IP Phones
 ip address 172.30.236.1 255.255.255.0
 ip helper-address 172.30.224.21
 no ip redirects
end
IPTAPPS-SW3560-2#
IPTAPPS-SW3560-2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
IPTAPPS-SW3560-2(config)#int vlan 236
IPTAPPS-SW3560-2(config-if)#ip pim sparse-dense
IPTAPPS-SW3560-2(config-if)#ip igmp version 3
IPTAPPS-SW3560-2(config-if)#end
IPTAPPS-SW3560-2#
IPTAPPS-SW3560-2#sh run int vlan 236
Building configuration...
Current configuration : 201 bytes
!
interface Vlan236
 description Voice VLAN - Cisco IP Phones
 ip address 172.30.236.1 255.255.255.0
 ip helper-address 172.30.224.21
 no ip redirects
 ip pim sparse-dense-mode
 ip igmp version 3
end
IPTAPPS-SW3560-2#

```

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

Verify your MPLS Provider Routes Multicast

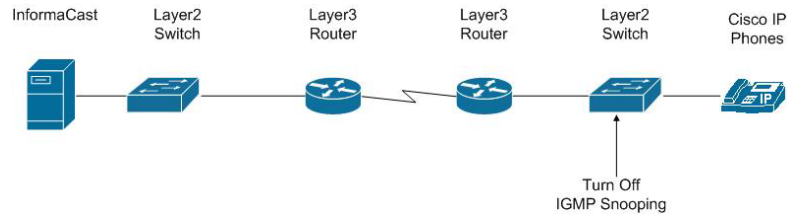
When InformaCast audio broadcasts are successful at the same location where InformaCast is located, but remote locations do not receive the audio, that indicates that the multicast audio traffic is not routing across the WAN link. Many Multiprotocol Label Switching (MPLS) network providers will not route 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

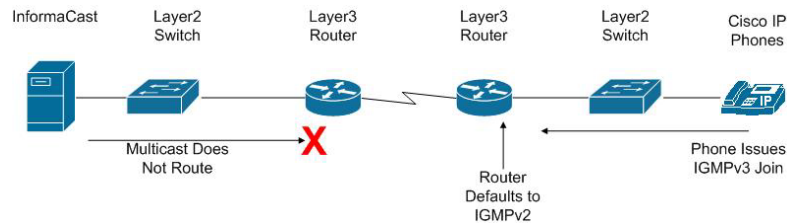
IGMP snooping has been seen to cause issues with Layer 2 switches. For this reason, if there are issues receiving the multicast audio stream at the phones, it would be worth testing if turning off IGMP snooping on the switches where phones are connected solves the problem. The following graphic illustrates 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 2-88). 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).

The screenshot shows a Wireshark packet capture with a filter of `ip.addr==172.30.236.209 || ip.addr==239.0.1.2`. The packet list pane shows several packets, with packet 110 (IGMP v3 Membership Report) circled in red. The packet details pane shows the following structure:

```

14#3A8081%2FInformaCast%2Fgenerated%2F370_380_pr1mary.xml%22%2F%3E%3CEXecuteItem%3D%22RTPMRX%3A239.0.1.2%3A20480%22%2F%3E%3CK%2F

```

The packet bytes pane shows the raw data of the IGMPv3 report, including the group address 239.0.1.2 and the report type 3 (Membership Report).

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.

```

Tera Term Web 3.1 - 172.30.224.1 VI
File Edit Setup Web Control Window Help
IPTAPPS-SW3560-2#
IPTAPPS-SW3560-2#sh run int vlan 236
Building configuration...

Current configuration : 156 bytes
!
interface Vlan236
 description Voice VLAN - Cisco IP Phones
 ip address 172.30.236.1 255.255.255.0
 ip helper-address 172.30.224.21
 no ip redirects
end

IPTAPPS-SW3560-2#
IPTAPPS-SW3560-2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
IPTAPPS-SW3560-2(config)#int vlan 236
IPTAPPS-SW3560-2(config-if)#ip pim sparse-dense
IPTAPPS-SW3560-2(config-if)#ip igmp version 3
IPTAPPS-SW3560-2(config-if)#end
IPTAPPS-SW3560-2#
IPTAPPS-SW3560-2#sh run int vlan 236
Building configuration...

Current configuration : 201 bytes
!
interface Vlan236
 description Voice VLAN - Cisco IP Phones
 ip address 172.30.236.1 255.255.255.0
 ip helper-address 172.30.224.21
 no ip redirects
 ip pim sparse-dense-mode
 ip igmp version 3
end
IPTAPPS-SW3560-2#

```

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



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
- “View Your License Key” on page 3-6

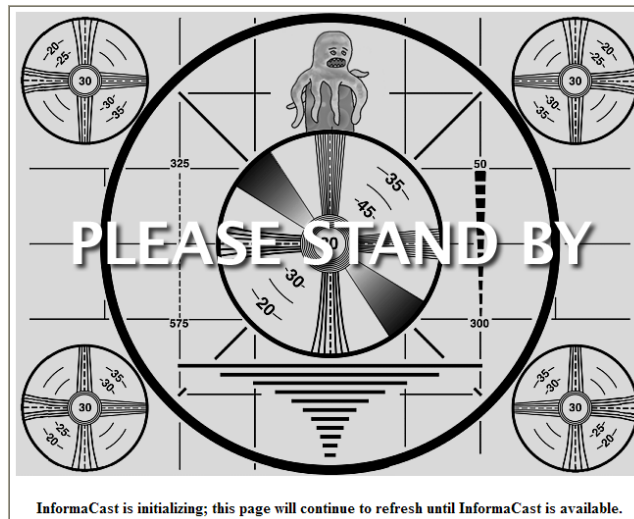
Log into InformaCast for the First Time

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 Unified Communications Manager, 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 your password in the **Password** field. The **Password** field is also case sensitive.

**Note**

These are your default credentials. “Change the Application Administrator’s Password” on page 6-2 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.

InformaCast®
basic paging
Provided by OEM Agreement with Cisco

Advanced Notification
Buy Try Learn Home Messages Recipients Speakers Bells Admin Plugins Help
Log Out

Fill out the form below to get started.

First Name (Business Owner or Contact) *

Last Name (Business Owner or Contact) *

Email Address (Business Owner or Contact) *

Phone Number (Business Owner or Contact) *

Company Name *

What best describes your role? *

Please choose one...

Get Started

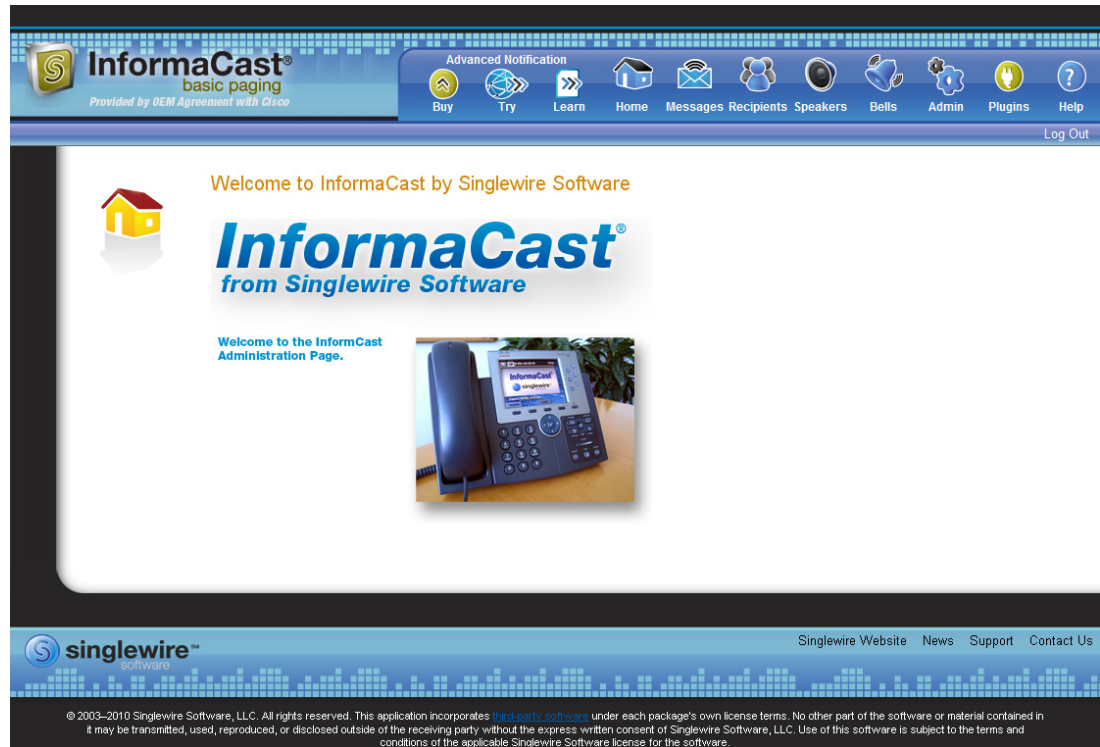
singlewire™
Singlewire Website News Support Contact Us

© 2003–2010 Singlewire Software, LLC. All rights reserved. This application incorporates [third party software](#) under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software.

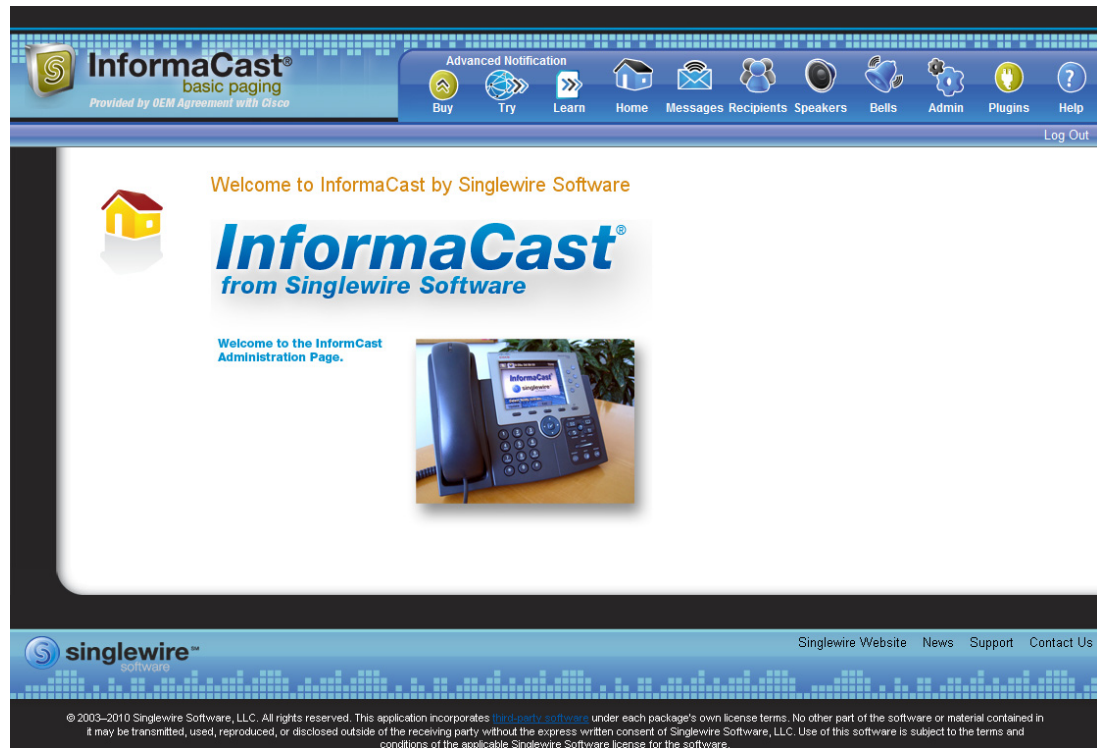
**Note**

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 “View Your License Key” on page 3-6.



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



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 4-38

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.

InformaCast® basic paging
Provided by OEM Agreement with Cisco

Advanced Notification
Buy Try Learn Home Messages Recipients Speakers Bells Admin Plugins Help Log Out

Admin | Overview

Welcome to the InformaCast configuration overview page. For specific configuration tasks, please use the "Admin" menu.

InformaCast Server

Version	11.5.1 Basic Paging license
Start Time	2015-07-23 09:30:34
Current Time	2015-07-23 13:40:35
Application Mode	Stand-alone

Cisco Unified Communications Manager

Cluster Version	Default configuration	10.5.2.12901-1
JTAPI Version	Cisco Jtapi version 10.5(2.12900)-1 Release	
Send Commands to Phones by JTAPI	false	

CTI Route Points

Name	DN	State
RP02	8881212	IN_SERVICE
RP01	9101000	IN_SERVICE

SIP Calls

There are no SIP calls.

Backup

Backup Activated	false
Next Scheduled Backup	
Backup Location	/usr/local/singlewire/InformaCast/backup

Phone Updates

Last Attempted Phone Rebuild	2015-07-23 13:13:00
Last Successful Phone Rebuild	2015-07-23 13:13:16
Last Attempted Phone Refresh	2015-07-23 13:21:00
Last Successful Phone Refresh	2015-07-23 13:21:00
Number of Phones Retrieved	26
Number of Phones Used / Licensed	0 / 50
Next Phone Rebuild	2015-07-23 14:13:00
Phone Refresh Interval (minutes)	23

SIP User Agent Status

User Agent is running

Multicast Ports

Number of Multicast Ports Configured	301
Number of Multicast Ports Used by Audio Broadcasts	0
Number of Multicast Ports Used by Talk and Listen Messages	0
Number of Multicast Ports Unused	301

singlewire software
Singlewire Website News Support Contact Us

© 2003–2015 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software.

Configure Your Default Unified Communications Manager 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 Unified Communications Manager cluster. These steps should be performed by your Unified Communications Manager administrator.



Warning

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

- Step 1** Go to **Admin | Telephony | Cisco Unified Communications Manager Cluster**. The Cisco Unified Communications Manager Cluster page appears.

The screenshot shows the InformaCast web interface. The top navigation bar includes links for Buy, Try, Learn, Home, Messages, Recipients, Speakers, Bells, Admin, Plugins, and Help. The main content area displays the breadcrumb path: Admin | Telephony | Cisco Unified Communications Manager Cluster. Below this, there is a table with one row: Default configuration, with an EDIT button. The footer contains the Singlewire logo and copyright information.

Cisco Unified Communications Manager Cluster Description	Action
Default configuration	EDIT

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

InformaCast[®] basic paging
Provided by OEM Agreement with Cisco

Advanced Notification
Buy Try Learn Home Messages Recipients Speakers Bells Admin Plugins Help
Log Out

Admin | Telephony | Cisco Unified Communications Manager Cluster | **Edit Telephony Configuration**

Telephony Configuration

Unified Communications Manager Cluster Description: Default configuration (required)

Unified Communications Manager Application User: APPLICATION_USER (required)

Unified Communications Manager Application Password:

Confirm Application Password:

Use Application User for AXL

Unified Communications Manager AXL User: AXL_USER (required)

Unified Communications Manager AXL Password:

Confirm AXL Password:

AXL IP Address(es):

Unified Communications Manager IP Address(es): 127.0.0.1 (required)

Choose SNMP version:
 SNMP v2 (required)
 SNMP v3

SNMP v2 Community Name:

Confirm SNMP v2 Community Name:

XML Push Authentication

If you are not using JTAPI to activate phones during broadcasts or if this is not your primary cluster, make sure the **URL Authentication** parameter for the Unified Communications Manager in this cluster (found in the **Phone URL Parameters** section of the **System | Enterprise Parameters** page) is set to the following value:

http:// :8081/InformaCast/phone/auth

Optionally, you can also tell InformaCast where to send authentication requests for commands that aren't coming from InformaCast. You only need to do this if, before installing InformaCast, you had set this Unified Communications Manager parameter to a non standard value. In such cases, copy the current Unified Communications Manager setting into the field below, before changing it to the value shown above.

Next Authentication URL:

If empty, non-InformaCast authentication requests from phones in this cluster will be sent to the default Unified Communications Manager authentication page, http://172.30.228.98/ccmciip/authenticate.jsp

Note: If you changed any Telephony Configuration settings, be sure to refresh the Recipient Group list before attempting to send a broadcast.

singlewire software
Singlewire Website News Support Contact Us

© 2003–2015 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software.

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

Step 4 Enter the username of the application user that you created earlier into the **Unified Communications Manager Application User** field (see Step 3 on page 2-71).

Step 5 Enter the password of the application user that you created earlier into the **Unified Communications Manager Application Password** and **Confirm Application Password** fields (see Step 4 on page 2-71). 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 Unified Communications Manager, which may pose a security risk. To close this potential security hole, your Unified Communications Manager 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 Unified Communications Manager.

**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 Unified Communications Manager administrator's username in the **Unified Communications Manager AXL User** field.

**Note**

This is the same username you use to access the Unified Communications Manager Administrator interface, often **CCMAdministrator**.

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

Step b. Enter the Unified Communications Manager administrator's password in the **Unified 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 Unified Communications Manager 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 Unified Communications Manager, 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 Unified Communications Manager server(s) in the **Unified Communications Manager IP Address(es)** field, which will be used when establishing a CTI (JTAPI) connection with Unified Communications Manager. You can enter any and all Unified Communications Managers running the CTI Manager service. Use the numeric IP addresses rather than DNS names.

When InformaCast needs to interact with the Unified Communications Manager, 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** Select the **SNMP v2** or **SNMP v3** radio button, depending on the version of SNMP you're using. The **SNMP v2** radio button is selected by default. If you select the **SNMP v3** radio button, the Edit Telephony Configuration page refreshes with new fields.

Choose SNMP version: SNMP v2 SNMP v3 (required)

SNMP v3 Username:

SNMP v3 Authentication Password:

Confirm SNMP v3 Authentication Password:

SNMP v3 Privacy Password:

Confirm SNMP v3 Privacy Password:

- Step 10** Enter the correct information depending on your version of SNMP:

- **SNMP v2.** Enter the name of your community string in the **SNMP v2 Community Name** and **Confirm SNMP v2 Community Name** fields. You created this in “Create an InformaCast SNMP v2 Community String” on page 2-49. The community name is entered twice to double-check for typing errors since its value is masked.
- **SNMP v3.** Enter your SNMP v3 user's name in the **SNMP v3 Username** field, your authentication password in the **SNMP v3 Authentication Password** and **Confirm SNMP v3 Authentication Password** fields, and your privacy password in the **SNMP v3 Privacy Password** and **Confirm SNMP v3 Privacy Password** fields. You created this user in “Create an SNMP v3 User” on page 2-51.

- Step 11** Enter the original value of Unified Communications Manager's **URL Authentication** field in the **Next Authentication URL** field. You made note of this in Step 3 on page 2-81.
- Step 12** Click the **Update** button. You will be redirected to the Cisco Unified Communications Manager Cluster page.

The screenshot shows the InformaCast Admin interface. The top navigation bar includes 'Buy', 'Try', 'Learn', 'Home', 'Messages', 'Recipients', 'Speakers', 'Bells', 'Admin', 'Plugins', and 'Help'. The main content area is titled 'Admin | Telephony | Cisco Unified Communications Manager Cluster'. A message states: 'Configuration changes saved. Remember to update your Recipient Groups to verify connectivity and membership.' Below this, it says 'Cisco Unified Communications Manager cluster whose phones will receive InformaCast broadcasts'. A table lists the cluster description and an 'EDIT' button.

Cisco Unified Communications Manager Cluster Description	Action
Default configuration	EDIT

Note: You must [refresh the Recipient Group list](#) before attempting to send a broadcast.

- Step 13** Click the **refresh the Recipient Group list** link. You will be redirected to the Edit Recipient Groups page.

The screenshot shows the InformaCast Admin interface for 'Recipients | Edit Recipient Groups'. The top navigation bar is the same as in the previous screenshot. The main content area has a 'Recipients' icon and several buttons: 'UPDATE' (Discover current IP phone information from Cisco Unified Communications Manager (may be time consuming)), 'SHOW ALL' (Show Defunct Phones), and 'PREVIOUS' (Page 1 of 1). Below these is a table with columns 'Name', 'Phones', and 'Action'.

Name	Phones	Action
(All Recipients)	26	EDIT COPY DELETE

- Step 14** Click the **Update** button to refresh InformaCast's information pertaining to recipient groups. You will be redirected to the Discover Recipient Groups page.

InformaCast® basic paging
Provided by OEM Agreement with Cisco

Advanced Notification
Buy Try Learn Home Messages Recipients Speakers Bells Admin Plugins Help

Log Out

Recipients | Edit Recipient Groups | Discover Recipient Groups

! Do you want to discover current IP phone information from Cisco Unified Communications Manager?

This command will query the Cisco Unified Communications Manager server to learn the IP addresses of all the phones that belong in the recipient groups you've set up. You only need to do this if you know you've just made changes to the Cisco Unified Communications Manager configuration that affect your phones and want those changes to be immediately detected by InformaCast.

When you run this command, it may take many seconds or even several minutes to complete. While it is running, you will not see any response in your web browser (you'll just see that the page is loading). This is normal; do not click **Cancel** or try to reload the page. Once the command has completed, you will see a confirmation message.

If you do actually want to run this command, click **Update** again now. Otherwise, you may click **Cancel** to return to the previous screen.

CANCEL UPDATE

singlewire™
Singlewire Website News Support Contact Us

© 2003–2010 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software.

- Step 15** 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.

InformaCast® basic paging
Provided by OEM Agreement with Cisco

Advanced Notification
Buy Try Learn Home Messages Recipients Speakers Bells Admin Plugins Help

Log Out

Recipients | Edit Recipient Groups

Recipient group members updated

UPDATE Discover current IP phone information from Cisco Unified Communications Manager (may be time consuming).

SHOW ALL Show Defunct Phones

PREVIOUS Page 1 of 1 NEXT Jump to page: GO Show 50 results per page Filter: ADD

Name	Phones	Action
(All Recipients)	26	EDIT COPY DELETE

singlewire™
Singlewire Website News Support Contact Us

© 2003–2010 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software.

Edit Your Default Cluster

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

- Step 1** Go to **Admin | Telephony | Cisco Unified Communications Manager Cluster**. The Cisco Unified Communications Manager Cluster page appears.

The screenshot shows the InformaCast web interface. At the top left is the InformaCast logo with the text "basic paging" and "Provided by OEM Agreement with Cisco". To the right is a navigation bar with icons for Buy, Try, Learn, Home, Messages, Recipients, Speakers, Bells, Admin, Plugins, and Help. Below the navigation bar is a breadcrumb trail: "Admin | Telephony | Cisco Unified Communications Manager Cluster". The main content area features a gear icon and the text "Cisco Unified Communications Manager cluster whose phones will receive InformaCast broadcasts". Below this is a table with two columns: "Cisco Unified Communications Manager Cluster Description" and "Action". The table contains one row with the description "Default configuration" and an "EDIT" button with a pencil icon.

Cisco Unified Communications Manager Cluster Description	Action
Default configuration	EDIT

At the bottom of the page, there is a footer with the Singlewire logo and the text "Singlewire Website News Support Contact Us". Below the footer is a copyright notice: "© 2003-2010 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software."

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

InformaCast®
basic paging
Provided by OEM Agreement with Cisco

Advanced Notification
Buy Try Learn Home Messages Recipients Speakers Bells Admin Plugins Help
Log Out

Admin | Telephony | Cisco Unified Communications Manager Cluster | Edit Telephony Configuration

Telephony Configuration

Primary Unified Communications Manager Cluster: Yes

Unified Communications Manager Cluster Description: Default configuration (required)

Unified Communications Manager Application User: ICVA (required)

Unified Communications Manager Application Password:

Confirm Application Password:

Use Application User for AXL

Unified Communications Manager AXL User: ccmadministrator (required)

Unified Communications Manager AXL Password:

Confirm AXL Password:

AXL IP Address(es):

Unified Communications Manager IP Address(es): (required)

Choose SNMP version: SNMP v2 (required) SNMP v3

SNMP v2 Community Name:

Confirm SNMP v2 Community Name:

XML Push Authentication

Make sure the **URL Authentication** parameter for the Communications Manager in this cluster (found in the **Phone URL Parameters** section of the **System | Enterprise Parameters** page) is set to the following value:

`http://172.30.227.201:8081/InformaCast/phone/auth`

Optionally, you can also tell InformaCast where to send authentication requests for commands that aren't coming from InformaCast. You only need to do this if, before installing InformaCast, you had set this Communications Manager parameter to a non standard value. In such cases, copy the current Communications Manager setting into the field below, before changing it to the value shown above.

Next Authentication URL:

If empty, non-InformaCast authentication requests from phones in this cluster will be sent to the default Communications Manager authentication page, `http://172.30.229.32/ccmcp/authenticate.jsp`

Note: If you changed any Telephony Configuration settings, be sure to refresh the Recipient Group list before attempting to send a broadcast.

singlewire™ software
Singlewire Website News Support Contact Us

© 2003–2010 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software.

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 Unified Communications Manager.

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.

The screenshot shows the InformaCast basic paging interface. The top navigation bar includes links for Buy, Try, Learn, Home, Messages, Recipients, Speakers, Bells, Admin, Plugins, and Help. The main content area is titled 'Recipients | Edit Recipient Groups' and features a table with the following data:

Name	Phones	Action
(All Recipients)	26	EDIT COPY DELETE

Additional interface elements include an 'UPDATE' button with a tooltip 'Discover current IP phone information from Cisco Unified Communications Manager (may be time consuming)', a 'SHOW ALL' button with a tooltip 'Show Defunct Phones', and a pagination control showing 'Page 1 of 1' and 'Show 50 results per page'. The footer contains the Singlewire logo and copyright information: '© 2003–2011 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software.'

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

The screenshot shows the 'Add Recipient Group' page in the InformaCast interface. At the top, there is a navigation bar with icons for Buy, Try, Learn, Home, Messages, Recipients, Speakers, Bells, Admin, Plugins, and Help. Below this, the page title is 'Recipients | Edit Recipient Groups | Add Recipient Group'. The main form has a 'Name' field (required) and a 'Tags' field with an 'Add A Tag' dropdown. Underneath, the 'Select Recipients' section offers four options: 'Individually', 'Filter with Recipient Groups', 'Filter with Rules', and 'Exclusions', each with an 'EDIT' link. A note states: 'Exclusions are only available when the Recipient Group is Filtered by Recipient Groups or Rules.' At the bottom of the form are 'VIEW', 'CANCEL', and 'UPDATE' buttons. The footer includes the Singlewire logo and copyright text: '© 2003–2011 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software.'

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 4-35). Existing tags will appear in the **Add a Tag** dropdown menu on the Add Recipient Group page.

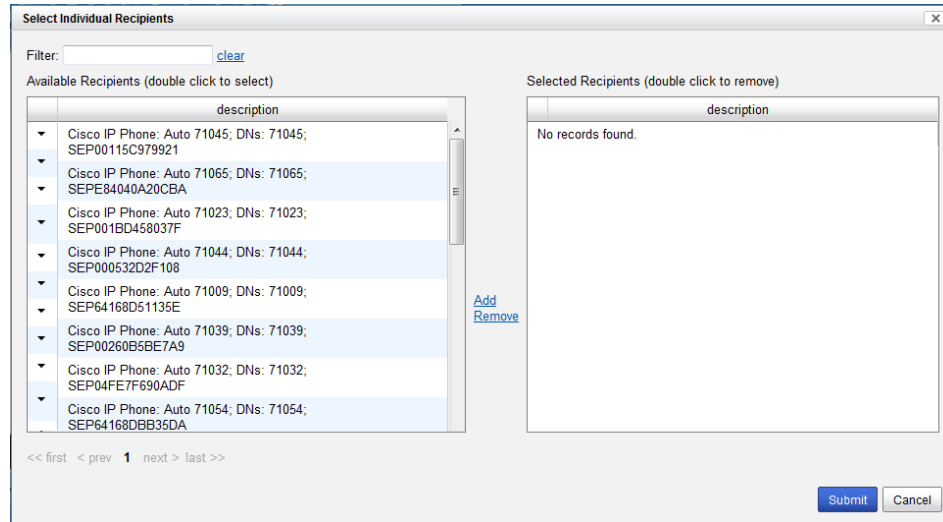
Decide whether you will add members to the group by selecting individual recipients, selecting existing recipient groups, or making rules:

- 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 Unified Communications Manager 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 Unified Communications Manager.

Matching Parameter	Description
Description	<p>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.</p> <p>The text you enter will be compared against the Device Description entries of phones registered with your Unified Communications Manager. 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.</p>
Directory Numbers	Phones that match the supplied phone number(s) assigned to them in Unified Communications Manager.
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 be 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 Unified Communications Manager.

- 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.

The screenshot displays the 'Add Recipient Group' interface in InformaCast. At the top, there's a navigation bar with icons for Buy, Try, Learn, Home, Messages, Recipients, Speakers, Bells, Admin, Plugins, and Help. The main content area has a breadcrumb trail: 'Recipients | Edit Recipient Groups | Add Recipient Group'. A form is present with a 'Name' field containing 'Humanities' and a 'Tags' field with an 'Add A Tag' button. Below this is the 'Select Recipients' section, which includes several options: 'Individually' (checked), 'Filter with Recipient Groups' (checked), 'Filter with Rules' (unchecked), and 'Exclusions' (unchecked). The 'Filter with Recipient Groups' option is expanded, showing a list of recipients: 'Cisco IP Phone: pl Site2 7960; DN: 5944, 5944; SEP00070E958C76', 'English', and 'History'. At the bottom of the form are three buttons: 'VIEW', 'CANCEL', and 'UPDATE'. The footer contains the Singlewire logo and copyright information.

- 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.

The screenshot displays the InformaCast basic paging web interface. At the top, there is a navigation bar with the InformaCast logo and a menu of icons for 'Buy', 'Try', 'Learn', 'Home', 'Messages', 'Recipients', 'Speakers', 'Bells', 'Admin', 'Plugins', and 'Help'. Below the navigation bar, the page title is 'Recipients | Edit Recipient Groups | Add Recipient Group'. The main form area contains the following elements:

- Name:** Humanities (required)
- Tags:** [] Add A Tag [v]
- Select Recipients:**
 - Individually [EDIT] [↗]
 - Filter with Recipient Groups [EDIT] [↗]
 - Filter with Rules
 - Logical Expression: disabled
 - 1 InformaCast Device Type [v] Does [v] Contain [v] [] Ignore Case [v] [REMOVE] [↗]
 - [ADD] [↗]
 - Exclusions [EDIT] [↗]

At the bottom of the form, there are three buttons: [VIEW] [↗], [CANCEL] [✕], and [UPDATE] [↗]. The footer of the page includes the Singlewire logo and copyright information: © 2003–2011 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software.



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 Unified Communications Manager 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 Unified Communications Manager server.
Can Display Text	Recipients that match (or don't match) in their ability to display text. ^b
Description	<p>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.</p> <p>The text you enter will be compared against the Device Description entries of phones registered with your Unified Communications Manager server. Any recipients whose descriptions match with the rule you've specified will be considered part of the recipient group.</p>
Directory Numbers	Phones that match (or don't match) the supplied phone number(s) assigned to them in the Unified Communications Manager 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 4-38 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 be 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 Unified Communications Manager.
Profile Description	Phones that match (or don't match) the Unified Communications Manager'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 4-38 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

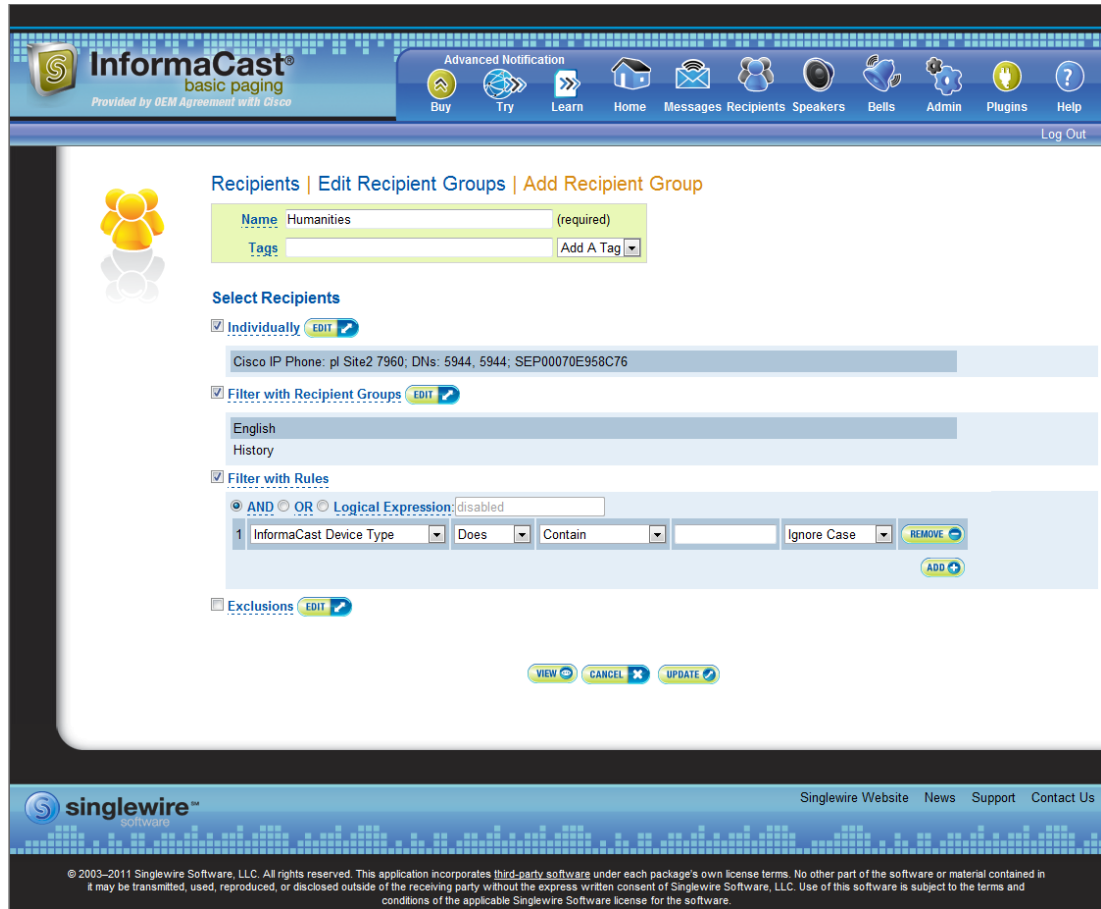
Use the steps in the following section to add exclusions to a recipient group, which allow recipients that had been included in a recipient group by a certain rule or through a recipient group to now be excluded.

- 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).

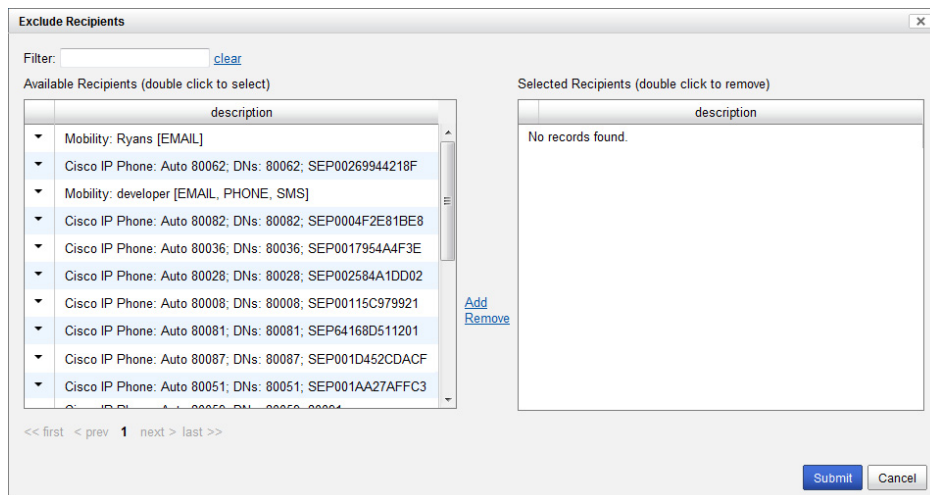


Note The Exclusions checkbox is only available if you select multiple existing recipient groups or create rules.

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 Unified Communications Manager 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 Unified Communications Manager server.
Description	<p>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.</p> <p>The text you enter will be compared against the Device Description entries of phones registered with your Unified Communications Manager server</p>
Directory Numbers	Phones that match the supplied phone number(s) assigned to them in the Unified Communications Manager 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 Unified Communications Manager.

- 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.

The screenshot shows the InformaCast basic paging configuration page. At the top, there is a navigation bar with icons for Buy, Try, Learn, Home, Messages, Recipients, Speakers, Bells, Admin, Plugins, and Help. The main content area is titled "Recipients | Edit Recipient Groups | Add Recipient Group". Below the title, there are input fields for "Name" (set to "Humanities") and "Tags" (with an "Add A Tag" button). The "Select Recipients" section includes three checked options: "Individually" (with an "EDIT" link), "Filter with Recipient Groups" (with an "EDIT" link), and "Filter with Rules" (with an "EDIT" link). Under "Filter with Rules", a rule is defined: "1 InformaCast Device Type Does Contain phone Ignore Case" with a "REMOVE" button and an "ADD" button. Below this, the "Exclusions" section is checked and contains one exclusion: "Cisco IP Phone: Auto 80082; DNs: 80082; SEP0004F2E81BE8". At the bottom of the form, there are "VIEW", "CANCEL", and "UPDATE" buttons. The footer of the page includes the Singlewire logo and copyright information.

- 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.

The screenshot displays the InformaCast interface for editing recipient groups. At the top, there's a navigation bar with icons for Buy, Try, Learn, Home, Messages, Recipients, Speakers, Bells, Admin, Plugins, and Help. The main content area is titled 'Recipients | Edit Recipient Groups'. It features a table with the following data:

Name	Phones	Action
(All Recipients)	1	[EDIT] [COPY] [DELETE]
English	1	[EDIT] [COPY] [DELETE]
History	8	[EDIT] [COPY] [DELETE]
Humanities	10	[EDIT] [COPY] [DELETE]

Below the table, there are controls for 'Page 1 of 1', 'Jump to page:', 'GO', 'Show 50 results per page', and 'Filter:'. Above the table, there are buttons for 'UPDATE' (with a checkmark), 'SHOW ALL', and 'ADD'. Text next to the 'UPDATE' button reads: 'Discover current IP phone information from Cisco Unified Communications Manager (may be time consuming)'. Another button says 'Show Defunct Phones'. The footer includes the Singlewire logo and copyright information: '© 2003–2011 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software.'

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

The screenshot displays the 'Edit Recipient Group' interface. At the top, there's a navigation bar with 'InformaCast basic paging' and a 'Log Out' link. Below the navigation bar, the page title is 'Recipients | Edit Recipient Groups | Edit Recipient Group'. The main content area includes:

- Name:** Humanities (required)
- Tags:** Add A Tag
- Select Recipients:**
 - Individually** (EDIT)
 - Filter with Recipient Groups** (EDIT)
 - Filter with Rules**
 - Logical Expression: disabled
 - 1 InformaCast Device Type Does Contain phone Ignore Case (REMOVE)
 - (ADD)
- Exclusions:**
 - (EDIT)
 - Cisco IP Phone: Auto 80082; DN: 80082; SEP0004F2E81BE8

At the bottom of the form area, there are buttons for 'VIEW', 'CANCEL', and 'UPDATE'. The footer contains the Singlewire logo and copyright information.

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.

The screenshot shows the InformaCast basic paging web interface. The top navigation bar includes 'Recipients' and 'Edit Recipient Groups'. Below the navigation bar, there are several action buttons: 'UPDATE' (Discover current IP phone information from Cisco Unified Communications Manager), 'SHOW ALL' (Show Defunct Phones), and 'ADD'. A table lists recipient groups with columns for 'Name', 'Phones', and 'Action'. The table contains four rows: '(All Recipients)', 'English', 'History', and 'Humanities'. Each row has a 'Phones' count and three action buttons: 'EDIT', 'COPY', and 'DELETE'. The bottom of the page features the Singlewire logo and copyright information.

Name	Phones	Action
(All Recipients)	1	EDIT COPY DELETE
English	1	EDIT COPY DELETE
History	8	EDIT COPY DELETE
Humanities	10	EDIT COPY DELETE

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

The screenshot shows the 'Edit Recipient Group' page in the InformaCast interface. The page has a blue header with the InformaCast logo and navigation icons. The main content area is white and contains the following elements:

- Recipients | Edit Recipient Groups | Edit Recipient Group** (Breadcrumbs)
- Name:** Humanities (required)
- Tags:** Add A Tag
- Select Recipients:**
 - Individually** (EDIT)
 - Filter with Recipient Groups** (EDIT)
 - Filter with Rules**
 - AND OR Logical Expression: disabled
 - 1 InformaCast Device Type Does Contain phone Ignore Case REMOVE ADD
 - Exclusions** (EDIT)
- VIEW CANCEL UPDATE** (Buttons)

The footer of the page includes the Singlewire logo and copyright information: © 2003–2011 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software.

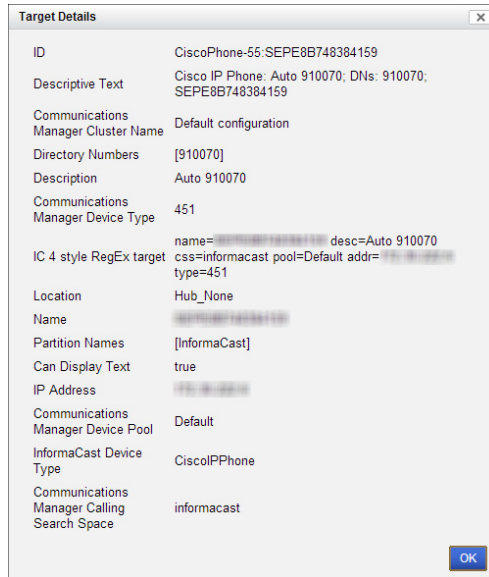
Step 3 Click the **View** button to list the recipients included in your recipient group. The View Recipients pop-up window appears.

The screenshot shows the 'View Recipients' pop-up window. It has a title bar with 'View Recipients' and a close button. The main area contains a table with the following data:

	Descriptive Text
▼	Cisco IP Phone: Ryan Fowler; DNs: 80380; SEP006440B57448
▼	Cisco IP Phone: Auto 80008; DNs: 80008; SEP00115C979921
▼	Cisco IP Phone: Auto 80030; DNs: 80030; SEP00115CD89F2A
▼	Cisco IP Phone: Auto 80089; DNs: 80089; SEP000427E69604
▼	Cisco IP Phone: Auto 80025; DNs: 80025; SEP00260B5BE7A9
▼	Cisco IP Phone: Auto 80082; DNs: 80082; SEP0004F2E81BE8
▼	Cisco IP Phone: Auto 80007; DNs: 80007; SEP00270D5A6C4D
▼	Cisco IP Phone: pl Site 1 Fancy Phone; DNs: 7900; SEP1C17D340F2B6
▼	Cisco IP Phone: Auto 80051; DNs: 80051; SEP001AA27AFFC3
▼	Cisco IP Phone: Auto 80062; DNs: 80062; SEP00269944218F

An 'OK' button is located at the bottom right of the window.

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.

InformaCast[®] basic paging
Provided by OEM Agreement with Cisco

Advanced Notification
Buy Try Learn Home Messages Recipients Speakers Bells Admin Plugins Help

Log Out

Recipients | Edit Recipient Groups

UPDATE Discover current IP phone information from Cisco Unified Communications Manager (may be time consuming).
SHOW ALL Show Defunct Phones

PREVIOUS Page 1 of 1 NEXT Jump to page: GO Show 50 results per page Filter: ADD

Name	Phones	Action
(All Recipients)	1	EDIT COPY DELETE
English	1	EDIT COPY DELETE
History	8	EDIT COPY DELETE
Humanities	10	EDIT COPY DELETE

singlewire™ Singlewire Website News Support Contact Us

© 2003–2011 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software.

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

The screenshot displays the 'Add Recipient Group' interface. At the top, there's a navigation bar with 'InformaCast basic paging' and various utility icons. The main content area is titled 'Recipients | Edit Recipient Groups | Add Recipient Group'. A form is visible with the following fields and sections:

- Name:** Humanities (copy) (required)
- Tags:** Add A Tag
- Select Recipients:** Includes a checked checkbox for 'Individually' and a list of selected recipients: 'Cisco IP Phone: pl Site 1 Fancy Phone; DNs: 7900; SEP1C17D340F2B6'.
- Filter with Recipient Groups:** Includes a checked checkbox and a list of selected groups: 'English', 'History'.
- Filter with Rules:** Includes a checked checkbox, radio buttons for 'AND' (selected) and 'OR', and a 'Logical Expression' field set to 'disabled'. Below this is a table of rules:

1	InformaCast Device Type	Does	Contain	phone	Ignore Case	REMOVE
---	-------------------------	------	---------	-------	-------------	--------
- Exclusions:** Includes a checked checkbox and a list of selected exclusions: 'Cisco IP Phone: Auto 80082; DNs: 80082; SEP0004F2E81BE8'.

At the bottom of the form, there are buttons for 'VIEW', 'CANCEL', and 'UPDATE'. The footer of the page includes the 'singlewire' logo and copyright information.



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 Unified Communications Manager 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).

InformaCast[®] basic paging
Provided by OEM Agreement with Cisco

Advanced Notification
Buy Try Learn Home Messages Recipients Speakers Bells Admin Plugins Help
Log Out

Recipients | Edit Recipient Groups | Edit Recipient Group

Name Humanities (required)
Tags Add A Tag

Select Recipients

Individually [EDIT](#)

Cisco IP Phone: Auto 700033; DNs: 700033; SEP000653DC398A
Defunct Device: CiscoPhone-55; SEP000F8F761B8B

Filter with Recipient Groups [EDIT](#)

English
History

Filter with Rules

AND OR Logical Expression: disabled

1	InformaCast Device Type	Does	Contain	phone	Ignore Case	REMOVE
---	-------------------------	------	---------	-------	-------------	------------------------

[ADD](#)

Exclusions [EDIT](#)

Cisco IP Phone: Auto 80082; DNs: 80082; SEP0004F2E81BE8

[VIEW](#) [CANCEL](#) [UPDATE](#)

singlewire[™] software
Singlewire Website News Support Contact Us

© 2003–2011 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software.

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

The screenshot shows the InformaCast basic paging interface. The top navigation bar includes icons for Buy, Try, Learn, Home, Messages, Recipients, Speakers, Bells, Admin, Plugins, and Help. The main content area is titled "Recipients | Edit Recipient Groups". It features a "SHOW ALL" button and a "Show Defunct Phones" button. Below these is a table with columns for Name, Phones, and Action. The table lists three recipient groups: "All Devices" (19 phones), "First Floor" (4 phones), and "Second Floor" (17 phones). Each group has Edit, Copy, and Delete buttons. The page also includes pagination controls and a footer with the Singlewire logo and copyright information.

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

The screenshot shows a "Defunct Phones" window. It includes a "REMOVE" button and a list of defunct devices. The list contains one entry: "Defunct Device: CiscoPhone-55:SEP00115C979921".

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

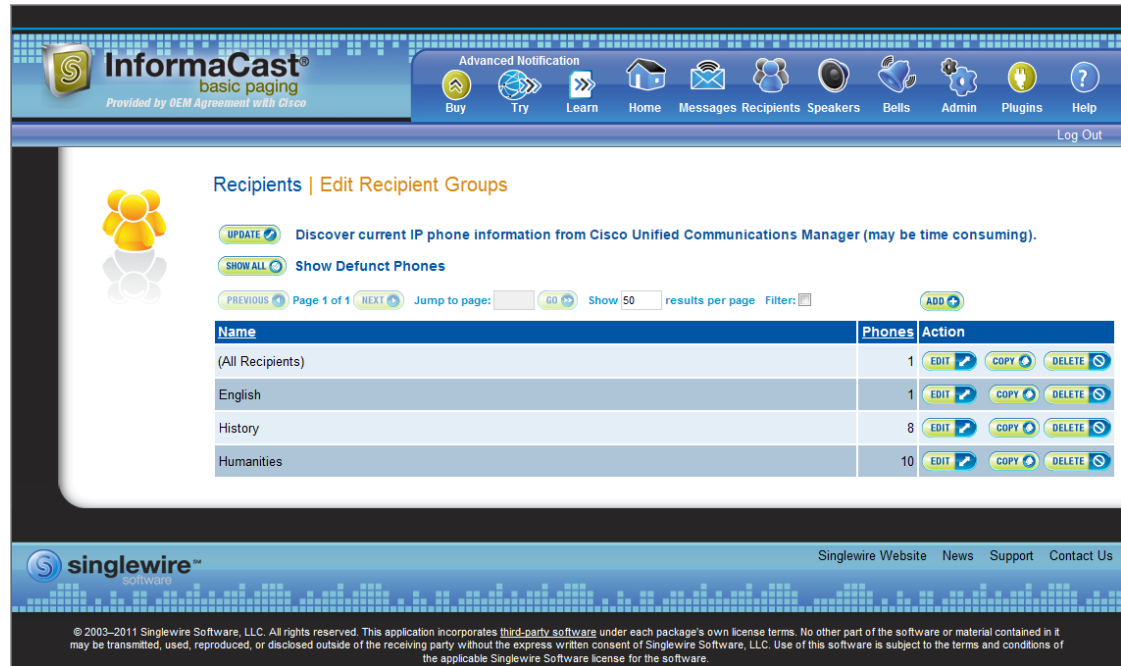


Note Recipient groups using rules do not recognize defunct phones as viable recipients for inclusion in recipient groups.

Delete a Recipient Group

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

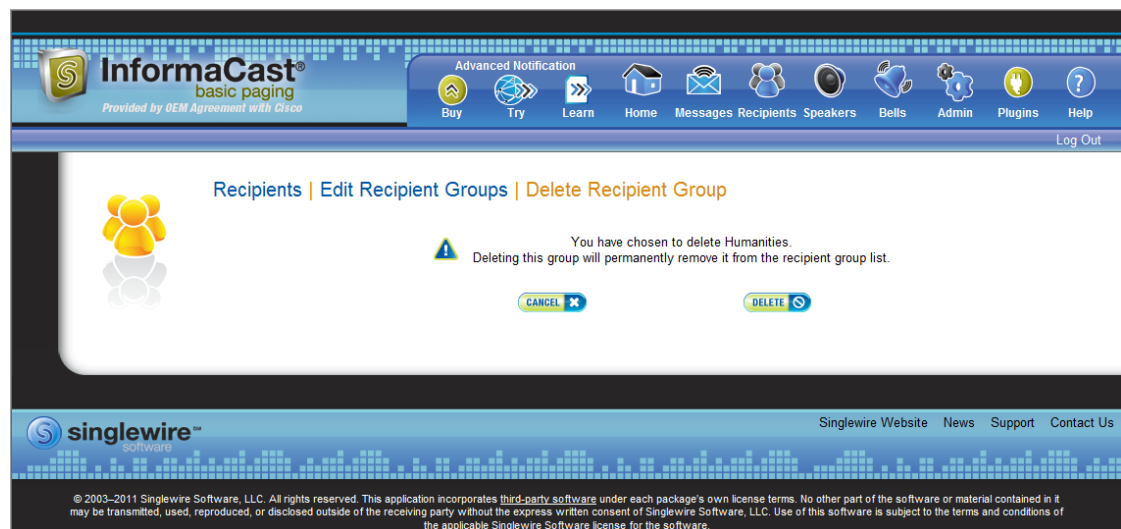
Step 1 Go to **Recipients | Edit Recipient Groups**. The Edit Recipient Groups page appears.



The screenshot shows the InformaCast basic paging interface. The top navigation bar includes links for Buy, Try, Learn, Home, Messages, Recipients, Speakers, Bells, Admin, Plugins, and Help. The main content area is titled 'Recipients | Edit Recipient Groups'. It features a table with the following data:

Name	Phones	Action
(All Recipients)	1	EDIT COPY DELETE
English	1	EDIT COPY DELETE
History	8	EDIT COPY DELETE
Humanities	10	EDIT COPY DELETE

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



The screenshot shows the InformaCast basic paging interface. The top navigation bar is the same as in the previous screenshot. The main content area is titled 'Recipients | Edit Recipient Groups | Delete Recipient Group'. It features a warning message:

You have chosen to delete Humanities.
Deleting this group will permanently remove it from the recipient group list.

Below the message are two buttons: **CANCEL** and **DELETE**.

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.

The screenshot shows the 'Recipients | Edit Tags' page in the InformaCast interface. At the top, there is a navigation bar with the InformaCast logo and 'basic paging' text, along with a note 'Provided by OEM Agreement with Cisco'. Below this is a menu with icons for 'Buy', 'Try', 'Learn', 'Home', 'Messages', 'Recipients', 'Speakers', 'Bells', 'Admin', 'Plugins', and 'Help'. The main content area is titled 'Recipients | Edit Tags' and features a 'New Tag(s):' input field with a '(comma-delimited)' label and an 'Add' button. Below the input field is a table with columns 'Name', 'Number of Groups', and 'Action'. The table is currently empty, displaying '< No Recipient Group Tags have been defined >'. The footer includes the 'singlewire' logo and links for 'Singlewire Website', 'News', 'Support', and 'Contact Us'.

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.

InformaCast[®]
basic paging
Provided by OEM Agreement with Cisco

Advanced Notification
Buy Try Learn Home Messages Recipients Speakers Bells Admin Plugins Help

Log Out

Recipients | Edit Tags

New Tag(s): (comma-delimited) **ADD**

Name	Number of Groups	Action
Business Group	1	EDIT DELETE
Financial Group	0	EDIT DELETE
Marketing Group	0	EDIT DELETE

singlewire™
Singlewire Website News Support Contact Us

© 2003–2010 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software.

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.

InformaCast[®]
basic paging
Provided by OEM Agreement with Cisco

Advanced Notification
Buy Try Learn Home Messages Recipients Speakers Bells Admin Plugins Help

Log Out

Recipients | Edit Tags

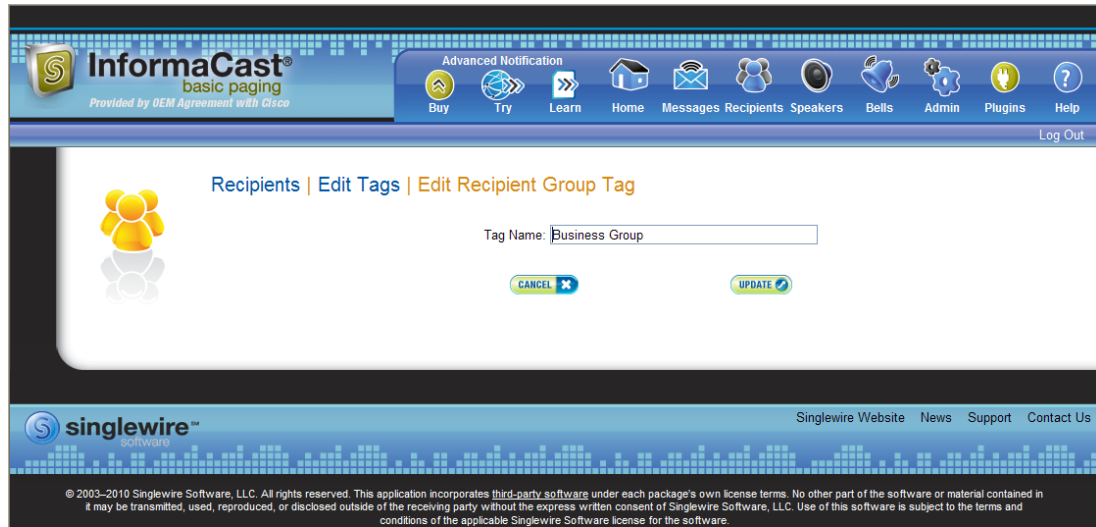
New Tag(s): (comma-delimited) **ADD**

Name	Number of Groups	Action
Business Group	1	EDIT DELETE
Financial Group	0	EDIT DELETE
Marketing Group	0	EDIT DELETE

singlewire™
Singlewire Website News Support Contact Us

© 2003–2010 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software.

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



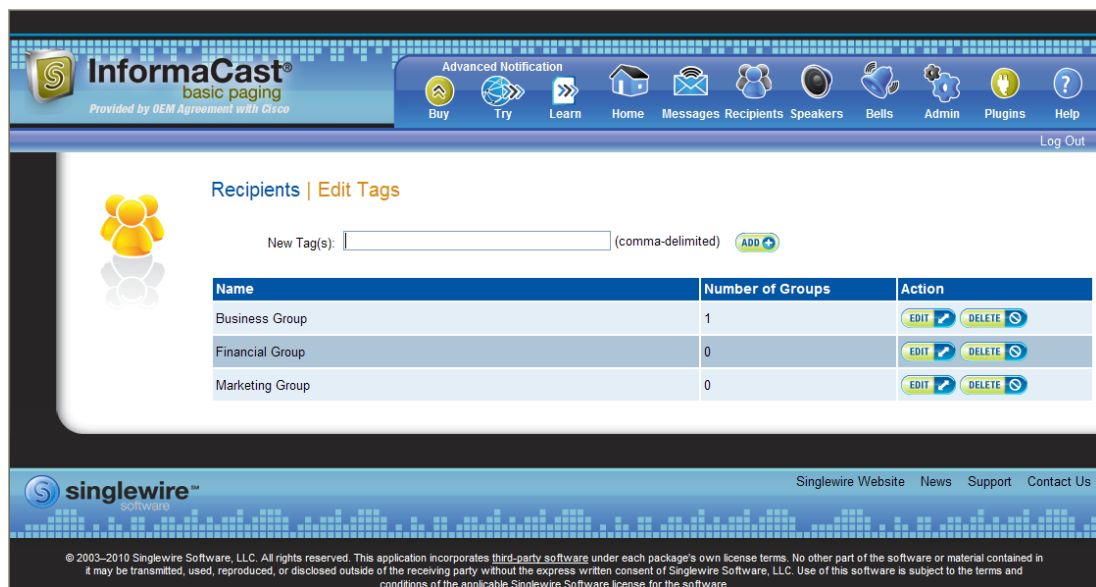
Step 3 Make your changes.

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
<code>i</code>	Case-insensitive match
<code>m</code>	The input is treated as consisting of multiple lines
<code>s</code>	The input is treated as consisting of a single line
<code>x</code>	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, Unified Communications Manager’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 | Cisco Unified Communications Manager Phone Updates**. The Cisco Unified Communications Manager Phone Updates page appears.

InformaCast®
basic paging
Provided by OEM Agreement with Cisco

Advanced Notification
Buy Try Learn Home Messages Recipients Speakers Bells Admin Plugins Help
Log Out

Admin | Telephony | Cisco Unified Communications Manager Phone Updates

Build list of registered phones
This process creates a list of registered phones and involves querying Unified Communications Manager to obtain the configuration and IP address for each registered phone.

If a field is not required, leaving it blank means "every." For example, leaving the **Hour** field blank would cause the update to be scheduled every hour of the day.

Job Description: Phone Data Update
Second: (required)
Minute: (required)
Hour: (24-hour time)
Month:
Day of Month:
Week Day:

Refresh list of registered phones
This process refreshes the configuration of previously registered phones. A refresh can be performed as frequently as once per minute.

Refresh Interval (minutes): (Blank or zero means do not perform refresh)

singlewire®
Singlewire Website News Support Contact Us

© 2003-2015 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software.



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.

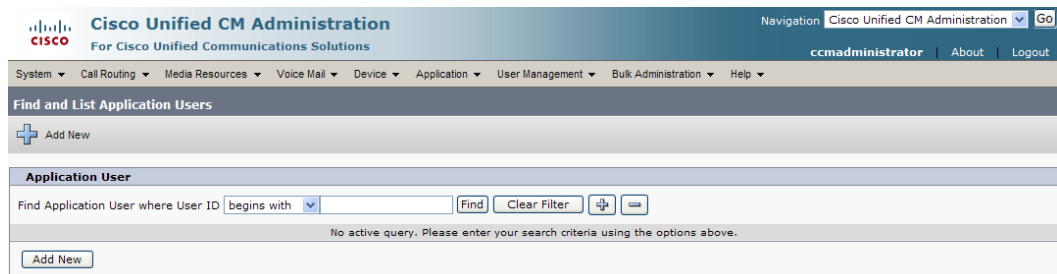
Determine the Busy State of a Phone with JTAPI

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 Unified Communications Manager itself, it is not practical or possible to monitor all phones in medium-to-large installations.



Note This procedure will only work when using Unified Communications Manager 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 Unified Communications Manager'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.

The screenshot shows the Cisco Unified CM Administration interface. The page title is "Find and List Application Users". The status bar indicates "16 records found". The table below lists the application users with their User IDs and a "Copy" icon.

<input type="checkbox"/>	User ID ^	Copy
<input type="checkbox"/>	AT214	
<input type="checkbox"/>	CCMORTSecureSysUser	
<input type="checkbox"/>	CCMORTSysUser	
<input type="checkbox"/>	CCMSysUser	
<input type="checkbox"/>	CUCService	
<input type="checkbox"/>	ICRAi	
<input type="checkbox"/>	IPMASecureSysUser	
<input type="checkbox"/>	IPMASysUser	
<input type="checkbox"/>	MattS	
<input type="checkbox"/>	TabSyncSysUser	
<input type="checkbox"/>	WDSecureSysUser	
<input type="checkbox"/>	WDSysUser	
<input type="checkbox"/>	ccmadministrator	
<input type="checkbox"/>	ramin	
<input type="checkbox"/>	user	
<input type="checkbox"/>	whjp	

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

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration Go
ccadministrator About Logout

System Call Routing Media Resources Voice Mail Device Application User Management Bulk Administration Help

Application User Configuration Related Links: Back To Find/List Go

Save Delete Copy Add New

Status
Add successful

Application User Information
User ID* Test Edit Credential
Password
Confirm Password
Digest Credentials
Confirm Digest Credentials
Presence Group* Standard Presence group
 Accept Presence Subscription
 Accept Out-of-dialog REFER
 Accept Unsolicited Notification
 Accept Replaces Header

Device Information
Available Devices: AT214, EmergencyRP, MattS_CTI, RelicastRP, SEP000BBED8055C
Controlled Devices: RelicastCTIport, RajCTI
Buttons: Find more Phones, Find more Route Points, Find more Pilot Points

CAPF Information
Associated CAPF Profiles
View Details

Permissions Information
Groups
Roles
Buttons: Add to User Group, Remove from User Group
View Details

Save Delete Copy Add New

* - indicates required item.

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.

Device Information
Available Devices: SEP001E138C7D81, SEP001E4A925F60, SEP003094C3F2DC, SEP243523452345, SEP432143214321
Controlled Devices: RelicastCTIport, RajCTI, InformaCastRaj, RajInformaCast
Buttons: Find more Phones, Find more Route Points, Find more Pilot Points

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 2-70).

Once you select the **Send Commands to Phones by JTAPI** checkbox, the **Create Telephony Terminals for all Phones** checkbox becomes visible.

Step 3 Select the **Create Telephony Terminals for all Phones** checkbox if you want to create CTI terminals for all phones in the primary cluster, which can improve phone activation times during broadcasts.

CTI terminals represent telephones in JTAPI; InformaCast can manipulate these phones (e.g. make calls, check their line states, send commands to them, etc.) through JTAPI. With the **Create Telephony Terminals for all Phones** checkbox enabled, every time InformaCast builds its phone cache, terminals will be created for any newly registered phones while terminals will be destroyed for phones no longer in the cache. If you switch back to creating terminals on an as-needed-basis or decide to no longer enable the **Send Commands to Phones by JTAPI** checkbox, all CTI terminals will be destroyed. The same holds true if you change the primary cluster to another cluster.



Note Unified Communications Manager limits an application user to 10,000 devices. If your primary cluster contains more than 10,000 phones and you select the **Create Telephony Terminals for all Phones** checkbox, InformaCast will fall back to creating terminals on an as-needed basis. This situation, if it occurs, will be logged in the Performance log, which is viewable by going to **Help | Support** and clicking the **Performance Log** link in the *Tools* section.

- Step 4** 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 5** 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 6** 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 5-46
- “Send a DialCast/Broadcast” on page 5-51
- “Cancel a DialCast/Broadcast” on page 5-52
- “Manage Call Detail Records” on page 5-53

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.

InformaCast® basic paging
Provided by OEM Agreement with Cisco

Advanced Notification
Buy Try Learn Home Messages Recipients Speakers Bells Admin Plugins Help
Log Out

Messages | Send or Edit Messages

In Basic Paging, you have access to one message only, Basic Paging Live Broadcast. Upgrading to Advanced Notification will allow you to use the other messages listed on this page. You will also be able to create your own messages.

PREVIOUS Page 1 of 1 NEXT Jump to page: GO Show 50 results per page Filter: ADD

Description	Short Text	Message Type	Action
Basic Paging Live Broadcast		Live Audio * °	SEND EDIT COPY DELETE
Example Ad-Hoc Broadcast	This is an ad-hoc broadcast.	Ad-Hoc Audio §	SEND EDIT COPY DELETE
Example failed mail server	Email is down at \${time} on \${date}	Text §	SEND EDIT COPY DELETE
Example Hammer	This is a broadcast of an industrial sounding hammer	Text and Pre-Recorded Audio §	SEND EDIT COPY DELETE
Example Humoctopus Alert	There is a Humoctopus in the building! --This is only a test.--	Text and Pre-Recorded Audio * §	SEND EDIT COPY DELETE
Example Monthly Meeting	Monthly company wide meeting is at 8:00. Press the details soft-key.	Text §	SEND EDIT COPY DELETE
Example Ring tone - Bell 1		Pre-Recorded Audio °	SEND EDIT COPY DELETE
Example Ring tone - Bell 2		Pre-Recorded Audio °	SEND EDIT COPY DELETE
Example Ring tone - Bell 3		Pre-Recorded Audio °	SEND EDIT COPY DELETE
Example Ring tone - Clock chime		Pre-Recorded Audio °	SEND EDIT COPY DELETE
Example Ring tone - Ding dong		Pre-Recorded Audio °	SEND EDIT COPY DELETE
Example Ring tone - Tone 1		Pre-Recorded Audio °	SEND EDIT COPY DELETE
Example Ring tone - Tone 2		Pre-Recorded Audio °	SEND EDIT COPY DELETE
Example Severe Weather	Severe weather is in the area at \${time} on \${date}.	Text §	SEND EDIT COPY DELETE
Example Singlewire Broadcast	This is a broadcast from Singlewire's Broadcast System!	Text and Pre-Recorded Audio §	SEND EDIT COPY DELETE
Example Tornado	There is a tornado in the area at \${time} on \${date}.	Text §	SEND EDIT COPY DELETE
Example Winter Weather	There is severe winter weather in the area at \${time} on \${date}.	Text §	SEND EDIT COPY DELETE

PREVIOUS Page 1 of 1 NEXT Jump to page: GO Show 50 results per page

* Message will skip phones that are in use.
§ Message is persistent.
° Message delivery is synchronized. It will start after a delay, and play only once.

singlewire software
Singlewire Website News Support Contact Us

© 2003–2014 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software.



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 5-52).

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, Unified Communications Manager) 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.
- **Secure media.** Used in conjunction with secure signalling, enables the exchange of RTP packets and DTMF tones in a secure fashion by using Secure Real-time Transport Protocol (SRTP).
- **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**

If you are running Unified Communications Manager in mixed mode and you want calls to and from InformaCast to use encrypted media, you must configure SRTP support (see “Enable SIP Call Security” on page 5-36).

**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.

**Note**

If you were previously using SIP and you had configured it to work with TLS, you will need to select the **Secure Signaling Required** checkbox on the SIP Call Security page before any InformaCast features using SIP will work (see “Enable SIP Call Security” on page 5-36).

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 5-8
- “Add a Route Pattern” on page 5-31

For a secure SIP trunk, follow these steps:

- “Manage SIP Certificates to Facilitate TLS Protocol” on page 5-10
- “View the InformaCast SIP Certificate” on page 5-11
- “Install the InformaCast SIP Certificate on Unified Communications Manager” on page 5-12
- “Add a SIP Trunk Security Profile That Uses TLS” on page 5-18
- “Add a SIP Profile for SRTP” on page 5-21
- “Add a SIP Trunk That Uses TLS” on page 5-24
- “Install Unified Communications Manager Certificates on InformaCast” on page 5-26
- “Add a Route Pattern” on page 5-31

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.

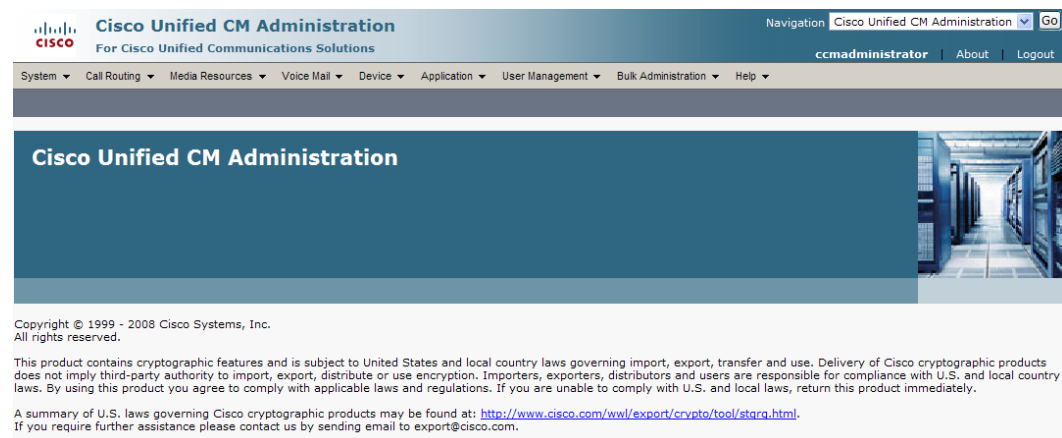


Note

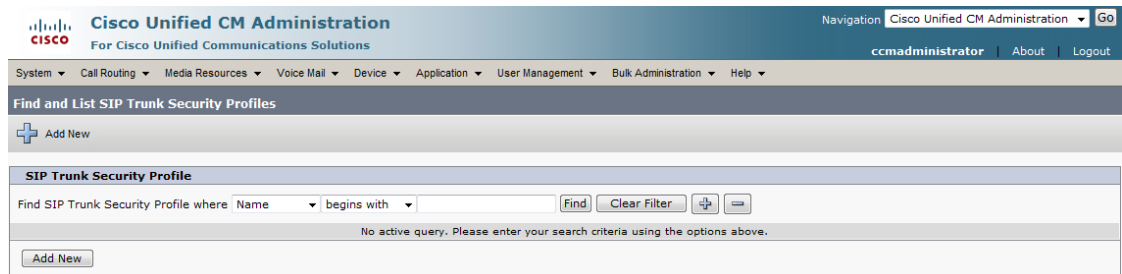
If you want to use TLS with your SIP trunk, follow the steps in “Add a SIP Trunk Security Profile That Uses TLS” on page 5-18.

Step 1

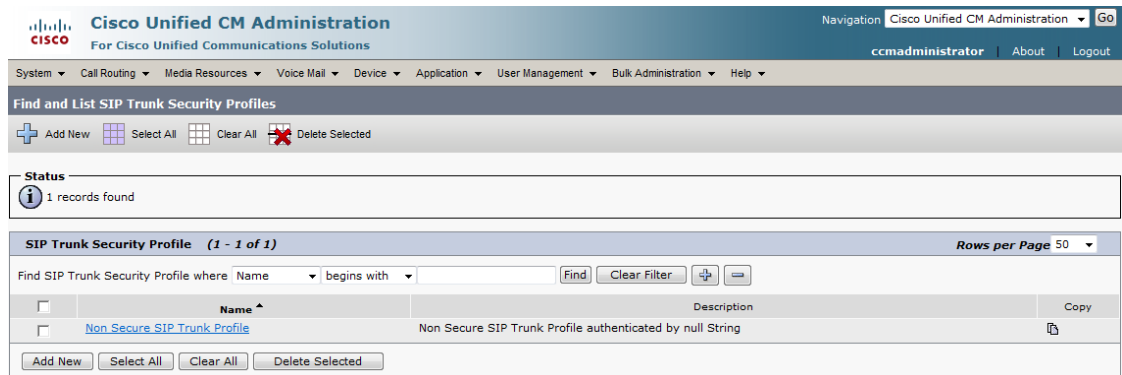
Open a web browser and log into the administration interface of the Unified Communications Manager server (the address will be similar to <https://<Unified Communications Manager IP Address>/ccmadmin>). The Cisco Unified CM Administration page appears.



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.

The screenshot shows the Cisco Unified CM Administration interface for configuring a SIP Trunk Security Profile. The page title is "SIP Trunk Security Profile Configuration". The status is "Ready". The configuration fields are:

- Name*: Non Secure SIP Trunk Profile
- Description: Non Secure SIP Trunk Profile authenticated by null Stri...
- Device Security Mode: Non Secure
- Incoming Transport Type*: TCP+UDP
- Outgoing Transport Type: TCP
- Enable Digest Authentication
- Nonce Validity Time (mins)*: 600
- X.509 Subject Name:
- Incoming Port*: 5060
- Enable Application Level Authorization
- Accept Presence Subscription
- Accept Out-of-Dialog REFER
- Accept Unsolicited Notification
- Accept Replaces Header

Below the form, there is a "Save" button and a note: "i *- indicates required item."

- 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** or **UDP** 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 5-24.

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.

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration | Go
ccmadadministrator | Search Documentation | About | Logout

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

Trunk Configuration Related Links: Back To Find/List | Go

Save

Status
Status: Ready

Device Information

Product: SIP Trunk
Device Protocol: SIP
Trunk Service Type: None(Default)
Device Name*:
Description:
Device Pool*: -- Not Selected --
Common Device Configuration: < None >
Call Classification*: Use System Default
Media Resource Group List: < None >
Location*: Hub_None
AAR Group: < None >
Tunneled Protocol*: None
QSIG Variant*: No Changes
ASN.1 ROSE OID Encoding*: No Changes
Packet Capture Mode*: None
Packet Capture Duration: 0
 Media Termination Point Required
 Retry Video Call as Audio
 Path Replacement Support
 Transmit UTF-8 for Calling Party Name
 Transmit UTF-8 Names in QSIG APDU
 Unattended Port
 SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.
Consider Traffic on This Trunk Secure*: When using both sRTP and TLS
Route Class Signaling Enabled*: Default
Use Trusted Relay Point*: Default
 PSTN Access
 Run On All Active Unified CM Nodes

Call Routing Information

Remote-Party-Id
 Asserted-Identity
Asserted-Type*: Default
SIP Privacy*: Default

Inbound Calls

Significant Digits*: All
Connected Line ID Presentation*: Default
Connected Name Presentation*: Default
Calling Search Space: < None >
AAR Calling Search Space: < None >
Prefix DN:
 Redirecting Diversion Header Delivery - Inbound

SIP Information

Destination

Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port	Status
1*	<input type="text"/>	<input type="text"/>	5060	N/A

MTP Preferred Originating Codec*: 711ulaw
BLF Presence Group*: Standard Presence group
SIP Trunk Security Profile*: -- Not Selected --
Rerouting Calling Search Space: < None >
Out-Of-Dialog Refer Calling Search Space: < None >
SUBSCRIBE Calling Search Space: < None >
SIP Profile*: -- Not Selected -- [View Details](#)
DTMF Signaling Method*: No Preference

Save

*- indicates required item.
**- Device reset is not required for changes to Packet Capture Mode and Packet Capture Duration.

- 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 2-56 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 2-59 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 5-7.
 - 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 5-31.
-

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.

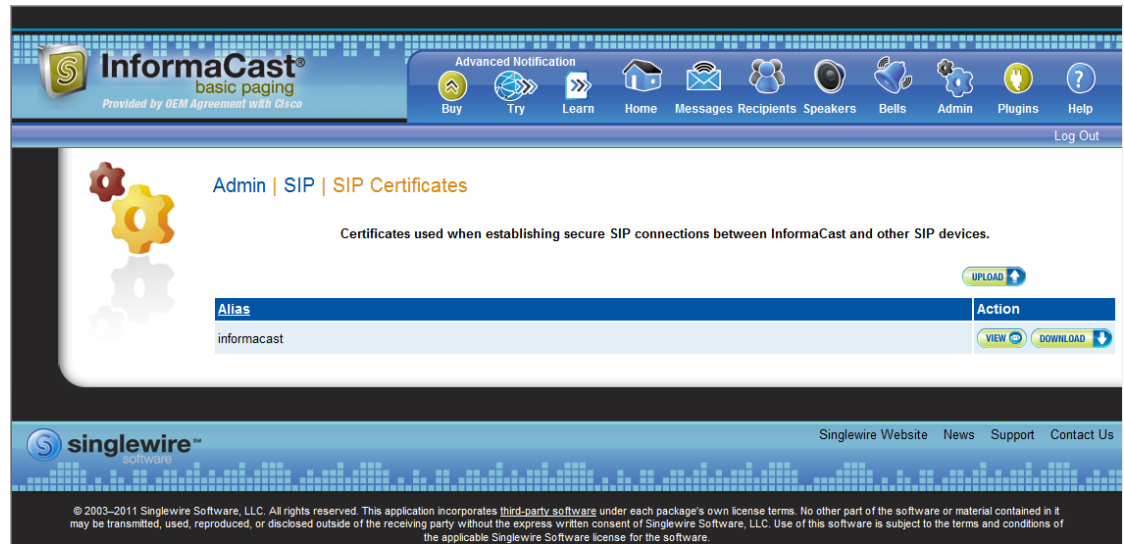
It is essential that the InformaCast certificate be downloaded and installed at each host that expects to use TLS as its SIP transport protocol with InformaCast. It is also essential that a certificate from each of those same hosts be uploaded to InformaCast. You will also need to modify it and its security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

When InformaCast is first installed, the key store only contains an RSA self-signed certificate for InformaCast. 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.

The screenshot shows the InformaCast basic paging administration interface. The top navigation bar includes links for Buy, Try, Learn, Home, Messages, Recipients, Speakers, Bells, Admin, Plugins, and Help. The main content area displays the SIP Certificate page for the alias 'informacast'. The certificate details are as follows:

```

Certificate for alias informacast:
[
Version: V3
Subject: CN=InformaCast-172.30.227.212
Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

Key: Sun RSA public key, 1024 bits
modulus:
1183697121016984262124186139075525433477849254894024690612744900000173735735326922621
154085776645914171069876103438026620403470446582208459226084141271592141747568141928
7976525350321996019091283029028515297515845874347643393471135200295957930875774977221
915286745498762127423199339533477897994916941166934273
public exponent: 65537
Validity: [From: Wed Nov 16 20:13:12 CST 2011,
To: Sat Apr 02 21:13:12 CDT 2039]
Issuer: CN=InformaCast-172.30.227.212
SerialNumber: [ 4ec46db8]
]
Algorithm: [SHA1withRSA]
Signature:
0000: 77 22 26 DF 15 E8 95 DD 0E 5C 50 FC 9C F6 ED BC w*&.....IP.....
0010: 36 9E 31 CC EF 2F 4A 11 52 F6 1E 4C 57 AB 79 4E 61.../J.R. LW.yN
  
```

A 'DONE' button is located at the bottom right of the certificate details area.

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

Install the InformaCast SIP Certificate on Unified Communications Manager

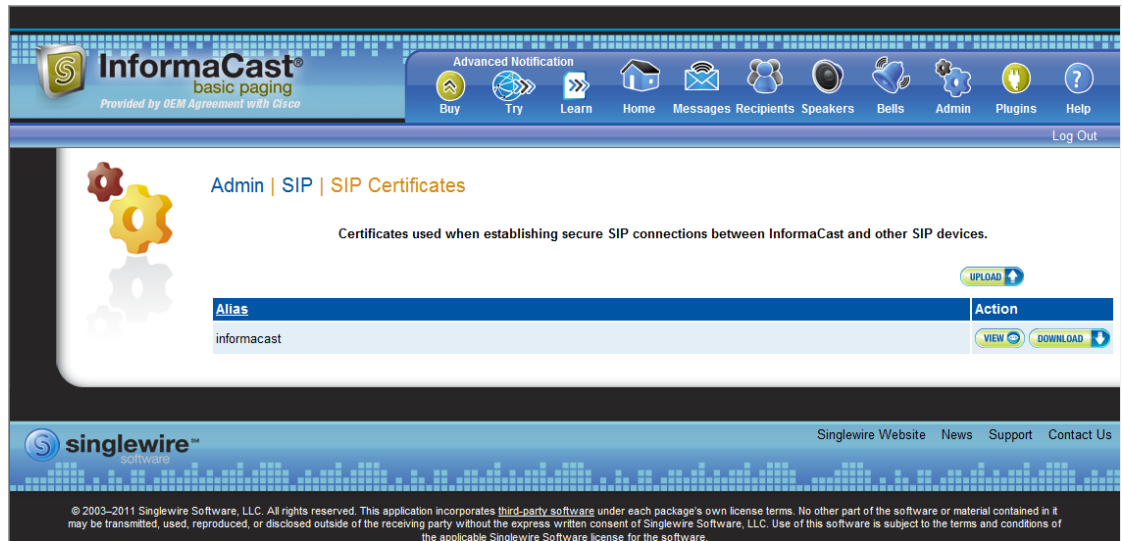
To use the TLS protocol between Unified Communications Manager and InformaCast, you will need to be using a SIP trunk for SIP configuration and install InformaCast's SIP certificate on all nodes in the Unified Communications Manager group used by the trunk's device pool.



Note

TLS certificates are regenerated whenever Unified Communications Manager 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.

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 Unified Communications Manager 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 Unified Communications Manager server (the address will be similar to <https://<Unified Communications Manager IP Address>/ccmadmin>). The Cisco Unified CM Administration page appears.



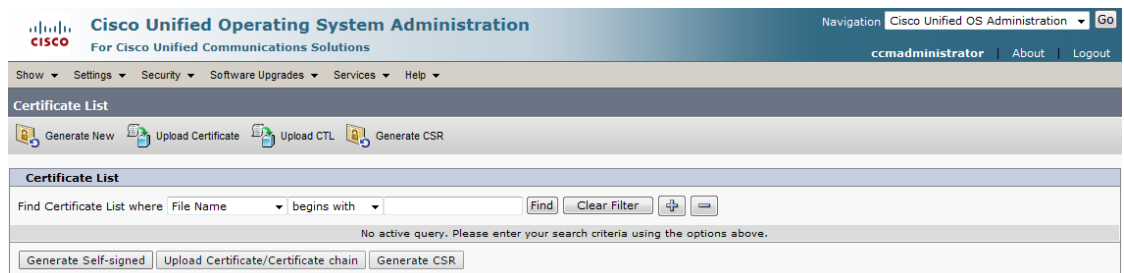
Step 5 Select **Cisco Unified OS Administration** from the **Navigation** dropdown menu and click the **Go** button. The Cisco Unified Operating System Administration page appears.



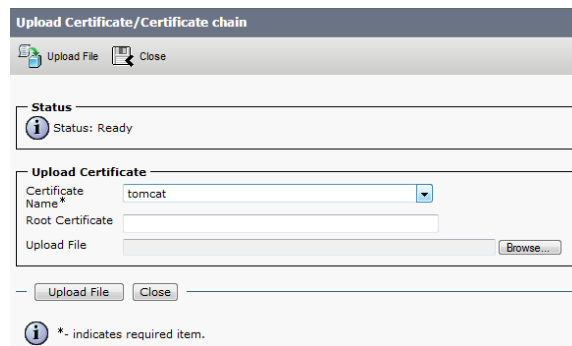
Step 6 Enter your Operating System Administration username and password in the **Username** and **Password** fields, respectively, and click the **Login** button. The Cisco Unified Operating System Administration page refreshes.



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

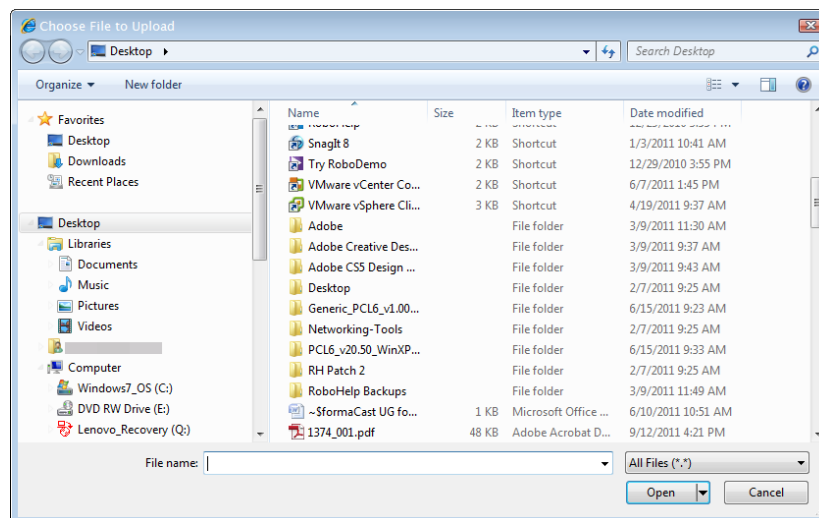


- Step 8** Click the **Upload Certificate/Certificate chain** button. The Upload Certificate/Certificate chain window appears.



- 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/Certificate chain window.

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

- Step 14** Perform these steps for each Unified Communications Manager server used by the SIP trunk.

If you are using a version of Unified Communications Manager prior to 11.5.1, this section's steps are complete. Proceed to "Add a SIP Trunk Security Profile That Uses TLS" on page 5-18.

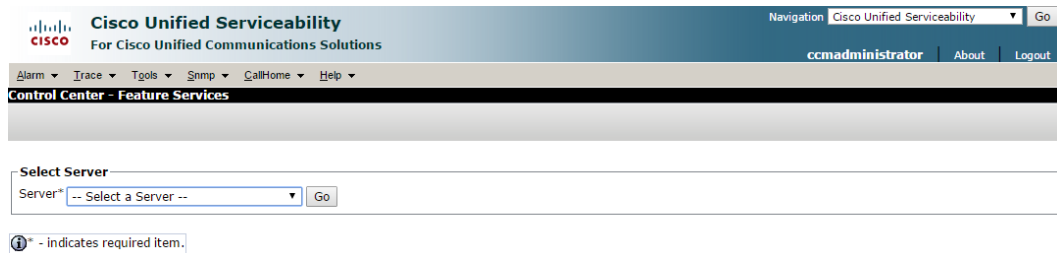
If you are using the 11.5.1 version of Unified Communications Manager or later, you will also need to perform Steps 15 through 22. Since these steps include restarting Unified Communications Manager, you should plan to perform these steps during a maintenance window to avoid disrupting your users.

Step 15 Select **Cisco Unified Serviceability** from the **Navigation** dropdown menu and click the **Go** button. The Cisco Unified Serviceability page appears.



Note You may have to log into Unified Communications Manager again.

Step 16 Go to **Tools | Control Center - Feature Services**. The Control Center - Feature Services page appears.



Step 17 Select your Unified Communications Manager server from the **Server** dropdown menu and click the **Go** button. The Control Center - Feature Services page refreshes.

Cisco Unified Serviceability
For Cisco Unified Communications Solutions

Navigation: Cisco Unified Serviceability Go
ccadministrator About Logout

Alarm Trace Tools Snmp CallHome Help

Control Center - Feature Services Related Links: Service Activation Go

Start Stop Restart Refresh Page

Status: Ready

Select Server
Server*: dev-ucm90-pub Go

Database and Admin Services

Service Name	Status	Activation Status	Start Time	Up Time
<input type="radio"/> Platform Administrative Web Service	Not Running	Deactivated		
<input type="radio"/> Cisco Bulk Provisioning Service	Started	Activated	Tue Feb 19 09:30:17 2013	379 days 02:50:26
<input type="radio"/> Cisco AXL Web Service	Started	Activated	Tue Feb 19 09:36:25 2013	379 days 02:44:18
<input type="radio"/> Cisco UXL Web Service	Not Running	Deactivated		
<input type="radio"/> Cisco TAPS Service	Not Running	Deactivated		

Performance and Monitoring Services

Service Name	Status	Activation Status	Start Time	Up Time
<input type="radio"/> Cisco Serviceability Reporter	Not Running	Deactivated		
<input type="radio"/> Cisco CallManager SNMP Service	Started	Activated	Tue Feb 19 09:30:15 2013	379 days 02:50:28

Directory Services

Service Name	Status	Activation Status	Start Time	Up Time
<input type="radio"/> Cisco DirSync	Started	Activated	Tue Feb 19 09:30:16 2013	379 days 02:50:27

CM Services

Service Name	Status	Activation Status	Start Time	Up Time
<input type="radio"/> Cisco CallManager	Started	Activated	Wed Oct 16 08:26:28 2013	140 days 04:54:15
<input type="radio"/> Cisco Messaging Interface	Not Running	Deactivated		
<input type="radio"/> Cisco Unified Mobile Voice Access Service	Not Running	Deactivated		
<input type="radio"/> Cisco IP Voice Media Streaming App	Started	Activated	Tue Feb 19 09:30:13 2013	379 days 02:50:30
<input type="radio"/> Cisco CTIManager	Started	Activated	Wed Jan 15 13:49:07 2014	48 days 22:31:36
<input type="radio"/> Cisco Extension Mobility	Started	Activated	Tue Mar 4 16:07:11 2014	0 days 20:13:32
<input type="radio"/> Cisco DHCP Monitor Service	Not Running	Deactivated		
<input type="radio"/> Cisco Intercluster Lookup Service	Not Running	Deactivated		
<input type="radio"/> Cisco Location Bandwidth Manager	Not Running	Deactivated		
<input type="radio"/> Cisco Dialed Number Analyzer Server	Not Running	Deactivated		
<input type="radio"/> Cisco Tftp	Started	Activated	Thu Jun 27 09:46:41 2013	251 days 03:34:02

CTI Services

Service Name	Status	Activation Status	Start Time	Up Time
<input type="radio"/> Cisco IP Manager Assistant	Not Running	Deactivated		
<input type="radio"/> Cisco WebDialer Web Service	Not Running	Deactivated		

Voice Quality Reporter Services

Service Name	Status	Activation Status	Start Time	Up Time
<input type="radio"/> Cisco Extended Functions	Not Running	Deactivated		

CDR Services

Service Name	Status	Activation Status	Start Time	Up Time
<input type="radio"/> Cisco SOAP - CDRonDemand Service	Not Running	Deactivated		
<input type="radio"/> Cisco CAR Web Service	Not Running	Deactivated		

Security Services

Service Name	Status	Activation Status	Start Time	Up Time
<input type="radio"/> Cisco CTL Provider	Not Running	Deactivated		
<input type="radio"/> Cisco Certificate Authority Proxy Function	Not Running	Deactivated		

Start Stop Restart Refresh

i* - indicates required item.

Step 18 Scroll to the *CM Services* area.

Step 19 Select the **Cisco CallManager** radio button.

Step 20 Scroll to the bottom of the page and click the **Restart** button.

Step 21 Click the **OK** button to accept any warnings. The service will restart.

- Step 22** Scroll to the top of the page and repeat Steps 17 through 21 for each Unified Communications Manager server used by the SIP trunk.

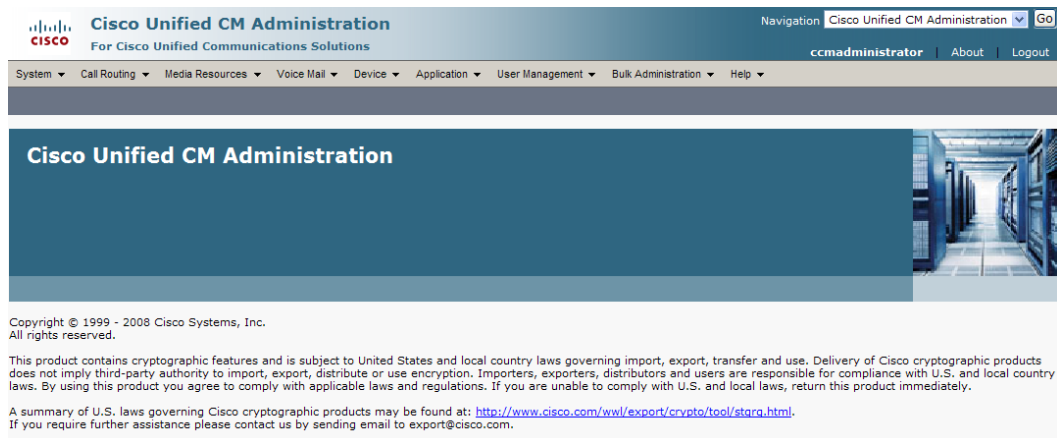
Add a SIP Trunk Security Profile That Uses TLS

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

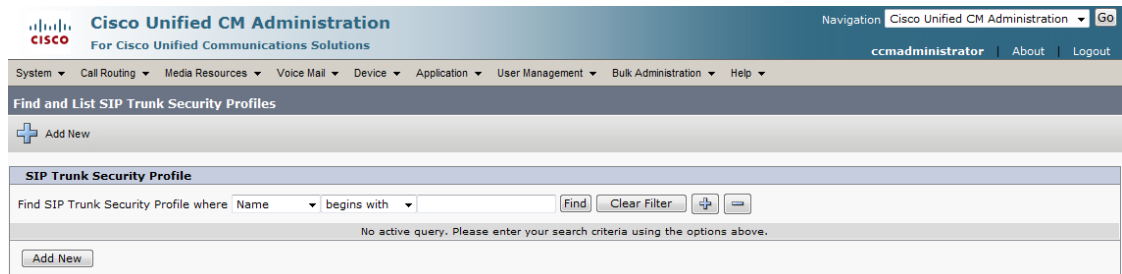
- Step 1** Select **Cisco Unified CM Administration** from the **Navigation** menu and click the **Go** button. The Cisco Unified CM Administration page appears.



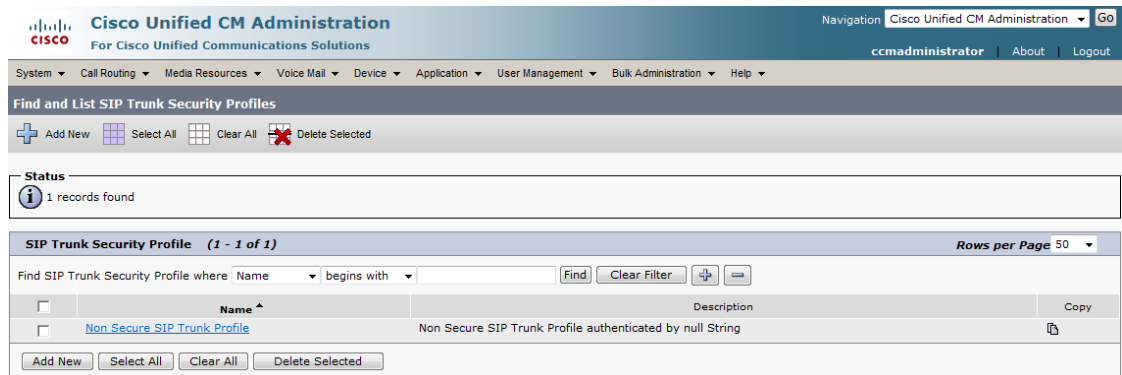
- Step 2** Enter your administrative username and password in the **Username** and **Password** fields, respectively, and click the **Login** button. The Cisco Unified CM Administration page refreshes.



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. InformaCast-TLS.
- 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- $\langle x.x.x.x \rangle$** in the **X.509 Subject Name** field, where $\langle x.x.x.x \rangle$ 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.

```

Certificate for alias informacast:
[
  Version: V3
  Subject: CN=InformaCast-172.30.227.212
  Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

  Key: Sun RSA public key, 1024 bits
  modulus:
118369712101698426212418613907552543347784925489402469061274490000173735735326922621
1540857756645914171069876103438026520403470446582208459226084141271592141747568141928
7976525350321996019091283029028515297515845874347643393471135200295957930875774977221
915286745498762127423199339533477897994916941166934273
  public exponent: 65537
  Validity: [From: Wed Nov 16 20:13:12 CST 2011,
  To: Sat Apr 02 21:13:12 CDT 2039]
  Issuer: CN=InformaCast-172.30.227.212
  SerialNumber: [ 4ec46db8]
]
Algorithm: [SHA1withRSA]
Signature:
0000: 77 22 26 DF 15 E8 95 DD 8E 5C 50 FC 9C F6 ED BC w*&.....\P.....
0010: 36 9E 31 CC EF 2F 4A 11 52 F6 1E 4C 57 AB 79 4E 6.1..J.R..LW.y\N

```

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

Step 12 Click the **Save** button.

Add a SIP Profile for SRTP

If you are using SRTP in your environment and have secure phones, you will need to add a new SIP profile.



Note If you are not using SRTP, you can skip this section.

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

Step 2 Click the **Find** button. The Find and List SIP Profiles page refreshes.

<input type="checkbox"/>	Name ^	Description	Copy
<input type="checkbox"/>	ICVA SIP Profile	ICVA SIP Profile needed for SRTP enabled ICs	
<input type="checkbox"/>	SIP Trunk Profile	Default SIP Profile	
<input type="checkbox"/>	Standard SIP Profile	Default SIP Profile	
	Standard SIP Profile For Cisco VCS	Default SIP Profile For Cisco Video Communication Server	
	Standard SIP Profile For TelePresence Conferencing	Default SIP Profile For Cisco TelePresence Conferencing	
	Standard SIP Profile For TelePresence Endpoint	Default SIP Profile For Cisco TelePresence Endpoint	
	Standard SIP Profile for Mobile Device	Default SIP Profile for Mobile Device	

Step 3 Click the **Standard SIP Profile** link. The SIP Profile Configuration page appears.

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration | Go
ccmadministrator | Search Documentation | About | Logout

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

SIP Profile Configuration Related Links: Back To Find/List | Go

Copy | Reset | Apply Config | Add New

Status

- Status: Ready
- All SIP devices using this profile must be restarted before any changes will take affect.

SIP Profile Information

Name*: Standard SIP Profile

Description: Default SIP Profile

Default MTP Telephony Event Payload Type*: 101

Early Offer for G.Clear Calls*: Disabled

User-Agent and Server header information*: Send Unified CM Version Information as User-Agen

Version in User Agent and Server Header*: Major And Minor

Dial String Interpretation*: Phone number consists of characters 0-9, *, #, anc

Confidential Access Level Headers*: Disabled

Redirect by Application

Disable Early Media on 180

Outgoing T.38 INVITE include audio mline

Use Fully Qualified Domain Name in SIP Requests

Assured Services SIP conformance

SDP Information

SDP Session-level Bandwidth Modifier for Early Offer and Re-invites*: TIAS and AS

SDP Transparency Profile: < None >

Accept Audio Codec Preferences in Received Offer*: Default

Require SDP Inactive Exchange for Mid-Call Media Change

Allow RR/RS bandwidth modifier (RFC 3556)

Trunk Specific Configuration

Reroute Incoming Request to new Trunk based on*: Never

RSVP Over SIP*: Local RSVP

Resource Priority Namespace List: < None >

Fall back to local RSVP

SIP Rel1XX Options*: Disabled

Video Call Traffic Class*: Mixed

Calling Line Identification Presentation*: Default

Session Refresh Method*: Invite

Early Offer support for voice and video calls*: Disabled (Default value)

Enable ANAT

Deliver Conference Bridge Identifier

Allow Passthrough of Configured Line Device Caller Information

Reject Anonymous Incoming Calls

Reject Anonymous Outgoing Calls

Send ILS Learned Destination Route String

Copy | Reset | Apply Config | Add New

i *- indicates required item.

Step 4 Click the **Copy** button. A SIP Profile Configuration page appears.

The screenshot shows the Cisco Unified CM Administration interface for SIP Profile Configuration. The page includes a navigation bar at the top with the Cisco logo and 'Cisco Unified CM Administration' text. Below the navigation bar, there are tabs for 'System', 'Call Routing', 'Media Resources', 'Advanced Features', 'Device', 'Application', 'User Management', 'Bulk Administration', and 'Help'. The main content area is titled 'SIP Profile Configuration' and contains several sections:

- Status:** Shows 'Status: Ready' and a note: 'All SIP devices using this profile must be restarted before any changes will take affect.'
- SIP Profile Information:** Contains fields for Name (Standard SIP Profile), Description (Default SIP Profile), Default MTP Telephony Event Payload Type (101), Early Offer for G.Clear Calls (Disabled), User-Agent and Server header information (Send Unified CM Version Information as User-Agen), Version in User Agent and Server Header (Major And Minor), Dial String Interpretation (Phone number consists of characters 0-9, *, #, anc), and Confidential Access Level Headers (Disabled). There are also several checkboxes for options like 'Redirect by Application', 'Disable Early Media on 180', 'Outgoing T.38 INVITE include audio mline', 'Use Fully Qualified Domain Name in SIP Requests', and 'Assured Services SIP conformance'.
- SDP Information:** Contains fields for SDP Session-level Bandwidth Modifier for Early Offer and Re-invites (TIAS and AS), SDP Transparency Profile (< None >), and Accept Audio Codec Preferences in Received Offer (Default). There are also checkboxes for 'Require SDP Inactive Exchange for Mid-Call Media Change' and 'Allow RR/RS bandwidth modifier (RFC 3556)'.
- Trunk Specific Configuration:** Contains fields for Reroute Incoming Request to new Trunk based on (Never), RSVP Over SIP (Local RSVP), Resource Priority Namespace List (< None >), SIP Rel1XX Options (Disabled), Video Call Traffic Class (Mixed), Calling Line Identification Presentation (Default), Session Refresh Method (Invite), and Early Offer support for voice and video calls (Disabled (Default value)). There are also several checkboxes for options like 'Enable ANAT', 'Deliver Conference Bridge Identifier', 'Allow Passthrough of Configured Line Device Caller Information', 'Reject Anonymous Incoming Calls', 'Reject Anonymous Outgoing Calls', and 'Send ILS Learned Destination Route String'.

At the bottom of the page, there are buttons for 'Copy', 'Reset', 'Apply Config', and 'Add New'. A note at the bottom left states: '*- indicates required item.'

Step 5 Enter a name for your SIP profile in the **Name** field, e.g. ICVA SIP Profile.

Step 6 Enter a description of your SIP profile in the **Description** field, e.g. SIP Profile for SRTP.

Step 7 Scroll down to the *Trunk Specific Configuration* section and select **Best Effort (no MTP inserted)** from the **Early Offer support for voice and video calls** dropdown menu.



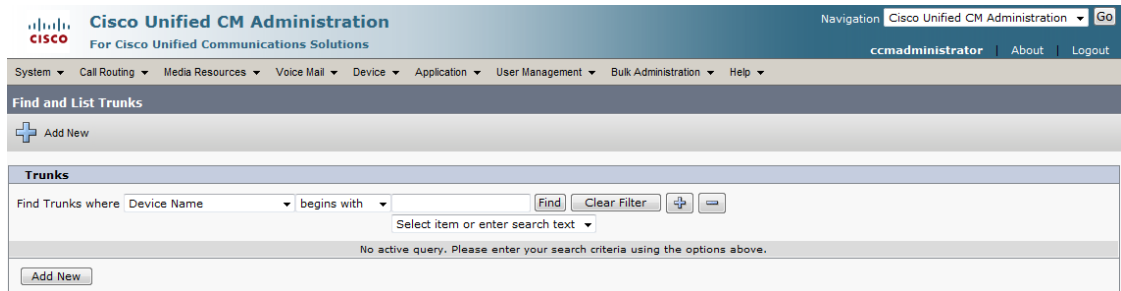
Note If you're using Unified Communications Manager 10.0.1, select the **Early Offer support for voice and video calls (insert MTP if needed)** checkbox.

Step 8 Click the **Save** button.

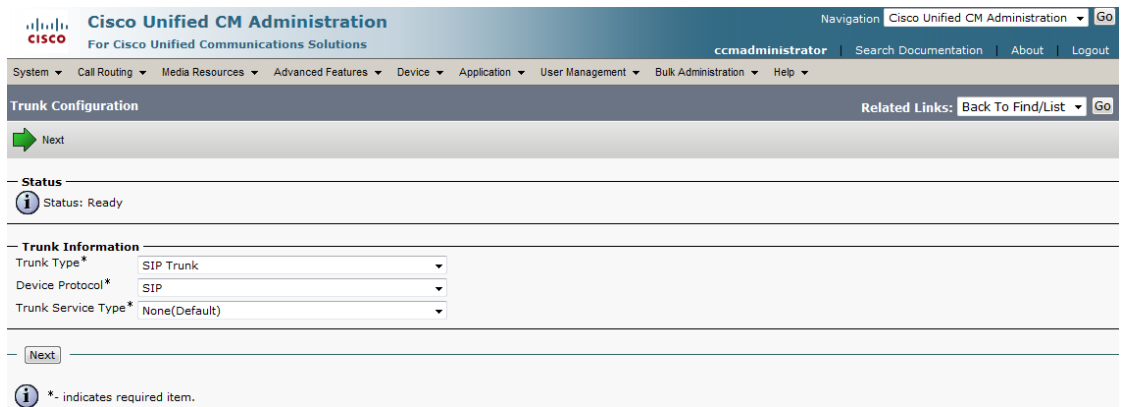
Add a SIP Trunk That Uses TLS

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 5-18.

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.

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration | Go
ccmadministrator | Search Documentation | About | Logout

System | Call Routing | Media Resources | Advanced Features | Device | Application | User Management | Bulk Administration | Help

Trunk Configuration Related Links: Back To Find/List | Go

Save

Status
Status: Ready

Device Information

Product: SIP Trunk
Device Protocol: SIP
Trunk Service Type: None(Default)
Device Name*:
Description:
Device Pool*: -- Not Selected --
Common Device Configuration: < None >
Call Classification*: Use System Default
Media Resource Group List: < None >
Location*: Hub_None
AAR Group: < None >
Tunneled Protocol*: None
QSIG Variant*: No Changes
ASN.1 ROSE OID Encoding*: No Changes
Packet Capture Mode*: None
Packet Capture Duration: 0

Media Termination Point Required
 Retry Video Call as Audio
 Path Replacement Support
 Transmit UTF-8 for Calling Party Name
 Transmit UTF-8 Names in QSIG APDU
 Unattended Port
 SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.
Consider Traffic on This Trunk Secure*: When using both sRTP and TLS
Route Class Signaling Enabled*: Default
Use Trusted Relay Point*: Default
 PSTN Access
 Run On All Active Unified CM Nodes

Call Routing Information

Remote-Party-Id
 Asserted-Identity
Asserted-Type*: Default
SIP Privacy*: Default

Inbound Calls

Significant Digits*: All
Connected Line ID Presentation*: Default
Connected Name Presentation*: Default
Calling Search Space: < None >
AAR Calling Search Space: < None >
Prefix DN:
 Redirecting Diversion Header Delivery - Inbound

SIP Information

Destination

Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port	Status
1*	<input type="text"/>	<input type="text"/>	5060	N/A

MTP Preferred Originating Codec*: 711ulaw
BLF Presence Group*: Standard Presence group
SIP Trunk Security Profile*: -- Not Selected --
Rerouting Calling Search Space: < None >
Out-Of-Dialog Refer Calling Search Space: < None >
SUBSCRIBE Calling Search Space: < None >
SIP Profile*: -- Not Selected -- [View Details](#)
DTMF Signaling Method*: No Preference

Save

i * - indicates required item.
i ** - Device reset is not required for changes to Packet Capture Mode and Packet Capture Duration.

- Step 7** Enter a name for your SIP trunk in the **Device Name** field, e.g. InformaCast/TLS.
- Step 8** Select the device pool you created in “Create a Device Pool” on page 2-56 from the **Device Pool** dropdown menu.
- Step 9** Select the **SRTP Allowed** checkbox if you are using SRTP.
- 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 2-59 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 (you entered this in Step 10 on page 5-20).
- Step 12** Enter **5061** in the **Destination Port** field.
- Step 13** Select the SIP trunk security profile you created in “Add a SIP Trunk Security Profile That Uses TLS” on page 5-18 from the **SIP Trunk Security Profile** dropdown menu.
- Step 14** Select the correct SIP profile from the **SIP Profile** dropdown menu:
- If you’re not using SRTP, select **Standard SIP Profile**
 - If you are using SRTP, select the SIP profile you created in “Add a SIP Profile for SRTP” on page 5-21
- Step 15** Click the **Save** button.

Install Unified Communications Manager Certificates on InformaCast

To use the TLS protocol between Unified Communications Manager and InformaCast, you will need to install Unified Communications Manager’s certificate on InformaCast.

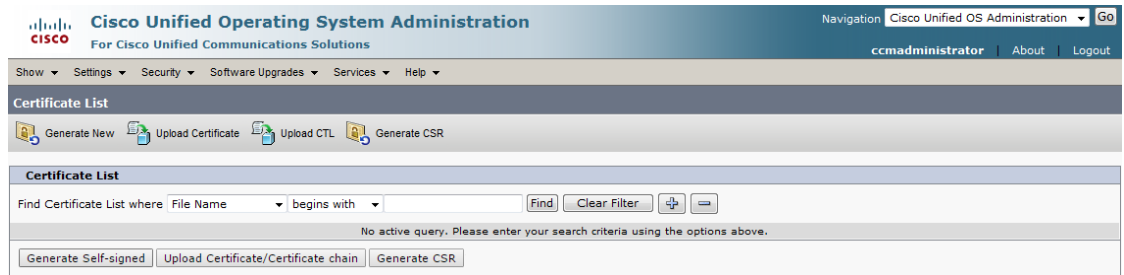
- Step 1** Select **Cisco Unified OS Administration** from the **Navigation** dropdown menu and click the **Go** button. The Cisco Unified Operating System Administration page appears.



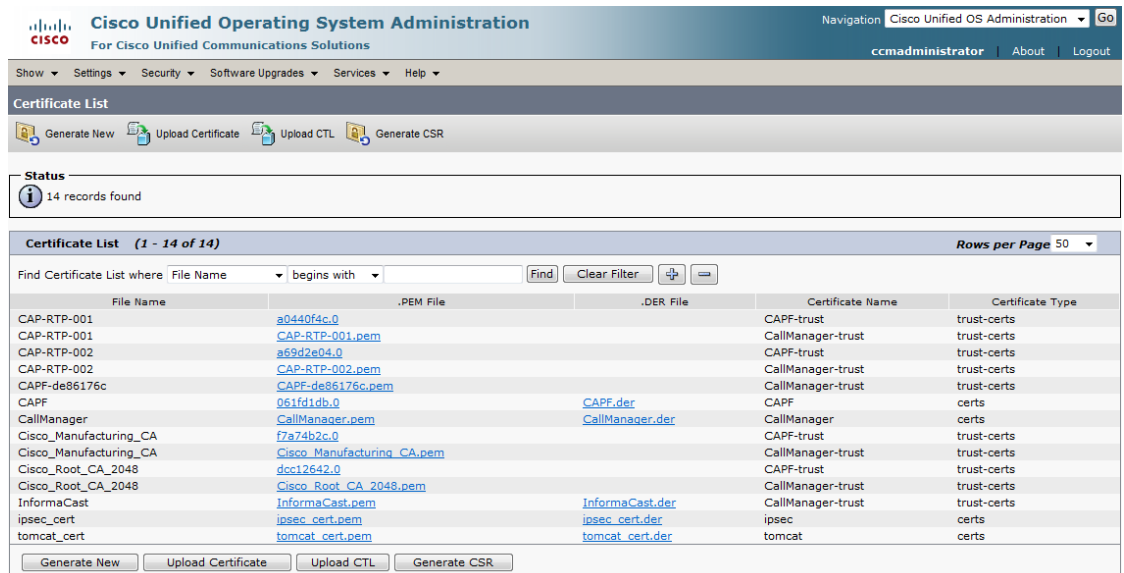
Step 2 Enter your Operating System Administration username and password in the **Username** and **Password** fields, respectively, and click the **Login** button. The Cisco Unified Operating System Administration page refreshes.



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.

Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions

Navigation: Cisco Unified OS Administration Go
ccmadministrator | About | Logout

Show Settings Security Software Upgrades Services Help

Certificate Configuration Related Links: Back To Find/List Go

Regenerate Download Generate CSR

Status
Status: Ready

Certificate Settings
File Name: CallManager.pem
Certificate Name: CallManager
Certificate Type: certs
Certificate Group: product-cm

Certificate File Data

```

Certificate:
Data:
  Version: 3 (0x2)
  Serial Number:
    18:64:e7:75:bc:7a:05:a7
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: CN=IPTAPPS-CCM60-PUB
  Validity
    Not Before: Jul  6 16:55:06 2009 GMT
    Not After : Jul  6 16:55:06 2014 GMT
  Subject: CN=IPTAPPS-CCM60-PUB
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
    Modulus (1024 bit):
      00:90:6c:4f:39:67:0a:4c:12:65:06:7b:92:68:76:
      2e:af:0f:6f:54:8d:eb:2f:4b:21:6b:3e:40:ce:53:
      f2:59:59:82:7f:20:88:25:33:ff:99:a4:3e:a1:25:
      c2:b2:b5:17:00:9f:d9:be:aa:27:6a:06:37:55:b5:
      64:a7:42:17:ed:70:fa:c2:f6:34:4f:7e:5f:50:e8:
      a9:1f:ef:12:ba:ec:fc:84:7b:c5:dc:8a:89:cb:72:
      e0:30:a1:89:4f:e1:9a:55:73:d8:a5:50:53:45:6a:
      34:1d:28:2b:e2:98:7a:15:5f:83:0b:26:76:42:1c:
  
```

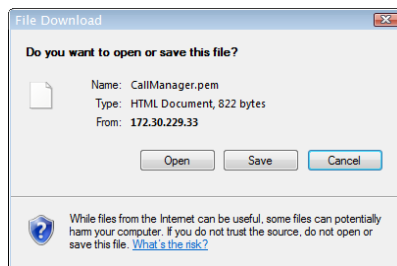
Regenerate Download Generate CSR

* - indicates required item.

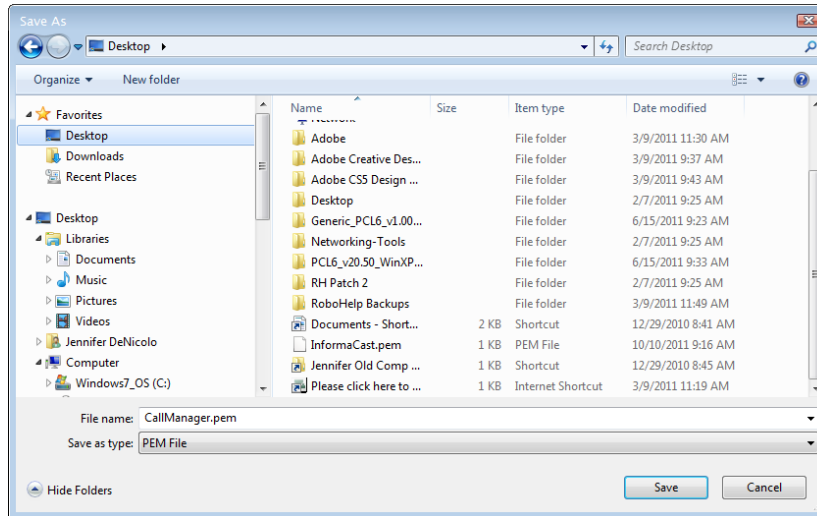


Note If you are using Unified Communications Manager 10.5 and later, you will click the **Common Name** link of the certificate that displays “CallManager” in the **Certificate** column of the Certificate List table.

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



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



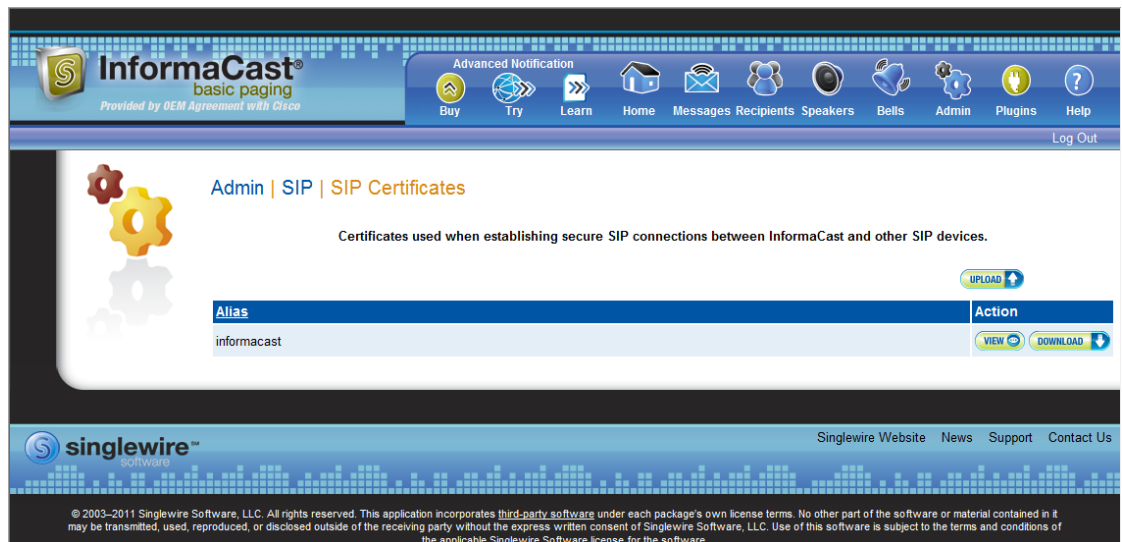
Step 8 Select a location accessible to InformaCast and click the **Save** button.



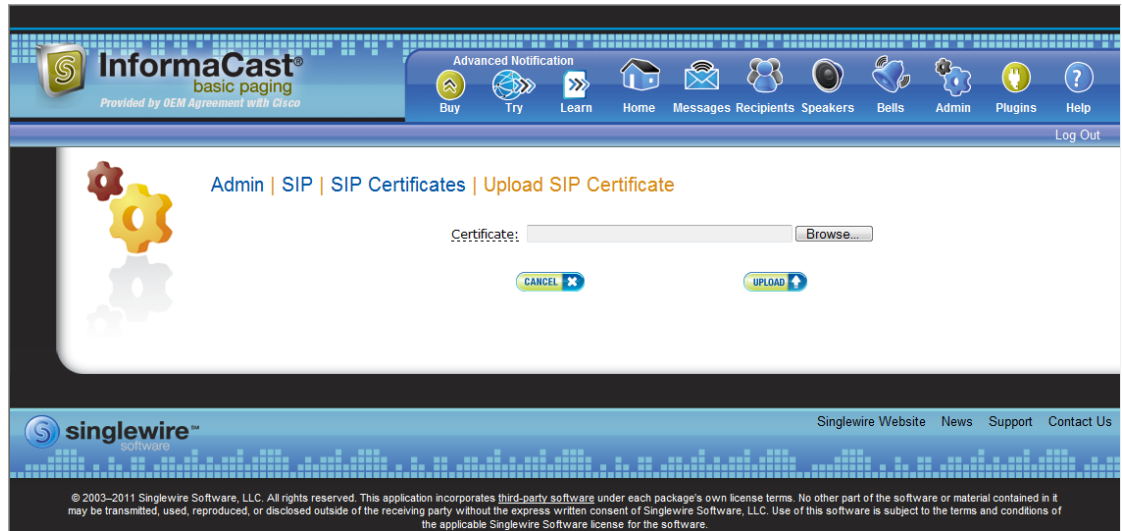
Note Perform Steps 1 through 8 for each Unified Communications Manager server that will communicating to InformaCast.

Step 9 Go back to your InformaCast window.

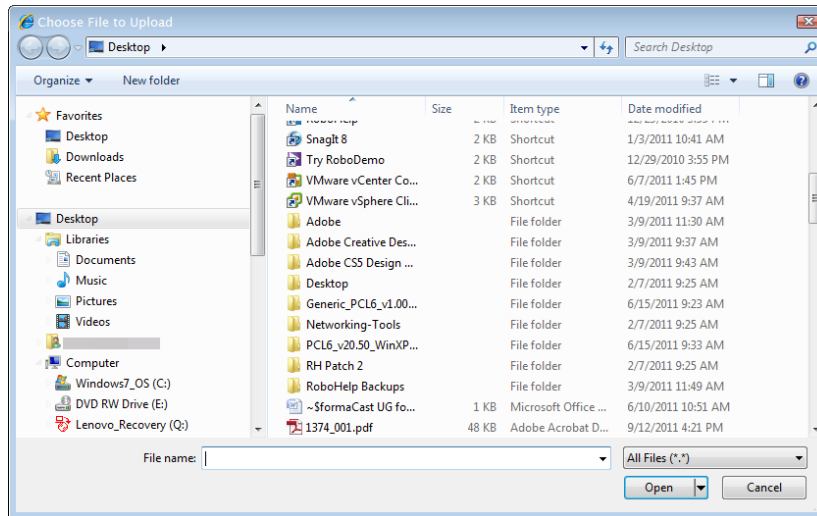
Step 10 Go to **Admin | SIP | SIP Certificates**. The SIP Certificates page appears.



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.

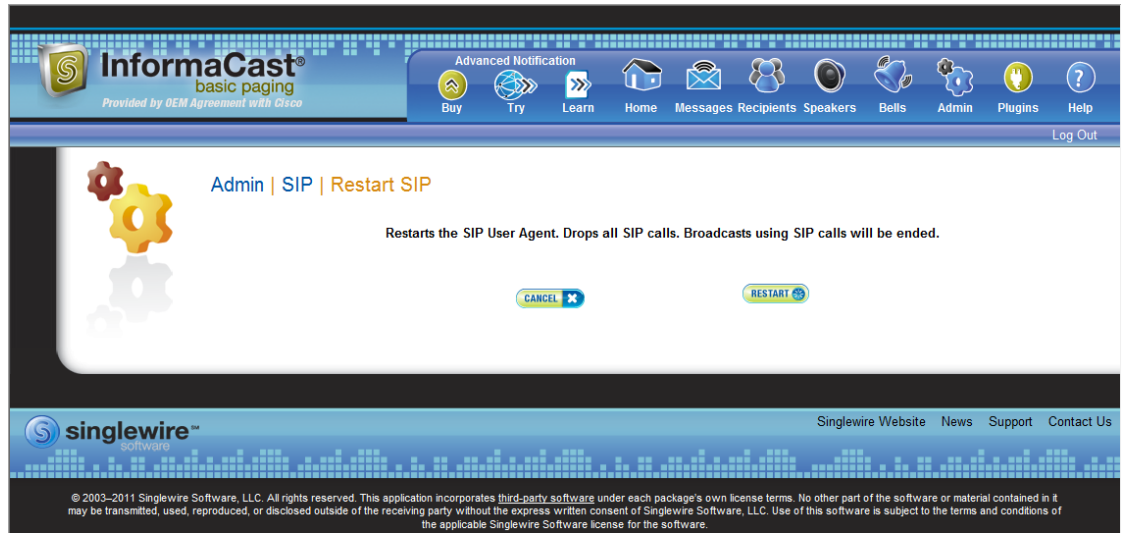
Step 14 Click the **Upload** button.

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.



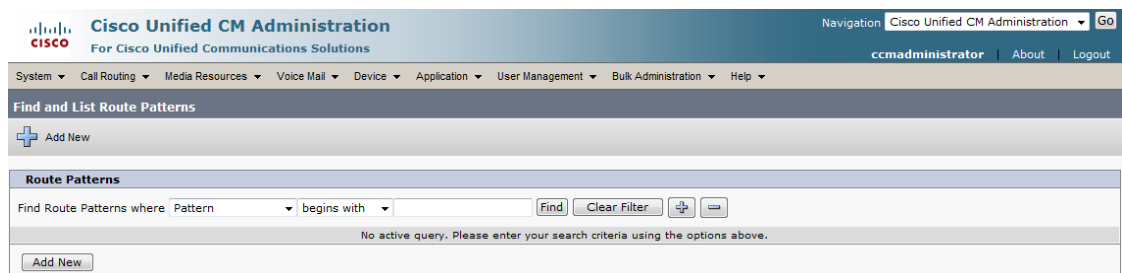
Caution

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 5-8 or “Add a SIP Trunk That Uses TLS” on page 5-24. In your route pattern, specify a range of DN’s that, when called, use the SIP trunk. Another option would be to use wild card patterns to match a range of 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.

The screenshot displays the 'Route Pattern Configuration' page in the Cisco Unified CM Administration interface. The page is organized into several sections:

- Status:** Shows 'Status: Ready'.
- Pattern Definition:** Contains fields for 'Route Pattern*', 'Route Partition' (set to '< None >'), 'Description', 'Numbering Plan' (set to '-- Not Selected --'), 'Route Filter' (set to '< None >'), 'MLPP Precedence*' (set to 'Default'), 'Gateway/Route List*' (set to '-- Not Selected --'), 'Route Option' (with 'Route this pattern' selected), 'Call Classification*' (set to 'OffNet'), and checkboxes for 'Allow Device Override', 'Provide Outside Dial Tone', 'Allow Overlap Sending', 'Urgent Priority', 'Require Forced Authorization Code', and 'Require Client Matter Code'. An 'Authorization Level*' field is set to '0'.
- Calling Party Transformations:** Includes a checkbox for 'Use Calling Party's External Phone Number Mask', 'Calling Party Transform Mask', 'Prefix Digits (Outgoing Calls)', 'Calling Line ID Presentation*' (set to 'Default'), and 'Calling Name Presentation*' (set to 'Default').
- Connected Party Transformations:** Includes 'Connected Line ID Presentation*' (set to 'Default') and 'Connected Name Presentation*' (set to 'Default').
- Called Party Transformations:** Includes 'Discard Digits' (set to '< None >'), 'Called Party Transform Mask', and 'Prefix Digits (Outgoing Calls)'. There is also a 'Save' button.
- ISDN Network-Specific Facilities Information Element:** Includes 'Network Service Protocol' (set to '-- Not Selected --'), 'Carrier Identification Code', and a table for 'Network Service' with columns for 'Service Parameter Name' and 'Service Parameter Value'. One entry is shown with 'Network Service' set to '-- Not Selected --', 'Service Parameter Name' set to '< Not Exist >', and an empty 'Service Parameter Value' field.

At the bottom, there is a legend: **i** *- indicates required item.

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 5-8 or “Add a SIP Trunk That Uses TLS” on page 5-24 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.

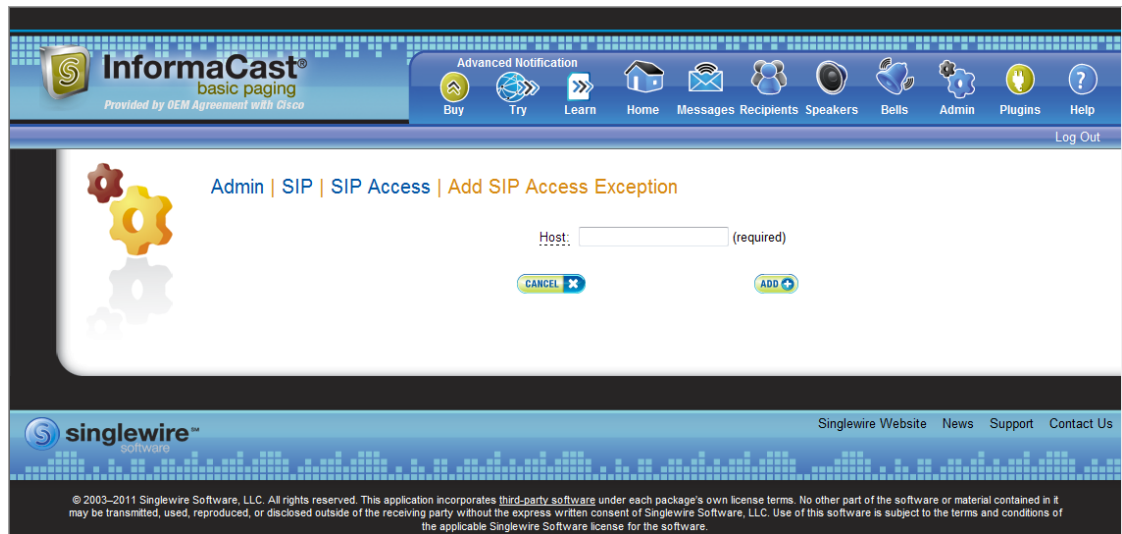
Step 1 Go to **Admin | SIP | SIP Access**. The SIP Access page appears.



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 include 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.

InformaCast®
basic paging
Provided by OEM Agreement with Cisco

Advanced Notification
Buy Try Learn Home Messages Recipients Speakers Bells Admin Plugins Help
Log Out

Admin | SIP | SIP Access

Exception added; will be permanent once the SIP Access is saved.

Controls access of inbound SIP calls to InformaCast.

Click to restore to default settings [RESTORE](#)

Note: You may have changes to commit. Click the update button to save your changes.

Allow Deny incoming SIP calls

Host exceptions that counteract the SIP access setting above [ADD](#)

Host	Access	Action
10.10.10.10	Allow	EDIT DELETE

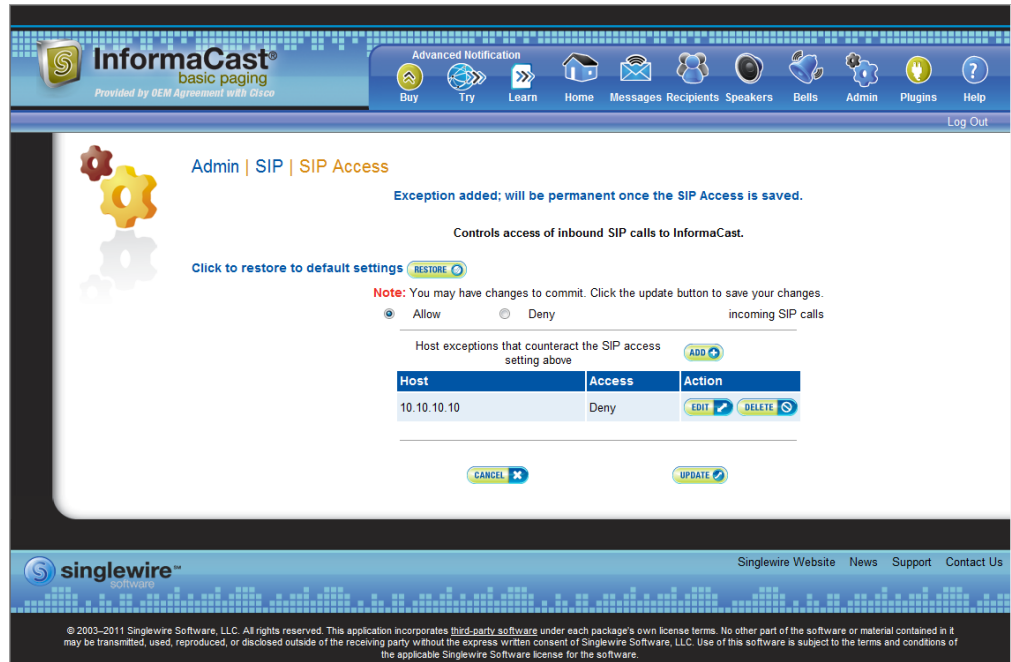
[CANCEL](#) [UPDATE](#)

singlewire™
© 2003–2011 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software.

Singlewire Website News Support Contact Us

**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 Call Security

**Note**

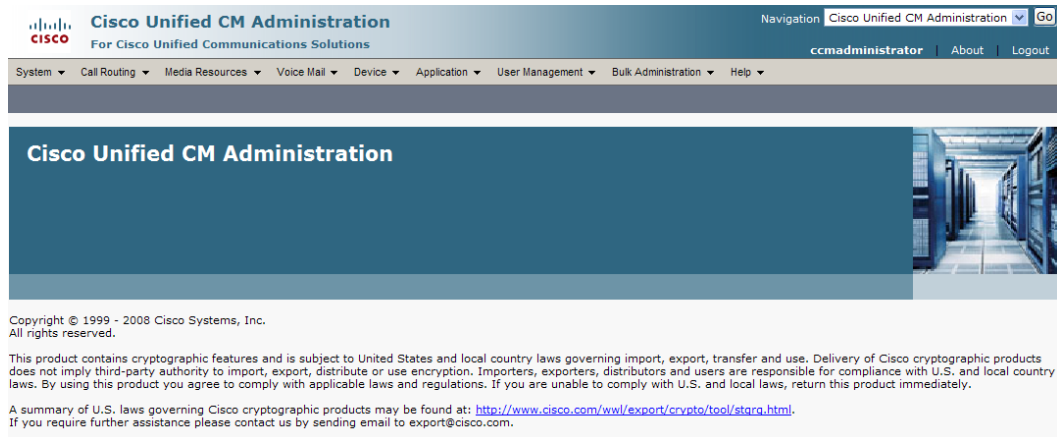
This section is optional depending on the security of your environment.

SIP call security controls the content of SIP calls made and received by InformaCast. SIP calls consist of SIP messages and the RTP packets that carry the audio and DTMF tones associated with the call. You can decide the level of security you use:

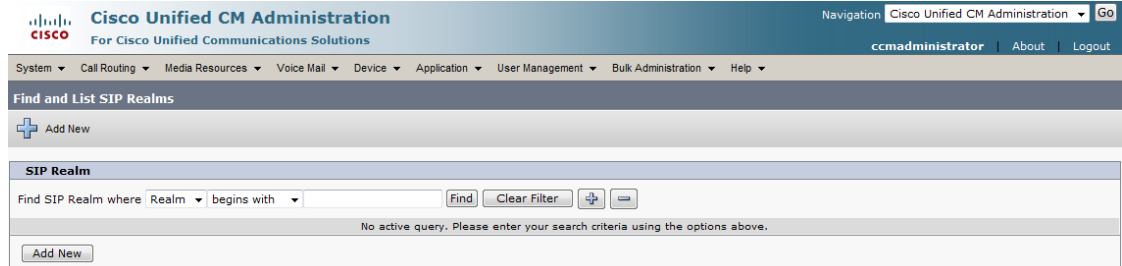
- **Default.** At this level, no encryption is used; it's just SIP over TCP or UDP.
- **Secure Signaling Required.** One level higher than the default, SIP messages are encrypted while being sent with the TLS transport protocol.
- **Secure RTP Allowed.** In conjunction with the **Secure Signaling Required** checkbox and with your Unified Communications Manager 10.x and later operating in mixed mode, this is the next level of security: SIP messages are sent with TLS and the RTP packets that carry the audio and DTMF tones are encrypted with SRTP.

- **Authenticate Incoming Requests.** Used with the default, secure signaling, and/or secure RTP options, this level of security authenticates the SIP messages used by incoming SIP calls by enabling or disabling digest authentication of incoming SIP requests.

Step 1 Open a web browser and log into the administration interface of the Unified Communications Manager server (the address will be similar to `https://<Unified Communications Manager 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 5-38.

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 a secure password in the **Digest Credentials** field.

Step 8 Enter a secure password in the **Confirm Digest Credentials** field.

Step 9 Click the **Save** button.

Step 10 Log into InformaCast (see “Log into InformaCast” on page 2-23 for specific steps). The InformaCast homepage appears.

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

The screenshot shows the InformaCast Admin interface for SIP Call Security. The page title is "Admin | SIP | SIP Call Security". Below the title, it says "Configures security used with SIP calls." There is a "Click to restore to default settings" button labeled "RESTORE". The configuration options are:

- Secure Signaling Required:
- Secure RTP Allowed:
- Authenticate Incoming Requests:

Below these are input fields for:

- Realm: InformaCast (required)
- Authentication Username: sipuser (required)
- Authentication Password: [input field]
- Confirm Authentication Password: [input field]
- Nonce Duration: 5 (dropdown menu)

At the bottom, there are "CANCEL" and "UPDATE" buttons.



Note By default, all call security is disabled.

Step 12 Select the **Secure Signaling Required** checkbox if you want to use the TLS transport protocol to send your SIP messages.

Step 13 Select the **Secure RTP Allowed** checkbox if you want to allow SRTP to handle your audio and DTMF tone packets (RTP will be used if SRTP isn't possible).



Note You must also have your Unified Communications Manager 10.x and later running in mixed mode and follow the steps for a secure SIP trunk in "Configure a SIP Trunk" on page 5-4.

Step 14 Select the **Authenticate Incoming Requests** checkbox to enable SIP authentication.

Step 15 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 16 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 17 Click the **Update** button to save your changes.

Enable Digest Authentication with SIP User Credentials



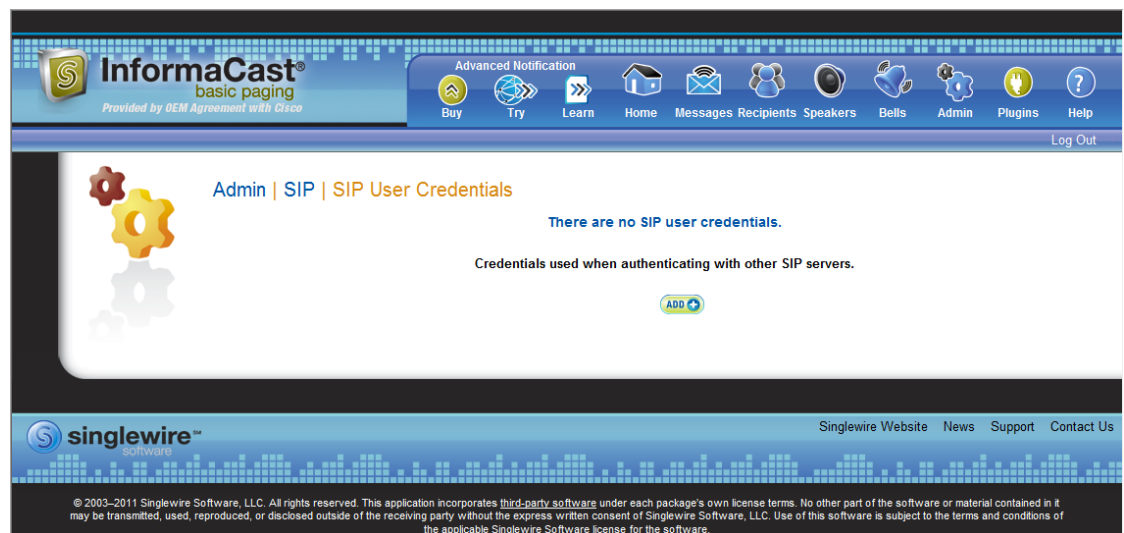
Note This section is optional depending on the security of your environment.

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.

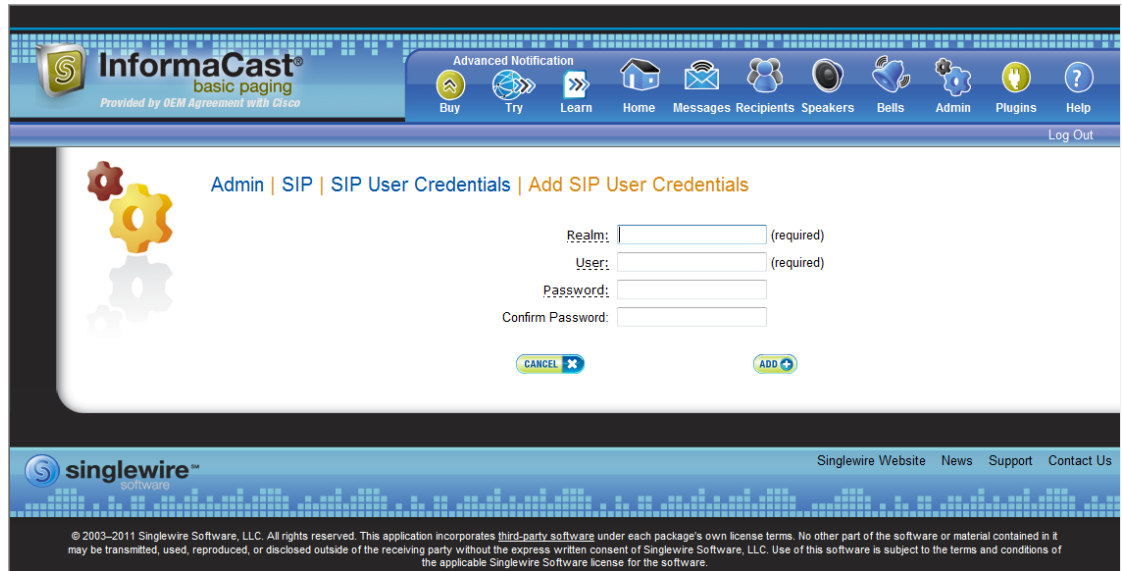
Add SIP User Credentials

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.



The screenshot displays the InformaCast basic paging administration interface. The top navigation bar includes the InformaCast logo, a navigation menu with icons for Buy, Try, Learn, Home, Messages, Recipients, Speakers, Bells, Admin, Plugins, and Help, and a Log Out link. The main content area shows the breadcrumb path: Admin | SIP | SIP User Credentials | Add SIP User Credentials. Below the breadcrumb is a form with four input fields: Realm (required), User (required), Password, and Confirm Password. At the bottom of the form are two buttons: CANCEL and ADD. The footer contains the Singlewire logo and copyright information.

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.

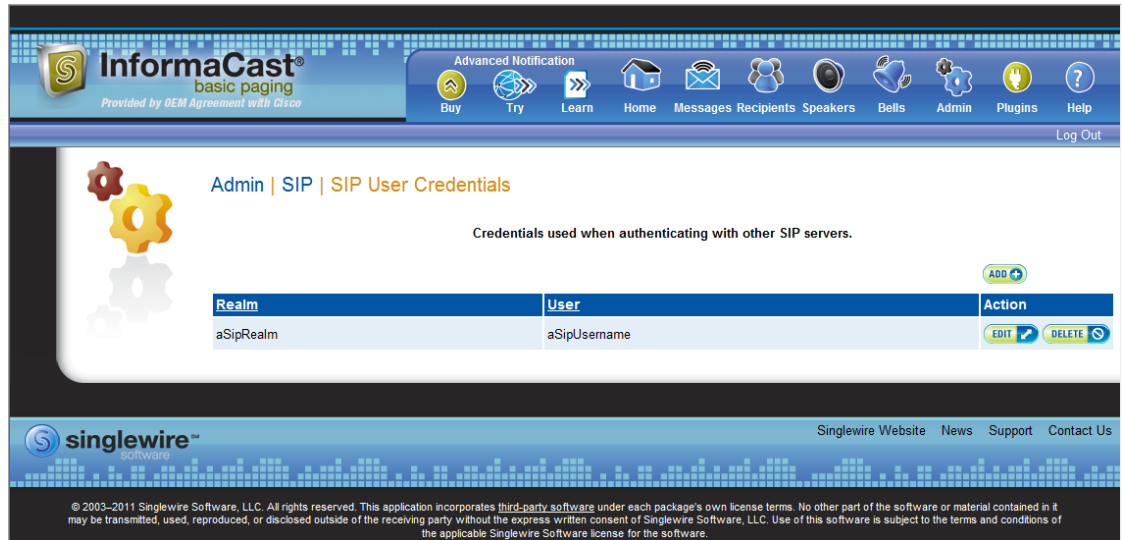
Step 5 Enter the password of the username associated with the SIP peer's SIP realm in the **Password** and **Confirm Password** fields.

Step 6 Click the **Add** button.

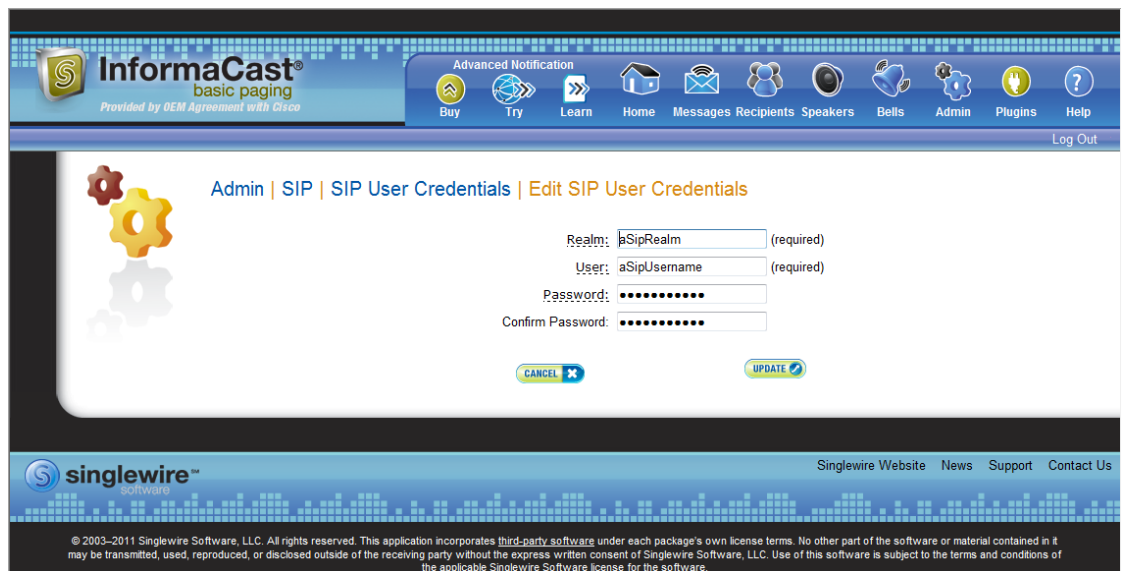
Edit SIP User Credentials

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.



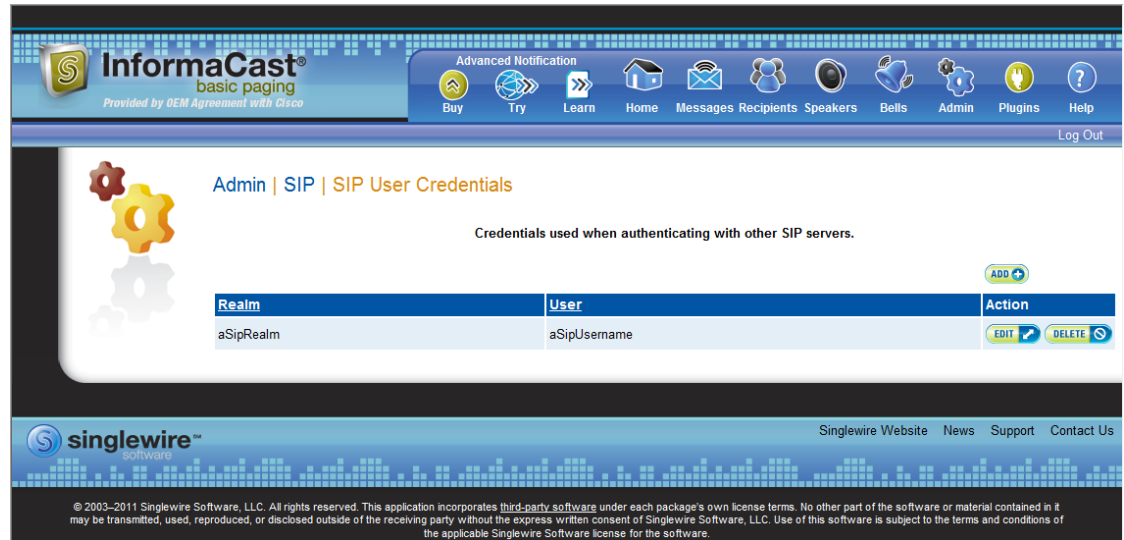
Step 3 Make your desired changes.

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

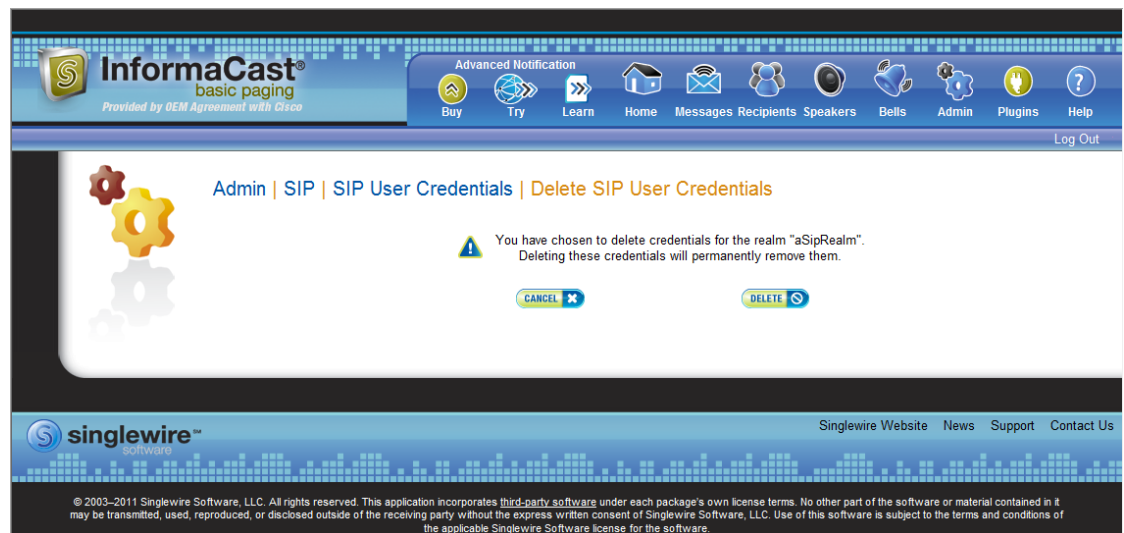
Delete SIP User Credentials

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 log generated for the SIP stack, sipStack.log, is accessible through the Support page (**Help | Support**). sipStack.log can reach 10MB in size; at which point, sipStack.log.1 will be created to house the original contents of sipStack.log and sipStack.log will now contain the newest information.



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.

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

The screenshot displays the 'Admin | SIP | SIP Stack' configuration page. At the top, there is a navigation bar with the InformaCast logo and various utility icons. The main content area features a breadcrumb trail 'Admin | SIP | SIP Stack' and a 'RESTORE' button. Below this, the text 'Provides low-level SIP functionality.' is followed by several configuration options: 'Enable Detailed Logging' (unchecked), 'Max Forwards' (70), 'Read Timeout' (1000), 'Cache Client Connections' (checked), and 'Cache Server Connections' (checked). 'CANCEL' and 'UPDATE' buttons are positioned at the bottom of the configuration section. The footer contains the Singlewire logo and copyright text: '© 2003–2014 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software.'



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.



Note If you enable detailed logging and the singlewireInformaCast service is restarted in Webmin or the virtual machine is restarted, you will need to re-enable detailed logging.

- **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.



Note

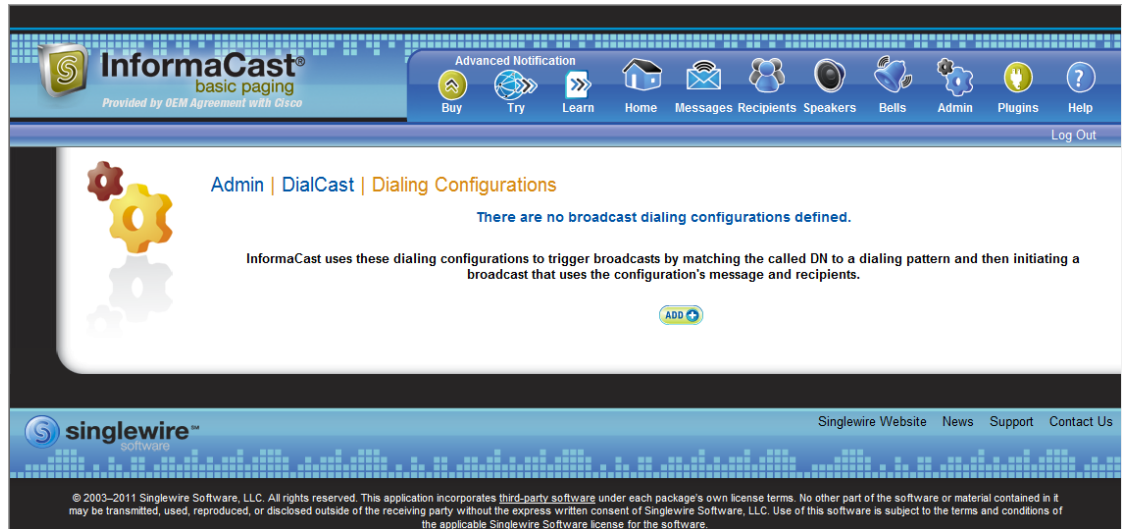
If you are running Unified Communications Manager in mixed mode and you want calls to and from InformaCast to use encrypted media, you must configure SRTP support (see "Enable SIP Call Security" on page 5-36).

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.

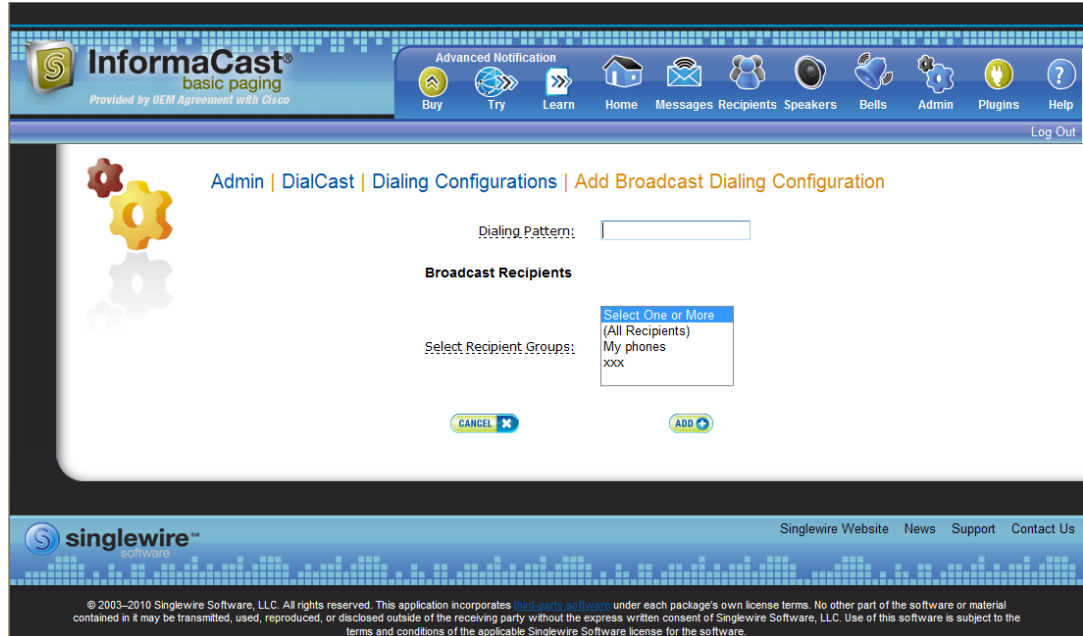
Add a Broadcast Dialing Configuration

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

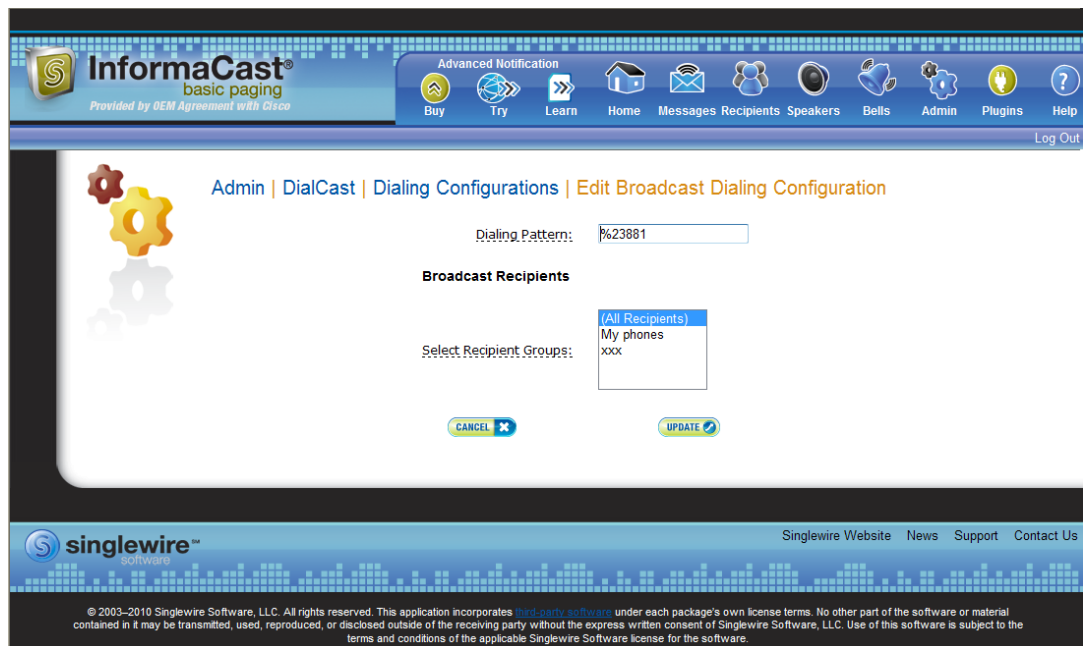
Once you have added dialing configurations, you may need to modify them.

Step 1 Go to **Admin | DialCast | Dialing Configurations**. The Dialing Configurations page appears.

The screenshot shows the InformaCast basic paging administration interface. The top navigation bar includes links for Buy, Try, Learn, Home, Messages, Recipients, Speakers, Bells, Admin, Plugins, and Help. The main content area displays the breadcrumb **Admin | DialCast | Dialing Configurations** and a description: "InformaCast uses these dialing configurations to trigger broadcasts by matching the called DN to a dialing pattern and then initiating a broadcast that uses the configuration's message and recipients." Below this is a table with columns for Dialing Pattern, Recipient Groups, and Action. One configuration is listed with a dialing pattern of 881 and recipient groups of (All Devices). An ADD button is visible above the table, and EDIT and DELETE buttons are visible below the table row.

Dialing Pattern	Recipient Groups	Action
881	(All Devices)	EDIT DELETED

- 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.

InformaCast[®]
basic paging
Provided by OEM Agreement with Cisco

Advanced Notification
Buy Try Learn Home Messages Recipients Speakers Bells Admin Plugins Help

Log Out

Admin | DialCast | Dialing Configurations

InformaCast uses these dialing configurations to trigger broadcasts by matching the called DN to a dialing pattern and then initiating a broadcast that uses the configuration's message and recipients.

ADD

Dialing Pattern	Recipient Groups	Action
881	(All Devices)	EDIT DELETE

singlewire[™]
software

Singlewire Website News Support Contact Us

© 2003–2010 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software.

Step 2 Click the **Delete** button next to the dialing configuration you want to delete. The Delete Broadcast Dialing Configuration page appears.

InformaCast[®]
basic paging
Provided by OEM Agreement with Cisco

Advanced Notification
Buy Try Learn Home Messages Recipients Speakers Bells Admin Plugins Help

Log Out

Admin | DialCast | Dialing Configurations | Delete Broadcast Dialing Configuration

You have chosen to delete the broadcast dialing configuration with the dialing pattern 881. Deleting this configuration will permanently remove it from the list of broadcast dialing configurations.

CANCEL DELETE

singlewire[™]
software

Singlewire Website News Support Contact Us

© 2003–2010 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software.

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 5-46).

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 5-47), which is tied to a SIP trunk (see “Configure a SIP Trunk” on page 5-4) in Unified Communications Manager. 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.”

The screenshot shows the InformaCast web interface. At the top, there is a navigation bar with the InformaCast logo and a navigation menu including Buy, Try, Learn, Home, Messages Recipients, Speakers, Bells, Admin, Plugins, and Help. Below the navigation bar, a notification states: "InformaCast is currently broadcasting. active broadcast(s)." Below this notification is a table of messages. The table has four columns: Description, Display Short Text, Type, and Action. The messages listed include Basic Paging Live Broadcast, Example Ad-Hoc Broadcast, Example failed mail server, Example Hammer, Example Humoctopus Alert, Example Monthly Meeting, Example Ring tone - Bell 1, Example Ring tone - Bell 2, Example Ring tone - Bell 3, Example Ring tone - Clock chime, Example Ring tone - Ding dong, Example Ring tone - Tone 1, Example Ring tone - Tone 2, Example Severe Weather, Example Singlewire Broadcast, Example Tomado, and Example Winter Weather. Each message row has a set of action buttons: SEND, EDIT, COPY, and DELETE. Below the table, there are navigation controls for the message list, including "Page 1 of 1", "Jump to page:", and "Show 50 results per page". At the bottom of the page, there is a footer with the Singlewire logo and copyright information.

Description	Display Short Text	Type	Action
Basic Paging Live Broadcast		Live Audio * *	SEND EDIT COPY DELETE
Example Ad-Hoc Broadcast	This is an ad-hoc broadcast.	Ad-Hoc Audio §	SEND EDIT COPY DELETE
Example failed mail server	Email is down at \$(time) on \$(date)	Text §	SEND EDIT COPY DELETE
Example Hammer	This is a broadcast of an industrial sounding hammer	Text and Pre-Recorded Audio §	SEND EDIT COPY DELETE
Example Humoctopus Alert	There is a Humoctopus in the building! --This is only a test.	Text and Pre-Recorded Audio * §	SEND EDIT COPY DELETE
Example Monthly Meeting	Monthly company wide meeting is at 8:00. Press the details soft-key.	Text §	SEND EDIT COPY DELETE
Example Ring tone - Bell 1		Pre-Recorded Audio *	SEND EDIT COPY DELETE
Example Ring tone - Bell 2		Pre-Recorded Audio *	SEND EDIT COPY DELETE
Example Ring tone - Bell 3		Pre-Recorded Audio *	SEND EDIT COPY DELETE
Example Ring tone - Clock chime		Pre-Recorded Audio *	SEND EDIT COPY DELETE
Example Ring tone - Ding dong		Pre-Recorded Audio *	SEND EDIT COPY DELETE
Example Ring tone - Tone 1		Pre-Recorded Audio *	SEND EDIT COPY DELETE
Example Ring tone - Tone 2		Pre-Recorded Audio *	SEND EDIT COPY DELETE
Example Severe Weather	Severe weather is in the area at \$(time) on \$(date).	Text §	SEND EDIT COPY DELETE
Example Singlewire Broadcast	This is a broadcast from Singlewire's Broadcast System!	Text and Pre-Recorded Audio §	SEND EDIT COPY DELETE
Example Tomado	There is a tomado in the area at \$(time) on \$(date).	Text §	SEND EDIT COPY DELETE
Example Winter Weather	There is severe winter weather in the area at \$(time) on \$(date).	Text §	SEND EDIT COPY DELETE

* Message will skip phones that are in use.
 § Message is persistent.
 * Message delivery is synchronized. It will start after a delay, and play only once.

Step 2 Click the **View** button to see a list of ongoing broadcasts. The Current Active Broadcasts page appears.

Description	Started	By User	Action
Sending broadcast (Example Singlewire Broadcast) to [Directory number: 71012]	Tue Dec 07 10:44:29 CST 2010	Temporary Administrator (admin)	END

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.

Manage Call Detail Records

When configured, InformaCast can create a call detail record for every SIP call it receives (DialCasts receive SIP calls). InformaCast can collect call data, such as changes to the call state and DTMF sent and received, as it interacts with the call and Unified Communications Manager. When the call ends, the collected data is written to an InformaCast directory accessible through the **Call Detail Records Directory** link on the Support page (**Help | Support**).

Collect Call Detail Records

You can collect call detail records and set a retention period that will eliminate saved records older than the set period through a scheduled job that runs every day at 3:30 a.m.

Step 1 Go to **Admin | System | Call Detail Records**. The Call Detail Records page appears.



Step 2 Select the **Write Call Detail Records** checkbox.

Step 3 Enter a numeric value in the **Call Detail Records Retention Period** field. This is the number of days a call detail record can age before it is removed from InformaCast.



Note Call detail records are written to InformaCast every minute. If you anticipate a large number of SIP calls, you may want to keep your retention period low.

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

View Call Detail Records

When InformaCast is configured to collect call detail records (see “Collect Call Detail Records” on page 5-54), those records are written to a directory accessible through the **Call Detail Records Directory** link on the Support page.

Step 1 Go to **Help | Support**. The Support page appears.

InformaCast[®]
basic paging
Provided by OEM Agreement with Cisco

Advanced Notification
Buy Try Learn Home Messages Recipients Speakers Bells Admin Plugins Help

Log Out

Help | Support

Your version of help is dependent on your version of Cisco Unified Communications Manager. InformaCast Basic Paging requires that your version of Cisco Unified Communications Manager be 9.0 or later.

If you have Unified Communications Manager 9.0 or later, you can contact Cisco directly for help: <http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html> or view InformaCast's installation and user guide.

If you have a version of Unified Communications Manager previous to 9.0, you have the following options:

- Click the **Try** icon to start your 60-day free trial of InformaCast Advanced Notification
- Click the **Buy** icon to obtain a demonstration, subscription, or purchased license for InformaCast Advanced Notification

Documentation

- [InformaCast User Guide](#)
- [Frequently Asked Questions](#)
- [Troubleshooting Guide](#)
- [API Documentation](#)
- [API Quick Start Guide](#)
- [End User License Agreement](#)

Tools

These links help carry out steps mentioned in the documentation, or suggested by technical support.

- [API Log](#) Shows requests made to the InformaCast REST API.
- [Calling Terminal Diagnostics](#) Shows the CTI ports and route points registered with InformaCast.
- [Call Detail Records Directory](#) Shows the directory containing the call detail records.
- [InformaCast Logs Directory](#) Shows the directory containing the InformaCast logs.
- [Log Tool](#) Collects and analyzes Singlewire log files for errors.
- [Performance Log](#) Contains information logged by InformaCast.
- [SIP Stack Log](#) Contains information logged by the SIP stack.
- [Summary Log](#) Contains a summary of broadcasts sent by InformaCast.

singlewire[®] software

Singlewire Website News Support Contact Us

© 2003–2016 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software.

Step 2 Click the **Call Detail Records Directory** link in the *Tools* area. The Call Detail Records Directory page appears.

The screenshot shows the InformaCast basic paging interface. The top navigation bar includes links for Buy, Try, Learn, Home, Messages, Recipients, Speakers, Bells, Admin, Plugins, and Help. The main content area displays the Call Detail Records Directory page, which includes a table of call detail records. The table has three columns: Name, Size (KB), and Last Modified. The records are listed as follows:

Name	Size (KB)	Last Modified
sip-201604131405.json	0.8	2016-04-13 09:06:00
sip-201604131403.json	0.8	2016-04-13 09:04:00
sip-201604122114.json	0.8	2016-04-12 16:15:00
sip-201604122113.json	0.8	2016-04-12 16:14:00
sip-201604122112.json	1.3	2016-04-12 16:13:00
sip-201604121939.json	0.8	2016-04-12 14:40:00
sip-201604121938.json	1.3	2016-04-12 14:39:00
sip-201604121937.json	1.2	2016-04-12 14:38:00

The footer of the page includes the Singlewire logo and the text: © 2003–2016 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software.

Call detail records are organized by date and time, e.g. sip-201603101453.json is a call detail record written on March 10, 2016 at 14:53 UTC. Each file may contain data for more than one call; the number of calls in a file depends on the number of calls ended during that particular minute.

Step 3 Click one of the **Name** links to view a call detail record. A call detail record might look similar to the following picture.

```
{
  "records": [
    {
      "callID": "afe09f80-70e15204-2a-a0e41eac@",
      "component": "DialCast",
      "start": "2016-04-13 09:04:52,678",
      "end": "2016-04-13 09:05:09,656",
      "duration": "000:00:00:16,978",
      "sessionActivity": [
        {
          "SIP": {
            "method": "INVITE",
            "time": "2016-04-13 09:04:52,678",
            "from": "105002",
            "fromHost": ":5061",
            "to": "#782",
            "toHost": ":5061",
            "earlyOffer": false,
            "userAgent": "Cisco-CUCM10.5",
            "transportProtocol": "TLS",
            "response": "200 (OK)"
          },
          "SDP": {
            "codec": "PCMU",
            "protocol": "RTP",
            "local": ":32094",
            "remote": ":18270",
            "streamDirection": ""
          }
        },
        {
          "SIP": {
            "method": "BYE",
            "time": "2016-04-13 09:05:09,655",
            "from": "105002",
            "fromHost": ":5061",
            "to": "#782",
            "toHost": ":5061",
            "userAgent": "Cisco-CUCM10.5",
            "transportProtocol": "TLS",
            "response": "200 (OK)"
          }
        }
      ]
    }
  ]
}
```

Each file has the following call detail record structure:

```
{ "records" : [ { <call 1> }, { <call 2> }, ... ] }
```

In the previous example, there is only one call in the record.

Each call within the record has the following structure:

```
{ <summary data>, "sessionActivity" : [ { <activity 1> }, { <activity 2> }, ... ] }
```


Summary data identifies the call and provides information about its date, duration, and the part of InformaCast that handled it, as shown in the following table:

Field	Definition	Example
callID	The unique identifier for the call	afe09f80-70e15204-2a-a0e41eac@172.30.228.160
component	The part of InformaCast handling the call, e.g. DialCast	DialCast
start	The date and time the call started, which corresponds to the time of the first INVITE request	2016-04-13 09:04:52,678
end	The date and time the call ended, which corresponds to the time of the BYE or CANCEL request	2016-04-13 09:05:09,656
duration	The length of the call in the format of: ddd:hh:mm:ss,mmm	000:00:00:16,978

Following summary data is session activity, which is comprised of SIP messages and DTMF sent and received during the call:

```
"sessionActivity" : [ { "SIP" : { <SIP-data> }, "SDP" : { <SDP-data> } }, ..., {
  "RTP" : {<RTP-data>}, "DTMF", {<DTMF-data> } }, ... ]
```

SIP data, as shown in the following table, includes SIP's message method, the date and time of the SIP message, the hosts sending and receiving the SIP message, etc.:

Field	Definition	Example
method	SIP's message method, e.g. INVITE, NOTIFY, INFO, BYE, CANCEL	INVITE
time	The date and time the SIP message was sent or received	2016-04-13 09:04:52,678
from	The source user in the SIP request; this will be a DN when interacting with Unified Communications Manager	105002
fromHost	The host sending the request	xxx.xx.xxx.xxx:5061
to	The destination user in the SIP request; this will be a DN when interacting with Unified Communications Manager	#782
toHost	The host receiving the request	xxx.xx.xxx.xxx:5061
earlyOffer	Whether the INVITE request contains an offer (true) or not (false)	false
userAgent	The SIP User Agent sending the request	Cisco-CUCM10.5
transportProtocol	The SIP transport protocol, which is obtained from the first VIA header in the request	TLS

Field	Definition	Example
negotiatedDtmfMethod	The DTMF transport method negotiated between InformaCast and Unified Communications Manager, e.g. NOTIFY, RFC_2833 (i.e. RTP), INFO	NOTIFY
response	The response code and explanation assigned to the SIP message; the default is 0 (unknown status)	200 (OK)

SDP data follows SIP data and includes the codec, Media Transport Protocol, local and remote media hosts, etc. as shown in the following table:

Field	Definition	Example
codec	The codec negotiated between InformaCast and Unified Communications Manager; currently, InformaCast supports only G.711 (PCM ULAW)	PCMU
protocol	The media transport protocol, e.g. RTP or SRTP	RTP
local	The local media host, i.e. InformaCast	xxx.xx.xxx.xxx:32094
remote	The remote media host; during a call with Unified Communications Manager, this will usually be a Cisco IP phone, but also might represent a music-on-hold server	xxx.xx.xxx.xxx18270
streamDirection	The media stream direction from the perspective of the host sending the INVITE request (see fromHost field in SIP data table), e.g. sendrecv, sendonly, recvonly, inactive; no value implies sendrecv	sendrecv

RTP data, not shown in the previous picture, follows SDP data and includes host and DTMF information, as shown in the following table:

Field	Definition	Example
time	The date and time when a DTMF tone was sent or received via RTP	2016-03-10 08:53:50,886
local	The local media host, i.e. InformaCast	xxx.xx.xxx.xxx:32094
remote	The remote media host; during a call with Unified Communications Manager, this will usually be a Cisco IP phone, but also might represent a music-on-hold server	xxx.xx.xxx.xxx18270

Lastly, DTMF data, not shown in the previous picture, includes the DTMF tone and its sent status, as shown in the following table:

Field	Definition	Example
tone	The DTMF tone that was sent or received, either by a SIP message or by RTP	3
sent	Whether InformaCast sent (true) or received (false) the DTMF tone	true



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.

InformaCast® basic paging
Provided by OEM Agreement with Cisco

Advanced Notification
Buy Try Learn Home Messages Recipients Speakers Bells Admin Plugins Help Log Out

Admin | Overview

Welcome to the InformaCast configuration overview page. For specific configuration tasks, please use the "Admin" menu.

InformaCast Server

Version	11.5.1 Basic Paging license
Start Time	2015-07-23 09:30:34
Current Time	2015-07-23 13:40:35
Application Mode	Stand-alone

Backup

Backup Activated	false
Next Scheduled Backup	
Backup Location	/usr/local/singlewire/InformaCast/backup

Cisco Unified Communications Manager

Cluster Version	Default configuration	10.5.2.12901-1
JTAPI Version	Cisco Jtapi version 10.5(2.12900)-1 Release	
Send Commands to Phones by JTAPI	false	

Phone Updates

Last Attempted Phone Rebuild	2015-07-23 13:13:00
Last Successful Phone Rebuild	2015-07-23 13:13:16
Last Attempted Phone Refresh	2015-07-23 13:21:00
Last Successful Phone Refresh	2015-07-23 13:21:00
Number of Phones Retrieved	26
Number of Phones Used / Licensed	0 / 50
Next Phone Rebuild	2015-07-23 14:13:00
Phone Refresh Interval (minutes)	23

CTI Route Points

Name	DN	State
RP02	8881212	IN_SERVICE
RP01	9101000	IN_SERVICE

SIP User Agent Status

User Agent is running

SIP Calls

There are no SIP calls.

Multicast Ports

Number of Multicast Ports Configured	301
Number of Multicast Ports Used by Audio Broadcasts	0
Number of Multicast Ports Used by Talk and Listen Messages	0
Number of Multicast Ports Unused	301

singlewire software
Singlewire Website News Support Contact Us

© 2003–2015 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software.

Beyond simply using InformaCast to send broadcasts, you can set up InformaCast backups and manage phone updates, SNMP monitoring, and session timeouts.

Change the Application Administrator's Password

The admin user, also known as the Application Administrator, is your preset InformaCast superuser, i.e. it holds all possible roles for InformaCast, and you initially set its password in Step 25 on page 2-17. Because of its elevated status, you may find it helpful to change this user's password periodically.



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.



Note

If you are using an older version of InformaCast, “Temporary Administrator” will appear at the top of the Change Password page.

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

Step 3 Enter a new password in the **New Password** and **Confirm Password** fields.



Note

When setting your password, you cannot use “changeMe.”

Step 4 Click the **Update** button.



Note

If the passwords you enter in both fields do not match, you will be prompted to try again.

**Tip**

When you change your Application Administrator password, it is a good idea to also change your OS Administrator password (see “Change the OS Administrator’s Password” on page 10-8).

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 6-4. 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 6-5), you will need to restart InformaCast whenever the content in the **Path** field changes. See “Start/Stop/Restart InformaCast and its Server” on page 9-5 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=<password>
rem Location of plink.exe
set plink=c:\plink.exe
```

Change **172.30.238.12** to InformaCast's IP address. Replace **<password>** with InformaCast's 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.

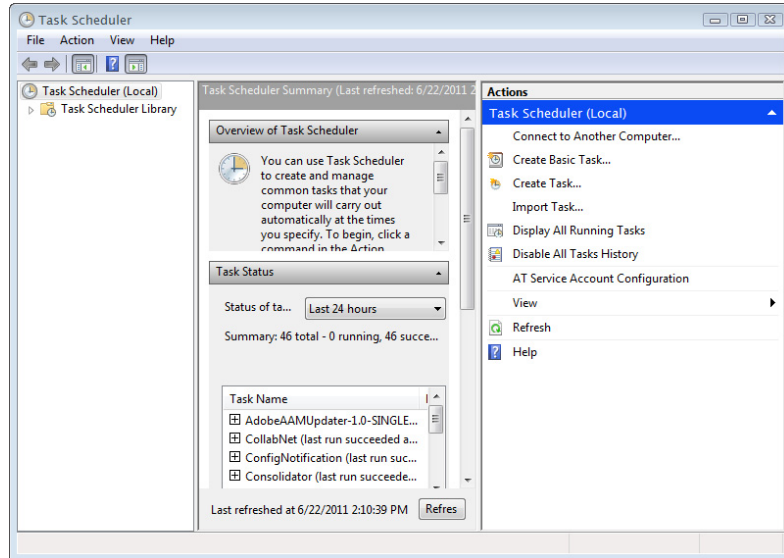
Step 8 Set up a Windows scheduled task to move the backup daily:

Step a. Go to **Control Panel | System and Security | Administrative Tools | Task Scheduler**.

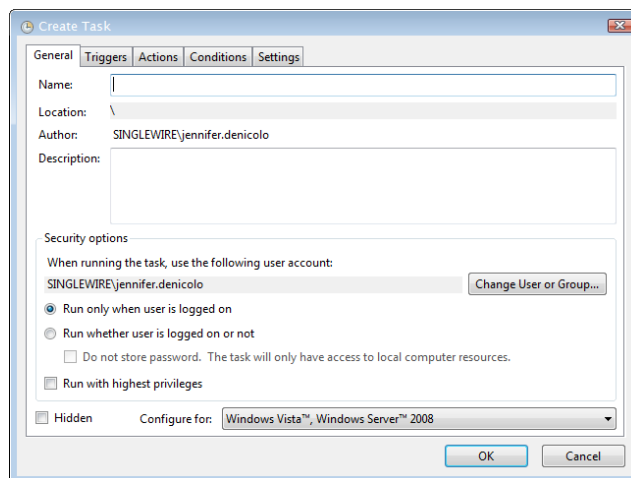


Note The scheduled tasks process is slightly different, depending on your version of Windows. The documented process may vary slightly from your environment.

The Task Scheduler window appears.



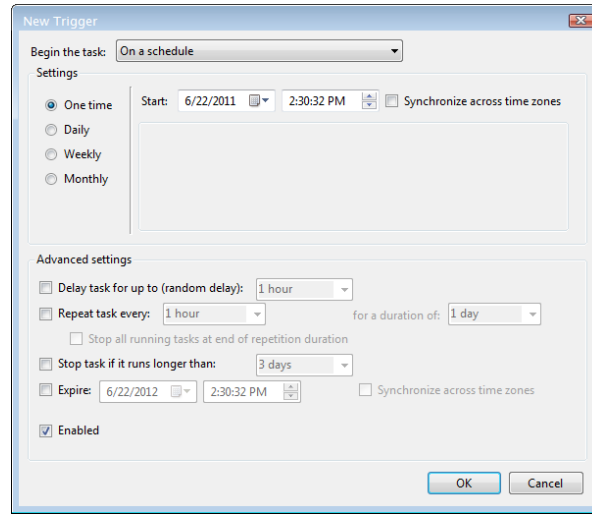
Step b. Go to **Action | Create Task**. The Create Task window appears.



Step c. Enter **InformaCast Backup** in the **Name** field.

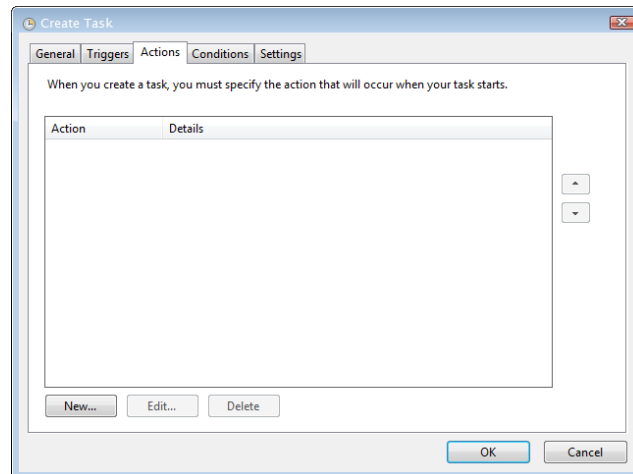
Step d. Select the **Run whether the user is logged on or not** radio button.

Step e. Click the **Triggers** tab and click its **New** button. The New Trigger dialog box appears.

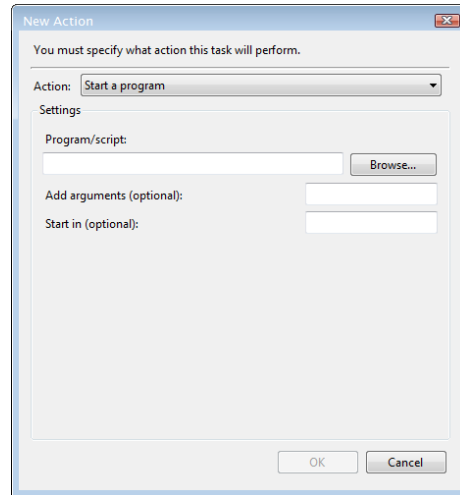


Step f. Configure the New Trigger dialog box to your specific environment and click the **OK** button.

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 2-27 for specific steps). The Webmin homepage appears.

Virtual Appliance Version	###
System hostname	singlewire
Operating system	Debian Linux 5.0
Webmin version	1.530
Time on system	Thu Jun 16 15:48:10 2011
Kernel and CPU	Linux 2.6.30-voyage on i686
Processor information	Quad-Core AMD Opteron(tm) Processor 2382, 1 cores
System uptime	3 days, 7 hours, 57 minutes
Running processes	48
CPU load averages	0.00 (1 min) 0.00 (5 mins) 0.00 (15 mins)
CPU usage	0% user, 0% kernel, 0% IO, 100% idle
Real memory	2.97 GB total, 32.40 MB used
Virtual memory	3.73 GB total, 0 bytes used
Local disk space	75.07 GB total, 1.78 GB used

Step 2 Go to **System | Bootup and Shutdown**. The Bootup and Shutdown page appears.

Login: admin

System

- Bootup and Shutdown
- Scheduled Cron Jobs
- Software Packages
- Networking
- Hardware
- System Time

Search:

System Information

Logout

Module Config

Bootup and Shutdown

Create a new bootup and shutdown action.

Action	At boot?	Description
<input type="checkbox"/> alsa-utils	No	This script stores and restores mixer levels on
<input type="checkbox"/> asterisk	No	Controls the Asterisk PBX
<input type="checkbox"/> atftpd	No	Launch atftpd server, a TFTP server useful
<input type="checkbox"/> awds	No	This script is used to start the AWDS daemon which provides
<input type="checkbox"/> batmand	No	/etc/init.d/batmand: start batmand
<input type="checkbox"/> bootlogd	No	Starts or stops the bootlogd log program
<input type="checkbox"/> bootmisc.sh	No	Some cleanup. Note, it need to run after mountnfs-bootclean.sh.
<input type="checkbox"/> checkfs.sh	No	Check all filesystems.
<input type="checkbox"/> checkroot.sh	No	Check to root file system.
<input type="checkbox"/> cron	Yes	cron is a standard UNIX program that runs user-specified
<input type="checkbox"/> dahdi	No	dahdi - load and configure DAHDI modules
<input type="checkbox"/> dnsmasq	No	DHCP and DNS server
<input type="checkbox"/> ebttables	No	Saves and restores the state of the ebttables rulesets.
<input type="checkbox"/> flashybrid	No	Flashybrid is a system to help in setting up and managing hybrid
<input type="checkbox"/> glibc.sh	No	
<input type="checkbox"/> gpsd	No	Start the GPS (Global Positioning System) daemon
<input type="checkbox"/> halt	No	
<input type="checkbox"/> hostapd	No	Userspace IEEE 802.11 AP and IEEE 802.1X/WPA/WPA2/EAP
<input type="checkbox"/> flashybrid	No	Flashybrid is a system to help in setting up and managing hybrid
<input type="checkbox"/> glibc.sh	No	
<input type="checkbox"/> gpsd	No	Start the GPS (Global Positioning System) daemon
<input type="checkbox"/> halt	No	
<input type="checkbox"/> single	No	executed by init(8) upon entering runlevel 1 (single).
<input type="checkbox"/> singlewireInformaCast	No	InformaCast application from Singlewire

Create a new bootup and shutdown action.

Start Stop Restart Start On Boot Disable On Boot Start Now and On Boot Disable Now and On Boot

Change to runlevel: Click this button to switch your system from the current runlevel to the selected one. This will cause all the actions in the current level to be stopped, and then all the actions in the new runlevel to be started.

Reboot System Click on this button to immediately reboot the system. All currently logged in users will be disconnected and all services will be re-started.

Shutdown System Click on this button to immediately shutdown the system. All services will be stopped, all users disconnected and the system powered off (if your hardware supports it).

Step 3 Scroll down the list of actions until you come to **singlewireInformaCast**. Click its link. The Edit Action page appears.

Login: admin

System

- Bootup and Shutdown
- Change Passwords
- Scheduled Cron Jobs
- Software Packages
- Networking
- Hardware
- System Information
- Logout

Module Index

Edit Action

Action Details

Name:

Action Script

```
#!/bin/sh
### BEGIN INIT INFO
# Short-Description: InformaCast
# Description: InformaCast application from Singlewire
### END INIT INFO

# Author: \[mailto:nicolas@singlewire.com\]
#

# Do NOT "set -e"

# PATH should only include /usr/* if it runs after the mountnfs.sh script
PATH=/sbin:/usr/sbin:/bin:/usr/bin
DESC="InformaCast"
NAME=singlewireInformaCast
```

Start at boot time? Yes No

Save Start Now Show Status Stop Now Delete

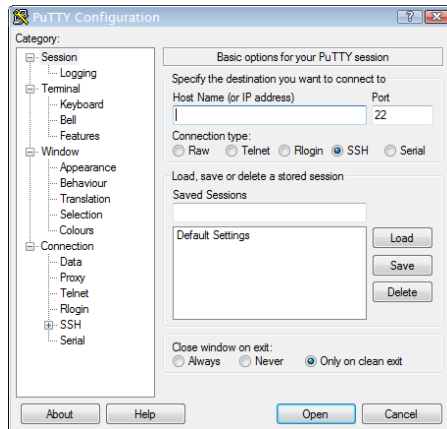
[Return to bootup and shutdown actions](#)

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.

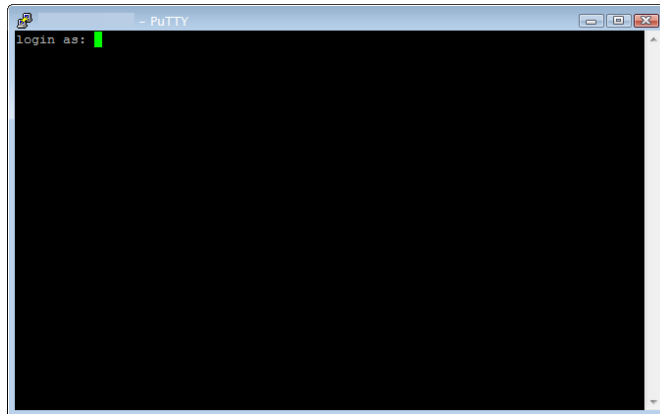


Step 6 Enter InformaCast's IP address in the **Host Name (or IP address)** field.

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.

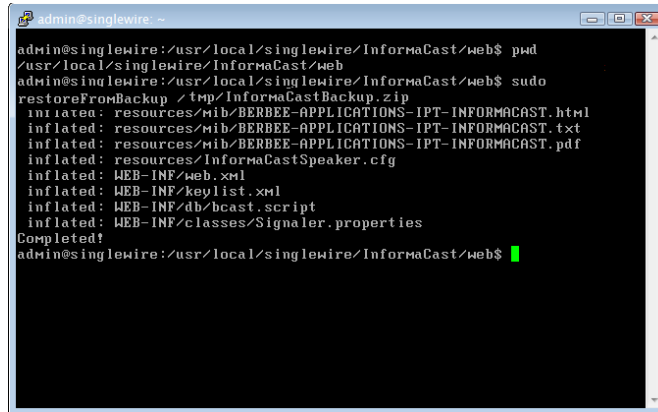


Step 10 Enter **admin** at the prompt and press the **Enter** key.

Step 11 Enter your OS password at the prompt and press the **Enter** key. The command-line interface refreshes, showing you that you're logged in.

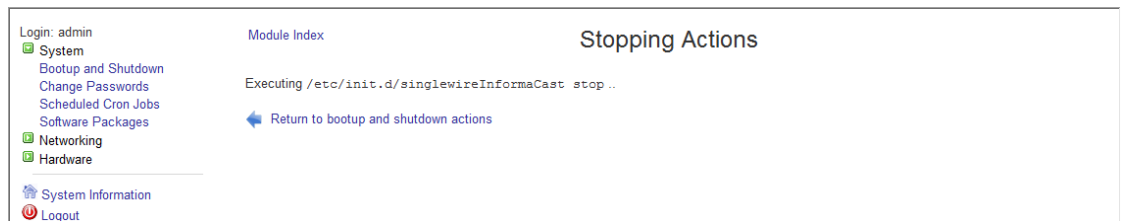


- Step 12** Enter `restoreFromBackup /<Directory of Backup>/InformaCastBackup.zip`, where `<Directory of Backup>` is the location of your `InformaCastBackup.zip` file, at the prompt and press the **Enter** key. The command-line interface refreshes, detailing the restoration process.



```
admin@singlewire: ~
admin@singlewire:/usr/local/singlewire/InformaCast/web$ pwd
/usr/local/singlewire/InformaCast/web
admin@singlewire:/usr/local/singlewire/InformaCast/web$ sudo
restoreFromBackup /tmp/InformaCastBackup.zip
inflated: resources/mib/BERBEE-APPLICATIONS-IPT-INFORMACAST.html
inflated: resources/mib/BERBEE-APPLICATIONS-IPT-INFORMACAST.txt
inflated: resources/mib/BERBEE-APPLICATIONS-IPT-INFORMACAST.pdf
inflated: resources/InformaCastSpeaker.cfg
inflated: WEB-INF/web.xml
inflated: WEB-INF/keylist.xml
inflated: WEB-INF/db/bcast.scrip
inflated: WEB-INF/classes/Signaler.properties
Completed!
admin@singlewire:/usr/local/singlewire/InformaCast/web$
```

- 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.

Login: admin

System

- Bootup and Shutdown
- Scheduled Cron Jobs
- Software Packages
- Networking
- Hardware
- System Time

Search:

System Information

Logout

Module Config

Bootup and Shutdown

Create a new bootup and shutdown action.

Action	At boot?	Description
<input type="checkbox"/> alsa-utils	No	This script stores and restores mixer levels on
<input type="checkbox"/> asterisk	No	Controls the Asterisk PBX
<input type="checkbox"/> atftpd	No	Launch atftpd server, a TFTP server useful
<input type="checkbox"/> awds	No	This script is used to start the AWDS daemon which provides
<input type="checkbox"/> batmand	No	/etc/init.d/batmand: start batmand
<input type="checkbox"/> bootlogd	No	Starts or stops the bootlogd log program
<input type="checkbox"/> bootmisc.sh	No	Some cleanup. Note, it need to run after mountnfs-bootclean.sh.
<input type="checkbox"/> checkfs.sh	No	Check all filesystems.
<input type="checkbox"/> checkroot.sh	No	Check to root file system.
<input type="checkbox"/> cron	Yes	cron is a standard UNIX program that runs user-specified
<input type="checkbox"/> dahdi	No	dahdi - load and configure DAHDI modules
<input type="checkbox"/> dnsmasq	No	DHCP and DNS server
<input type="checkbox"/> ebttables	No	Saves and restores the state of the ebttables rulesets.
<input type="checkbox"/> flashybrid	No	Flashybrid is a system to help in setting up and managing hybrid
<input type="checkbox"/> glibc.sh	No	
<input type="checkbox"/> gpsd	No	Start the GPS (Global Positioning System) daemon
<input type="checkbox"/> halt	No	
<input type="checkbox"/> hostapd	No	Userspace IEEE 802.11 AP and IEEE 802.1X/WPA/WPA2/EAP
<input type="checkbox"/> flashybrid	No	Flashybrid is a system to help in setting up and managing hybrid
<input type="checkbox"/> glibc.sh	No	
<input type="checkbox"/> gpsd	No	Start the GPS (Global Positioning System) daemon
<input type="checkbox"/> halt	No	
<input type="checkbox"/> single	No	executed by init(8) upon entering runlevel 1 (single).
<input type="checkbox"/> singlewireInformaCast	No	InformaCast application from Singlewire

Create a new bootup and shutdown action.

Start Stop Restart Start On Boot Disable On Boot Start Now and On Boot Disable Now and On Boot

Change to runlevel: Click this button to switch your system from the current runlevel to the selected one. This will cause all the actions in the current level to be stopped, and then all the actions in the new runlevel to be started.

Reboot System Click on this button to immediately reboot the system. All currently logged in users will be disconnected and all services will be re-started.

Shutdown System Click on this button to immediately shutdown the system. All services will be stopped, all users disconnected and the system powered off (if your hardware supports it).

Step 15 Scroll down the list of actions until you come to **singlewireInformaCast**. Click its link. The Edit Action page appears.

Login: admin

System

- Bootup and Shutdown
- Change Passwords
- Scheduled Cron Jobs
- Software Packages
- Networking
- Hardware
- System Information
- Logout

Module Index

Edit Action

Action Details

Name: singlewireInformaCast

Action Script

```
#!/bin/sh
### BEGIN INIT INFO
# Short-Description: InformaCast
# Description: InformaCast application from Singlewire
### END INIT INFO

# Author: [REDACTED]

# Do NOT "set -e"

# PATH should only include /usr/* if it runs after the mountnfs.sh script
PATH=/sbin:/usr/sbin:/bin:/usr/bin
DESC="InformaCast"
NAME=singlewireInformaCast
```

Start at boot time? Yes No

Save Start Now Show Status Stop Now Delete

[Return to bootup and shutdown actions](#)

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, Unified Communications Manager'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 | Cisco Unified Communications Manager Phone Updates**. The Unified Communications Manager Phone Updates page appears.

The screenshot shows the InformaCast basic paging administration interface. The top navigation bar includes links for Buy, Try, Learn, Home, Messages, Recipients, Speakers, Bells, Admin, Plugins, and Help. The main content area is titled "Admin | Telephony | Cisco Unified Communications Manager Phone Updates".

Build list of registered phones
 This process creates a list of registered phones and involves querying Unified Communications Manager to obtain the configuration and IP address for each registered phone.

If a field is not required, leaving it blank means "every." For example, leaving the **Hour** field blank would cause the update to be scheduled every hour of the day.

Job Description: Phone Data Update
 Second: (required)
 Minute: (required)
 Hour: (24-hour time)
 Month:
 Day of Month:
 Week Day:

Refresh list of registered phones
 This process refreshes the configuration of previously registered phones. A refresh can be performed as frequently as once per minute.

Refresh Interval (minutes): (Blank or zero means do not perform refresh)

Buttons: CANCEL, UPDATE

Footer: singlewire software, Singlewire Website, News, Support, Contact Us
 © 2003–2015 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software.



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

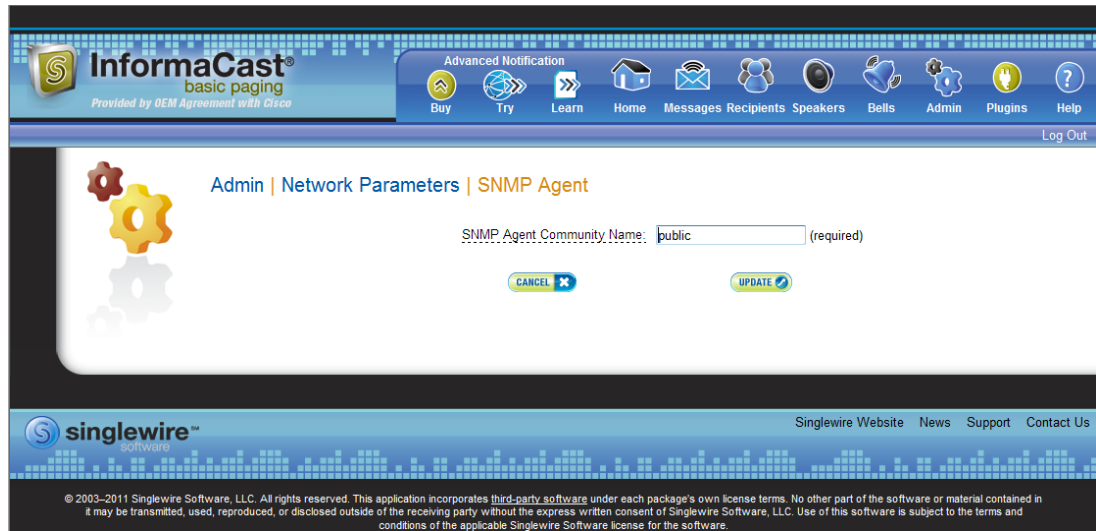
InformaCast has an embedded SNMP agent that can be paired with your own Network Management Software (NMS) in order to monitor certain aspects of InformaCast (i.e. the number of broadcasts sent, the length of time the application has been running, etc.). Through the import of a Management Information 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.



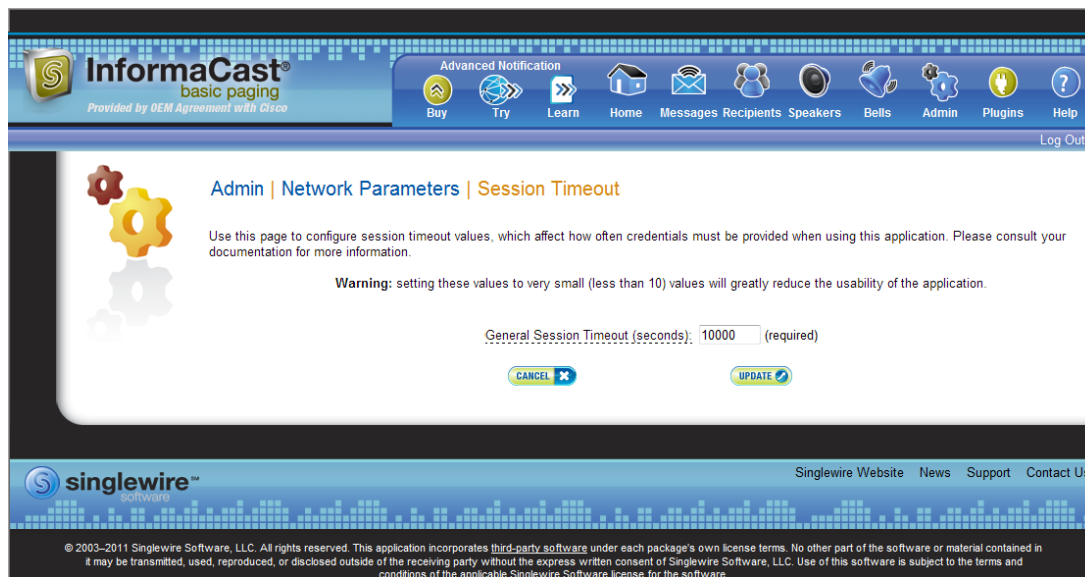
Step 2 Enter an SNMP community name in the **SNMP Agent Community Name** field. This community name and the one that your NMS is configured to use when talking to InformaCast must match in order for SNMP monitoring to work.

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 10-15.

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 Unified Communications Manager in Basic InformaCast, upgrading to Advanced InformaCast and then configuring Unified Communications Manager before downgrading to Basic InformaCast will require you to perform all the steps in “Integrate Unified Communications Manager” on page 2-45 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
- Unified Communications Manager 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

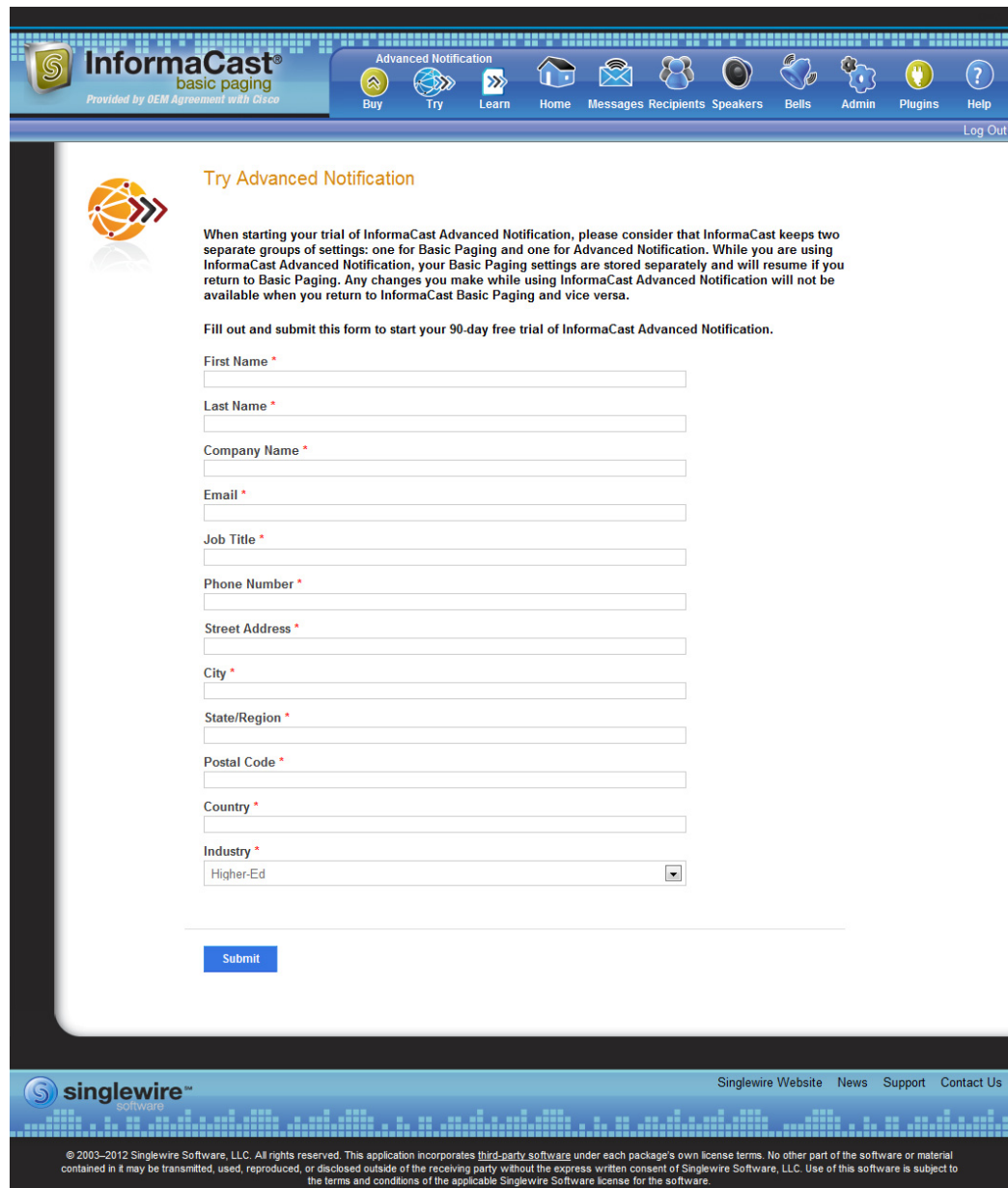
You will want to access the InformaCast Virtual Appliance Help System for Advanced Notification in a Cisco Unified Communications Manager Environment in order to make full use of all of InformaCast’s functionality. After upgrading, it can be obtained from **Help | InformaCast User Guide**. If you are 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.



InformaCast[®] basic paging
Provided by OEM Agreement with Cisco

Advanced Notification
Buy Try Learn Home Messages Recipients Speakers Bells Admin Plugins Help
Log Out

Try Advanced Notification

When starting your trial of InformaCast Advanced Notification, please consider that InformaCast keeps two separate groups of settings: one for Basic Paging and one for Advanced Notification. While you are using InformaCast Advanced Notification, your Basic Paging settings are stored separately and will resume if you return to Basic Paging. Any changes you make while using InformaCast Advanced Notification will not be available when you return to InformaCast Basic Paging and vice versa.

Fill out and submit this form to start your 90-day free trial of InformaCast Advanced Notification.

First Name *

Last Name *

Company Name *

Email *

Job Title *

Phone Number *

Street Address *

City *

State/Region *

Postal Code *

Country *

Industry *

Higher-Ed

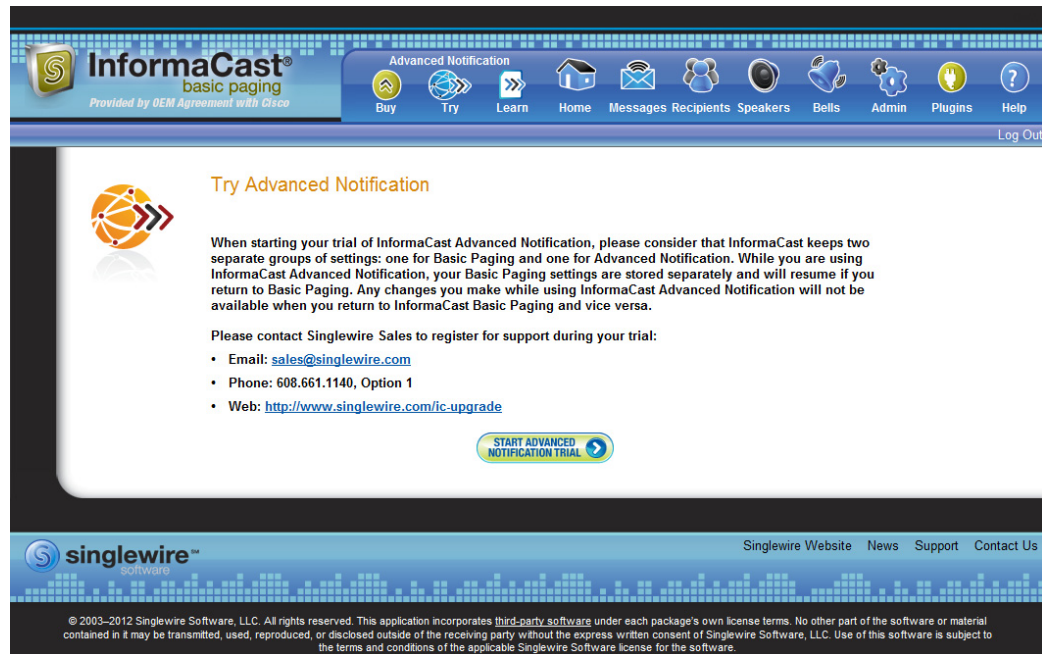
Submit

singlewire™ software

Singlewire Website News Support Contact Us

© 2003–2012 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software.

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.



InformaCast®
basic paging
Provided by OEM Agreement with Cisco

Advanced Notification

Buy Try Learn Home Messages Recipients Speakers Bells Admin Plugins Help

Log Out

Try Advanced Notification

When starting your trial of InformaCast Advanced Notification, please consider that InformaCast keeps two separate groups of settings: one for Basic Paging and one for Advanced Notification. While you are using InformaCast Advanced Notification, your Basic Paging settings are stored separately and will resume if you return to Basic Paging. Any changes you make while using InformaCast Advanced Notification will not be available when you return to InformaCast Basic Paging and vice versa.

Please contact Singlewire Sales to register for support during your trial:

- Email: sales@singlewire.com
- Phone: 608.661.1140, Option 1
- Web: <http://www.singlewire.com/ic-upgrade>

START ADVANCED NOTIFICATION TRIAL

singlewire™

Singlewire Website News Support Contact Us


© 2003–2012 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software.

Click the **Start Advanced Notification Trial** button. The Singlewire InformaCast Software License Agreement page appears.

InformaCast[®]
advanced notification

Advanced Notification
Buy Learn Home Messages Recipients Speakers Bells Admin Plugins Help

license expiration: Jan 12, 2013 Log Out


 **Singlewire InformaCast[®] Software License Agreement**

Copyright © 2010-12 Singlewire Software, LLC. All rights reserved.

This Singlewire InformaCast Software License Agreement is made by and between You (as defined below) and Singlewire Software, LLC, a Wisconsin limited liability company ("SINGLEWIRE"). This Software License Agreement and any order forms or sales orders for Software issued by SINGLEWIRE are referred to collectively herein as this "Agreement."

This Agreement constitutes a binding contract between You and SINGLEWIRE (together, the "Parties" and individually, each a "Party"). BY CLICKING THE "I ACCEPT" BUTTON BELOW, BY ACCEPTING THE TERMS OF THIS AGREEMENT THROUGH AN ORDER FORM THAT INCORPORATES THIS AGREEMENT, AND/OR BY USING THE SOFTWARE, YOU ARE ACCEPTING AND AGREEING TO THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT, CLICK THE "I DECLINE" BUTTON BELOW AND DO NOT USE THE SOFTWARE. IF YOU ARE AGREEING TO THIS AGREEMENT ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THIS AGREEMENT, AND "YOU" AND "YOUR" AS USED HEREIN SHALL REFER TO SUCH ENTITY.

THIS AGREEMENT IS EXPRESSLY CONDITIONED UPON THE PROVISIONS CONTAINED HEREIN, AND THE SINGLEWIRE TERMS AND CONDITIONS DOCUMENT LOCATED AT WWW.SINGLEWIRE.COM/TERMS (THE "ADDITIONAL TERMS"), WHICH IS INCORPORATED BY REFERENCE INTO THIS AGREEMENT AS IF FULLY STATED HEREIN. IN THE EVENT OF A CONFLICT BETWEEN THE ADDITIONAL TERMS AND THE TERMS OF THIS SOFTWARE LICENSE AGREEMENT WITH RESPECT TO THE SOFTWARE, THE TERMS OF THIS SOFTWARE LICENSE AGREEMENT SHALL CONTROL. ANY ADDITIONAL OR DIFFERENT TERMS OR CONDITIONS IN ANY FORM DELIVERED BY YOU OR ON YOUR BEHALF, WHETHER IN A PURCHASE ORDER OR OTHERWISE, ARE HEREBY DEEMED TO BE MATERIAL ALTERATIONS, AND NOTICE OF OBJECTION TO THEM AND REJECTION OF THEM IS HEREBY GIVEN BY SINGLEWIRE.

 Singlewire Website News Support Contact Us

© 2003-2012 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software.

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.

The screenshot shows the InformaCast Advanced Notification homepage. At the top, there is a navigation bar with the InformaCast logo and a list of menu items: Buy, Learn, Home, Messages, Recipients, Speakers, Bells, Admin, Plugins, and Help. A license expiration notice for Oct 26, 2012 is displayed. The main content area features a 'LIMITED TIME TRIAL - InformaCast Advanced Notification' banner with the InformaCast logo and a list of features. The footer includes the Singlewire logo and copyright information.

InformaCast® advanced notification

Advanced Notification

Buy Learn Home Messages Recipients Speakers Bells Admin Plugins Help

license expiration: Oct 26, 2012 Log Out

LIMITED TIME TRIAL - InformaCast Advanced Notification

InformaCast® advanced notification

InformaCast Advanced Notification is a powerful life-safety solution that will help you protect your people and property.


Learn how to implement and use these features in InformaCast Advanced Notification.


- Live Audio Paging to Cisco IP Phones
- Integration to Existing Overhead Paging (Not Available in Trial)
- Text and Audio to Cisco Phones and Endpoints
- Support for IP Speakers
- 911 (Emergency) Call Alerting/Recording (Not Available in Trial)
- Weather Notification
- Dynamic Conference Call
- Message Confirmation
- Pre-recorded and Scheduled Broadcasts
- Notification to Computers
- Reach Mobile/Remote Users
- Reach Social Media
- Bell/Shift Scheduler
- Regional/National Event Notification
- Send Notification from Events: Motion, Temperature, Door Opening, etc.
- Trigger Other Systems: Door Access, Lighting, Machines, etc.

singlewire™ Singlewire Website News Support Contact Us

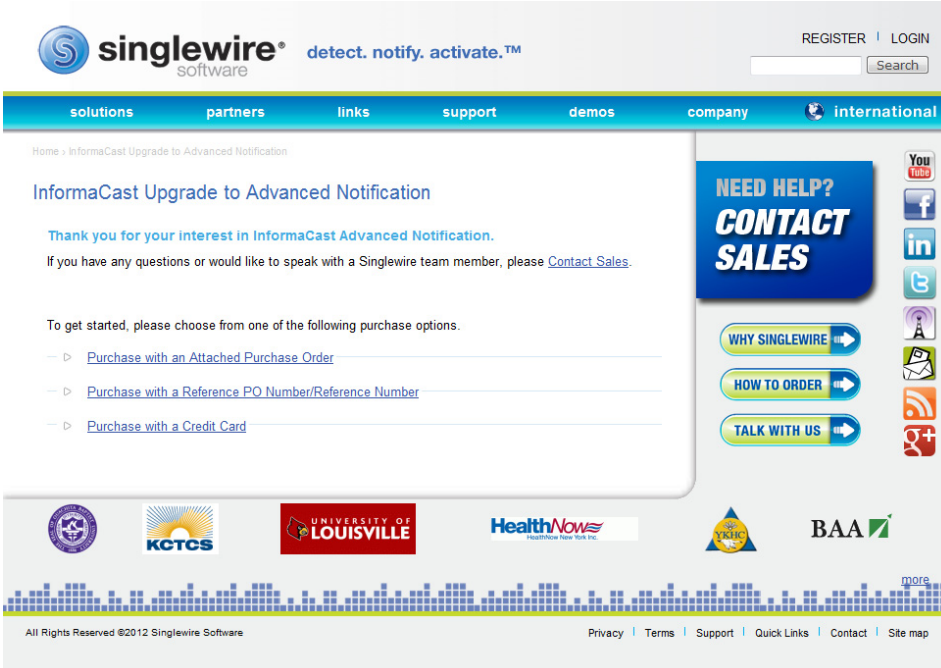
© 2003-2012 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software.

Buy Advanced Notification

By clicking the **Buy** icon () any time while using Basic InformaCast, 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.



The screenshot shows the Singlewire Software website interface. At the top, there is a logo for Singlewire Software with the tagline 'detect. notify. activate.™'. To the right of the logo are links for 'REGISTER' and 'LOGIN', and a search bar. Below the logo is a navigation menu with links for 'solutions', 'partners', 'links', 'support', 'demos', 'company', and 'international'. The main content area is titled 'InformaCast Upgrade to Advanced Notification' and includes a thank you message and a link to 'Contact Sales'. Below this, there are three purchase options: 'Purchase with an Attached Purchase Order', 'Purchase with a Reference PO Number/Reference Number', and 'Purchase with a Credit Card'. On the right side, there is a 'NEED HELP? CONTACT SALES' button and a vertical list of social media icons (YouTube, Facebook, LinkedIn, Twitter, RSS, etc.). At the bottom, there are logos for various partners including KCTCS, University of Louisville, HealthNow, and BAA. The footer contains copyright information and links for 'Privacy', 'Terms', 'Support', 'Quick Links', 'Contact', and 'Site map'.

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.

The information you're looking for is available online.



UPGRADE NOW

Use your mobile phone to scan this QR code or visit us online at:
www.singlewire.com/ic-upgrade

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 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.

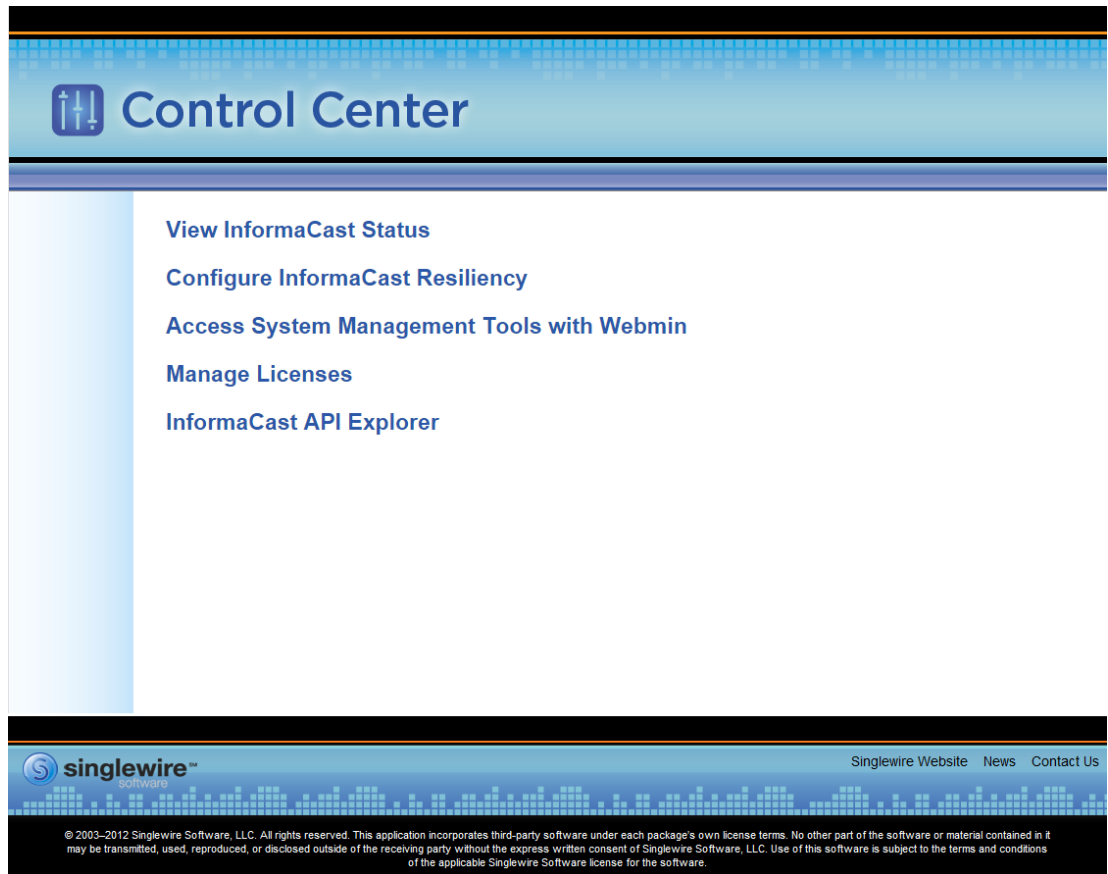
**Note**

Bell schedules, the number of IP phones and speakers, Unified Communications Manager 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](#).

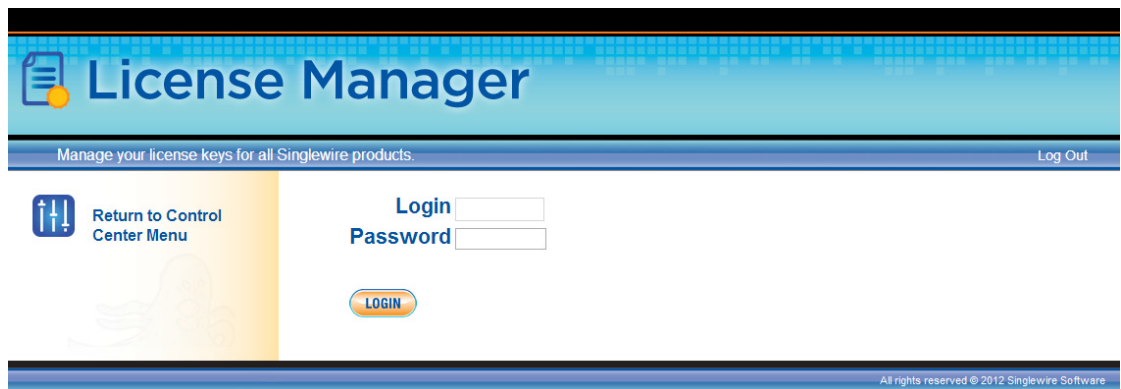
**Warning**

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.

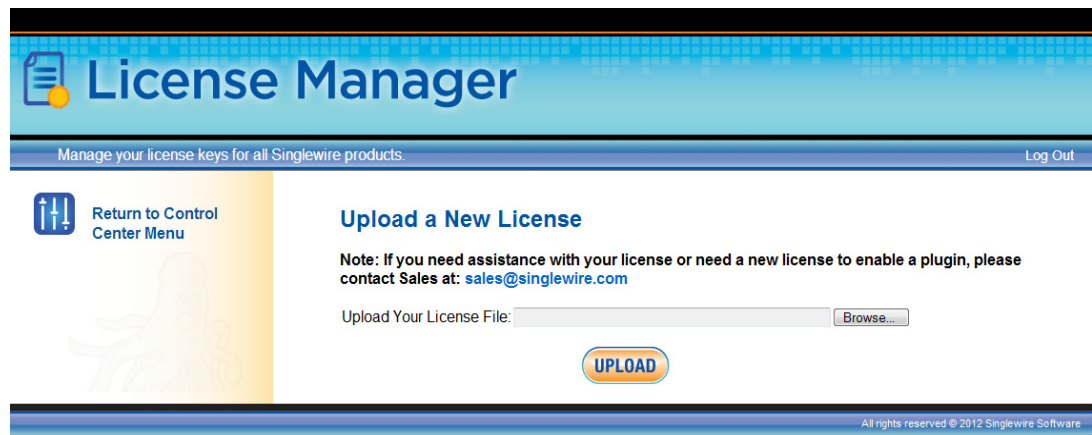
- Step 1** Log into the Control Center (see “Log into the Control Center” on page 2-25 for specific steps). The Control Center menu page appears.



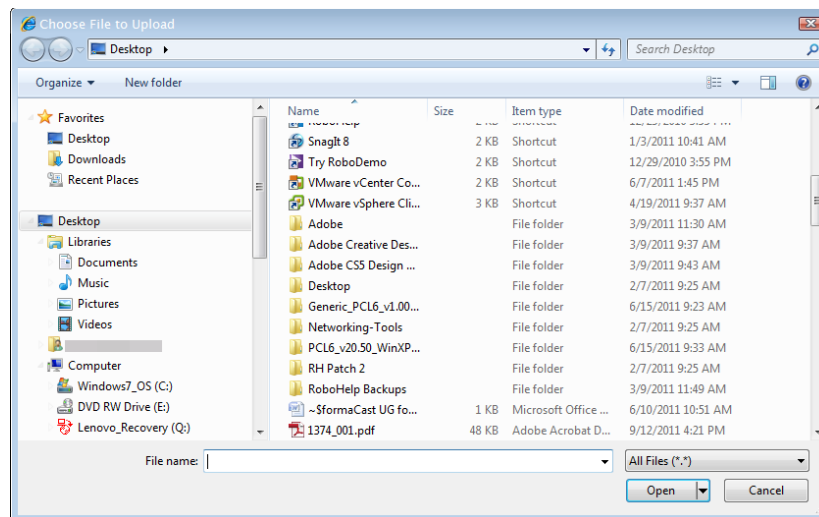
- Step 2** Click the **Manage Licenses** link. The License Manager page appears.



Step 3 Enter your OS credentials in the **Login** and **Password** fields. 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.

License Manager

Manage your license keys for all Singlewire products. Log Out

Return to Control Center Menu

License Status

License file installed. Restart any running applications that have had their license changed.

Note: If you need assistance with your license or need a new license to enable a plugin, please contact Sales at: sales@singlewire.com

The currently installed License Keys contain the following features:

InformaCast

Issuer: `nicksmueller`
Created: Mon Feb 27 15:13:09 CST 2012
Licensee: nick
IP Restriction: 172.30.227.233
Expiration: No expiration
Features: Audio, Clustering, MessageConfirmation
Parameters: MaxBellSchedules=50, MaxIPSpeakers=100, MaxPhones=500, MaxVersion=8.3, Scheme=Subscription

CallAware

Issuer: `nicksmueller`
Created: Mon Feb 27 15:14:15 CST 2012
Licensee: nick
IP Restriction: 172.30.227.233
Expiration: No expiration
Features:
Parameters:

IC Plugin: ICAP

Issuer: `katie henkel`
Created: Fri Jan 27 11:25:12 CST 2012
Licensee: Katie for Testing
IP Restriction: Not restricted
Expiration: No expiration
Features:
Parameters:

IC Plugin: ConferenceCall

Issuer: `katie henkel`
Created: Mon Jun 27 10:32:10 CDT 2011
Licensee: Katie for testing
IP Restriction: Not restricted
Expiration: No expiration
Features:
Parameters:

IC Plugin: DMM

Issuer: `katie henkel`
Created: Wed Jul 20 13:47:30 CDT 2011
Licensee: Katie for testing
IP Restriction: Not restricted
Expiration: No expiration
Features:
Parameters:

Replace Your License(s): No file chosen

UPLOAD

All rights reserved © 2012 Singlewire Software

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 Unified Communications Manager, 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 a signed certificate (see “Create and Install a Signed Certificate” on page 2-38).

- 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 9-5), 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 Unified Communications Manager’s Enterprise Parameters? Please see Steps 4 and 5 on page 2-81.
 - 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 2-88.
- 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 Unified Communications Manager. 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 4-38.
- 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 10-9 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 2-88.

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, accessible through the **InformaCast Logs Directory** link on the Support page (**Help | Support**), is the place to look.

Another log file generated in the InformaCast logs directory is sipStack.log (go to **Help | Support**). Please see “Manage the SIP Stack” on page 5-44 for more information.

Problem I had detailed SIP logging enabled but I’m not seeing changes in sipStack.log.

Solution SIP logging will automatically change from detailed logging to standard logging when:

- The singlewireInformaCast service is restarted (or stopped then started) in Webmin
- The virtual machine is restarted (or stopped then started)

If you would like to enable detailed logging, follow the steps in “Manage the SIP Stack” on page 5-44.

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 29 on page 2-20.

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:

- “Access InformaCast Virtual Appliance” on page 2-22
- “Log into InformaCast” on page 2-23

- “Log into the Control Center” on page 2-25
- “Log into Webmin” on page 2-27

Problem What are my OS or application credentials?

Solution Your OS credentials allow you to enter Webmin and Control Center as an administrator or access the Virtual Appliance’s command line through SSH. Your application credentials allow you to enter InformaCast as an administrator. By default, both your OS and application usernames are “admin.” If you lose or can’t remember the password to your OS or application credentials, [contact Singlewire Support](#). They can help reset the passwords for you.

Problem What characters are allowed for my OS and application credentials, and what kind of restrictions are in place?

Solution When creating your OS and application credentials, the characters in the following table are allowed.

Symbol	Description
!	Exclamation mark
"	Double quotes (or speech marks)
#	Number
\$	Dollar
%	Percent
&	Ampersand
'	Single quote
(Open parenthesis (or open bracket)
)	Close parenthesis (or close bracket)
*	Asterisk
+	Plus
,	Comma
-	Hyphen
.	Period, dot or full stop
/	Slash or divide
0	Zero
1	One
2	Two
3	Three
4	Four
5	Five
6	Six
7	Seven
8	Eight

Symbol	Description
9	Nine
:	Colon
;	Semicolon
<	Less than (or open angled bracket)
=	Equals
>	Greater than (or close angled bracket)
?	Question mark
@	At symbol
A/a	Upper- or lowercase A
B/b	Upper- or lowercase B
C/c	Upper- or lowercase C
D/d	Upper- or lowercase D
E/e	Upper- or lowercase E
F/f	Upper- or lowercase F
G/g	Upper- or lowercase G
H/h	Upper- or lowercase H
I/i	Upper- or lowercase I
J/j	Upper- or lowercase J
K/k	Upper- or lowercase K
L/l	Upper- or lowercase L
M/m	Upper- or lowercase M
N/n	Upper- or lowercase N
O/o	Upper- or lowercase O
P/p	Upper- or lowercase P
Q/q	Upper- or lowercase Q
R/r	Upper- or lowercase R
S/s	Upper- or lowercase S
T/t	Upper- or lowercase T
U/u	Upper- or lowercase U
V/v	Upper- or lowercase V
W/w	Upper- or lowercase W
X/x	Upper- or lowercase X
Y/y	Upper- or lowercase Y
Z/z	Upper- or lowercase Z
[Opening bracket

Symbol	Description
\	Backslash
]	Closing bracket
^	Caret - circumflex
_	Underscore
`	Grave accent

In addition, the following password restrictions apply:

- The maximum password length is 15 characters
- The minimum password length is six characters
- Passwords cannot be “changeMe”
- Passwords must be different from your usernames
- Passwords must contain at least one lowercase letter
- Passwords must contain at least one number
- Passwords must contain at least one of the following characters: !"#%&'()*+,-./:;<=>?@[\\]^_`
- Passwords can only contain ASCII characters (see the previous table)
- Passwords may not be palindromes (e.g. 1!Madam!1)

Problem I set the passwords for my OS and application credentials when I installed and/or upgraded InformaCast. Why am I being asked to set it again?

Solution Did you change your password back to changeMe? That password is not a valid entry.

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 10-1
- “Start an Application on InformaCast Virtual Appliance” on page 10-3
- “Restart an Application on InformaCast Virtual Appliance” on page 10-5
- “Reboot the InformaCast Virtual Appliance” on page 10-7

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 10-14 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 Unified Communications Manager'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 Unified Communications Manager 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 Unified Communications Manager'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 Unified Communications Manager's administrative interface and ensure that your application user's credentials in InformaCast match those in Unified Communications Manager.
- **SNMP Community Name.** Verify that the value you entered here matches the value in Unified Communications Manager. Use the [Multicast Testing Tool](#) to verify SNMP functionality.

Problem I'm seeing the error, "Default configuration Not Connected," in the Unified 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 information from Unified Communications Manager. Once this is done, the Unified Communications Manager information appears correctly on the Admin Overview page.

Phone Discovery

Problem I've added new phones to Unified Communications Manager 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 Unified Communications Manager) 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 Unified Communications Manager cluster. Schedule your phone caches to rebuild through the Unified Communications Manager Phone Updates page (**Admin | Telephony | Cisco Unified Communications Manager Phone Updates**).

Problem There are phones missing from my recipient groups.

Solution If InformaCast is unable to learn about the phones in your Unified Communications Manager environment, it cannot work properly. It must do this by interacting with the Unified Communications Manager 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 Unified Communications Manager 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 Unified Communications Manager 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 Unified Communications Manager server. Make sure that these are correct. Start by logging into your Unified Communications Manager 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 Unified Communications Manager server. Make sure the **Unified Communications Manager IP Address(es)** field on the Edit Telephony Configuration page contains the correct numeric IP address of your Unified Communications Manager server.
- SNMP is properly enabled. Ensure that SNMP is enabled on all cluster nodes. See "Configure Unified Communications Manager SNMP" on page 2-46 for information about configuring SNMP v2 or SNMP v3. You can use the [Multicast Testing Tool](#) to troubleshoot SNMP further.
- You're using a supported Unified Communications Manager version. See "Prerequisites" on page 1-2 for the list of supported Unified Communications Managers. If you're running an older version of Unified Communications Manager, 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 Unified Communications Manager cluster node.
- There are usable phones registered. If everything else seems fine, it's worth double-checking, via the Unified Communications Manager 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 Unified Communications Manager 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.

Problem I'm using the E.164 dial plan and I just upgraded to InformaCast 11.0.5. I have several recipient groups set up that use rules to match DN's for inclusion and now those recipient groups aren't showing any recipients.

Solution With the upgrade to InformaCast 11.0.5, the E.164 dial plan is explicitly supported. You no longer have to enter a leading backslash when creating rules for your recipient groups on the Add/Edit Recipient Group page. Adjust your filters from `\+<DN>` to `+<DN>` and your matched DN's should appear.

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 Unified Communications Manager: 9.1.1 or 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 Unified Communications Manager versions 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, 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 Unified Communications Manager, but didn't upgrade JTAPI on the Virtual Appliance
- Unified Communications Manager'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 Unified Communications Manager. 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	2010-07-13 09:00	false	3333		
RajCTI2	IN_SERVICE	2010-07-13 09:00	false	2222		
RajCTI1	IN_SERVICE	2010-07-13 09:00	false	1111		
RajCTI7	IN_SERVICE	2010-07-13 09:00	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	2010-07-07 09:00	false	25667	Call ID : 60808/1 Calling : 25667 Called : 8510028	k@01/13/2011 10:08:46 AM

You can use the Calling Terminal Diagnostics page to verify that your CTI devices in Unified Communications Manager 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 My DialCasts are failing and when I check the Performance log, I see a CallMapper error. How can I fix this?

Solution If your message's **Description** field (on the Add/Edit Message page) contains \$ or \, you must escape those characters with a \ in order to use the Add/Edit Broadcast Dialing Configuration page's **Message Description** field. This same configuration applies to the **Name** field on the Add/Edit Recipient Group page and the **Recipient Group Name** field on the Add/Edit Broadcast Dialing Configuration page.

For example, your message's **Description** field is **Meeting Message Using \$ and **. In the **Message Description** field on the Add/Edit Broadcast Dialing Configuration page, you must have **Meeting Message Using \\$ and ** in order for a match to occur.

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.

Problem My SIP trunk and InformaCast are configured to use SRTP but RTP is always used.

Solution SRTP is available when Unified Communications Manager is in mixed mode. If you are unsure of your Unified Communications Manager's mode, contact your administrator. Once you know your Unified Communications Manager is in mixed mode, check these other configurations:

- Did you add a new SIP profile for the SIP trunk? SRTP won't work until this new profile is created and attached to your SIP trunk. You must also select the **SRTP Allowed** checkbox for your SIP trunk. See "Add a SIP Profile for SRTP" on page 5-21 and "Add a SIP Trunk That Uses TLS" on page 5-24 for more information.
- In InformaCast, verify that the **Secure Signaling Required** and **Secure RTP Allowed** checkboxes are selected on the SIP Call Security page (see "Enable SIP Call Security" on page 5-36).

Problem I hear a busy signal when I dial my SIP route pattern on a non-secure phone (this route pattern is set up as a DialCast dialing pattern). My call goes through when I dial the same route pattern on a secure phone.

Solution Are you using SIP with TLS and SRTP? The same SIP route pattern will not work on secure and non-secure phones when SRTP is enabled and the SIP profile for the trunk is the standard SIP profile.

Add a new SIP profile with **Best Effort (no MTP inserted)** selected from the **Early Offer support for voice and video calls** dropdown menu, then associate it with the SIP trunk. Verify that the **SRTP Allowed** checkbox is selected for your SIP trunk. See "Add a SIP Profile for SRTP" on page 5-21 and "Add a SIP Trunk That Uses TLS" on page 5-24 for more information.

In addition, SRTP is only available when Unified Communications Manager is in mixed mode. If you are unsure of your Unified Communications Manager's mode, contact your administrator.

Lastly, in InformaCast, verify that the **Secure Signaling Required** and **Secure RTP Allowed** checkboxes are selected on the SIP Call Security page (see "Enable SIP Call Security" on page 5-36).

Problem I hear a busy signal when I dial the route pattern for my SIP trunk that uses TLS (this route pattern is set up as a dialing configuration in DialCast).

Solution Make sure the **Secure Signaling Required** checkbox is selected on InformaCast's SIP Call Security page (see "Enable SIP Call Security" on page 5-36). The **Secure RTP Allowed** checkbox on the same page should not be selected unless you are planning to use SRTP.

It is also a good idea to check the SIP trunk configuration in Unified Communications Manager does not have the **SRTP Allowed** checkbox selected on the Trunk Configuration page (see "Add a SIP Trunk That Uses TLS" on page 5-24 for more information).

Backups

Problem My InformaCast backups keep failing.

Solution Do you have special characters in your Application Administrator password (i.e. the password you use when logging into InformaCast and PushToTalk)? Running the `dobackup.cmd` script will fail if your password has special characters. Consider changing your password.

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 10-15.

Problem I upgraded InformaCast and I was previously using SIP. Since the upgrade, broadcasts triggered by DialCast aren’t working.

Solution Were your DialCasts using secure SIP (i.e. SIP over TLS)? Due to the added features of SIP, you need to perform some new configuration steps before SIP will work. Review your SIP configuration and select the **Secure Signaling Required** checkbox on the SIP Call Security page (see “Enable SIP Call Security” on page 5-36). Once you save your changes, your DialCasts will function again.

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 Unified Communications Manager'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 Unified Communications Manager's administrative interface and ensure that your application user's credentials in InformaCast match those in Unified Communications Manager.
- **SNMP Community Name.** Verify that the value you entered here matches the value in Unified Communications Manager. 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 Unified Communications Manager. Once this is done, the Unified Communications Manager 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 Unified Communications Manager using SNMP and AXL. If you have phones missing from a recipient group, ensure the following:

- The Unified Communications Manager Admin account has the correct username/password information
- SNMP is enabled on all Unified Communications Manager cluster nodes
- SNMP community strings have READ permissions on all Unified Communications Manager cluster nodes
- SNMP community strings are the same on all Unified Communications Manager cluster nodes
- Nothing is blocking UDP port 161 from InformaCast to all Unified Communications Manager cluster nodes

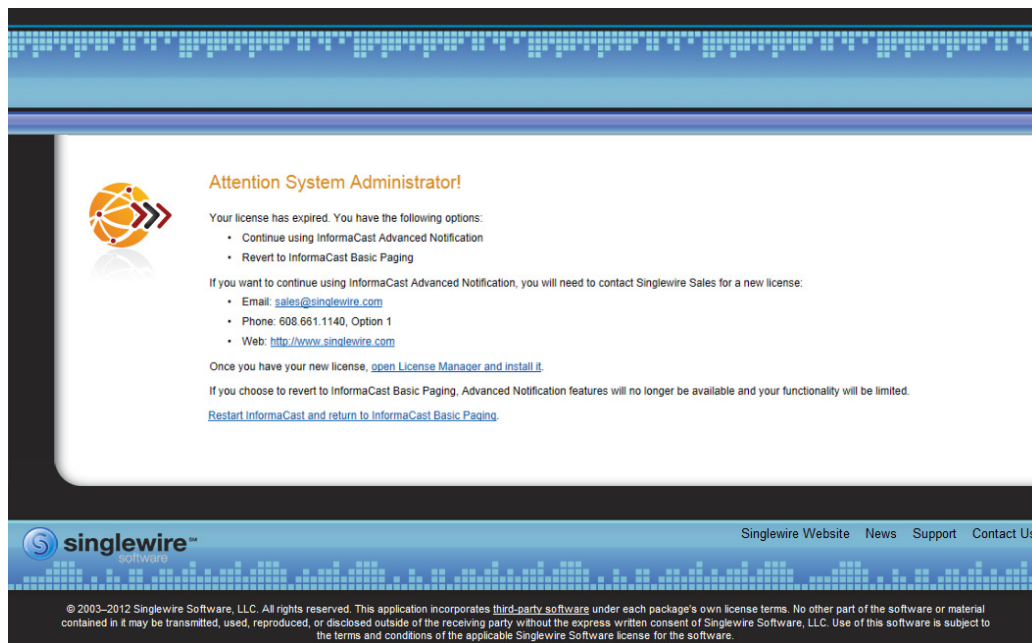
You can use the [Multicast Testing Tool](#) to troubleshoot SNMP further.

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.

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 2-27 for specific steps). The Webmin homepage appears.

The screenshot shows the Webmin interface with the 'System Information' page selected. The page displays system details for a virtual appliance named 'singlewire'. The details include system hostname, operating system, Webmin version, time on system, kernel and CPU information, processor information, system uptime, running processes, CPU load averages, CPU usage, real memory, virtual memory, and local disk space. Each resource usage section includes a blue progress bar indicating the amount used relative to the total available.

Virtual Appliance Version	###
System hostname	singlewire
Operating system	Debian Linux 5.0
Webmin version	1.530
Time on system	Thu Jun 16 15:48:10 2011
Kernel and CPU	Linux 2.6.30-voyage on i686
Processor information	Quad-Core AMD Opteron(tm) Processor 2382, 1 cores
System uptime	3 days, 7 hours, 57 minutes
Running processes	48
CPU load averages	0.00 (1 min) 0.00 (5 mins) 0.00 (15 mins)
CPU usage	0% user, 0% kernel, 0% IO, 100% idle
Real memory	2.97 GB total, 32.40 MB used
Virtual memory	3.73 GB total, 0 bytes used
Local disk space	75.07 GB total, 1.78 GB used

Step 2 Go to **System | Bootup and Shutdown**. The Bootup and Shutdown page appears.

Login: admin
 System
 Bootup and Shutdown
 Scheduled Cron Jobs
 Software Packages
 Networking
 Hardware
 System Time
 Search:
 System Information
 Logout

Module Config: Bootup and Shutdown

Create a new bootup and shutdown action.

Action	At boot?	Description
<input type="checkbox"/> alsa-utils	No	This script stores and restores mixer levels on
<input type="checkbox"/> asterisk	No	Controls the Asterisk PBX
<input type="checkbox"/> atftpd	No	Launch atftpd server, a TFTP server useful
<input type="checkbox"/> awds	No	This script is used to start the AWDS daemon which provides
<input type="checkbox"/> batmand	No	/etc/init.d/batmand: start batmand
<input type="checkbox"/> bootlogd	No	Starts or stops the bootlogd log program
<input type="checkbox"/> bootmisc.sh	No	Some cleanup. Note, it need to run after mountnfs-bootclean.sh.
<input type="checkbox"/> checkfs.sh	No	Check all filesystems.
<input type="checkbox"/> checkroot.sh	No	Check to root file system.
<input type="checkbox"/> cron	Yes	cron is a standard UNIX program that runs user-specified
<input type="checkbox"/> dahdi	No	dahdi - load and configure DAHDI modules
<input type="checkbox"/> dnsmasq	No	DHCP and DNS server
<input type="checkbox"/> ebttables	No	Saves and restores the state of the ebttables rulesets.
<input type="checkbox"/> flashybrid	No	Flashybrid is a system to help in setting up and managing hybrid
<input type="checkbox"/> glibc.sh	No	
<input type="checkbox"/> gpsd	No	Start the GPS (Global Positioning System) daemon
<input type="checkbox"/> halt	No	
<input type="checkbox"/> hostapd	No	Userspace IEEE 802.11 AP and IEEE 802.1X/WPA/WPA2/EAP
<input type="checkbox"/> flashybrid	No	Flashybrid is a system to help in setting up and managing hybrid
<input type="checkbox"/> glibc.sh	No	
<input type="checkbox"/> gpsd	No	Start the GPS (Global Positioning System) daemon
<input type="checkbox"/> halt	No	
<input type="checkbox"/> single	No	executed by init(8) upon entering runlevel 1 (single).
<input type="checkbox"/> singlewireInformaCast	No	InformaCast application from Singlewire

Create a new bootup and shutdown action.

Start Stop Restart Start On Boot Disable On Boot Start Now and On Boot Disable Now and On Boot

Change to runlevel: 2 Click this button to switch your system from the current runlevel to the selected one. This will cause all the actions in the current level to be stopped, and then all the actions in the new runlevel to be started.

Reboot System Click on this button to immediately reboot the system. All currently logged in users will be disconnected and all services will be re-started.

Shutdown System Click on this button to immediately shutdown the system. All services will be stopped, all users disconnected and the system powered off (if your hardware supports it).

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.

Login: admin
 System
 Bootup and Shutdown
 Change Passwords
 Scheduled Cron Jobs
 Software Packages
 Networking
 Hardware
 System Information
 Logout

Module Index: Edit Action

Action Details

Name: singlewireInformaCast

Action Script

```
#!/bin/sh
### BEGIN INIT INFO
# Short-Description: InformaCast
# Description: InformaCast application from Singlewire
### END INIT INFO

# Author: [REDACTED]

# Do NOT "set -e"

# PATH should only include /usr/* if it runs after the mountnfs.sh script
PATH=/sbin:/usr/sbin:/bin:/usr/bin
DESC="InformaCast"
NAME=singlewireInformaCast
```

Start at boot time? Yes No

Save Start Now Show Status Stop Now Delete

Return to bootup and shutdown actions

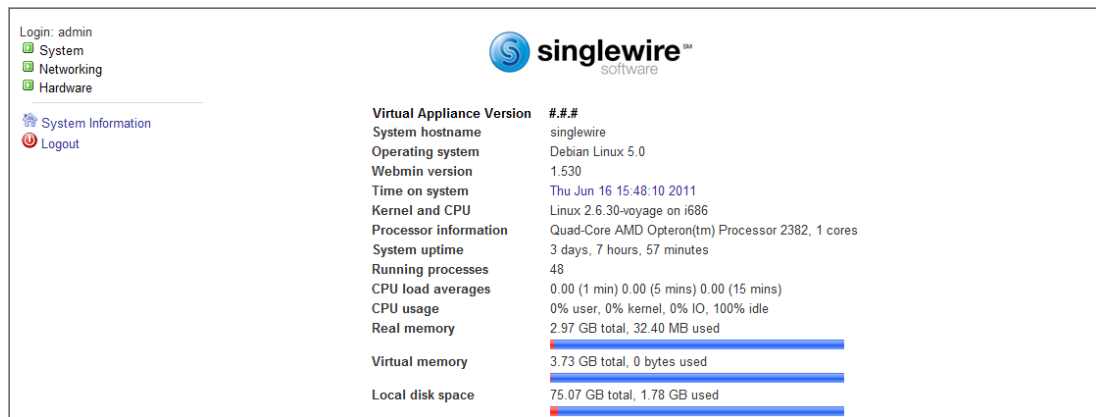
Step 4 Click the **Stop Now** button. It will take a minute or so for the application to stop.



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 2-27 for specific steps). The Webmin homepage appears.



Step 2 Go to **System | Bootup and Shutdown**. The Bootup and Shutdown page appears.

The screenshot shows the 'Bootup and Shutdown' configuration page. On the left is a navigation menu with 'System' selected. The main area is titled 'Module Config' and 'Bootup and Shutdown'. It contains a table of actions with columns for 'Action', 'At boot?', and 'Description'. The 'singlewireInformaCast' action is highlighted in yellow. Below the table are buttons for 'Start', 'Stop', 'Restart', 'Start On Boot', 'Disable On Boot', 'Start Now and On Boot', and 'Disable Now and On Boot'. At the bottom, there are buttons for 'Change to runlevel:', 'Reboot System', and 'Shutdown System', each with a brief description of its function.

Action	At boot?	Description
<input type="checkbox"/> alsa-utils	No	This script stores and restores mixer levels on
<input type="checkbox"/> asterisk	No	Controls the Asterisk PBX
<input type="checkbox"/> atftpd	No	Launch atftpd server, a TFTP server useful
<input type="checkbox"/> awds	No	This script is used to start the AWDS daemon which provides
<input type="checkbox"/> batmand	No	/etc/init.d/batmand: start batmand
<input type="checkbox"/> bootlogd	No	Starts or stops the bootlogd log program
<input type="checkbox"/> bootmisc.sh	No	Some cleanup. Note, it need to run after mountnfs-bootclean.sh.
<input type="checkbox"/> checkfs.sh	No	Check all filesystems.
<input type="checkbox"/> checkroot.sh	No	Check to root file system.
<input type="checkbox"/> cron	Yes	cron is a standard UNIX program that runs user-specified
<input type="checkbox"/> dahdi	No	dahdi - load and configure DAHDI modules
<input type="checkbox"/> dnsmasq	No	DHCP and DNS server
<input type="checkbox"/> ebttables	No	Saves and restores the state of the ebttables rulesets.
<input type="checkbox"/> flashybrid	No	Flashybrid is a system to help in setting up and managing hybrid
<input type="checkbox"/> glibc.sh	No	
<input type="checkbox"/> gpsd	No	Start the GPS (Global Positioning System) daemon
<input type="checkbox"/> halt	No	
<input type="checkbox"/> hostapd	No	Userspace IEEE 802.11 AP and IEEE 802.1X/WPA/WPA2/EAP
<input type="checkbox"/> flashybrid	No	Flashybrid is a system to help in setting up and managing hybrid
<input type="checkbox"/> glibc.sh	No	
<input type="checkbox"/> gpsd	No	Start the GPS (Global Positioning System) daemon
<input type="checkbox"/> halt	No	
<input type="checkbox"/> single	No	executed by init(8) upon entering runlevel 1 (single).
<input type="checkbox"/> singlewireInformaCast	No	InformaCast application from Singlewire

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.

The screenshot shows the 'Edit Action' configuration page. The left navigation menu has 'System' selected. The main area is titled 'Module Index' and 'Edit Action'. It displays the 'Action Details' for 'singlewireInformaCast'. The 'Action Script' field contains a shell script. Below the script, there are radio buttons for 'Start at boot time?' (Yes/No). At the bottom, there are buttons for 'Save', 'Start Now', 'Show Status', 'Stop Now', and 'Delete'. A link 'Return to bootup and shutdown actions' is also present.

```

Name: singlewireInformaCast
Action Script:
#!/bin/sh
### BEGIN INIT INFO
# Short-Description: InformaCast
# Description: InformaCast application from Singlewire
### END INIT INFO

# Author: [REDACTED]
#

# Do NOT "set -e"

# PATH should only include /usr/* if it runs after the mountnfs.sh script
PATH=/sbin:/usr/sbin:/bin:/usr/bin
DESC="InformaCast"
NAME=singlewireInformaCast

Start at boot time?  Yes  No

```

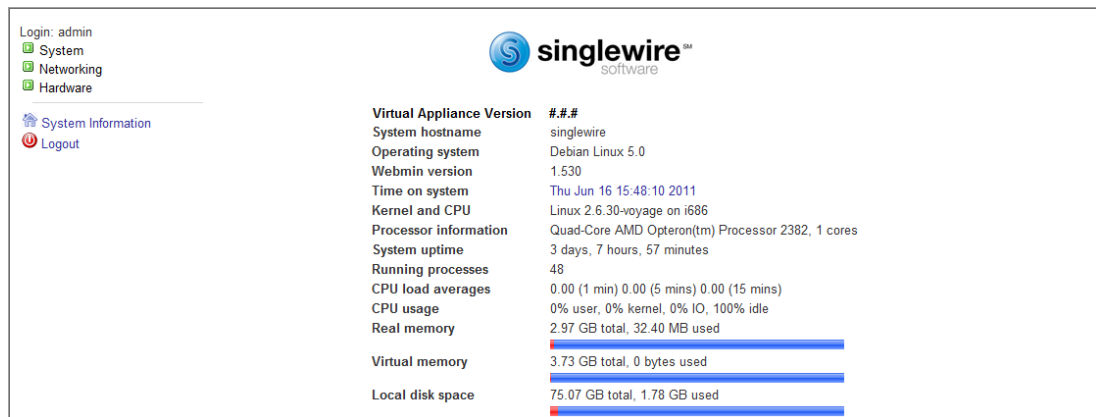
Step 4 Click the **Start Now** button. It will take a minute or so for the application to start.



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 2-27 for specific steps). The Webmin homepage appears.



Step 2 Go to **System | Bootup and Shutdown**. The Bootup and Shutdown page appears.

Login: admin

System

- Bootup and Shutdown
- Scheduled Cron Jobs
- Software Packages
- Networking
- Hardware
- System Time

Search:

System Information

Logout

Module Config

Bootup and Shutdown

Create a new bootup and shutdown action.

Action	At boot?	Description
<input type="checkbox"/> alsa-utils	No	This script stores and restores mixer levels on
<input type="checkbox"/> asterisk	No	Controls the Asterisk PBX
<input type="checkbox"/> atftpd	No	Launch atftpd server, a TFTP server useful
<input type="checkbox"/> awds	No	This script is used to start the AWDS daemon which provides
<input type="checkbox"/> batmand	No	/etc/init.d/batmand: start batmand
<input type="checkbox"/> bootlogd	No	Starts or stops the bootlogd log program
<input type="checkbox"/> bootmisc.sh	No	Some cleanup. Note, it need to run after mountnfs-bootclean.sh.
<input type="checkbox"/> checkfs.sh	No	Check all filesystems.
<input type="checkbox"/> checkroot.sh	No	Check to root file system.
<input type="checkbox"/> cron	Yes	cron is a standard UNIX program that runs user-specified
<input type="checkbox"/> dahdi	No	dahdi - load and configure DAHDI modules
<input type="checkbox"/> dnsmasq	No	DHCP and DNS server
<input type="checkbox"/> ebtables	No	Saves and restores the state of the ebtables rulesets.
<input type="checkbox"/> flashybird	No	Flashybird is a system to help in setting up and managing hybrid
<input type="checkbox"/> glibc.sh	No	
<input type="checkbox"/> gpsd	No	Start the GPS (Global Positioning System) daemon
<input type="checkbox"/> halt	No	
<input type="checkbox"/> hostapd	No	Userspace IEEE 802.11 AP and IEEE 802.1X/WPA/WPA2/EAP
<input checked="" type="checkbox"/> singlewireInformaCast	No	Flashybird is a system to help in setting up and managing hybrid
<input type="checkbox"/> glibc.sh	No	
<input type="checkbox"/> gpsd	No	Start the GPS (Global Positioning System) daemon
<input type="checkbox"/> halt	No	
<input type="checkbox"/> single	No	executed by init(8) upon entering runlevel 1 (single).
<input type="checkbox"/> singlewireInformaCast	No	InformaCast application from Singlewire

Create a new bootup and shutdown action.

Start Stop Restart Start On Boot Disable On Boot Start Now and On Boot Disable Now and On Boot

Change to runlevel: Click this button to switch your system from the current runlevel to the selected one. This will cause all the actions in the current level to be stopped, and then all the actions in the new runlevel to be started.

Reboot System Click on this button to immediately reboot the system. All currently logged in users will be disconnected and all services will be re-started.

Shutdown System Click on this button to immediately shutdown the system. All services will be stopped, all users disconnected and the system powered off (if your hardware supports it).

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.

Login: admin

System

- Bootup and Shutdown
- Change Passwords
- Scheduled Cron Jobs
- Software Packages
- Networking
- Hardware

System Information

Logout

Module Index

Restarting Actions

Executing /etc/init.d/singlewireInformaCast restart ..

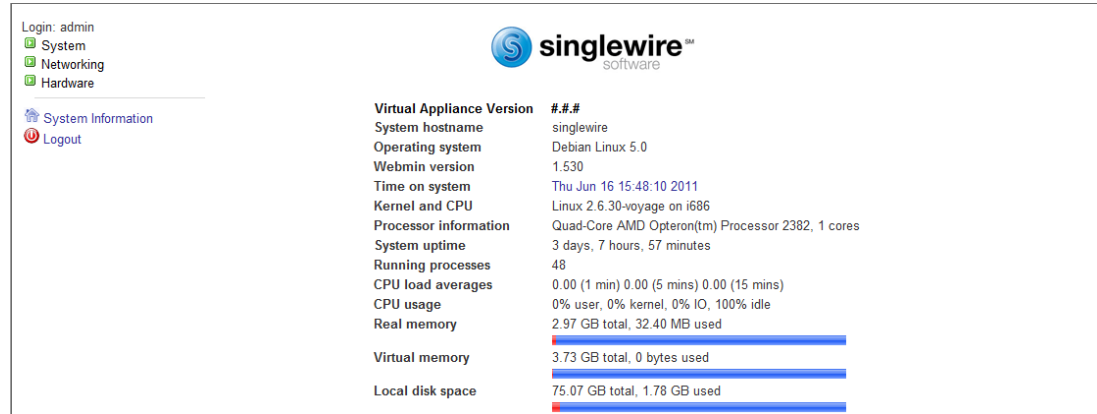
Restarting InformaCast: singlewireInformaCast

It will take a minute for your application to restart.

Reboot the InformaCast Virtual Appliance

Follow these steps to reboot the InformaCast Virtual Appliance.

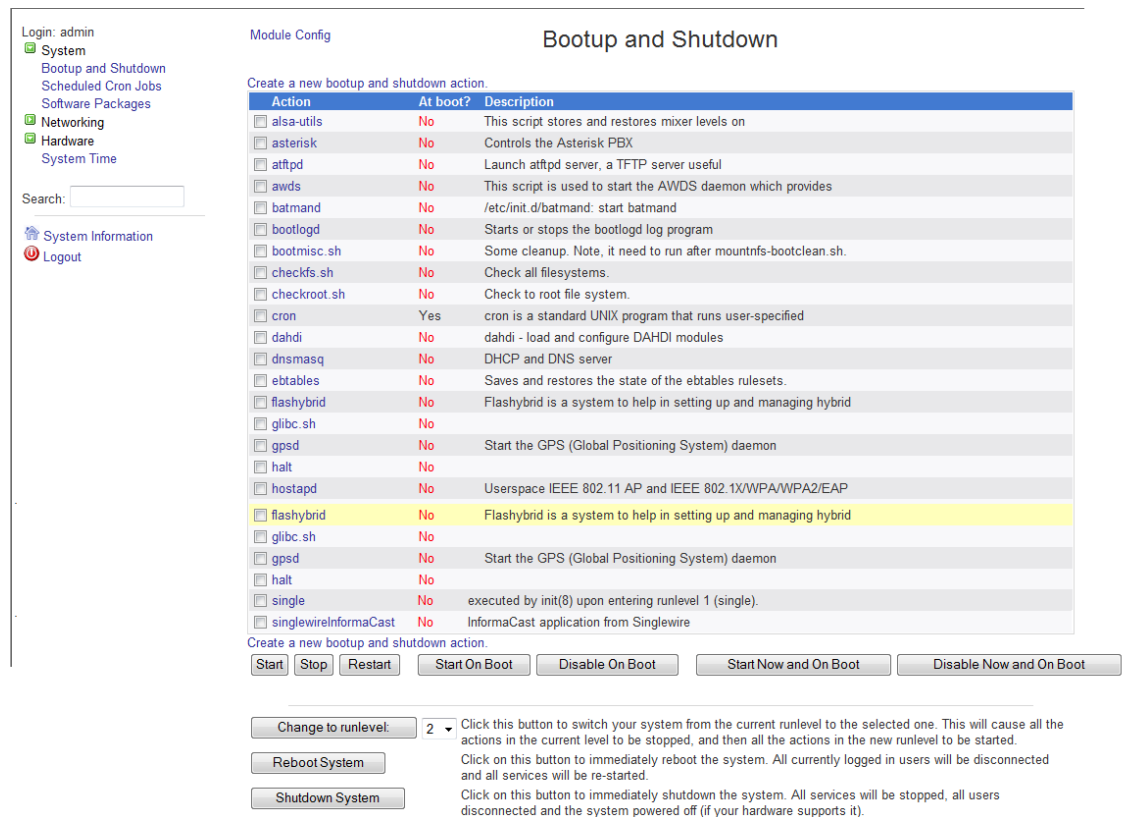
- Step 1** Log into Webmin (see “Log into Webmin” on page 2-27 for specific steps). The Webmin homepage appears.



The screenshot shows the Webmin homepage for a singlewire virtual appliance. The left sidebar contains navigation links: System, Networking, Hardware, System Information, and Logout. The main content area displays system information:

Virtual Appliance Version	###
System hostname	singlewire
Operating system	Debian Linux 5.0
Webmin version	1.530
Time on system	Thu Jun 16 15:48:10 2011
Kernel and CPU	Linux 2.6.30-voyage on i686
Processor information	Quad-Core AMD Opteron(tm) Processor 2382, 1 cores
System uptime	3 days, 7 hours, 57 minutes
Running processes	48
CPU load averages	0.00 (1 min) 0.00 (5 mins) 0.00 (15 mins)
CPU usage	0% user, 0% kernel, 0% IO, 100% idle
Real memory	2.97 GB total, 32.40 MB used
Virtual memory	3.73 GB total, 0 bytes used
Local disk space	75.07 GB total, 1.78 GB used

- Step 2** Go to **System | Bootup and Shutdown**. The Bootup and Shutdown page appears.



The screenshot shows the 'Bootup and Shutdown' page in Webmin. The left sidebar contains navigation links: System, Bootup and Shutdown, Scheduled Cron Jobs, Software Packages, Networking, Hardware, System Time, Search, System Information, and Logout. The main content area displays a table of bootup and shutdown actions:

Action	At boot?	Description
<input type="checkbox"/> alsa-utils	No	This script stores and restores mixer levels on
<input type="checkbox"/> asterisk	No	Controls the Asterisk PBX
<input type="checkbox"/> atftpd	No	Launch atftpd server, a TFTP server useful
<input type="checkbox"/> awds	No	This script is used to start the AWDS daemon which provides
<input type="checkbox"/> batmand	No	/etc/init.d/batmand: start batmand
<input type="checkbox"/> bootlogd	No	Starts or stops the bootlogd log program
<input type="checkbox"/> bootmisc.sh	No	Some cleanup. Note, it need to run after mountnfs-bootclean.sh.
<input type="checkbox"/> checkfs.sh	No	Check all filesystems.
<input type="checkbox"/> checkroot.sh	No	Check to root file system.
<input type="checkbox"/> cron	Yes	cron is a standard UNIX program that runs user-specified
<input type="checkbox"/> dahdi	No	dahdi - load and configure DAHDI modules
<input type="checkbox"/> dnsmasq	No	DHCP and DNS server
<input type="checkbox"/> ebttables	No	Saves and restores the state of the ebttables rulesets.
<input type="checkbox"/> flashybrid	No	Flashybrid is a system to help in setting up and managing hybrid
<input type="checkbox"/> glibc.sh	No	
<input type="checkbox"/> gpsd	No	Start the GPS (Global Positioning System) daemon
<input type="checkbox"/> halt	No	
<input type="checkbox"/> hostapd	No	Userspace IEEE 802.11 AP and IEEE 802.1X/WPA/WPA2/EAP
<input type="checkbox"/> flashybrid	No	Flashybrid is a system to help in setting up and managing hybrid
<input type="checkbox"/> glibc.sh	No	
<input type="checkbox"/> gpsd	No	Start the GPS (Global Positioning System) daemon
<input type="checkbox"/> halt	No	
<input type="checkbox"/> single	No	executed by init(8) upon entering runlevel 1 (single).
<input type="checkbox"/> singlewireInformaCast	No	InformaCast application from Singlewire

Below the table are buttons for creating a new bootup and shutdown action, and buttons for Start, Stop, Restart, Start On Boot, Disable On Boot, Start Now and On Boot, and Disable Now and On Boot.

At the bottom, there is a 'Change to runlevel:' dropdown menu set to '2', and buttons for 'Reboot System' and 'Shutdown System'. A detailed description of the 'Change to runlevel:' button is provided:

Click this button to switch your system from the current runlevel to the selected one. This will cause all the actions in the current level to be stopped, and then all the actions in the new runlevel to be started.

Click on this button to immediately reboot the system. All currently logged in users will be disconnected and all services will be re-started.

Click on this button to immediately shutdown the system. All services will be stopped, all users disconnected and the system powered off (if your hardware supports it).

Step 3 Scroll to the bottom of the page and click the **Reboot System** button. The Reboot page appears.

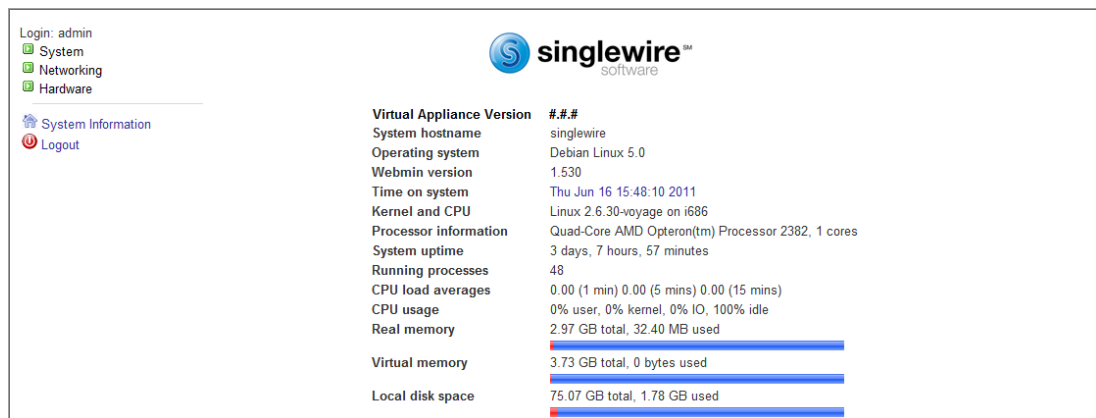


Step 4 Click the **Reboot System** button. The server will shutdown, then restart.

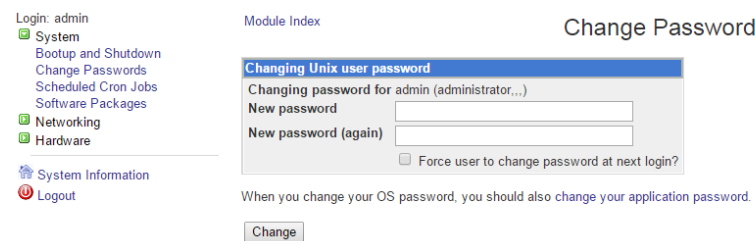
Change the OS Administrator's Password

Your OS credentials are used to enter Webmin and Control Center and when using SSH to access the Virtual Appliance, and you initially set the OS Administrator's password in Step 23 on page 2-16. Because of its elevated status, you may find it helpful to change this password periodically.

Step 1 Log into Webmin (see "Log into Webmin" on page 2-27 for specific steps). The Webmin homepage appears.



Step 2 Go to **System | Change Passwords**. The Change Password page appears.



Step 3 Enter a new OS Administrator password in the **New password** and **New password (again)** fields.



Note When setting your password, you cannot use “changeMe.”

Step 4 Skip the **Force user to change password at next login?** checkbox.

Step 5 Click the **Change** button.



Tip When you change your OS Administrator password, it is a good idea to also change your Application Administrator password (see “Change the Application Administrator’s Password” on page 6-2).

Change InformaCast Virtual Appliance’s IP Address

When changing the IP address of the InformaCast Virtual Appliance, use the following steps.



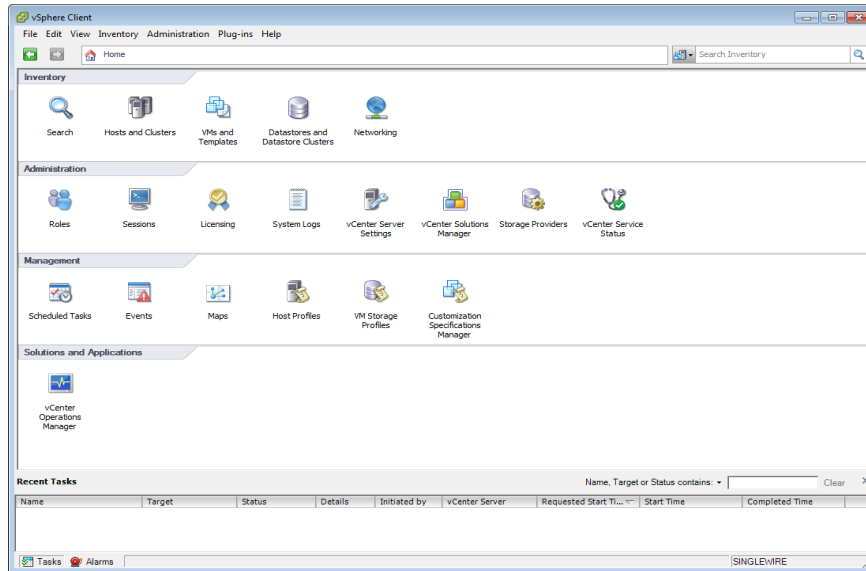
Note Performing these steps will set all of your Singlewire applications to start when the server boots.



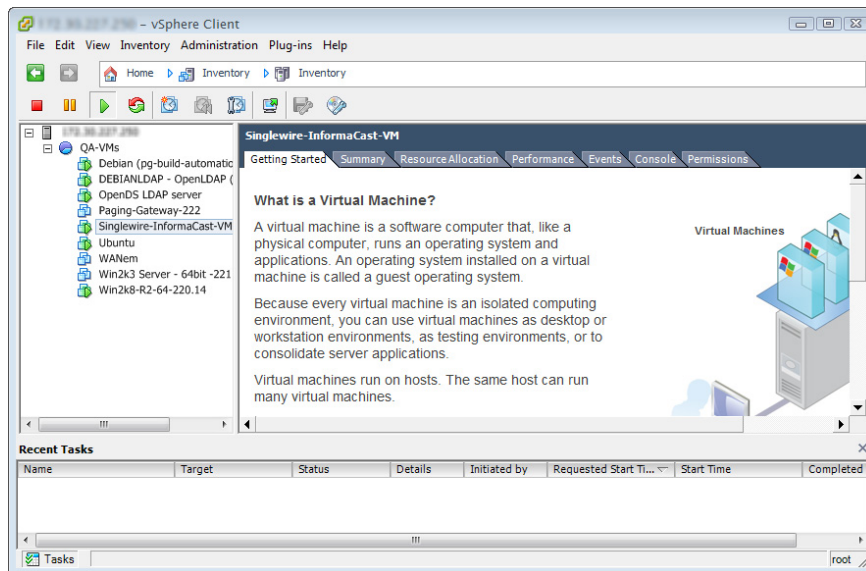
Warning **If you plan to switch between Basic and Advanced InformaCast and you change your IP address, you will need to redeploy the InformaCast OVA (see “Install InformaCast Virtual Appliance” on page 2-6).**

Step 1 Stop your Singlewire applications (see “Stop an Application on InformaCast Virtual Appliance” on page 10-1).

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

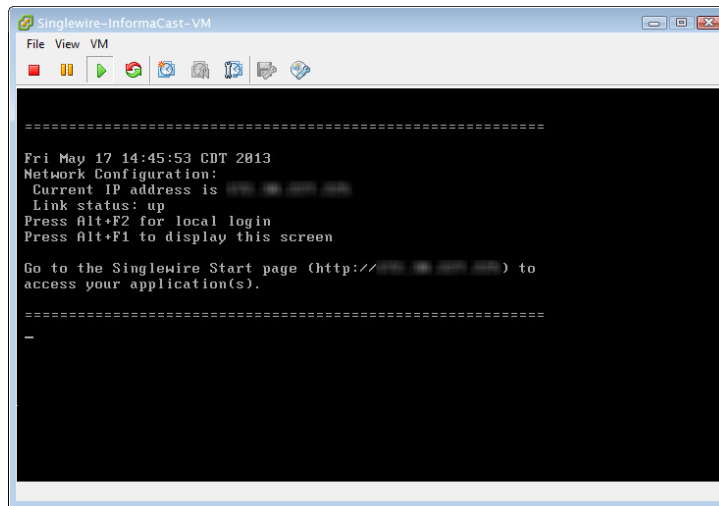


Step 3 Click the **Inventory** icon () on the vSphere Client window. The vSphere Client window refreshes.

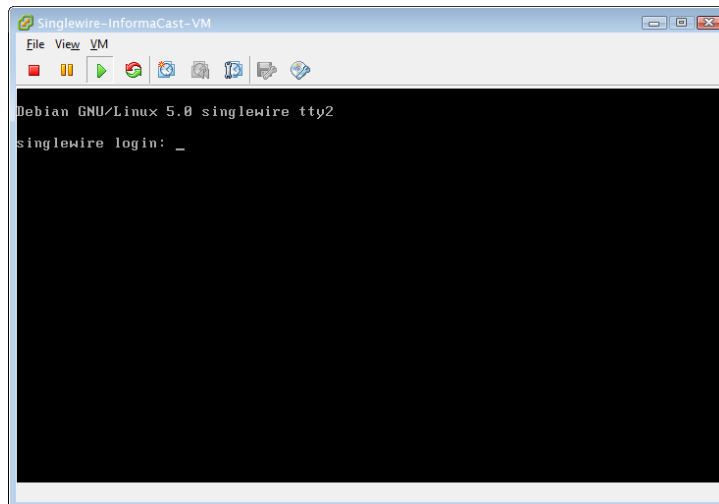


Step 4 Select your virtual machine (by default, this is Singlewire InformaCast VM).

Step 5 Go to **Inventory** | **Virtual Machine** | **Open Console**. The Singlewire InformaCast VM console window appears.

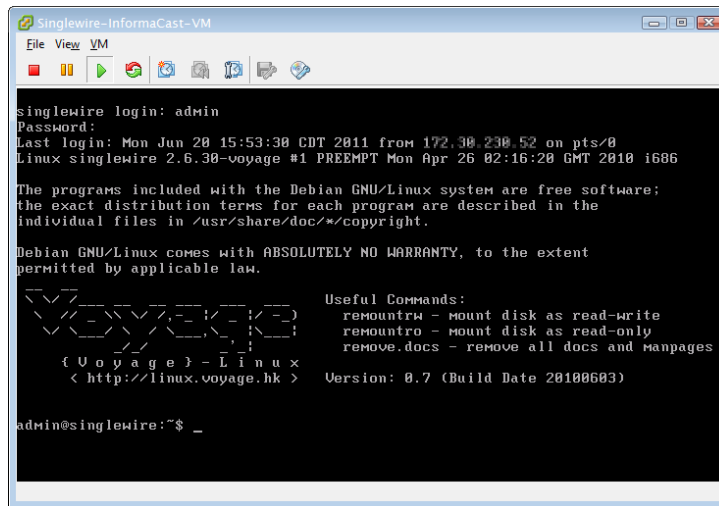


Step 6 Press **Alt + F2** in the Singlewire InformaCast VM console window. The Singlewire InformaCast VM console window refreshes.



Step 7 Enter **admin** at the **singlewire login** prompt and press the **Enter** key.

- Step 8** Enter your OS password at the **Password** prompt and press the **Enter** key. The Singlewire InformaCast VM console window refreshes.



```

Singlewire-InformaCast-VM
File View VM
singlewire login: admin
Password:
Last login: Mon Jun 20 15:53:30 CDT 2011 from 172.30.230.52 on pts/0
Linux singlewire 2.6.30-voyage #1 PREEMPT Mon Apr 26 02:16:20 GMT 2010 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

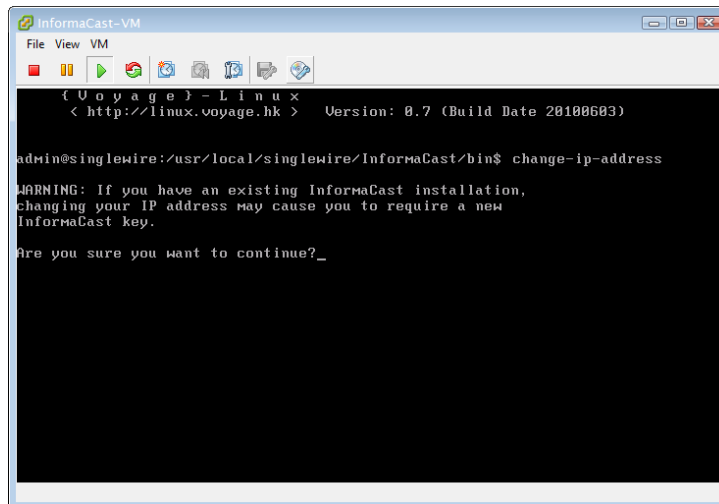
      _   _
     / \ / \
    /  V  V \
   /_____\  \
  { U o y a g e } - L i n u x
  < http://linux.voyage.hk >

Useful Commands:
  remountrw - mount disk as read-write
  remountro - mount disk as read-only
  remove.docs - remove all docs and manpages
Version: 0.7 (Build Date 20100603)

admin@singlewire:~$ _

```

- Step 9** Enter **change-ip-address** and press the **Enter** key. The Singlewire InformaCast VM console window refreshes.



```

InformaCast-VM
File View VM
{ U o y a g e } - L i n u x
< http://linux.voyage.hk > Version: 0.7 (Build Date 20100603)

admin@singlewire:/usr/local/singlewire/InformaCast/bin$ change-ip-address

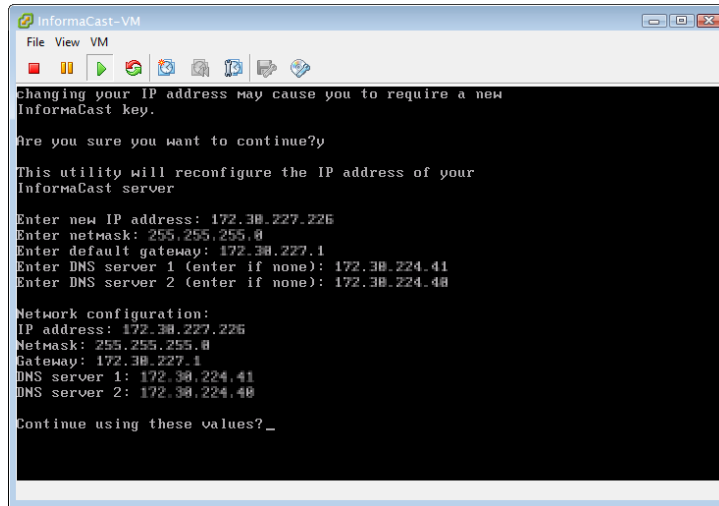
WARNING: If you have an existing InformaCast installation,
changing your IP address may cause you to require a new
InformaCast key.

Are you sure you want to continue?_

```

- 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.



```

InformaCast-VM
File View VM
changing your IP address may cause you to require a new
InformaCast key.
Are you sure you want to continue?y
This utility will reconfigure the IP address of your
InformaCast server
Enter new IP address: 172.30.227.226
Enter netmask: 255.255.255.0
Enter default gateway: 172.30.227.1
Enter DNS server 1 (enter if none): 172.30.224.41
Enter DNS server 2 (enter if none): 172.30.224.40

Network configuration:
IP address: 172.30.227.226
Netmask: 255.255.255.0
Gateway: 172.30.227.1
DNS server 1: 172.30.224.41
DNS server 2: 172.30.224.40
Continue using these values?_

```

Step 15 Enter **Y** and press the **Enter** key.

Step 16 Enter **Exit** and press the **Enter** key.

Step 17 For InformaCast, log into Unified Communications Manager, 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.



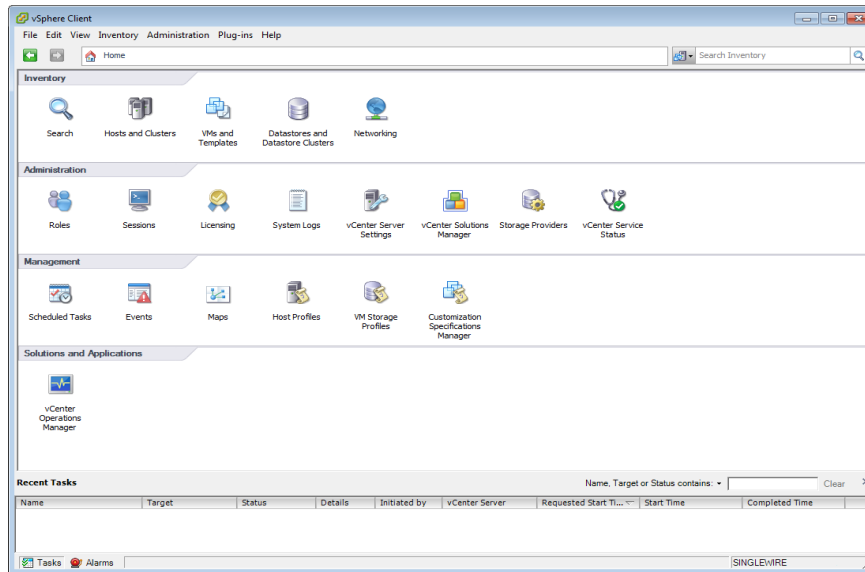
Note InformaCast SIP certificates are regenerated whenever InformaCast is installed or its IP address is changed, so if you are using TLS protocol with SIP, you will need to install the InformaCast SIP certificate on all Unified Communications Managers in your InformaCast environment (see “Install the InformaCast SIP Certificate on a SIP Device” in the “InformaCast Installation and User Guide.”)

Step 18 Reset all of your phones.

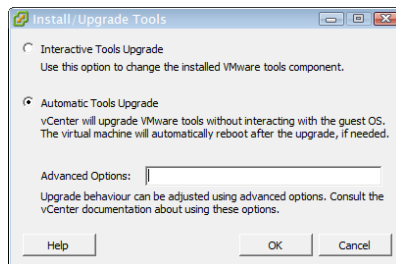
Upgrade your VMware Tools

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 2-23 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 10-15. 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 2-27 for specific steps). The Webmin homepage appears.

The screenshot shows the Webmin interface with the 'System Information' page selected. The page displays various system metrics and hardware information. The Singlewire logo is visible in the top right corner.

Virtual Appliance Version	###
System hostname	singlewire
Operating system	Debian Linux 5.0
Webmin version	1.530
Time on system	Thu Jun 16 15:48:10 2011
Kernel and CPU	Linux 2.6.30-voynage on i686
Processor information	Quad-Core AMD Opteron(tm) Processor 2382, 1 cores
System uptime	3 days, 7 hours, 57 minutes
Running processes	48
CPU load averages	0.00 (1 min) 0.00 (5 mins) 0.00 (15 mins)
CPU usage	0% user, 0% kernel, 0% IO, 100% idle
Real memory	2.97 GB total, 32.40 MB used
Virtual memory	3.73 GB total, 0 bytes used
Local disk space	75.07 GB total, 1.78 GB used

- 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 10-15.

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_11.5.2.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_11.5.2.deb.

The upload process is detailed in the next section.

- **9.1.1, 11.0.1, 11.0.2, 11.0.5, or 11.5.1 Virtual Appliance to Current Version.** Your download will include one package file: CiscoPagingServer_11.5.2.deb.

The upload process is detailed in the next section.

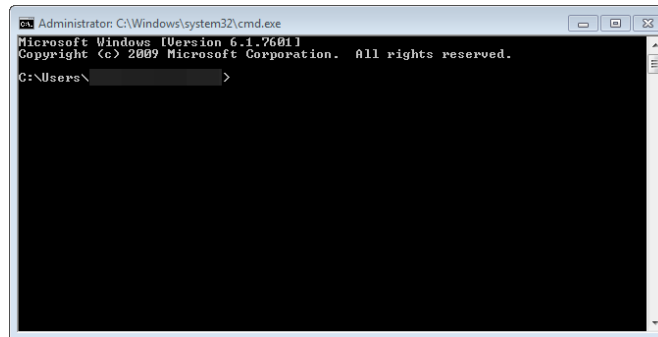
Install a New Software Package

Once you've obtained your package file(s), you can install them and update your version of InformaCast Virtual Appliance:

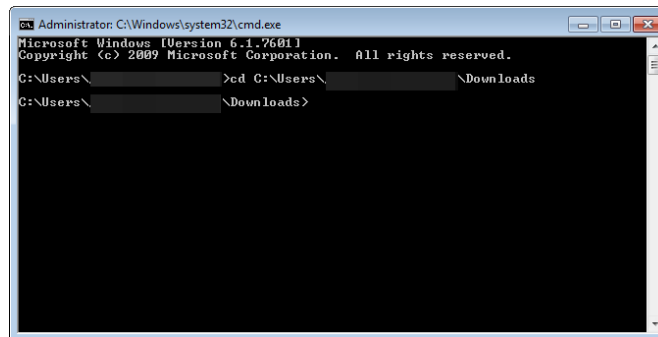
- Upgrading from an 8.3 or 8.4 version to the current version calls for three files (CiscoPagingServer_8.5.1.deb, CiscoPagingServer_9.1.1.deb, and CiscoPagingServer_11.5.2.deb) to be uploaded
- Upgrading from 8.5.1, 9.0.1, or 9.0.2 to the current version calls for two files (CiscoPagingServer_9.1.1.deb and CiscoPagingServer_11.5.2.deb) to be uploaded
- Upgrading from 9.1.1, 11.0.1, 11.0.2, 11.0.5, or 11.5.1 to the current version only calls for one file (CiscoPagingServer_11.5.2.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.

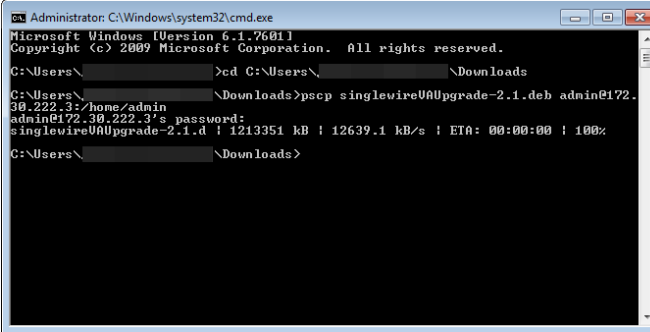


- Step b.** Enter `cd <directory>` and press the **Enter** key, where <directory> is the location of your .deb file(s). The command window refreshes to the location of your directory.



- 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.



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\>cd C:\Users\Downloads
C:\Users\Downloads>scp singlewireVAPUpgrade-2.1.deb admin@172.30.222.3:/home/admin
admin@172.30.222.3's password:
singlewireVAPUpgrade-2.1.d | 1213351 kB | 12639.1 kB/s | ETA: 00:00:00 | 100%
C:\Users\Downloads>
```

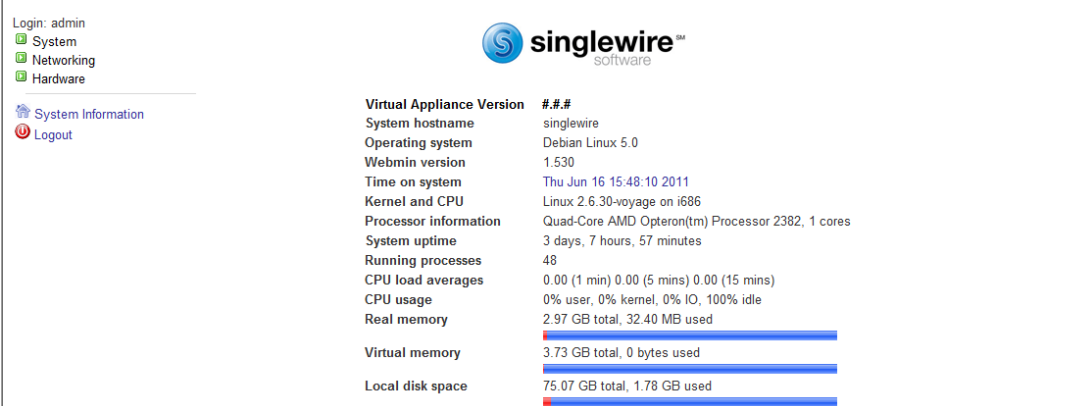
Step e. Repeat Steps a through d until you've copied all of your .deb files to the Virtual Appliance.

Step 3 Log into Webmin (see “Log into Webmin” on page 2-27 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.



singlewire™ software

Virtual Appliance Version #.#.#

System hostname	singlewire
Operating system	Debian Linux 5.0
Webmin version	1.530
Time on system	Thu Jun 16 15:48:10 2011
Kernel and CPU	Linux 2.6.30-voyage on i686
Processor information	Quad-Core AMD Opteron(tm) Processor 2382, 1 cores
System uptime	3 days, 7 hours, 57 minutes
Running processes	48
CPU load averages	0.00 (1 min) 0.00 (5 mins) 0.00 (15 mins)
CPU usage	0% user, 0% kernel, 0% IO, 100% idle
Real memory	2.97 GB total, 32.40 MB used
Virtual memory	3.73 GB total, 0 bytes used
Local disk space	75.07 GB total, 1.78 GB used

Login: admin

- System
- Networking
- Hardware

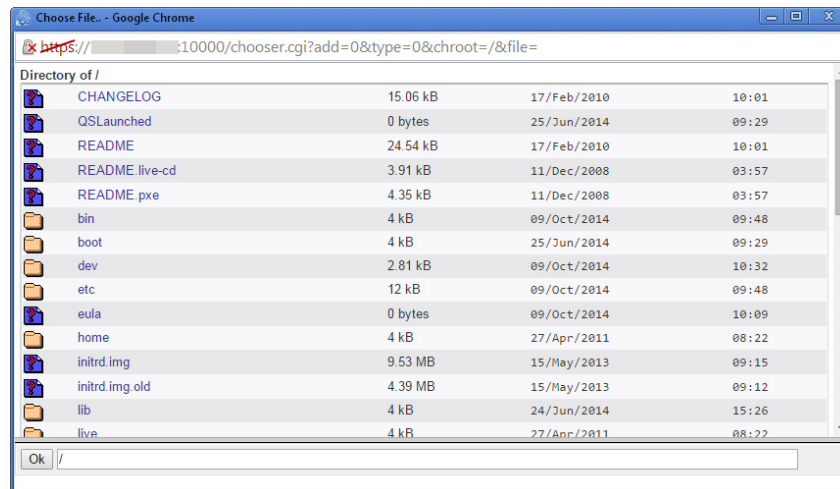
System Information

Logout

Step 4 Go to **System | Software Packages**. The Software Packages page appears.

The screenshot shows the 'Software Packages' page. On the left is a navigation menu with 'System Information' and 'Logout' selected. The main content area has a 'Software Packages' header. Below it are sections for 'Installed Packages', 'Install a New Package', 'Identify a File', and 'Upgrade All Packages'. The 'Install a New Package' section has four radio buttons: 'From local file' (selected), 'From uploaded file', 'From ftp or http URL', and 'Package from APT'. There are input fields and buttons for each option. The 'Upgrade All Packages' section has a blue header 'APT package upgrade options' and three rows of radio buttons for 'Resynchronize package list (update)', 'Upgrade mode', and 'Only show which packages would be upgraded'. An 'Upgrade Now' button is at the bottom.

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.

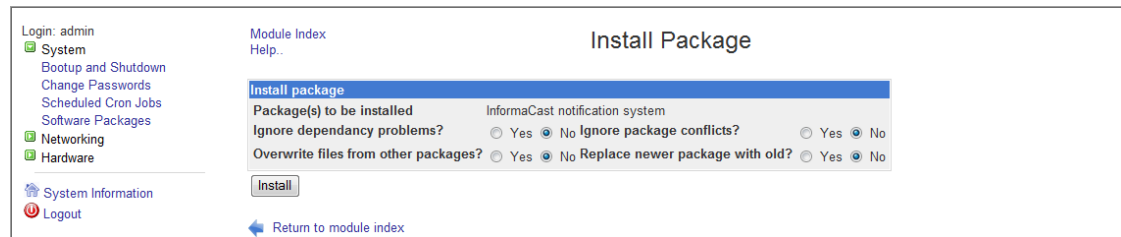


Step 6 Navigate to where you saved the InformaCast Virtual Appliance software package(s) you downloaded earlier (/home/admin in the example). Depending on the version of InformaCast Virtual Appliance from which you are upgrading, you will select one of the following:

- 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, 11.0.1, 11.0.2, 11.0.5, or 11.5.1 version of InformaCast Virtual Appliance:
CiscoPagingServer_11.5.2.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.

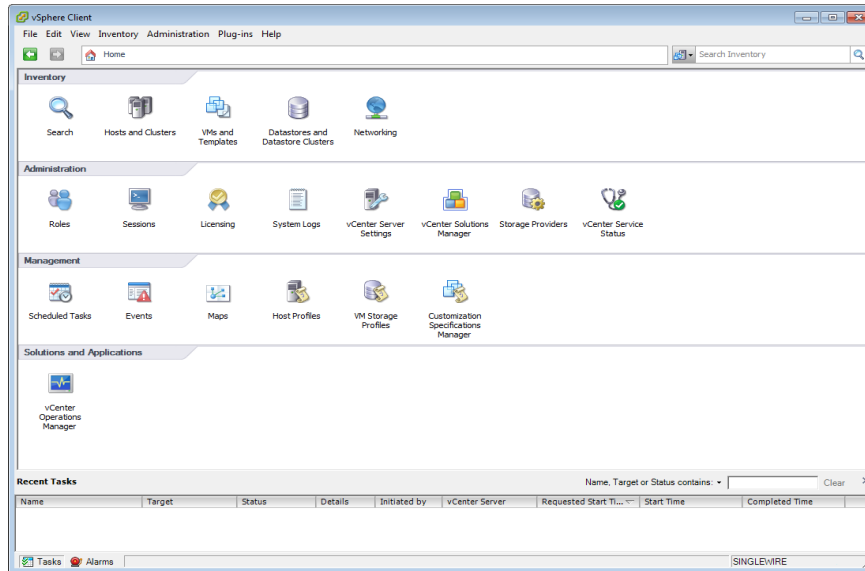
Step 9 Determine your next steps depending on the version of the Virtual Appliance from which you are upgrading:

- 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 10-7)
 - 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 10-7)
 - Go to **System** | **Software Packages** and follow Steps 5 through 8 one more time, selecting the CiscoPagingServer_11.5.2.deb file
 - 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 10-7)
 - Go to **System** | **Software Packages** and follow Steps 5 through 8 one more time, selecting the CiscoPagingServer_11.5.2.deb file
 - Proceed with Step 10
- If you are upgrading from the 9.1.1, 11.0.1, 11.0.2, 11.0.5, or 11.5.1 version of InformaCast Virtual Appliance proceed with Step 10

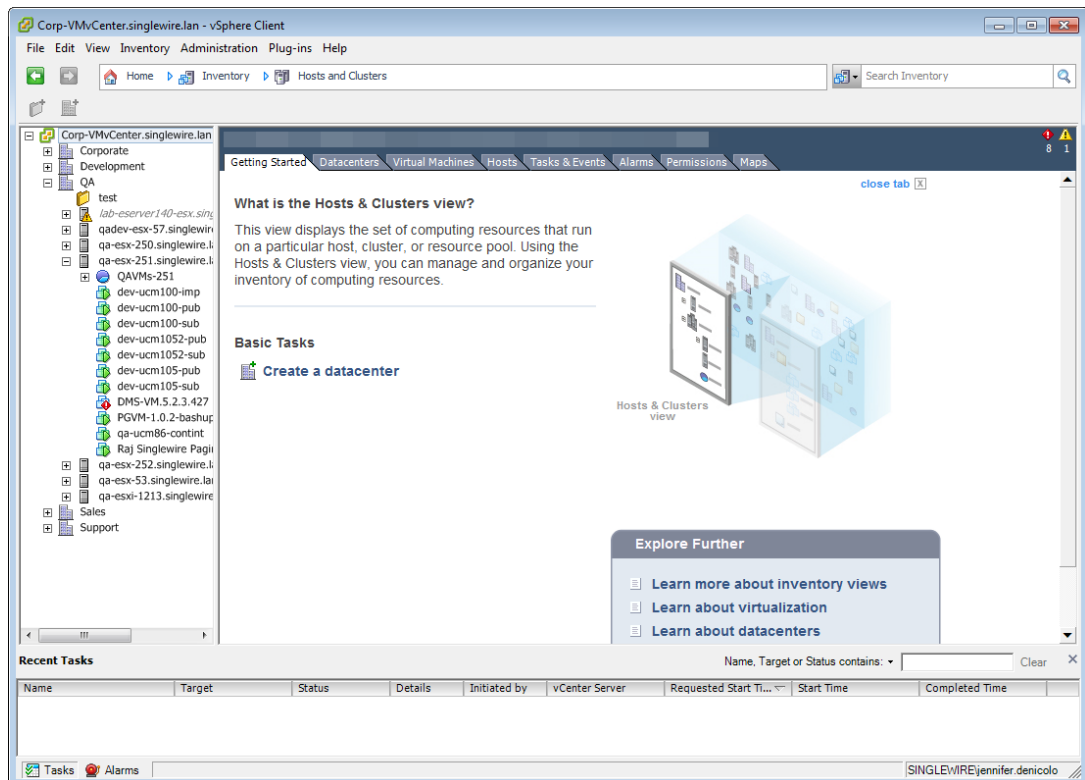


Note Leave this window open. You will come back to it in the next section.

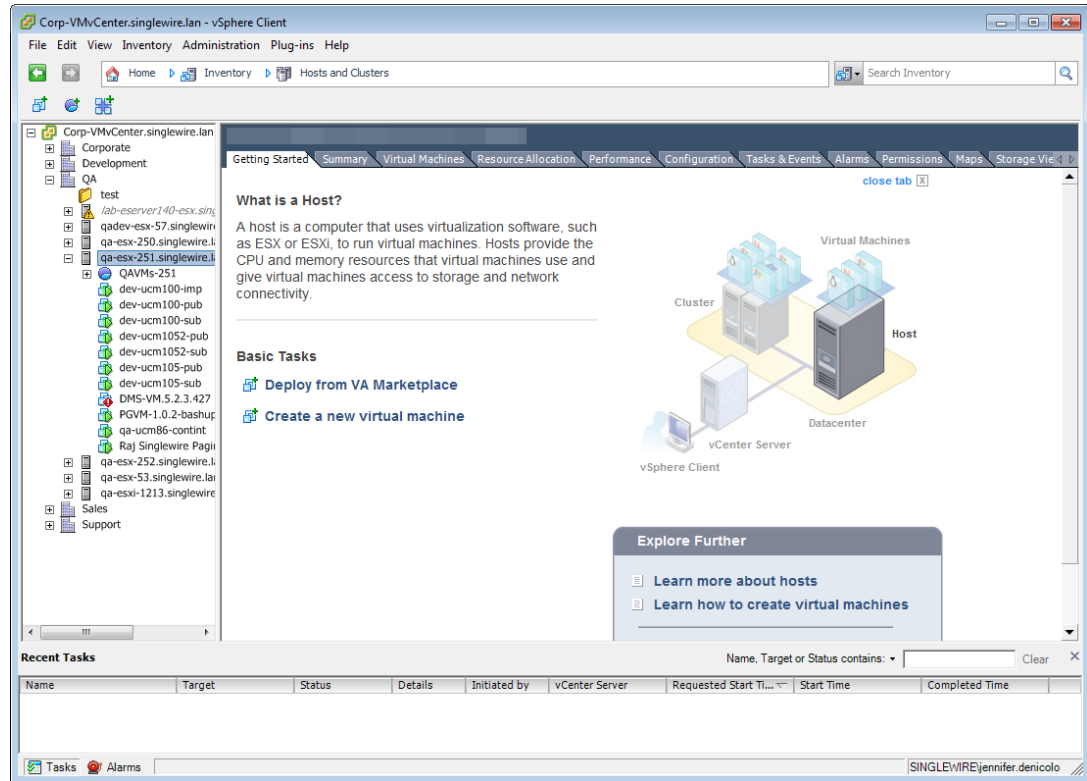
Step 10 Open and log into the vSphere client. The vSphere Client window appears.



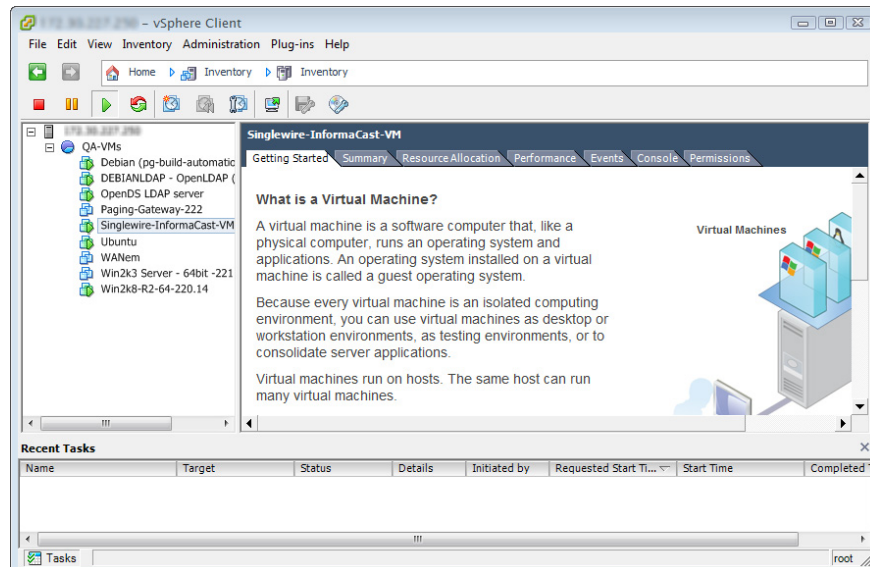
Step 11 Click the **Hosts and Clusters** icon (🖥️). The vSphere Client window refreshes.



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

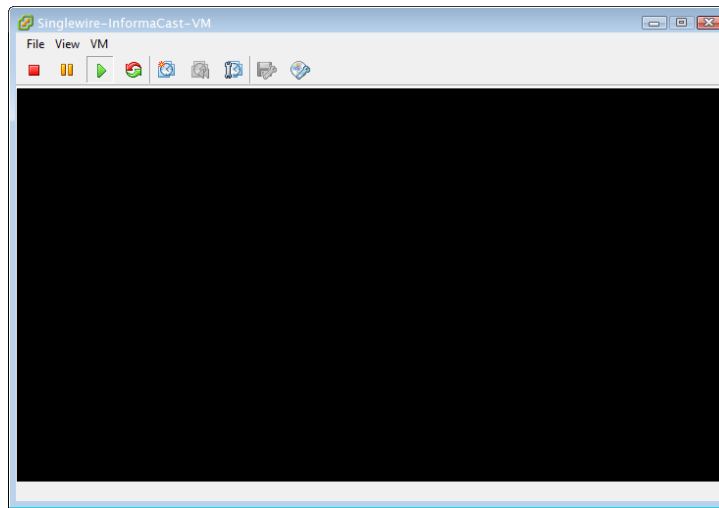


Step 13 Go to **View | Inventory | VMs and Templates**. The vSphere Client window refreshes.

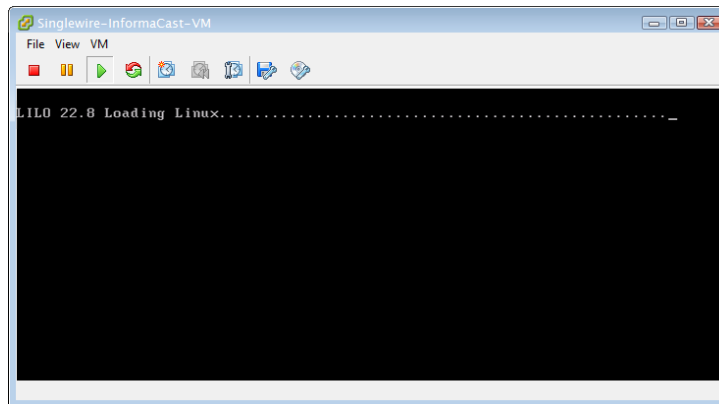


Step 14 Select your virtual machine.

Step 15 Go to **Inventory** | **Virtual Machine** | **Open Console**. The Singlewire InformaCast VM console window appears.



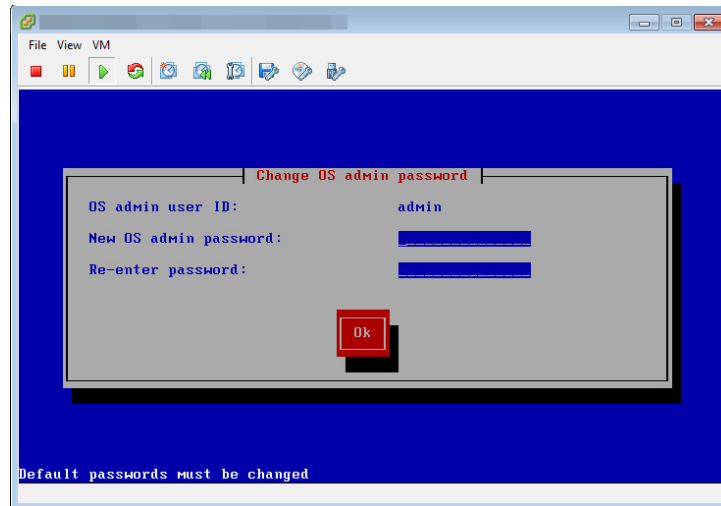
The Singlewire InformaCast VM console window begins booting the virtual machine.



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

If you were using “changeMe” as your previous OS and/or Application Administrator passwords (i.e. the passwords you used when logging into Webmin, Control Center, or InformaCast, and when using SSH to access the Virtual Appliance), when the InformaCast Virtual Appliance is done booting, you

will be prompted to change your passwords (see picture and Steps 16 through 19). If you were not using “changeMe,” the Virtual Appliance will finish its boot process, which may take a minute or so. Skip to Step 20 on page 10-25.

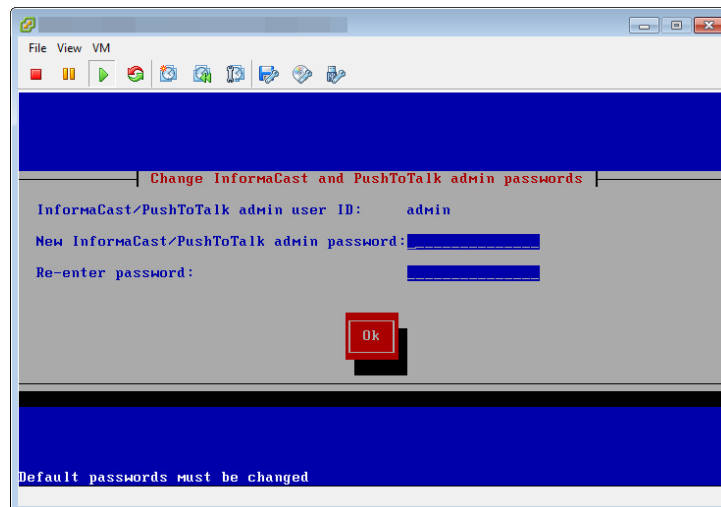


- Step 16** Enter a new password in the **New OS admin password** field, press the **Tab** key, and enter the password again in the **Re-enter password** field. Your OS credentials are used to enter Webmin and Control Center and when using SSH to access the Virtual Appliance.



Note When setting your password, you cannot use “changeMe.”

- Step 17** Press the **Enter** key three times to advance to the next screen in the console window where you will be prompted to change the Application Administrator’s password.



- Step 18** Enter a new password in the **New InformaCast/PushToTalk admin password** field, press the **Tab** key, and enter the password again in the **Re-enter password** field. Your application credentials are used to enter InformaCast and PushToTalk.



Note When setting your password, you cannot use “changeMe.”



Note PushToTalk is only available for Advanced InformaCast users.

Step 19 Press the **Enter** key three times. The Virtual Appliance will finish its boot process, which may take a minute or so.

Step 20 Create a new snapshot of your Virtual Appliance.

Step 21 Clear your web browser’s cache.

Step 22 Remove your already installed .deb files by following Steps a and b on page 10-17 and entering **rm <.deb filename>** for each .deb file you’ve copied over.



Note If you were previously using SIP and you had configured it to work with TLS, you will need to select the **Secure Signaling Required** checkbox on the SIP Call Security page before any InformaCast features using SIP will work (see “Enable SIP Call Security” on page 5-36).

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.



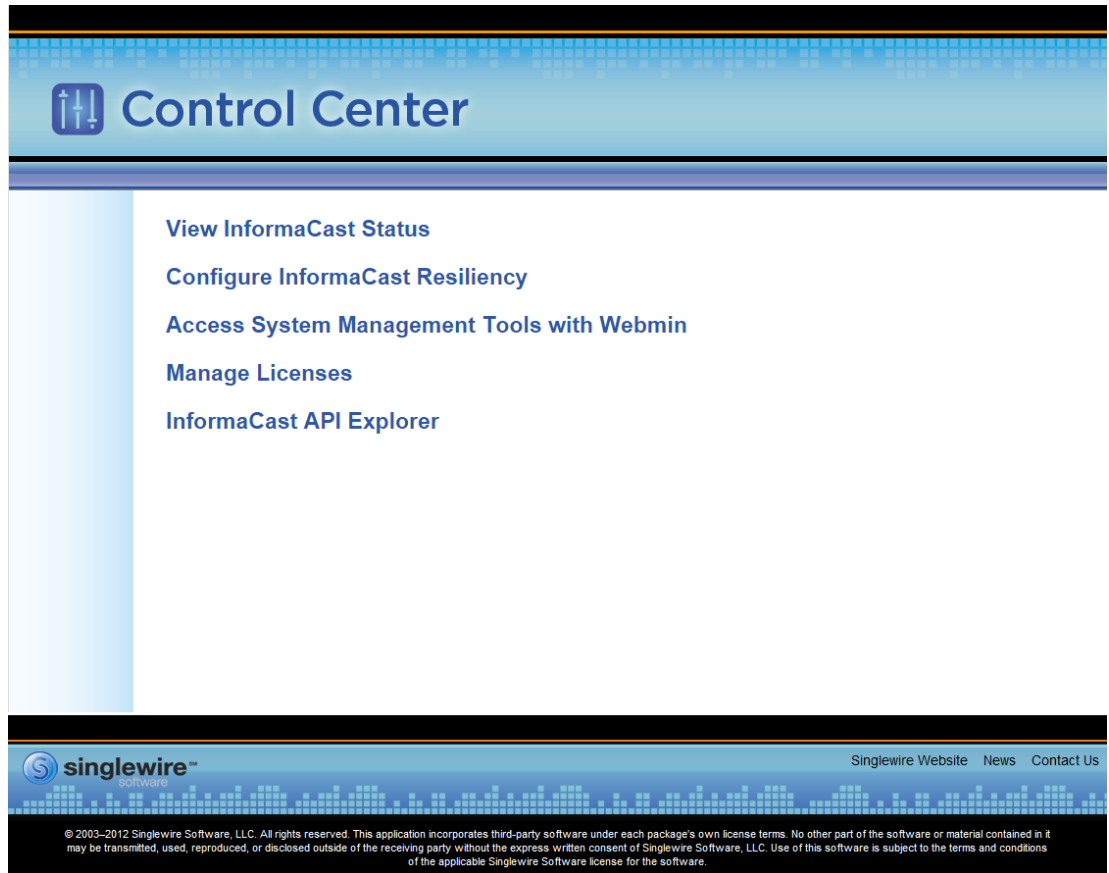
Tip Make sure to save your XML license key file to a safe location that can be accessed by the machine running your web browser.

Step 1 Log into the Control Center (see “Log into the Control Center” on page 2-25 for specific steps).



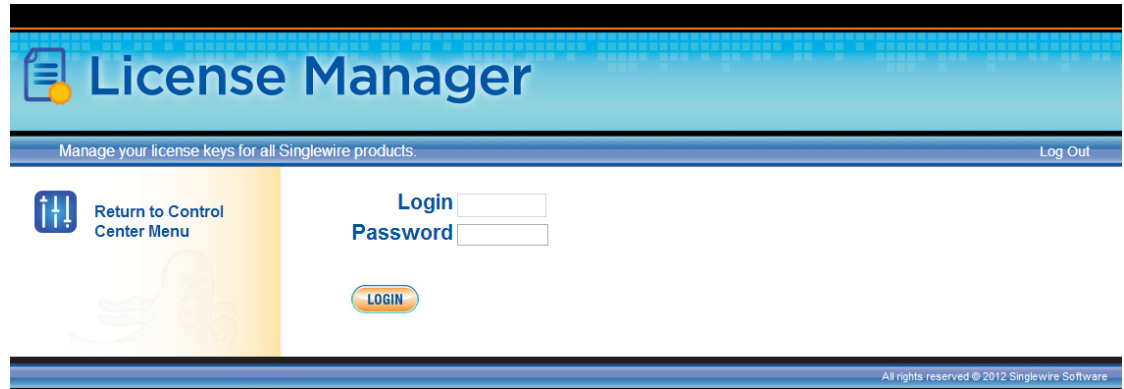
Note For versions of InformaCast Virtual Appliance prior to 8.4, you will need to go to <https://<InformaCast Virtual Appliance IP Address>:8463/LicenseManager>, where <InformaCast Virtual Appliance IP Address> is InformaCast Virtual Appliance’s statically configured IP address. Skip to Step 3 on page 10-27.

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.

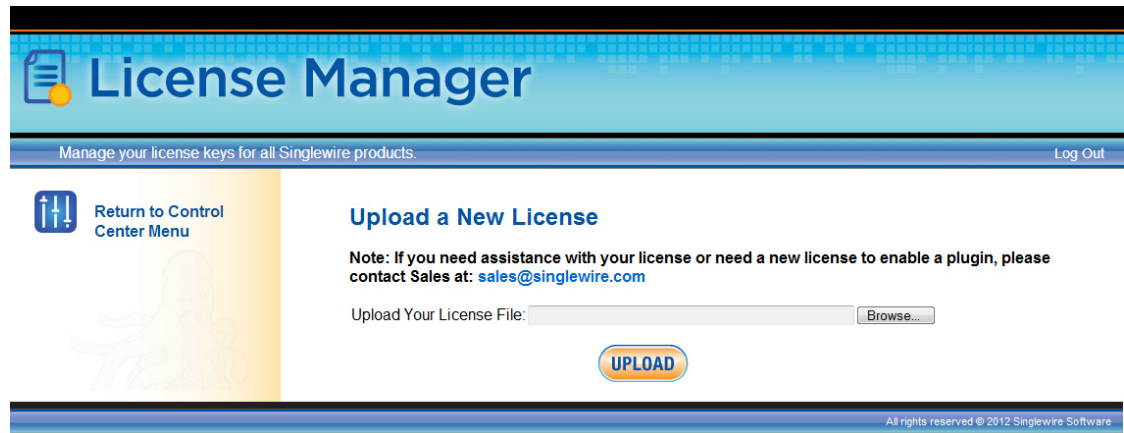
Step 2 Click the **Manage Licenses** link. The License Manager page appears.



The screenshot shows the License Manager interface. At the top, there is a blue header with a document icon and the text "License Manager". Below the header, a blue bar contains the text "Manage your license keys for all Singlewire products." and a "Log Out" link. The main content area is divided into two columns. The left column has a yellow background with a "Return to Control Center Menu" link and a faint image of a person. The right column contains a "Login" field, a "Password" field, and a blue "LOGIN" button. At the bottom right, there is a small copyright notice: "All rights reserved © 2012 Singlewire Software."

Step 3 Enter your OS credentials in the **Login** and **Password** fields.

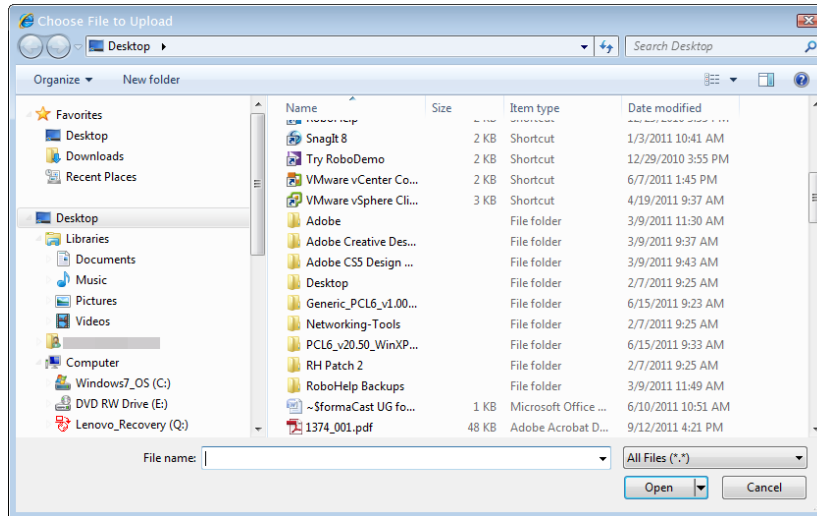
Step 4 Click the **Login** button. The Upload a New License page appears.



The screenshot shows the License Manager interface after clicking the "Login" button. The header and navigation bar are the same as in the previous screenshot. The main content area now features a "Return to Control Center Menu" link on the left and a "Upload a New License" section on the right. The "Upload a New License" section includes a note: "Note: If you need assistance with your license or need a new license to enable a plugin, please contact Sales at: sales@singlewire.com". Below the note is a text input field labeled "Upload Your License File:" followed by a "Browse..." button. A blue "UPLOAD" button is positioned below the input field. At the bottom right, the same copyright notice is present: "All rights reserved © 2012 Singlewire Software."

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 5 Click the **Browse** button. The Choose File to Upload window appears.



Step 6 Navigate to where you saved your new license file, select it, and click the **Open** button.

- Step 7** Click the **Upload** button on the Upload a New License page. The License Status page with a confirmation that the license has been uploaded.

License Manager
Manage your license keys for all Singlewire products. Log Out

Return to Control Center Menu

License Status

License file installed. Restart any running applications that do not automatically reload their license.

Note: If you need assistance with your license or need a new license to enable a plugin, please contact Sales at: sales@singlewire.com

Warning: Uploading a license that indicates Advanced Notification may cause an automatic and immediate restart of InformaCast. Please refer to your documentation for more information.

The currently installed License Keys contain the following features:

[InformaCast](#)

Issuer: [redacted]
Created: Wed Feb 13 15:31:40 CST 2013
Licensee: *** LAB USE ONLY ***
 Singlewire Test License Generated by [redacted]
 *** LAB USE ONLY ***

IP Restriction: Not restricted
Expiration: No expiration
Features: Audio, MessageConfirmation
Parameters: MaxBellSchedules=500, MaxIPSpeakers=1000, MaxPhones=5000, MaxVersion=9.0, Scheme=Subscription

[IC.Plugin: Inbound RSS](#)

Issuer: [redacted]
Created: Wed Feb 13 15:31:40 CST 2013
Licensee: *** LAB USE ONLY ***
 Singlewire Test License Generated by [redacted]
 *** LAB USE ONLY ***

IP Restriction: Not restricted
Expiration: No expiration
Features:
Parameters:

Replace Your License(s):

All rights reserved © 2012 Singlewire Software

**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 8 Return to your Webmin tab/window and click the **Bootup and Shutdown** link. The Bootup and Shutdown page appears.

Module Config **Bootup and Shutdown**

Create a new bootup and shutdown action.

Action	At boot?	Description
<input type="checkbox"/> alsa-utils	No	This script stores and restores mixer levels on
<input type="checkbox"/> asterisk	No	Controls the Asterisk PBX
<input type="checkbox"/> atftpd	No	Launch atftpd server, a TFTP server useful
<input type="checkbox"/> awds	No	This script is used to start the AWDS daemon which provides
<input type="checkbox"/> batmand	No	/etc/init.d/batmand: start batmand
<input type="checkbox"/> bootlogd	No	Starts or stops the bootlogd log program
<input type="checkbox"/> bootmisc.sh	No	Some cleanup. Note, it need to run after mountnfs-bootclean.sh.
<input type="checkbox"/> checkfs.sh	No	Check all filesystems.
<input type="checkbox"/> checkroot.sh	No	Check to root file system.
<input type="checkbox"/> cron	Yes	cron is a standard UNIX program that runs user-specified
<input type="checkbox"/> dahdi	No	dahdi - load and configure DAHDI modules
<input type="checkbox"/> dnsmasq	No	DHCP and DNS server
<input type="checkbox"/> ebttables	No	Saves and restores the state of the ebttables rulesets.
<input type="checkbox"/> flashybridge	No	Flashybridge is a system to help in setting up and managing hybrid
<input type="checkbox"/> glibc.sh	No	
<input type="checkbox"/> gpsd	No	Start the GPS (Global Positioning System) daemon
<input type="checkbox"/> halt	No	
<input type="checkbox"/> hostapd	No	Userspace IEEE 802.11 AP and IEEE 802.1X/WPA/WPA2/EAP
<input type="checkbox"/> flashybridge	No	Flashybridge is a system to help in setting up and managing hybrid
<input type="checkbox"/> glibc.sh	No	
<input type="checkbox"/> gpsd	No	Start the GPS (Global Positioning System) daemon
<input type="checkbox"/> halt	No	
<input type="checkbox"/> single	No	executed by init(8) upon entering runlevel 1 (single).
<input type="checkbox"/> singlewireInformaCast	No	InformaCast application from Singlewire

Create a new bootup and shutdown action.

Click this button to switch your system from the current runlevel to the selected one. This will cause all the actions in the current level to be stopped, and then all the actions in the new runlevel to be started.

Click on this button to immediately reboot the system. All currently logged in users will be disconnected and all services will be re-started.

Click on this button to immediately shutdown the system. All services will be stopped, all users disconnected and the system powered off (if your hardware supports it).

Step 9 Select all of your Singlewire applications that were affected by your new license and click the **Restart** button. The Restarting Actions page appears.

Module Index **Restarting Actions**

Executing /etc/init.d/singlewireInformaCast restart ..

Restarting InformaCast: singlewireInformaCast.

Executing /etc/init.d/singlewireLPI restart ..

Restarting LPI: singlewireLPI

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 11.5.2

The following information pertains to InformaCast 11.5.2.

Compatibility

InformaCast is compatible with the following versions of Cisco Unified Communications Manager server (including Business Edition 6000): 9.0.1, 9.1.2, 10.0.1, 10.5.2, 11.0.1, and 11.5.1.

New Features

New Upgrade File. A new file (CiscoPagingServer_11.5.2.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_11.5.2.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_11.5.2.deb)
- For 9.1.1, 11.0.1, 11.0.2, 11.0.5, or 11.5.1 to the current version, you will install one package file (CiscoPagingServer_11.5.2.deb)

InformaCast Virtual Appliance 8.5.1 and 9.1.1 are waypoints in the upgrade process. For 8.3 or 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 11.5.2. 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 11.5.2. For 9.1.1, 11.0.1, 11.0.2, 11.0.5, and 11.5.1 versions of the Virtual Appliance, you can upgrade directly to 11.5.2.

Resolved Caveats

You can find the latest resolved caveat information for InformaCast by using Cisco's Bug Search tool (<https://tools.cisco.com/bugsearch/>) to query defects. To access the Bug Search tool, you must have a valid Cisco.com user ID and password.

InformaCast 11.5.1

The following information pertains to InformaCast 11.5.1.

Compatibility

InformaCast is compatible with the following versions of Cisco Unified Communications Manager server (including Business Edition 6000): 9.0.1, 9.1.2, 10.0.1, 10.5.2, 11.0.1, and 11.5.1.

New Features

- **Improved Phone Activation Times During Broadcasts.** A new checkbox, **Create Telephony Terminals for all Phones**, has been added to the Broadcast Parameters page (**Admin | Broadcast Parameters**) that, when enabled, creates CTI terminals for all phones in the primary cluster, which can improve phone activation times during broadcasts. Every time InformaCast builds its phone cache, terminals will be created for any newly registered phones while terminals will be destroyed for phones no longer in the cache. Unified Communications Manager limits an application user to 10,000 devices. If your primary cluster contains more than 10,000 phones and you select the **Create Telephony Terminals for all Phones** checkbox, InformaCast will fall back to creating terminals on an as-needed basis.
- **New Parameter for API Browser Access.** InformaCast uses API services in its communication with Unified Communication Manager. In order for this communication to work properly, if you are using Unified Communications Manager 11.5.1 and later, you need to set your authentication method for API browser access to **Basic**.
- **New Call Detail Records Collection.** You can collect call detail records and set a retention period that will eliminate saved records older than the set period through a scheduled job that runs every day at 3:30 a.m. When configured, InformaCast creates a call detail record for every SIP call it receives or makes, e.g. calls made through DialCasts. InformaCast collects call data, such as changes to the call state and DTMF sent and received, as it interacts with a call and Unified Communications Manager. When the call ends, the collected data is written to an InformaCast directory accessible through the **Call Detail Records Directory** link on the Support page.
- **New SRTP Support.** For Unified Communications Managers 10.x and later in mixed mode, InformaCast now supports SRTP packets in unicast streams. SRTP provides encryption, message authentication, integrity, and replay protection for RTP packets. With the addition of SRTP support, InformaCast is interoperable with Unified Communications Manager in FIPS and FedRAMP modes. If you were previously using SIP and you had configured it to work with TLS, you will need to select the **Secure Signaling Required** checkbox on the SIP Call Security page before any InformaCast features using SIP will work.
- **Improved Logging for the SIP Stack.** The SIP Stack log (available by going to **Help | Support**) has been improved to log the message body of SIP requests along with the headers that were already being monitored. This more robust logging can further aid in troubleshooting various SIP issues.
- **New CTI Connection Information.** InformaCast's Overview page has a new table column, CTI Provider, that lists the Unified Communications Manager with which it has established a connection. If no connection has been established, "DISCONNECTED" will appear.
- **Newly Supported Phone.** InformaCast now supports the 8851NR Cisco IP phone model.
- **New Operating System.** The Virtual Appliance is now running an updated operating system that includes the latest bug fixes and security patches.

- **New Upgrade File.** A new file (CiscoPagingServer_11.5.1.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_11.5.1.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_11.5.1.deb)
 - For 9.1.1, 11.0.1, 11.0.2, or 11.0.5 to the current version, you will install one package file (CiscoPagingServer_11.5.1.deb)

InformaCast Virtual Appliance 8.5.1 and 9.1.1 are waypoints in the upgrade process. For 8.3 or 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 11.5.1. 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 11.5.1. For 9.1.1, 11.0.1, 11.0.2, and 11.0.5 versions of the Virtual Appliance, you can upgrade directly to 11.5.1.

Resolved Issues

Establish CTI Connections After InformaCast’s Initialization. In previous versions of InformaCast, CTI connections were being established while InformaCast was still initializing. This could cause problems if calls arrived during initialization because InformaCast was not prepared to start broadcasts. CTI connections are now established after InformaCast initializes, which solves the issue.

Resolved Caveats

CDETs ID	Title
CSCux54435	Remove SSLRC4 Cipher Suites
CSCux97095	InformaCast and CVE-2016-0777 and CVE-2016-0778
CSCuy36612	Evaluation of informacast for glibc_feb_2016
CSCuy54654	Evaluation of informacast for OpenSSL March 2016
CSCuz52548	Evaluation of informacast for OpenSSL May 2016

InformaCast 11.0.5

Compatibility

InformaCast is compatible with the following versions of Cisco Unified Communications Manager server (including Business Edition 6000): 8.5.1, 8.6.1, 9.0.1, 9.1.2, 10.0.1, 10.5.2, or 11.0.1.

New Features

- **New Password Security.** For new installations of InformaCast 11.0.5, you are now required to set both your OS and Application Administrator passwords before the Virtual Appliance is completely installed. Similarly, if you are upgrading to InformaCast 11.0.5 and your password was previously changeMe, you will be forced to change your password. By default, both your OS and Application Administrator usernames are “admin.” Your OS credentials allow you to enter Webmin and

Control Center as an administrator or access the Virtual Appliance's command line through SSH. Your application credentials allow you to enter InformaCast as an administrator. When setting your OS or Application Administrator passwords, you cannot use "changeMe."

- **New Support for the E.164 Dial Plan.** InformaCast supports the E.164 dial plan. You can now use E.164 DNs in the InformaCast web and phone user interfaces. In addition, you no longer have to enter a leading backslash when creating rules for your recipient groups on the Add/Edit Recipient Group page. Adjust your filters from \+<DN> to +<DN> and your matched DNs should appear.
- **New Supported ESXi Version.** VMware ESXi 6.0 is now supported by the Virtual Appliance.
- **New Supported SNMP Version.** InformaCast now supports SNMP v3, which allows encryption of phone information traffic between InformaCast and Cisco Unified Communications Manager. When configuring SNMP in Unified Communications Manager, you can set up the V3 option and then enter the corresponding SNMP v3 user's name and password information in InformaCast's updated Edit Telephony Configuration page (**Admin** | **Telephony** | **Cisco Unified Communications Manager Cluster** | **Edit** button).
- **Updated SIP Stack Logging.** The two previous logs generated for the SIP stack have been combined into one, sipStack.log, which is accessible through the Support page (**Help** | **Support**).
- **Enhanced Retention of Log Files.** As InformaCast is in use in increasingly busier environments, more is being written to the Performance and Summary log files. Previously, InformaCast retained 10 of each, but with increased logging these can roll over quickly, and if not checked immediately, relevant information can be lost. Therefore, 100 Performance and Summary log files are now kept to alleviate this situation.
- **New Upgrade File.** A new file (CiscoPagingServer_11.0.5.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_11.0.5.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_11.0.5.deb)
 - For 9.1.1, 11.0.1, or 11.0.2 to the current version, you will install one package file (CiscoPagingServer_11.0.5.deb)

InformaCast Virtual Appliance 8.5.1 and 9.1.1 are waypoints in the upgrade process. For 8.3 or 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 11.0.5. 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 11.0.5. For 9.1.1, 11.0.1, and 11.0.2 versions of the Virtual Appliance, you can upgrade directly to 11.0.5.

- **API Troubleshooting.** The API documentation (www.singlewire.com/help/InformaCastAPI/v11.0.5/index.html) now has a "Troubleshooting" section. Check there for common problems and their solutions.

Announcements

- **Streamlined Support for VMware ESXi 4.x.** Releases of InformaCast subsequent to 11.0.5 will no longer support VMware ESXi 4.x due its end of availability and end of support status with VMware.
- **Streamlined Support for CUCM.** Releases of InformaCast subsequent to 11.0.5 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>)

Resolved Caveats

CDETs ID	Title
CSCuv19098	Answerfile-based installation fails
CSCuu57988	Require default credentials to change

New Caveats

CDETs ID	Title
CSCuv84361	Moving InformaCast backup fails when OS password has special characters

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

CDET's 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

CDET's 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

CDET's 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 Credentials

The username and password you use to enter InformaCast and PushToTalk as an administrator. By default, the username is “admin” and you are forced to set your password when installing the Virtual Appliance.

Application User

A user within Cisco Unified Communications Manager 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 Unified Communications Manager 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 Unified Communications Manager 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 Unified Communications Manager's web server, which responds with an XML-formatted response. InformaCast uses AXL to gather phone information from Unified Communications Manager.

BAT

Bulk Administration Tool. A web-based application for Unified Communications Manager 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 Unified Communications Manager'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 Unified Communications Manager 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 Unified Communications Manager applications and InformaCast to create virtual lines. CTI ports are configured through the same Cisco Unified Communications Manager Administration area as phones, but require different configuration settings.

Device Association

A link that allows a specific Unified Communications Manager user to control a device (such as a CTI port) within the Unified Communications Manager 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 Unified Communications Manager 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 Unified Communications Manager Administration interface.

Device Pool

In Unified Communications Manager, 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, Unified Communications Manager 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 Unified Communications Manager 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 Unified Communications Manager 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.

OS Credentials

The username and password you use to enter Webmin and Control Center and when using SSH to access the Virtual Appliance. By default, the username is “admin” and you are forced to set your password when installing the Virtual Appliance.

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 Unified Communications Manager 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 Unified Communications Manager 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 Unified Communications Manager 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.



Index

A

Access

- InformaCast 1-1
- InformaCast Virtual Appliance 1-22
- License Manager 1-30
- Singlewire Start Page 1-22
- Webmin 1-35

Access InformaCast 1-23, 1-27, 1-2

Active Broadcasts 1-53

Add

- Broadcast Dialing Configuration 1-47
- 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 1-31
- SIP Access Exception 1-34
- SIP Trunk Security Profile 1-5
- SIP User Credentials 1-40
- TLS SIP Profile 1-21
- TLS SIP Trunk 1-24
- TLS SIP Trunk Security Profile 1-18

Administer

- Installation 1-88
- Recipients 1-38

Advanced Functionality Definition 1-5, 1-1

Advanced InformaCast 1-1

API 1-1, 1-10

Application Credentials 1-17, 1-2, 1-24

Application Credentials, Troubleshooting 1-3, 1-5

Authentication URL 1-80

AXL Credentials 1-2, 1-9

B

Backup

- Configure InformaCast 1-4
- InformaCast 1-3
- Move ZIP File to a Safe Location 1-5
- Troubleshooting 1-11

Basic Functionality Definition 1-5, 1-1

Basic InformaCast Upgrade 1-1

Basic License Definition 1-6

Broadcast

- Cancel 1-52
- Send a Broadcast 1-51

Broadcast Dialing Configuration

- Add 1-47
- Delete 1-50

Edit 1-48

Broadcasts

- Parameters 1-45
- Troubleshooting 1-10

Buy Advanced Notification 1-8

C

Call Detail Records

- Collect 1-54
- DTMF Data 1-60
- Manage 1-53
- RTP Data 1-59
- SDP Data 1-59
- Session Activity 1-58
- SIP Data 1-58
- Summary Data 1-58
- View 1-55

Calling Terminal Diagnostics 1-9

Cancel

- Audio Broadcast 1-52

Change

- Application Administrator Password 1-2
- OS Administrator Password 1-8

Change IP Address 1-2, 1-9

Cisco Unified Communications Manager

- Add Access Control Group 1-66
- Application User 1-70
- Authentication URL 1-80
- Calling Search Space 1-59
- Configure SNMP 1-46
- Create a Community String 1-49
- Create CTI Ports 1-61
- Create Route Partition 1-58
- Device Pool 1-56
- Enable SNMP 1-46
- G.711 Codec 1-54
- Integrate 1-45
- JTAPI and Phones' Busy States 1-42
- Reboot Phones 1-83
- Test Phones 1-85
- Web Access for Phones 1-73

Collect Call Detail Records 1-54

Command Line Interface 1-11

Configure

- Default Unified Communications Manager Cluster 1-2
- InformaCast Backups 1-4
- Messages and Broadcasts 1-1
- Recipients 1-1
- Session Timeouts 1-18
- SIP Trunk 1-4
- SNMP Monitoring 1-16
- Update JTAPI 1-30

Control Center

- OS Credentials 1-16
- Copy
 - Recipient Group 1-30
- Create
 - Signed Certificate 1-38
 - SIP Trunk 1-8
 - SNMP v3 User 1-51
- CTI Credentials 1-2, 1-9
- D**
- Defunct Phones 1-32
- Delete
 - Broadcast Dialing Configuration 1-50
 - Defunct Phones from InformaCast 1-32
 - Recipient Group 1-34
 - SIP User Credentials 1-43
- Demonstration License Definition 1-6
- Determine Phones' Busy States 1-42
- DialCast
 - Manage SIP Functionality 1-4
- DialCasts 1-10
 - Add Broadcast Dialing Configuration 1-47
 - Cancel 1-52
 - Delete Broadcast Dialing Configuration 1-50
 - Edit Broadcast Dialing Configuration 1-48
 - Manage 1-46
 - Send 1-51
- E**
- Edit
 - Broadcast Dialing Configuration 1-48
 - Default Unified Communications Manager Cluster 1-9
 - Recipient Group 1-25
 - SIP User Credentials 1-42
- Enable
 - Web Access for Individual Phones 1-76
 - Web Access for Multiple Phones 1-73, 1-74
 - Web Access for Phones 1-73
- Encrypted Media 1-2, 1-4, 1-46
- ESXi 1-6
- EULA Error 1-2
- F**
- FAQ 1-1
 - Capture Traffic 1-2
 - Create Recipient Groups 1-2
 - Exceeded License Key 1-1
 - HTTP Status 500 Error 1-1
 - IP Address 1-2, 1-9
 - New IP Address 1-2, 1-9
 - No Text or Audio Broadcasts 1-2
 - Signed Certificate 1-1
 - Voicemail 1-2
- Free Trial 1-4
- Frequently Asked Questions, see FAQ 1-1
- H**
- Help 1-12
- I**
- InformaCast
 - Access 1-1
 - Application Credentials 1-17, 1-2, 1-24
 - Configure Messages and Broadcasts 1-1
 - Configure Recipients 1-1
 - DSCP Quality of Service Policies 1-5
 - Log In Initially 1-2
 - Maintain 1-1
 - Manage Telephony 1-2
 - Reboot Phones 1-83
 - Set Authentication URL 1-80
 - Test Phones 1-85
 - Upgrade from Basic to Advanced 1-1
- InformaCast IP Address 1-23, 1-27, 1-2
- InformaCast Virtual Appliance
 - Access 1-22
 - API 1-1, 1-10
 - Change OS Administrator Password 1-8
 - Command Line Interface 1-11
 - Configure Backups 1-4
 - Control Center Interface 1-10
 - Definition of 1-1
 - Documentation 1-12
 - Embedded SNMP Agent 1-16
 - Hardware Requirements 1-3
 - Help 1-12
 - Icons, Description of 1-9
 - Illustrations 1-7
 - Install 1-1, 1-6
 - Install Cisco Unified Communications Manager Certificates 1-26
 - Install SIP Certificate 1-12
 - Intended Audience 1-1
 - Interface Orientation 1-7
 - License 1-6
 - Licensing 1-5
 - Manage Backups 1-3
 - Multicast 1-2, 1-88, 1-94, 1-95, 1-96
 - Notification Boxes Explained 1-2
 - Open 1-23, 1-27, 1-2
 - Plan your Multicast Environment 1-1
 - Port Configuration 1-3
 - Prepare your Multicast Environment 1-1
 - Prerequisites 1-2
 - Remove Defunct Phones 1-32
 - Restore from Backup 1-8
 - Set the System Time 1-35
 - Singlewire Start Page 1-8
 - Support 1-12
 - Test Multicast 1-2
 - Troubleshooting 1-12
 - Update JTAPI 1-30
 - Upgrade 1-15
 - Upgrade License 1-9
 - Upgrade, Determine Version 1-15
 - Upgrade, Upload New License 1-25
 - User Guide Standards 1-1
 - Versions 1-15
 - Web Interface 1-9
 - Webmin 1-11
- InformaCast Virtual Appliance Version 1-29
- InformaCastBackup.ZIP 1-5
- Install
 - Administration 1-88
 - Cisco Unified Communications Manager 1-45

- Cisco Unified Communications Manager Certificates on InformaCast 1-26
 - Cisco Unified Communications Manager SNMP v2 1-49
 - Configure Cisco Unified Communications Manager SNMP 1-46
 - Create a Calling Search Space 1-59
 - Create Access Control Group 1-66
 - Create Application User 1-70
 - Create CTI Ports 1-61
 - Create Device Pool 1-56
 - Create Route Partition 1-58
 - Enable Cisco Unified Communications Manager SNMP 1-46
 - Enable Web Access for Phones 1-73
 - InformaCast SIP Certificate 1-12
 - InformaCast Virtual Appliance 1-6
 - Reboot Phones 1-83
 - Set Authentication Method for API Browser Access 1-82
 - Set Authentication URL 1-80
 - Set G.711 Codec 1-54
 - Signed Certificate 1-38
 - Test Phones 1-85
 - Unified Communications Manager SNMP v3 1-51
 - Install InformaCast 1-1
 - Interface Orientation 1-7
 - IP Address, Change 1-2, 1-9
- J**
- JTAPI 1-30, 1-42, 1-45
- L**
- License
 - Demonstration, Definition of 1-6
 - Perpetual, Definition of 1-6
 - Subscription, Definition of 1-6
 - Trial, Definition of 1-6
 - License Definitions 1-5
 - License Key 1-5, 1-6, 1-9
 - Exceed 1-6, 1-13, 1-1
 - Upload New 1-25
 - License Key, Dependent Features 1-9
 - License Manager, Access 1-30
 - Live Audio Broadcast 1-51
 - Log into InformaCast 1-21, 1-23, 1-2
 - Log into InformaCast Initially 1-2
 - Log into PushToTalk 1-24
 - Log into the Control Center 1-25
 - Log into Webmin 1-27
 - Logs
 - Performance 1-6, 1-13, 1-1, 1-2, 1-1
 - Summary 1-1, 1-6
- M**
- Maintain InformaCast 1-1
 - Manage
 - Broadcast Parameters 1-45
 - Call Detail Records 1-53
 - DialCasts 1-46
 - Digest Authentication with SIP User Credentials 1-40
 - InformaCast Backups 1-3
 - InformaCast Telephony 1-2
 - Installation Administration 1-88
 - Messages 1-1
 - New License 1-25
 - New License Key 1-9
 - Phone Updates 1-40, 1-14
 - Recipient Administration 1-38
 - Recipient Groups 1-11
 - SIP Access to InformaCast 1-33
 - SIP Call Security 1-36
 - SIP Certificates 1-10
 - SIP Functionality 1-4
 - SIP Stack 1-44
 - Management Information Base 1-16
 - 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
 - Mixed Mode 1-2, 1-4, 1-46
 - Multicast 1-46
 - IGMP Snooping 1-96
 - IGMPv3 1-96
 - MPLS Provider 1-95
 - Network Capture 1-89, 1-92
 - PIM 1-94
 - Plan your environment 1-1
 - Review Configuration 1-88
 - Test Configuration 1-2
 - Testing Tool 1-2
 - Traffic Capture 1-88
 - Troubleshooting 1-88, 1-1
 - Multicast Environment Preparation
 - InformaCast Virtual Appliance 1-1
- N**
- Network DSCP QoS 1-5, 1-10
 - Network Management Software 1-16
 - Network Traffic Capture
 - Obtain 1-89
 - Read 1-92
 - Notification Box
 - Caution 1-2
 - Note 1-2
 - Tip 1-2
 - Warning 1-2
- O**
- OS Administrator 1-16
 - OS Credentials 1-8
 - OS Credentials, Troubleshooting 1-3, 1-5
- P**
- Password Requirements 1-3
 - Performance Log 1-6, 1-13, 1-1, 1-2, 1-1
 - Perpetual InformaCast 1-8
 - Perpetual License Definition 1-6
 - Phones, Reboot 1-83
 - Phones, Test 1-85

Port Configuration 1-3
 PushToTalk Application Credentials 1-17, 1-24

R

Reboot
 Phones 1-83
 Reboot InformaCast Virtual Machine 1-5, 1-7
 Recipient Group Tags
 Add 1-35
 Delete 1-37
 Description of 1-35
 Edit 1-36
 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 1-38
 Copy 1-30
 Delete 1-34
 Edit 1-25
 Manage 1-11
 Regular Expressions 1-39
 Remove Defunct Phones 1-32
 Remove Rules 1-21
 Subnet Matching 1-38
 Tag 1-35, 1-36, 1-37
 View Recipients 1-27
 Recipients
 Administration 1-38
 Configure 1-1
 Regular Expressions
 Group Recipients 1-39
 Release Notes 1-1
 11.0.1 1-6
 11.0.1.a 1-6
 11.0.2 1-5
 11.0.5 1-3
 11.5.1 1-2
 8.3 1-15
 8.3.a 1-14
 8.4.a 1-12
 8.5.1 1-12
 9.0.1 1-10
 9.0.2 1-9
 9.1.1 1-8
 InformaCast 11.5.2 1-1
 Remove
 Defunct Phones 1-32
 Recipient Group Rules 1-21
 Restart
 SIP 1-45
 Restart InformaCast 1-5
 Restore InformaCast from Backup 1-8

S

Send
 DialCast 1-51
 Live Audio Broadcast 1-51
 Send Commands to Phones by JTAPI, Troubleshooting 1-8
 Server Hardening

Troubleshooting 1-1
 Session Timeouts, Configure 1-18
 Set Authentication URL 1-80
 Set System Time 1-35
 Signed Certificate 1-22, 1-38
 Singlewire Start Page 1-8
 Singlewire Start Page, Access 1-22
 SIP 1-4
 Add a Route Pattern 1-31
 Add a SIP Trunk Security Profile 1-5
 Add a TLS SIP Profile 1-21
 Add a TLS SIP Trunk 1-24
 Add a TLS SIP Trunk Security Profile 1-18
 Add Access Exception 1-34
 Add User Credentials 1-40
 Allow/Deny Access to InformaCast 1-33
 Call Detail Records 1-53, 1-54, 1-55
 Configure a SIP Trunk 1-4
 Create a SIP Trunk 1-8
 Delete SIP User Credentials 1-43
 Edit User Credentials 1-42
 Enable Digest Authentication with SIP User Credentials 1-40
 Enable SIP Call Security 1-36
 Install Cisco Unified Communications Manager Certificates on InformaCast 1-26
 Install InformaCast SIP Certificate 1-12
 Manage SIP Certificates 1-10
 Manage SIP Stack 1-44
 Restart 1-45
 Upgrade Troubleshooting 1-12
 View InformaCast SIP Certificate 1-11
 SIP Functionality
 Manage 1-4
 SNMP v2 1-49
 SNMP v3 1-51
 SNMP, Configure Monitoring 1-16
 SRTP 1-21
 SRTP, Troubleshooting 1-11
 SSLMGR 1-38
 Start InformaCast 1-3
 Start Page 1-22, 1-23, 1-27, 1-2
 Start/Stop InformaCast 1-5
 Stop InformaCast 1-1
 Subnet Matching 1-38
 Subscription InformaCast 1-8
 Subscription License Definition 1-6
 Summary Log 1-1, 1-6
 Support 1-12

T

Test
 Phones 1-85
 Test Multicast 1-2
 TLS
 Add a SIP Profile 1-21
 Add a SIP Trunk 1-24
 Add a SIP Trunk Security Profile 1-18
 Definition 1-10
 Install Cisco Unified Communications Manager Certificates on InformaCast 1-26
 Install the InformaCast SIP Certificate 1-12

- Manage SIP Certificates 1-10
- Trial License Definition 1-6
- Troubleshooting 1-12, 1-1
 - Authentication 1-6
 - Backups 1-11
 - Broadcasts 1-8
 - Detailed SIP Logging 1-2
 - EULA Error 1-2
 - Log Files 1-1
 - Log into InformaCast 1-21, 1-2
 - Multicast 1-1
 - Phone Discovery 1-7
 - Server Hardening 1-1
 - SIP and Upgrades 1-12
 - Start/Stop/Restart and Reboot InformaCast 1-5
 - Upgrade from Basic to Advanced 1-12
 - Upgrade InformaCast Virtual Appliance 1-12
 - VMware Tools 1-5, 1-14
- Troubleshooting SRTP 1-11
- Try Advanced Notification 1-4

U

- Unified Communications Manager
 - Create an SNMP v3 User 1-51
 - Mixed Mode, Encrypted Media 1-2, 1-4, 1-46
 - Set Authentication Method for API Browser Access 1-82
- Unified Communications Manager Clusters
 - Default 1-2, 1-9
- Update InformaCast's Phone Information 1-40, 1-14
- Upgrade
 - How To Steps 1-12
- Upgrade InformaCast 1-1
 - Basic to Advanced 1-1
 - Buy Advanced Notification 1-8
 - Differences Between Versions 1-15
 - Enter New License Key 1-9
 - Errors on Telephony Configuration 1-13
 - Install a Software Package 1-16
 - Missing Cisco Unified Communications Manager Information 1-13
 - Missing Phones 1-13
 - Note the Differences 1-2
 - Try Advanced Notification 1-4
- Upgrade InformaCast EX
 - Obtain Software Package 1-15
- Upgrade InformaCast Virtual Appliance 1-15
 - Determine Your Current Version 1-15
 - Upload New License 1-25

V

- Version, InformaCast Virtual Appliance 1-29, 1-15
- View
 - Active Broadcasts 1-53
 - Call Detail Records 1-55
 - InformaCast SIP Certificate 1-11
 - License Key 1-6
 - Recipients in a Recipient Group 1-27
- Virtual Appliance 1-6
 - Webmin 1-11
- Virtual Machine 1-6
- Virtual Machine Control Center Interface 1-10
- VMware 1-6
- VMware Tools 1-5, 1-14

W

- Web Access, Individual Phones 1-76
- Web Access, Multiple Phones 1-73, 1-74
- Web Access, Phones 1-73
- Web Interface 1-9
- Webmin 1-11
 - OS Credentials 1-16
- Webmin, Access 1-35
- Website Certificate 1-38