InformaCast Virtual Appliance Basic Paging®

Version 12.5.1

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

November 16, 2018

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.

Last Updated: November 16, 2018

CONTENTS

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/v12.5.1/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.

- U n d e r l i n e d t e x t 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 IP phones if you intend to use them as recipients
- Use of one of the following supported browsers: Firefox 62, Chrome 70, MS Edge 44, and 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: 10.0.1, 10.5.2, 11.0.1, 11.5.1, 12.0.1, and 12.5.1

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 5-38).

- 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 https://www.singlewire.com/compatibility-matrix 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 Local Network Traffic

Port	Protocol	Application and/or Purpose	Specification	Access Restriction Recommendations
22	TCP	Secure shell (SSH) for server management	RFC 4253	Restrict access to management subnets
80	TCP	Redirect to InformaCast Virtual Appliance landing page's secure web interface	RFC 2616	Restrict access to management subnets
123	UDP	Network Time Protocol (NTP)	RFC 9505	Restrict access to time servers
443	TCP	InformaCast Virtual Appliance landing page's secure web interface	RFC 2616	Restrict access to management subnets
1161	UDP	InformaCast SNMP	RFC 1157	Restrict access to management subnets
8081	TCP	InformaCast's non-secure web interface	RFC 2616	Restrict to IP phone subnets
8101	TCP	Control Center's non-secure web interface	RFC 2616	Restrict access to management subnets
8444	TCP	InformaCast's secure web interface	RFC 2616	Restrict access to management subnets and API clients
8463	TCP	Control Center's secure web interface	RFC 2616	Restrict access to management subnets
10000	TCP	Redirect to webmin interface on https://<InformaCast Virtual Appliance IP Address>/webmin	RFC 2616	Restrict access to management subnets
32068-32468	UDP	InformaCast's inbound RTP streams (inbound calls to CTI ports and inbound SIP)	RFC 3550	Unrestricted access
5060-1	TCP	InformaCast's SIP	RFC 3261	Restrict access using InformaCast SIP access

Table 2: Outbound Local Network Traffic

Port	Protocol	Application and/or Purpose	Specification
80	TCP	InformaCast's outbound connections to IP phones	RFC 2616
161	UDP	Unified Communications Manager SNMP phone data	RFC 1157
427	UDP and TCP	InformaCast SLP	RFC 2608
443	TCP	Secure web interface for Unified Communications Manager AXL web services	RFC 2616
2748	TCP	Unified Communications Manager CTI ports/route points	N/A
20480-21080	UDP	Default multicast ports to which InformaCast sends audio	RFC 3550
32068-32468	UDP	InformaCast's outbound RTP streams (outbound calls to CTI ports and outbound SIP)	RFC 3550

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.

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 Cisco's Solution Reference Network Design (SRND) guide 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.

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

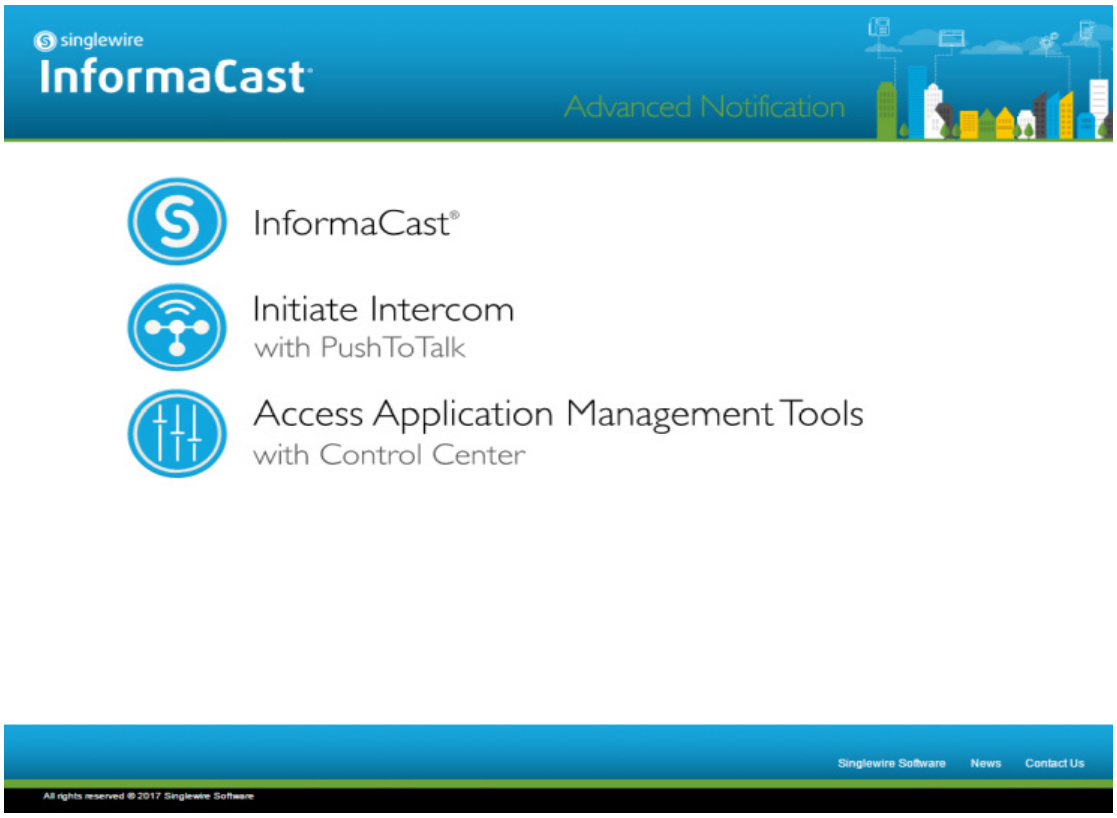
If you have a specific task in mind, peruse the "Contents" on page i-iii to locate the instructions for that task. Additionally, the index that starts on page IN-1 can help you locate desired information.

InformaCast has multiple user interfaces:

- Singlewire landing page
- InformaCast web interface
- Control Center
- Virtual machine administrative web interface (Webmin)
- Command line interface (CLI)

Singlewire Landing Page

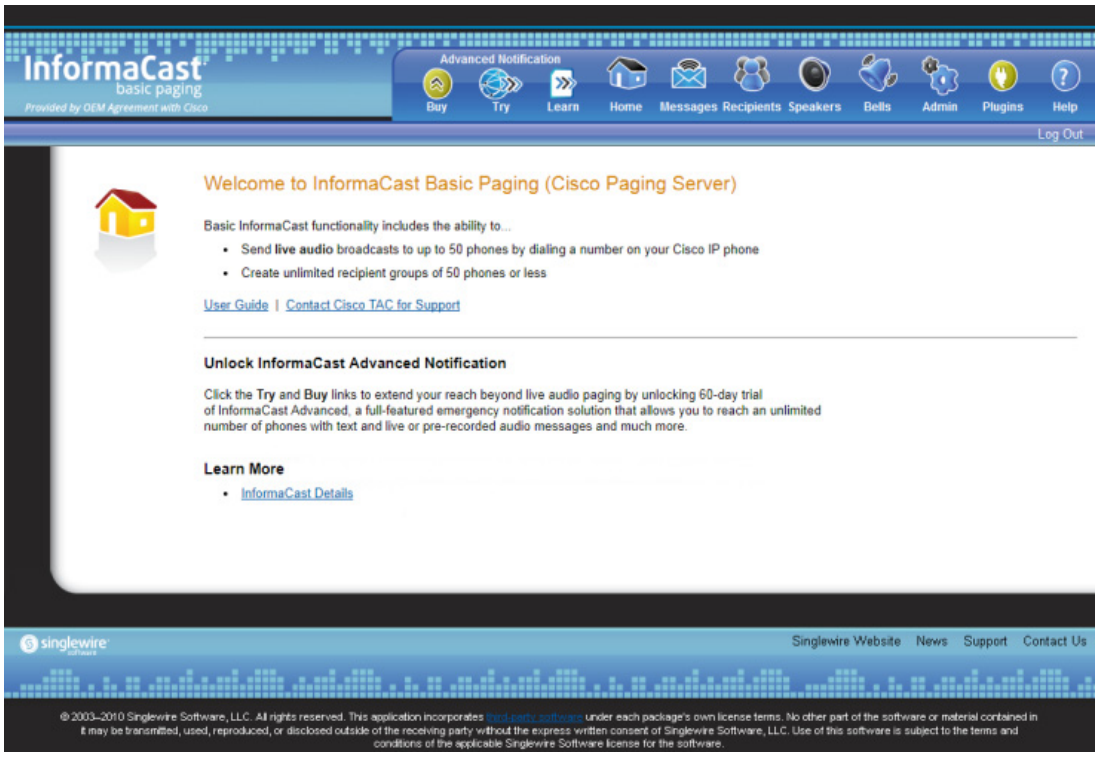
The Singlewire landing page is accessible through a web browser addressed with the IP address of your Virtual Appliance, and it contains links to InformaCast and the Control Center.



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:

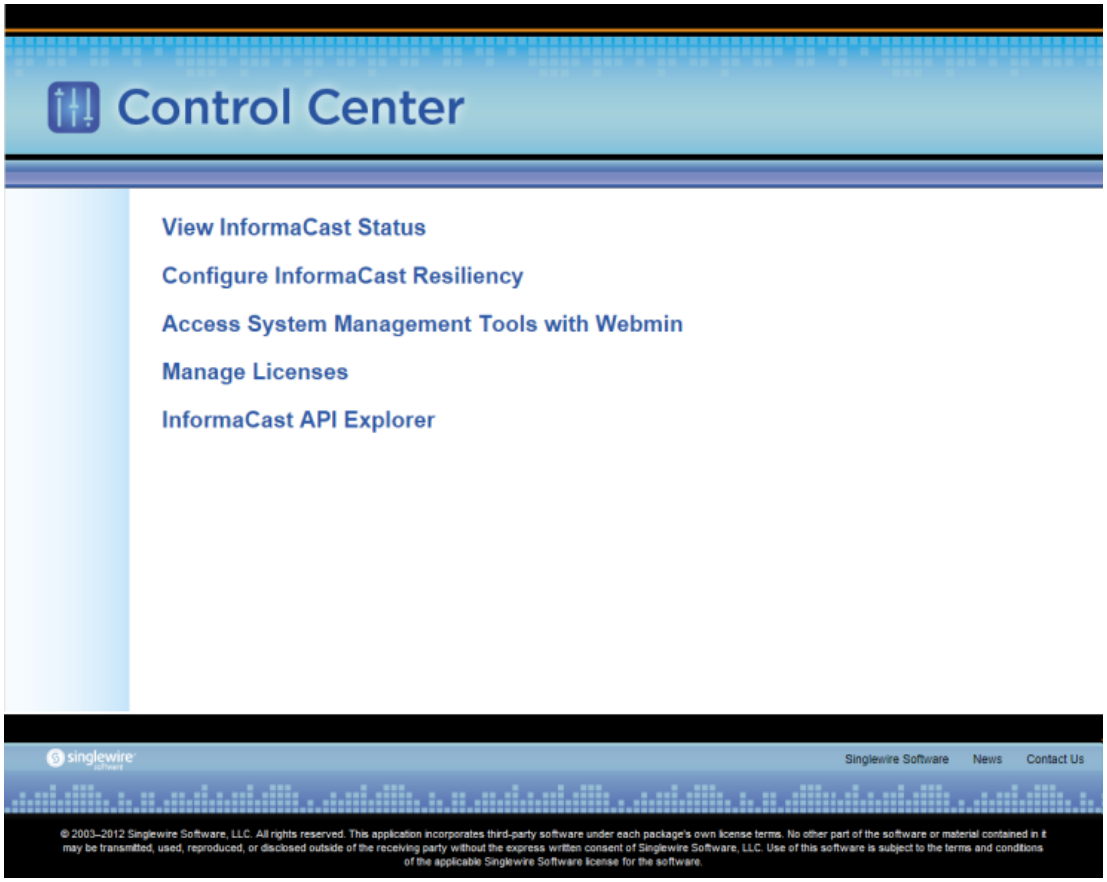
- **Home.** InformaCast's homepage, complete with RSS news feed.
- **Messages.** The message administration page.
- **Recipients.** The recipient group administration page, allowing you to create and manage recipient groups.
- **Admin.** The configuration overview page, allowing you to view scheduled 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

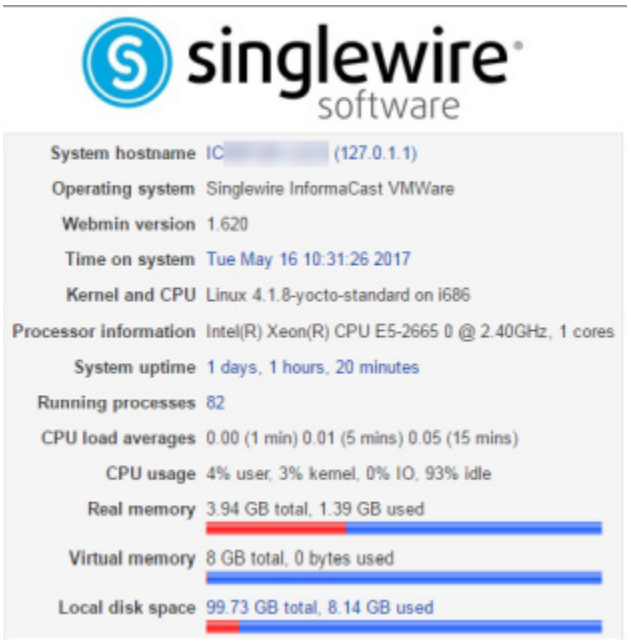
Control Center is designed to be an inclusive destination for application- and system-level accessories. Here, you can view InformaCast's status (e.g. running time, JTAPI version, etc.) or access the License Manager to update your Basic license with an Advanced version (see "Upload a New License" on page 9-109). 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/v12.5.1/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.

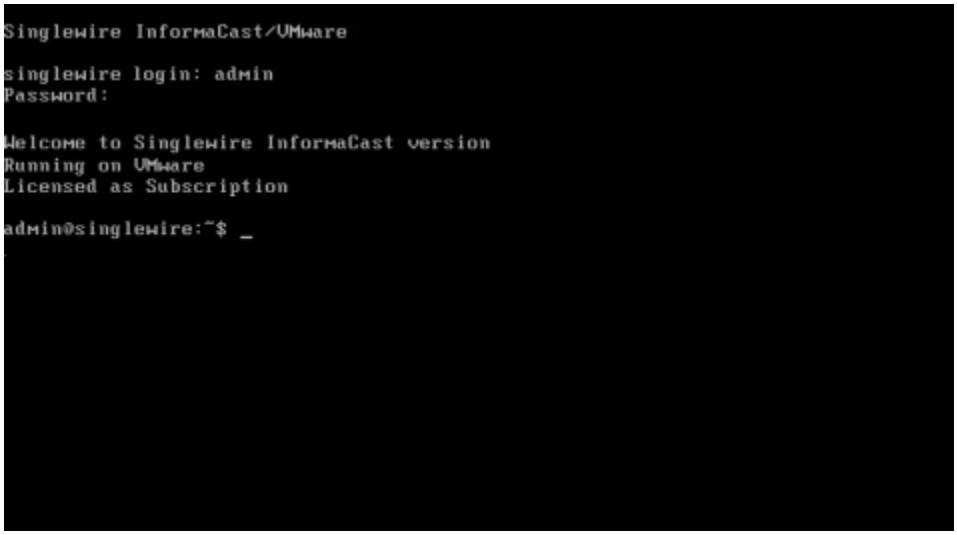
Virtual Appliance Administrative Web Interface (Webmin)

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.



Command Line Interface

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



Note Rudimentary knowledge of bash is required to use the command line interface. If files are to be edited on the virtual machine itself, knowledge of the nano text editor is also required. If you are not familiar with the nano editor, you can optionally transfer files that need to be modified to another machine, edit them there, and then transfer the modified file back to the InformaCast virtual machine. The transfer process can be achieved via an SCP (Secure Copy) client, such as PSCP on Windows. PuTTY, available as a free download, 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.

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.

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
- "Deploy InformaCast" on page 2-6
- "Log into InformaCast Virtual Appliance's Interfaces" on page 2-29
- "Integrate Unified Communications Manager" on page 2-42
- "Manage Installation Administration" on page 2-85

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 Cisco's sample configuration for multicasting over a generic routing encapsulation (GRE) tunnel for details

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
Cisco Worldwide Contacts	Cisco TAC Telephone Numbers and Additional Resources
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. There are three options available to you with the Multicast Testing Tool:

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

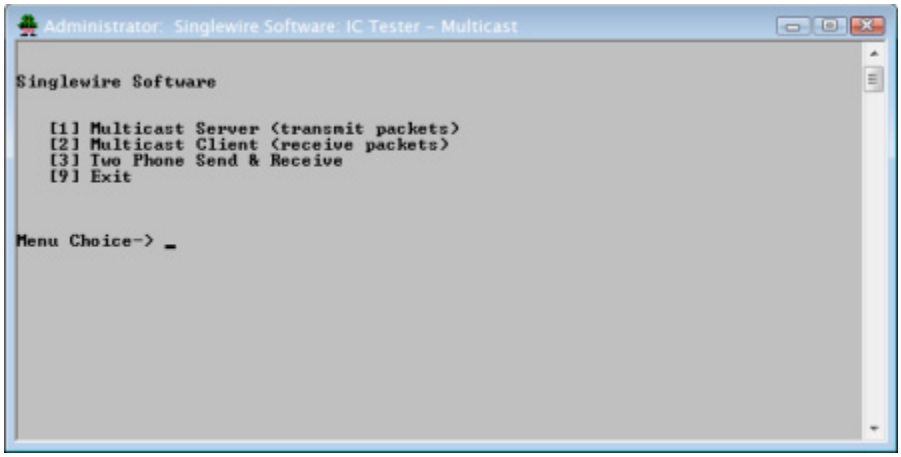
Note Typically, you will want to run Options 1 and 2 in tandem: Option 1 on a Windows machine on the same subnet as InformaCast and Option 2 on the location of your recipients (i.e. a PC on the same VLAN as your recipients).

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

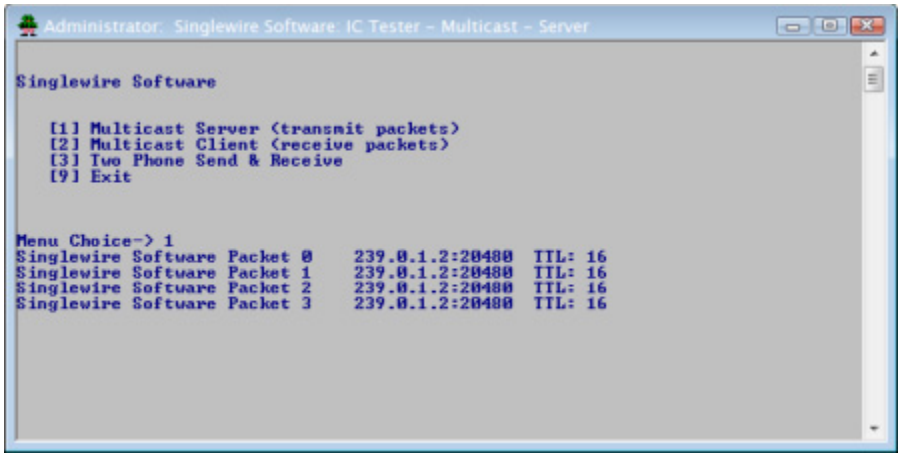
Use Options 1 and 2

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

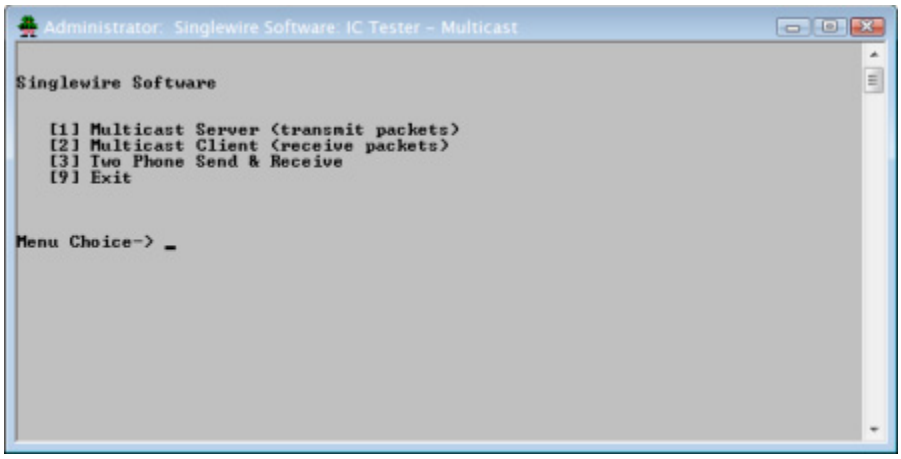
Step 1 Open the **IC_Tester_Mcast.exe** file on a Windows machine on the same subnet as the Virtual Appliance. The IC Tester - Multicast window appears.



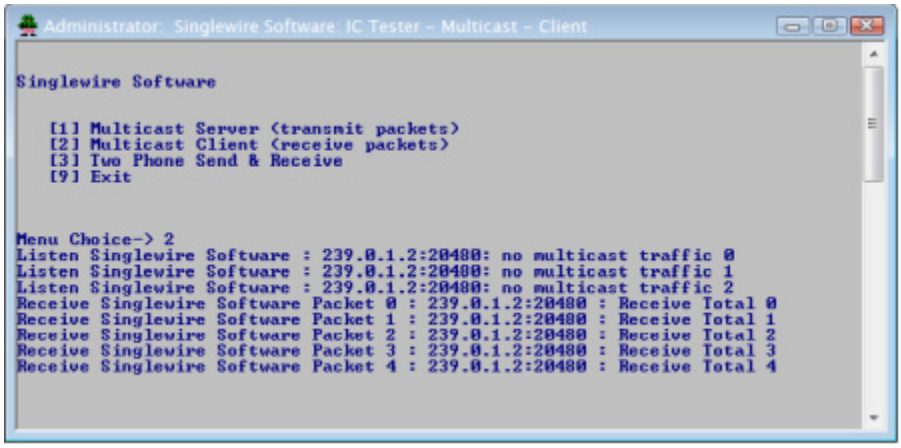
Step 2 Enter **1** at the **Menu Choice** prompt and press the **Enter** key. The IC Tester - Multicast window refreshes, showing multicast packets being sent across your network.



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



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



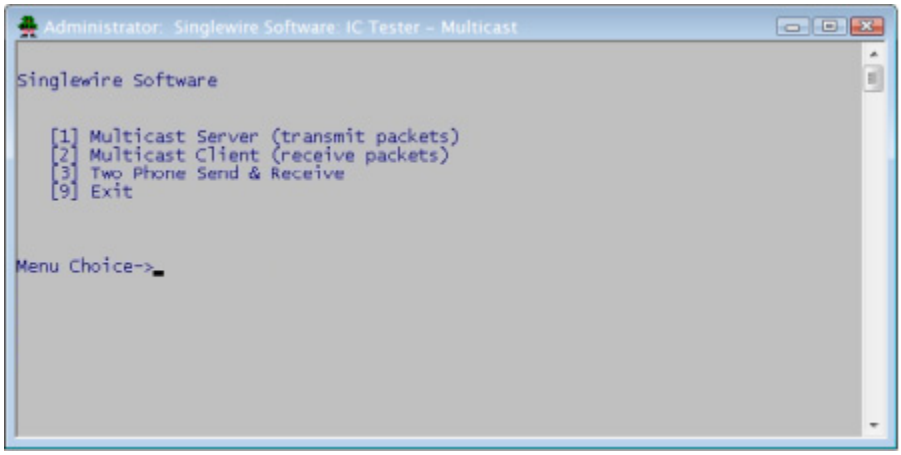
If you receive a “no multicast traffic” result, you can try Option 3, follow the recommendations in “Review Multicast Configuration” on page 2-85, or see “Multicast” on page 9-1.

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.



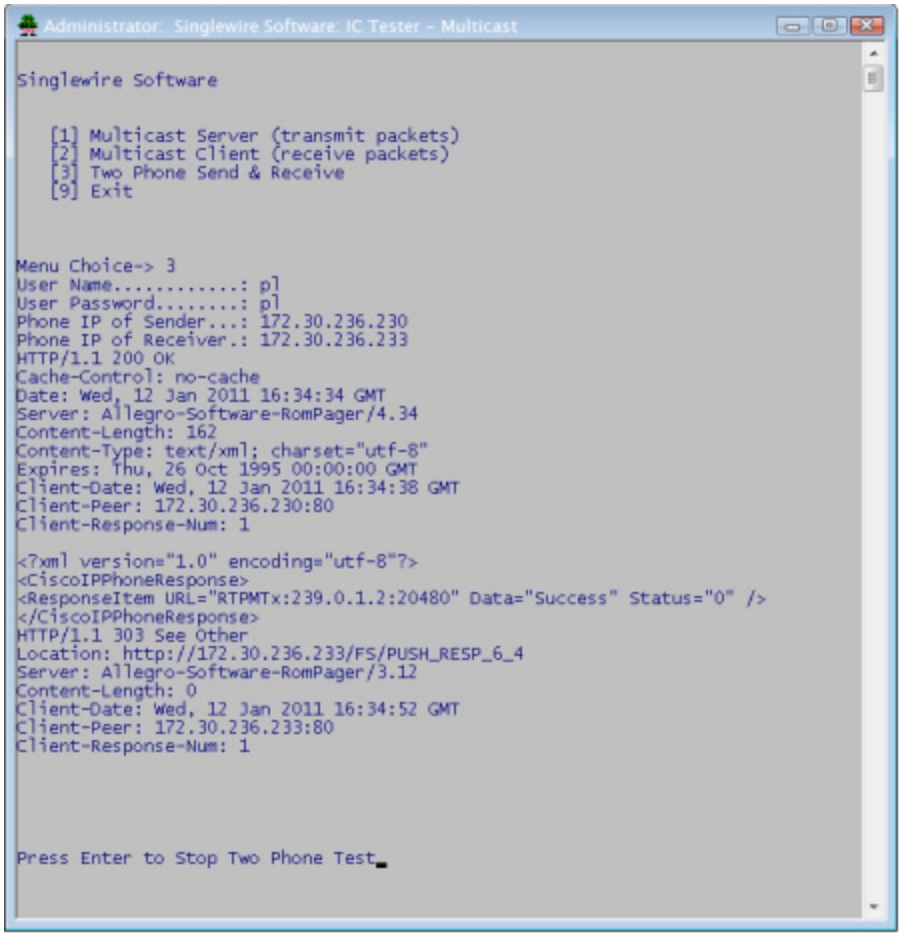
Step 2 Enter **3** at the **Menu Choice** prompt and press the **Enter** key.

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.



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 2-85 or see "Multicast" on page 9-1.

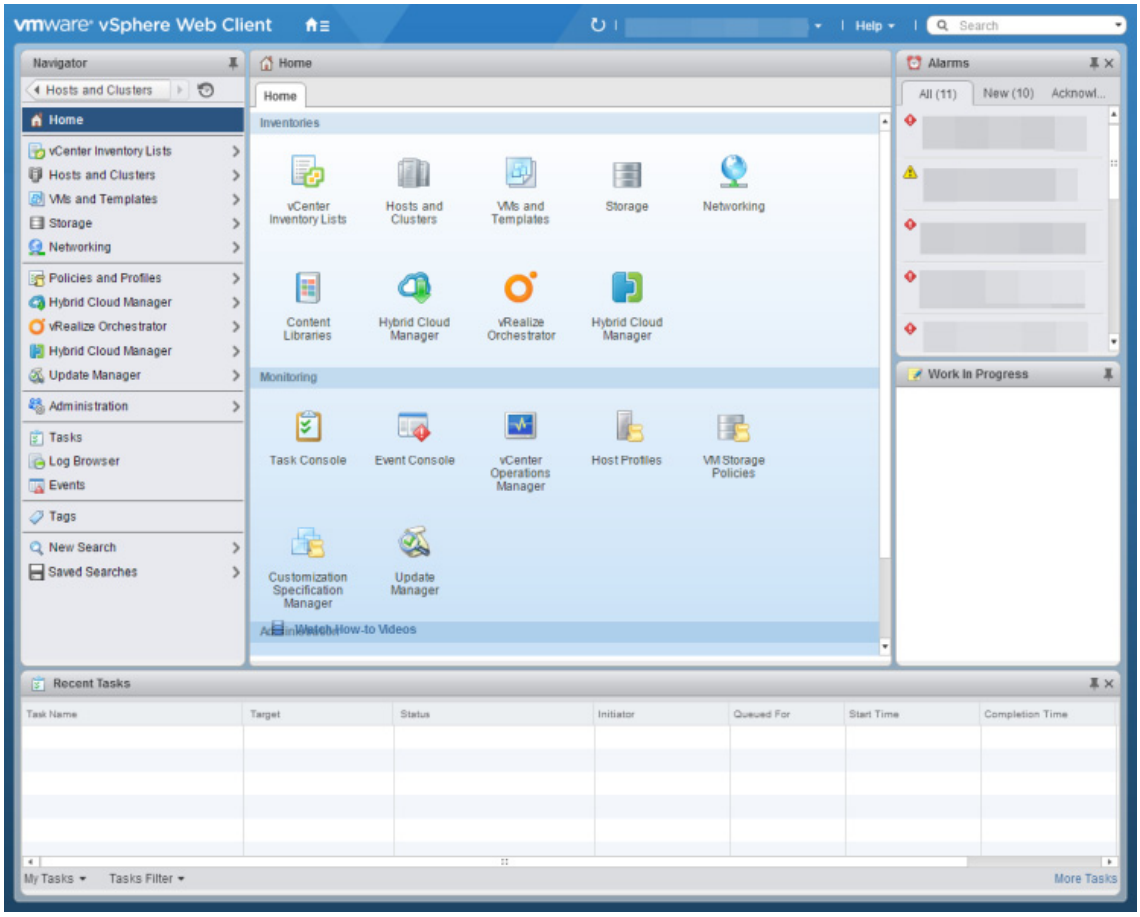
Deploy InformaCast

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

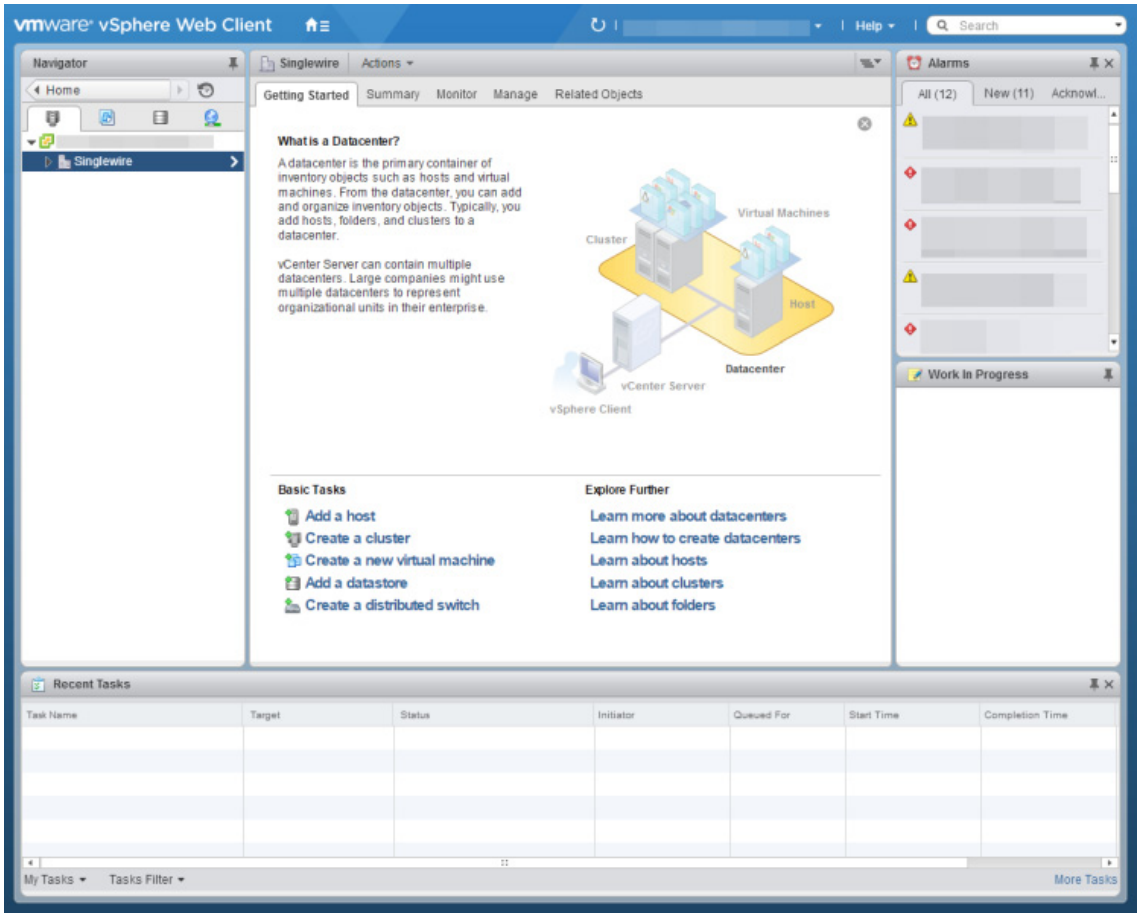
Step 1 Download the OVA file from Cisco's website.

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).

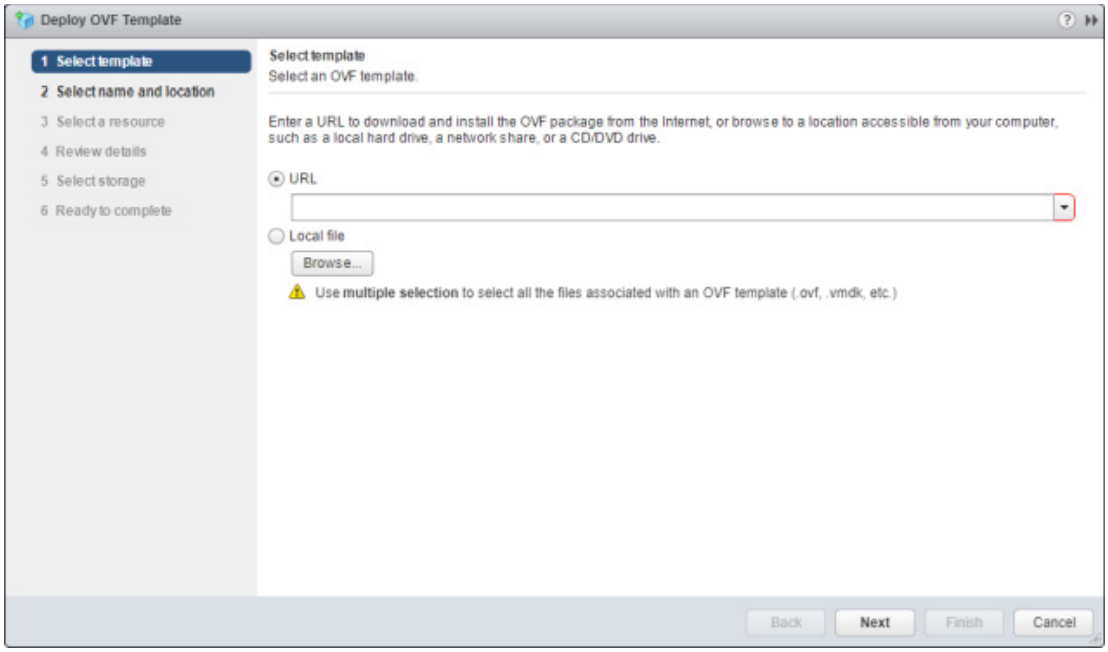
Step 2 Open a web browser and log into your vSphere web client. The vSphere Web Client page appears.



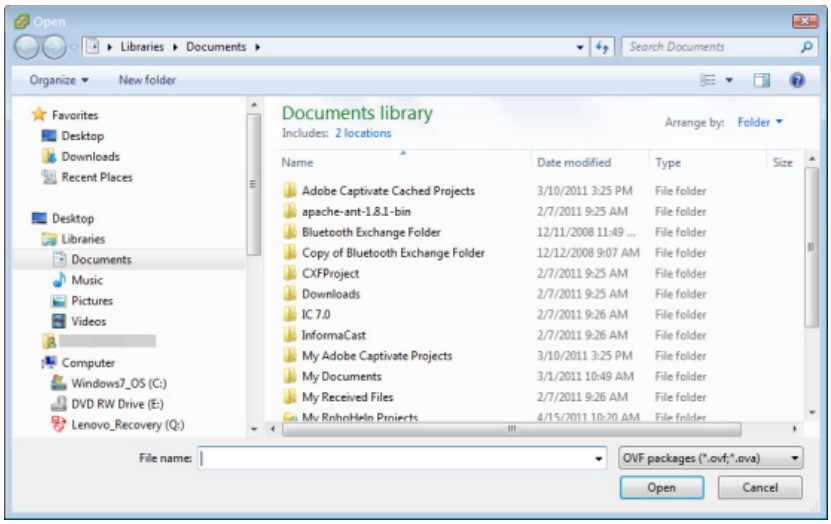
Step 3 Click the **Hosts and Clusters** icon. The vSphere Web Client page refreshes.



Step 4 Go to **Actions** | **Deploy OVF Template**. The Deploy OVF Template pop-up window appears

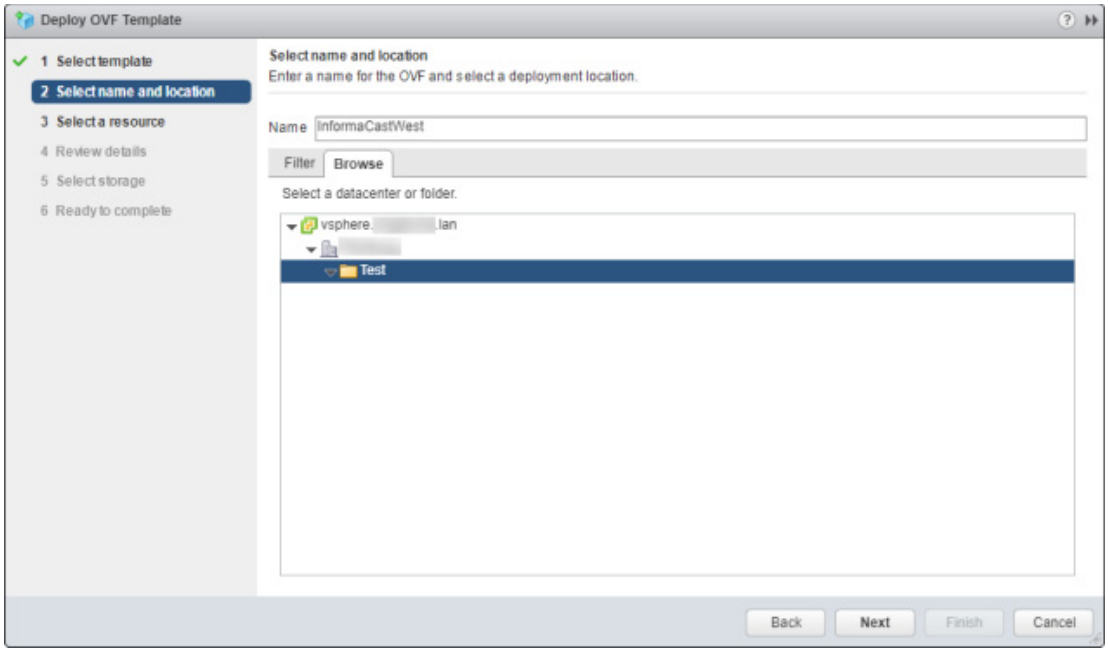


Step 5 Click the **Local File** radio button and click its **Browse** button. The Open dialog box appears.



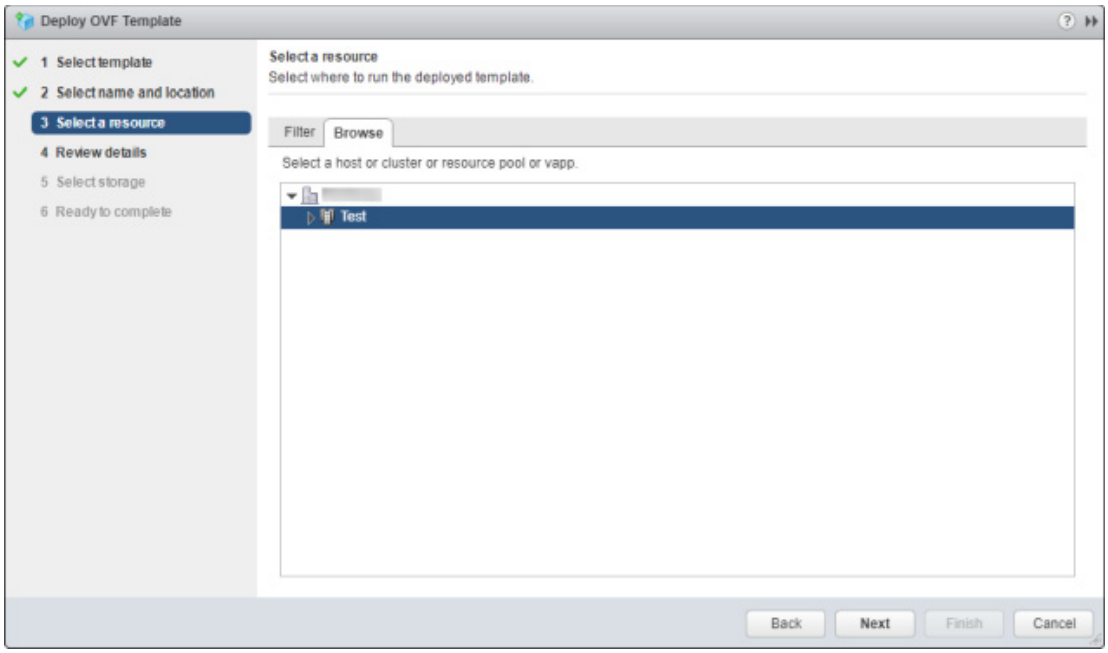
Step 6 Navigate to where you saved the OVA file (or to the OVA file on the supplied DVD), select it, and click the **Open** button.

Step 7 Click the **Next** button. The Deploy OVF Template pop-up window refreshes,



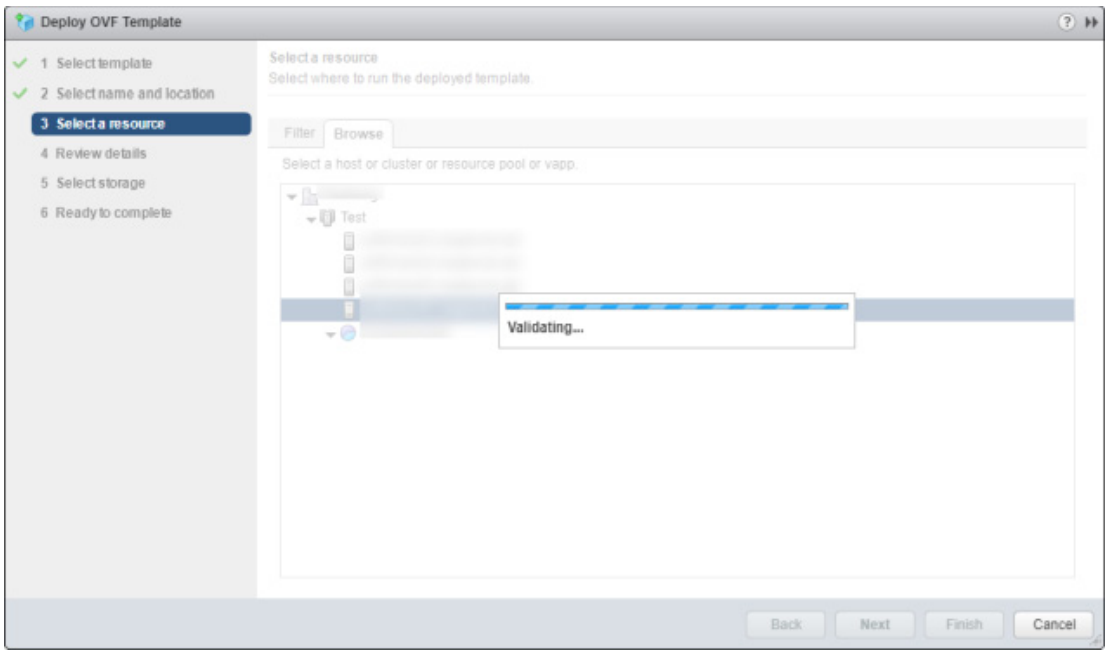
Step 8 Enter a name for your virtual machine in the **Name** field, e.g. InformaCastWest.

Step 9 Select a deployment location for your virtual machine from the **Browse** tab and click the **Next** button. The Deploy OVF Template pop-up window refreshes

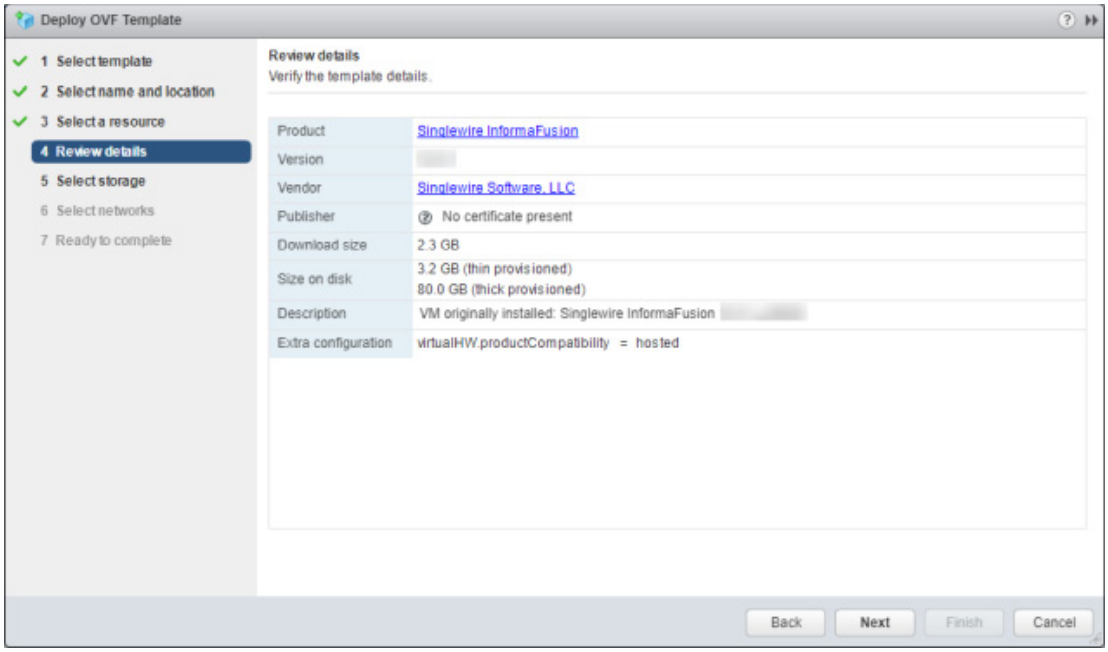


Tip It is good practice to place the Virtual Appliance on the same VLAN as your Unified Communications Manager.

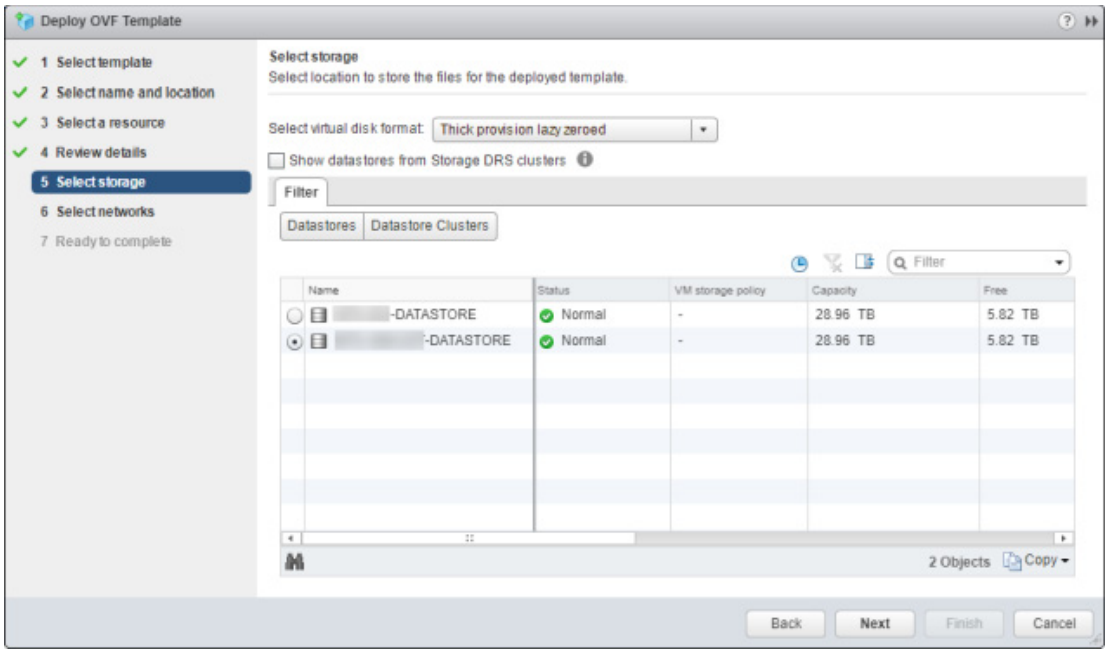
Step 10 Select a location from which to run your deployed template from the **Browse** tab and click the **Next** button. The Deploy OVF template dialog box refreshes.



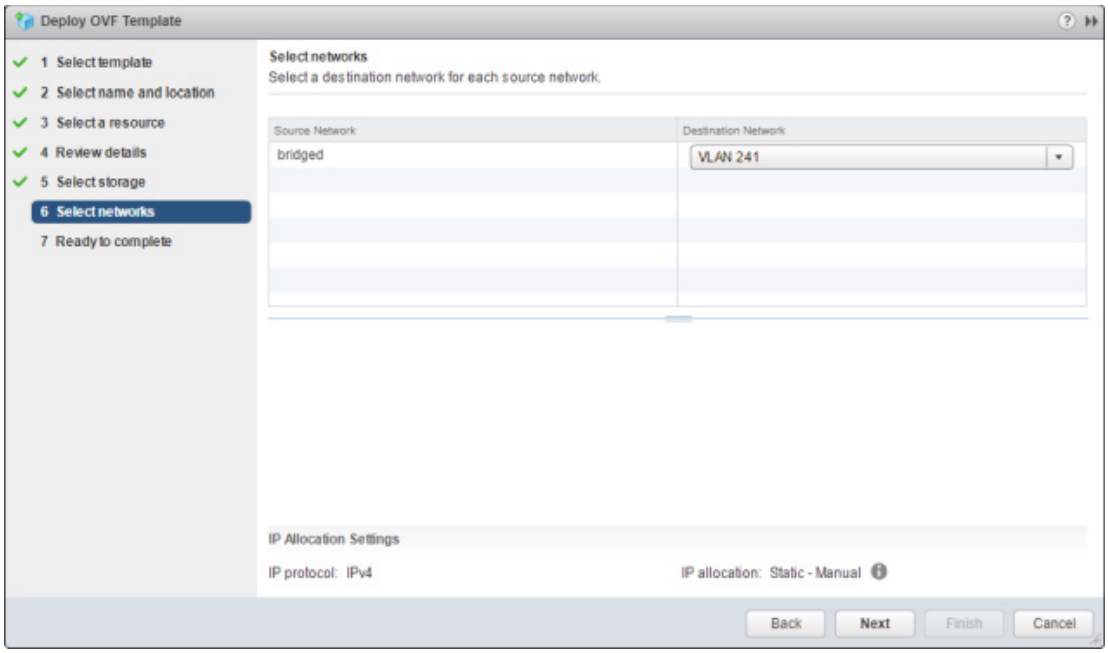
Once validation is complete, the Deploy OVF template dialog box refreshes.



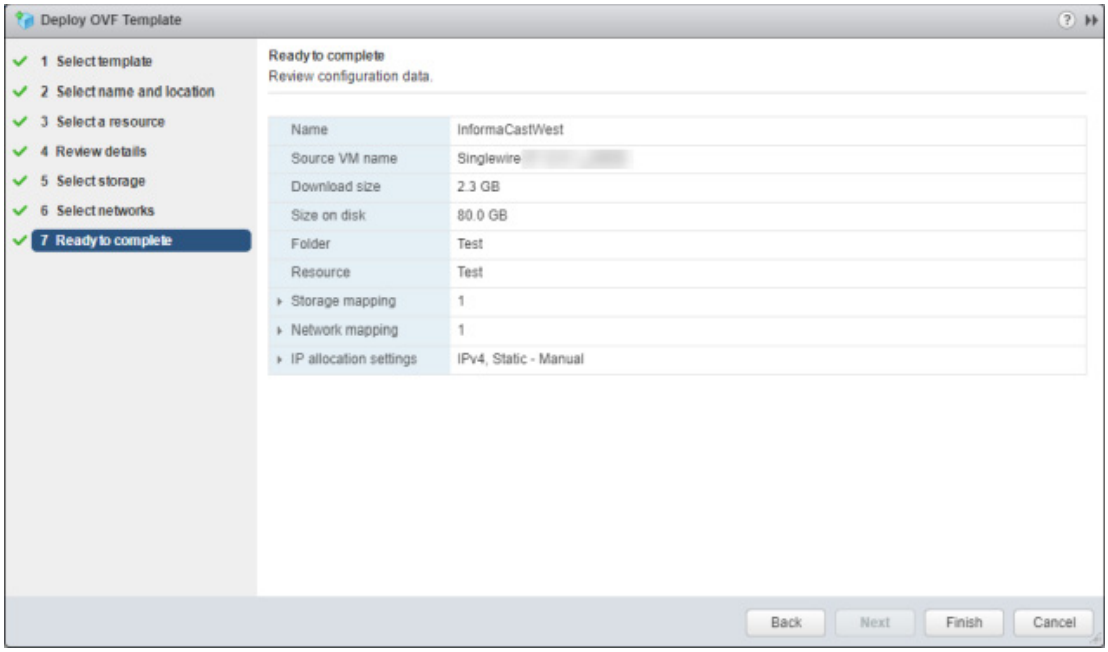
Step 11 Click the **Next** button. The Deploy OVF Template pop-up window refreshes.



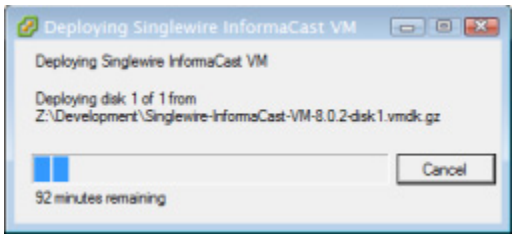
Step 12 Select a format and storage location for your deployed template and click the **Next** button. The Deploy OVF Template pop-up window refreshes.



Step 13 Select a destination network and click the **Next** button. The Deploy OVF Template pop-up window refreshes.

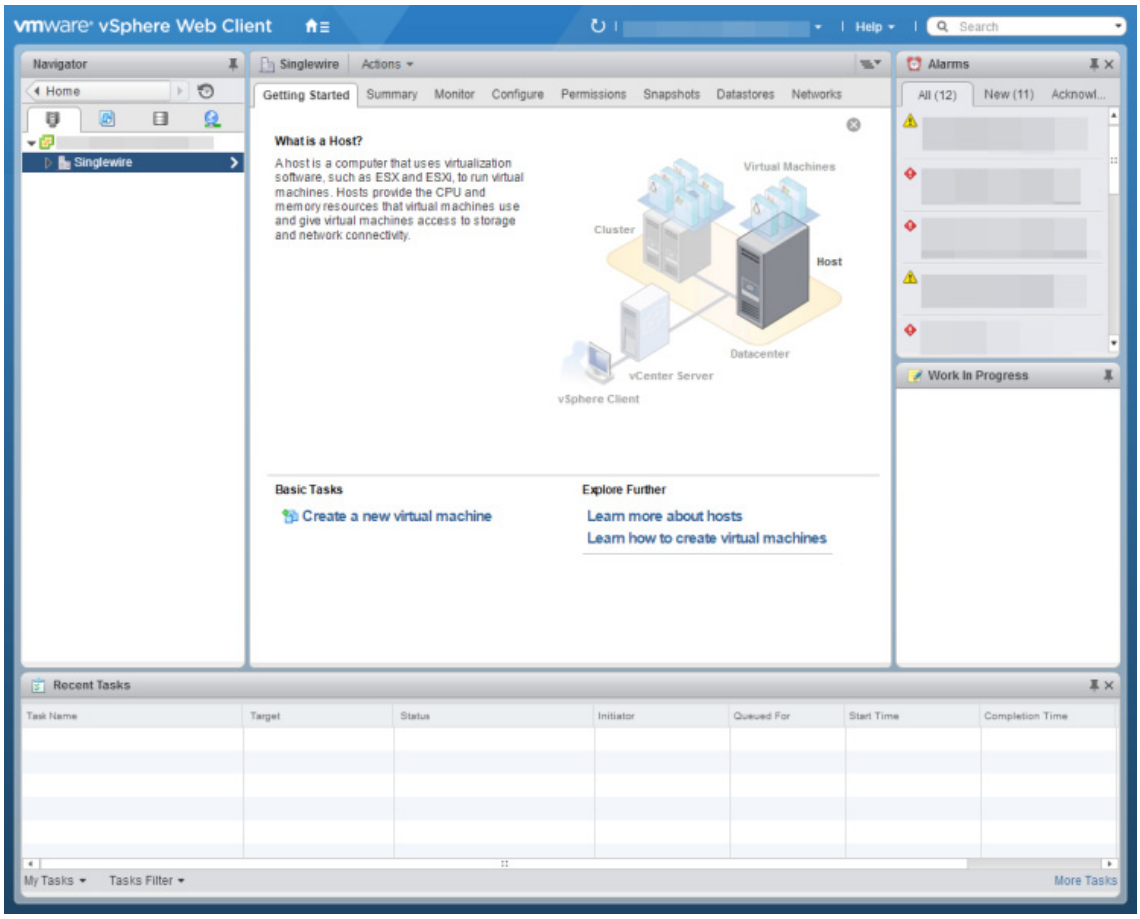


Step 14 Review your information and click the **Finish** button. InformaCast Virtual Appliance will begin importing.

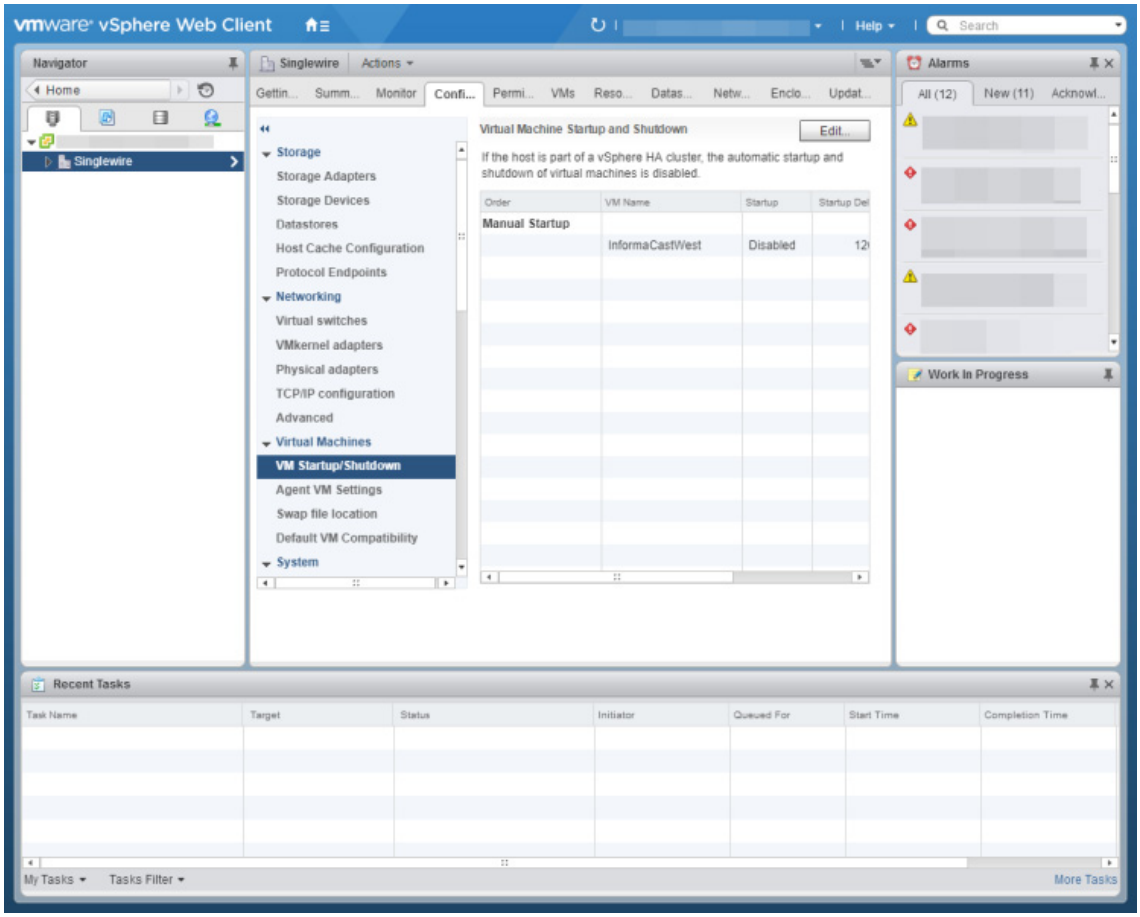


When it's finished, click the **Close** button.

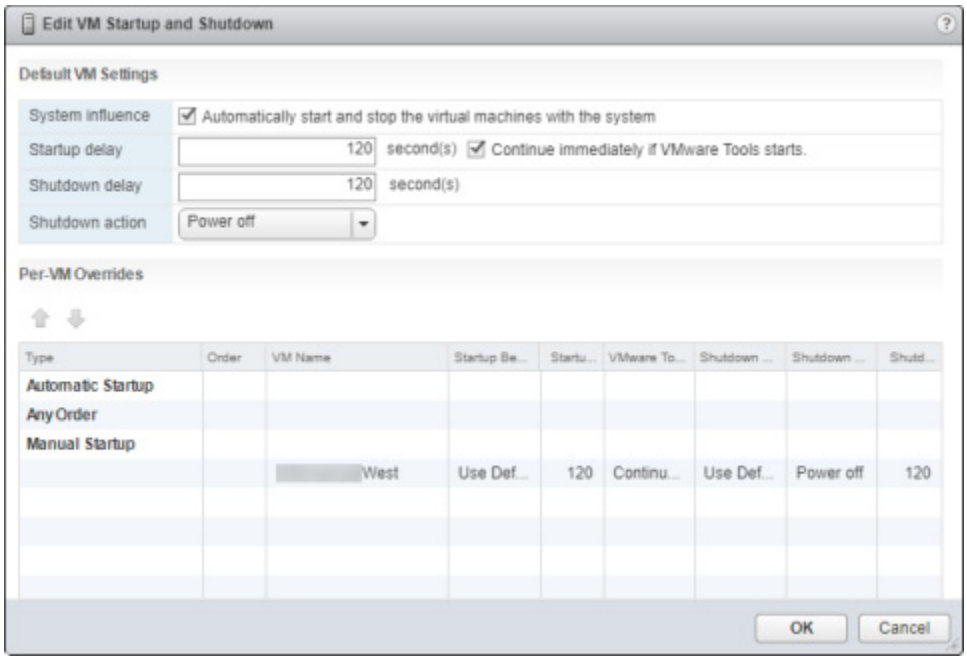
Step 15 Go back to your vSphere Web Client window and in the left pane, click the server hosting your InformaCast Virtual Appliance virtual machine. The vSphere Web Client window's right pane refreshes.



Step 16 Click the **Configure** tab. The vSphere Web Client window's right pane refreshes.



Step 17 Click the **VM Startup/Shutdown** link under **Virtual Machines**, then its **Edit** button. The Edit VM Startup and Shutdown pop-up window appears.

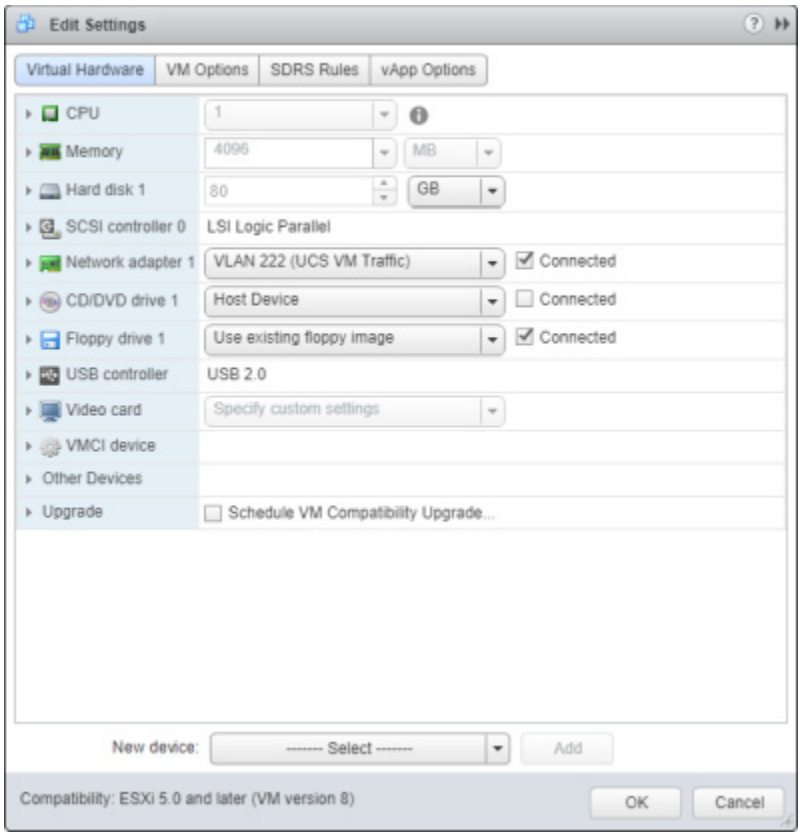


Step 18 Ensure the **Automatically start and stop the virtual machines with the system** checkbox is selected.

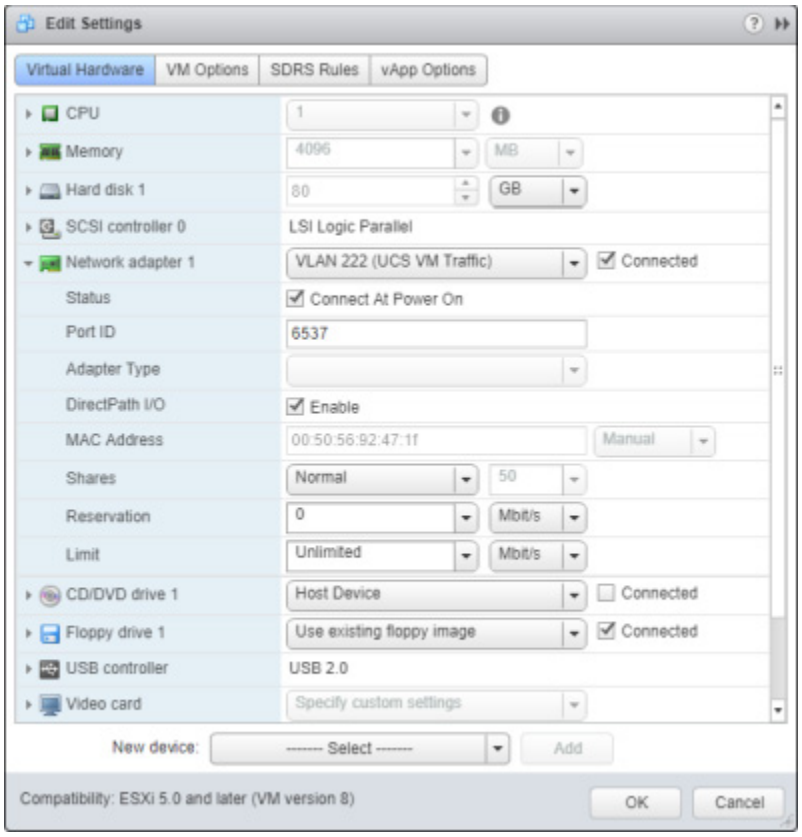
Step 19 Select your virtual machine in the table and click the **Up** arrow to move it from **Manual Startup** to **Automatic Startup**.

Step 20 Click the **OK** button in the Edit VM Startup and Shutdown pop-up window to save your changes. The InformaCast Virtual Appliance will now start and stop automatically with the server on which it's housed.

Step 21 Right click your virtual machine in the vSphere Web Client window's left pane and select **Edit Settings**. The Edit Settings pop-up window appears.



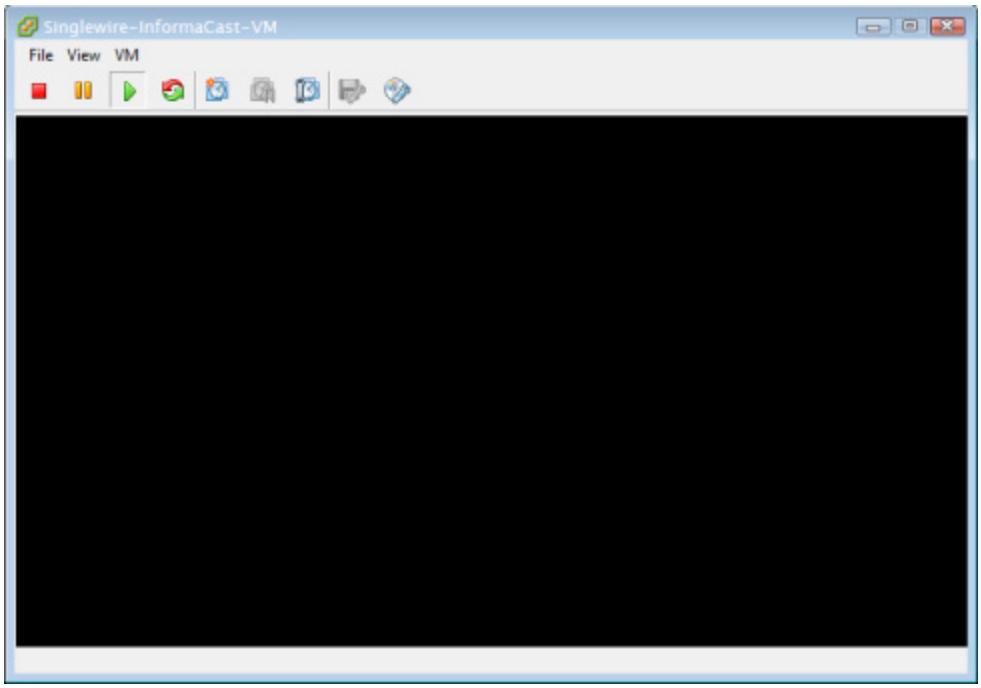
Step 22 Click the **Network adaptor 1** dropdown arrow on the **Virtual Hardware** tab. The Edit Settings pop-up window refreshes.



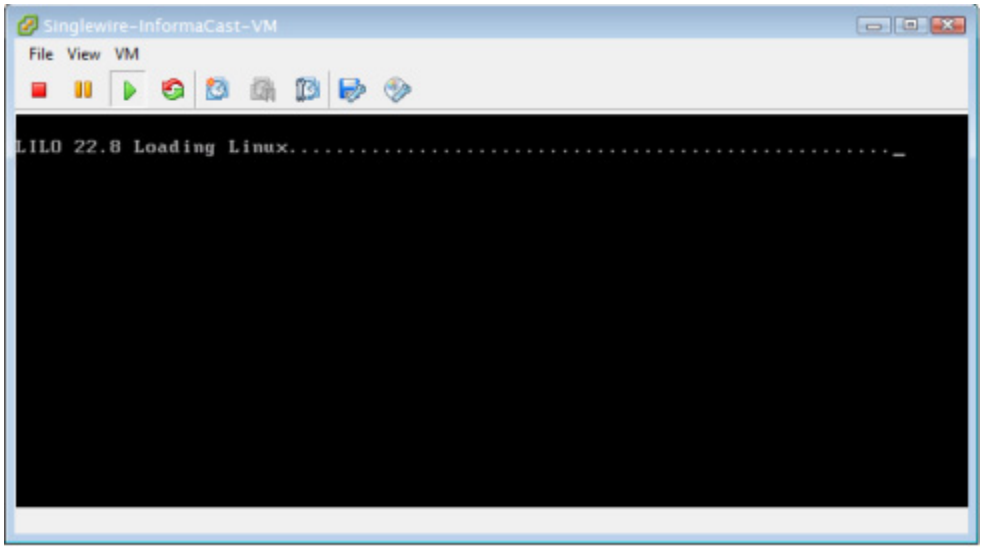
Step 23 Ensure the **Connect At Power On** checkbox is selected.

Step 24 Click the **OK** button in the Edit Settings pop-up window to save your changes.

Step 25 Go back to your vSphere Web Client window, right click your virtual machine in the left pane and select **Open Console**. The Singlewire InformaCast VM console window appears.

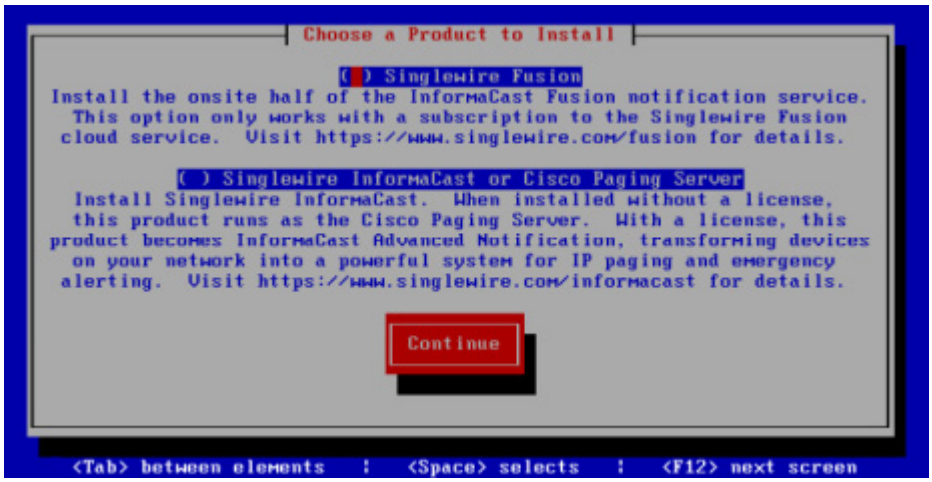


Step 26 Click the green arrow button to turn on the virtual machine. The Singlewire InformaCast VM console window begins booting the virtual machine.



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

When the InformaCast Virtual Appliance is done booting, you should see a request to select your product.

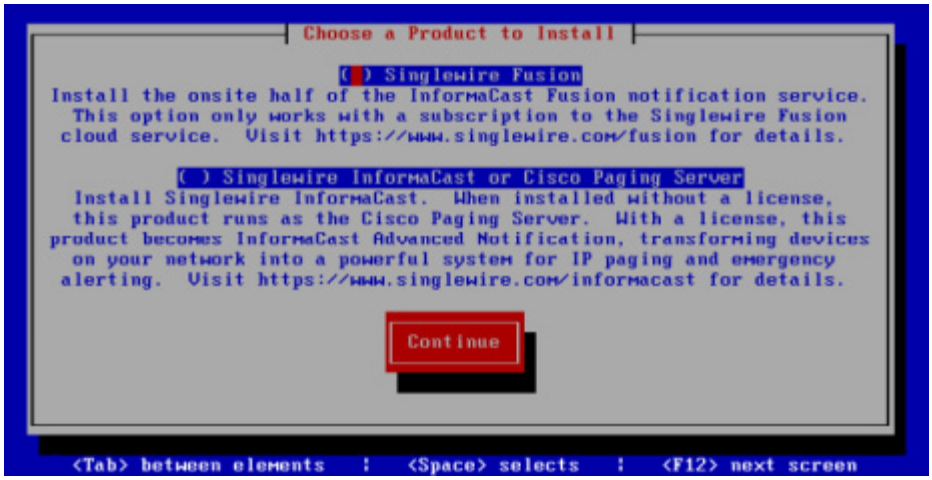


Step 27 Leave your Singlewire InformaCast VM console window open and continue with "Set the Initial Configuration."

Set the Initial Configuration

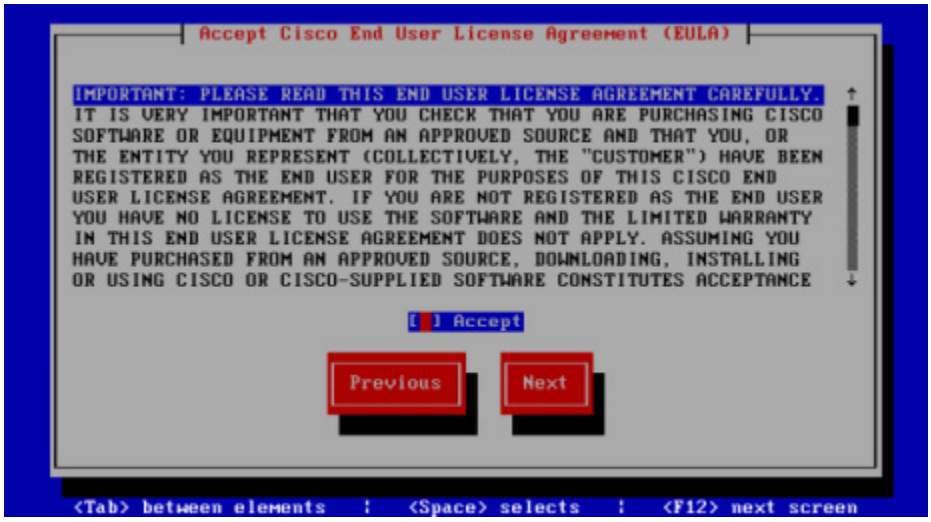
Once you have completed the steps in "Deploy InformaCast" on page 2-6, you will need to set InformaCast's initial network configuration.

Step 1 Return to your Singlewire InformaCast VM console window. You should see a request to select your product.



Step 2 Press the **Tab** key followed by the **Spacebar** to select **Cisco Paging Server**.

Step 3 Press the **Tab** key once to highlight the **Continue** button, then press the **Spacebar** to select it. You will be prompted to accept Cisco's End User License Agreement (EULA).

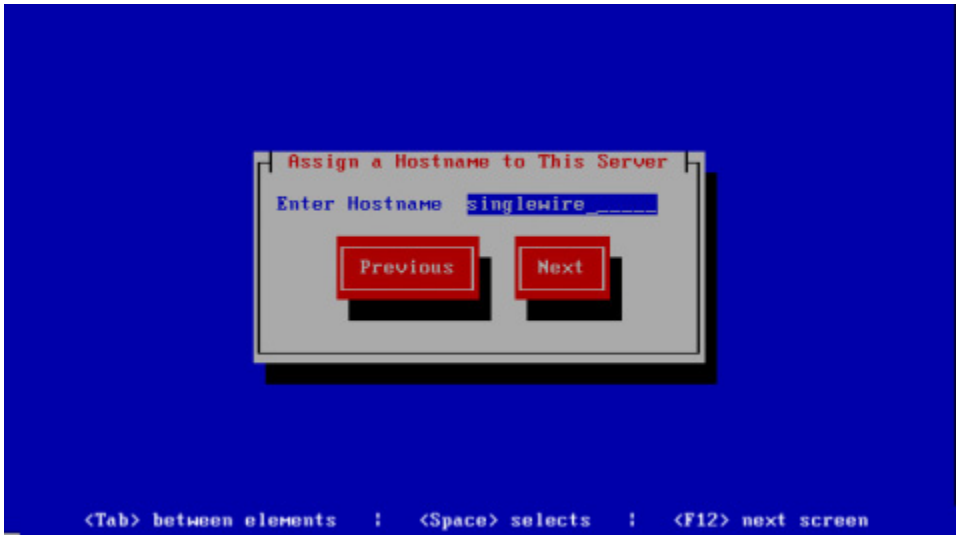


Step 4 Press the **Tab** key to highlight the **Accept** checkbox, then press the **Spacebar** to accept the EULA.

Step 5 Press the **Tab** key twice to highlight the **Next** button, then press the **Spacebar** to select it. You will be prompted to accept Singlewire's End User License Agreement.

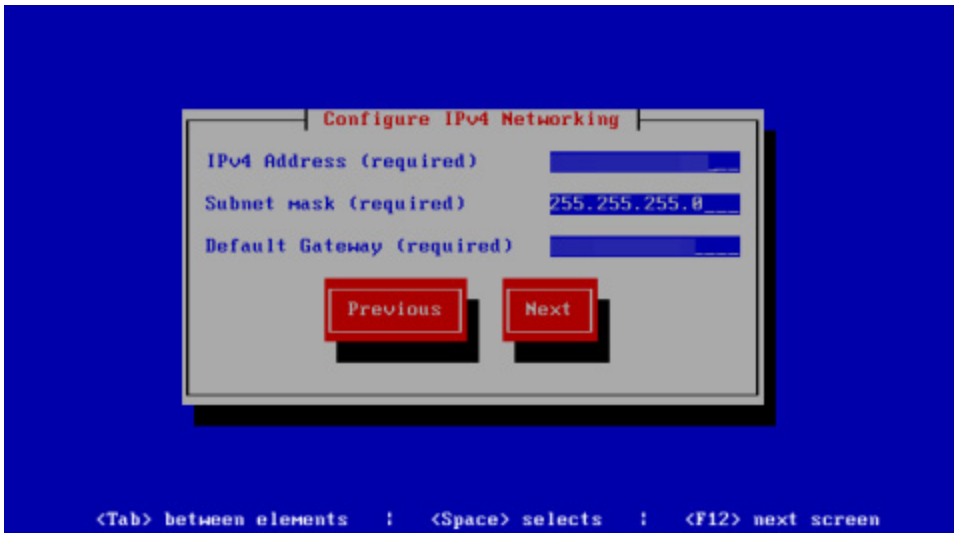
Step 6 Press the **Tab** key to highlight the **Accept** checkbox, then press the **Spacebar** to accept the EULA.

Step 7 Press the **Tab** key twice to highlight the **Next** button, then press the **Spacebar** to select it. You will be prompted to assign a hostname to your server.



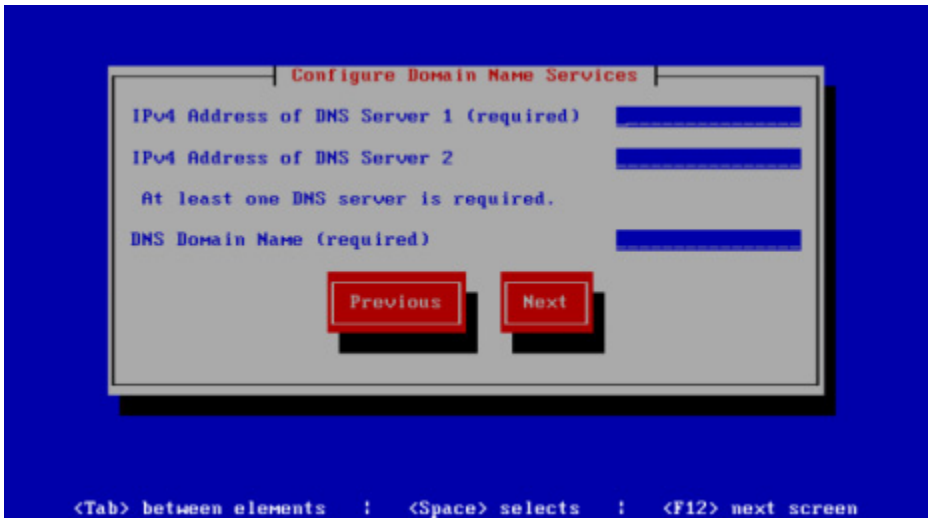
Step 8 Enter a hostname for your InformaCast Virtual Appliance in the **Enter Hostname** field, e.g. InformaCastWest. This hostname will appear in Webmin's user interface.

Step 9 Press the **Tab** key to highlight the **Next** button, then the **Spacebar** to select it. The InformaCast Virtual Appliance then attempts to use DHCP to find suitable IP addresses on your network. The Singlewire InformaCast VM console window refreshes.

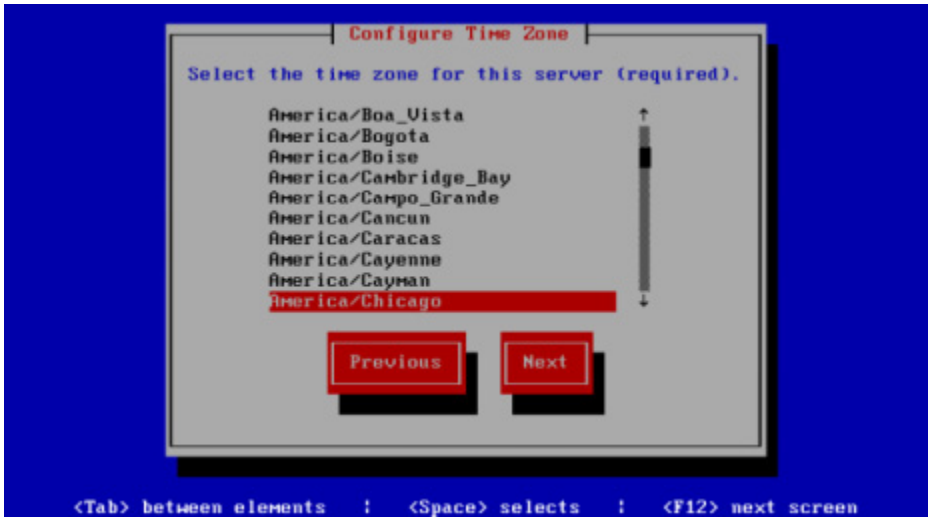


Step 10 Accept these IP addresses or provide valid ones of your own in the **IPv4 Address**, **Subnet Mask**, and **Default Gateway** fields.

Step 11 Press the **Tab** key to highlight the **Next** button, then the **Spacebar** to select it. The Singlewire InformaCast VM console window refreshes.

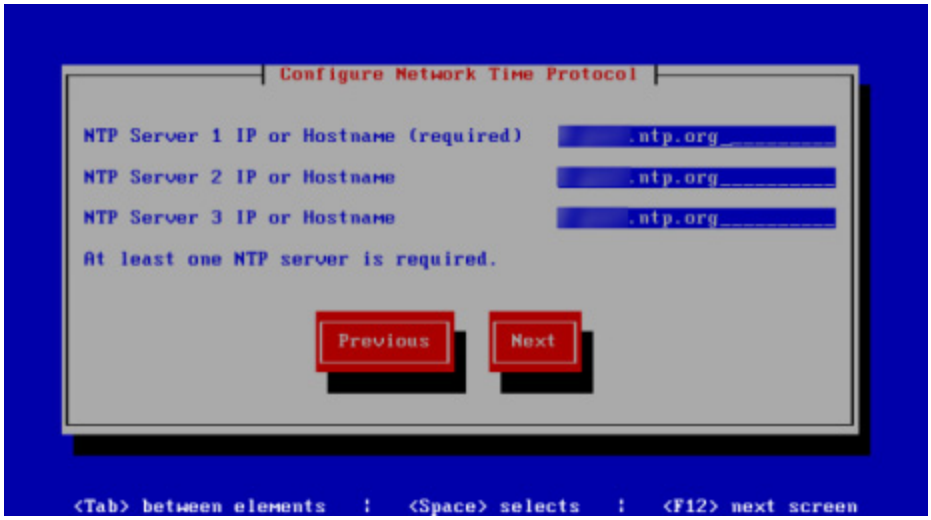


Step 12 Enter at least one DNS server IP address in the field provided or accept the one provided to you and enter a DNS domain name. Press the **Tab** key to highlight the **Next** button, then the **Spacebar** to select it. The Singlewire InformaCast VM console window refreshes.



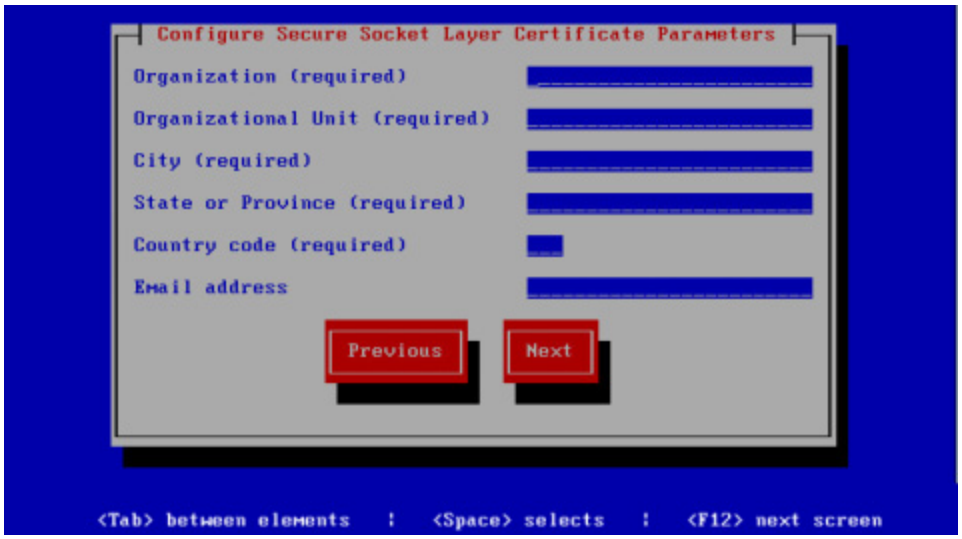
Step 13 Use the arrow keys to select a time zone for your InformaCast Virtual Appliance server.

Step 14 Press the **Tab** key to highlight the **Next** button, then the **Spacebar** to select it. The InformaCast Virtual Appliance then attempts to find an NTP server on your network. The Singlewire InformaCast VM console window refreshes.



Step 15 Accept the suggested NTP server IP address or provide a valid one of your own in the **NTP Server 1 IP or Hostname** field.

Step 16 Press the **Tab** key to highlight the **Next** button, then the **Spacebar** to select it. The Singlewire InformaCast VM console window refreshes.



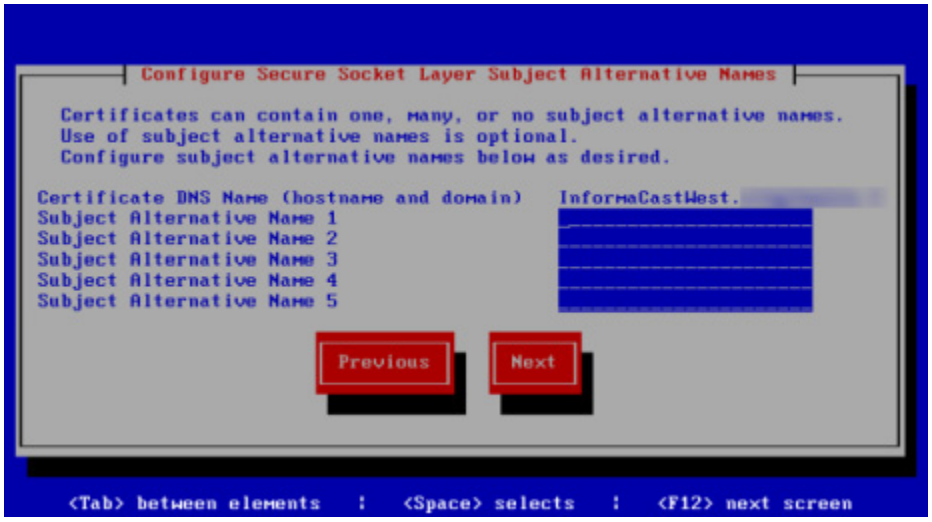
Step 17 Enter the information necessary for a signed certificate (while the information is required, signing the certificate is not). A signed certificate, which can protect against Man-in-the-Middle (MITM) attacks, is an electronic document that proves ownership of a public key; it includes information about the key, its owner's identity, and the digital signature of a certificate authority (CA).

You must enter the information dictated by your certificate authority in its required form:

- Your organization's name, e.g. Acme Company

- Your organizational unit, e.g. Security
- Your city, e.g. Madison
- Your state or province, e.g. WI
- The alphabetic abbreviation for your country, e.g. US for United States
- An email address (optional)

Step 18 Press the **Tab** key to highlight the **Next** button, then the **Spacebar** to select it. The Singlewire InformaCast VM console window refreshes.



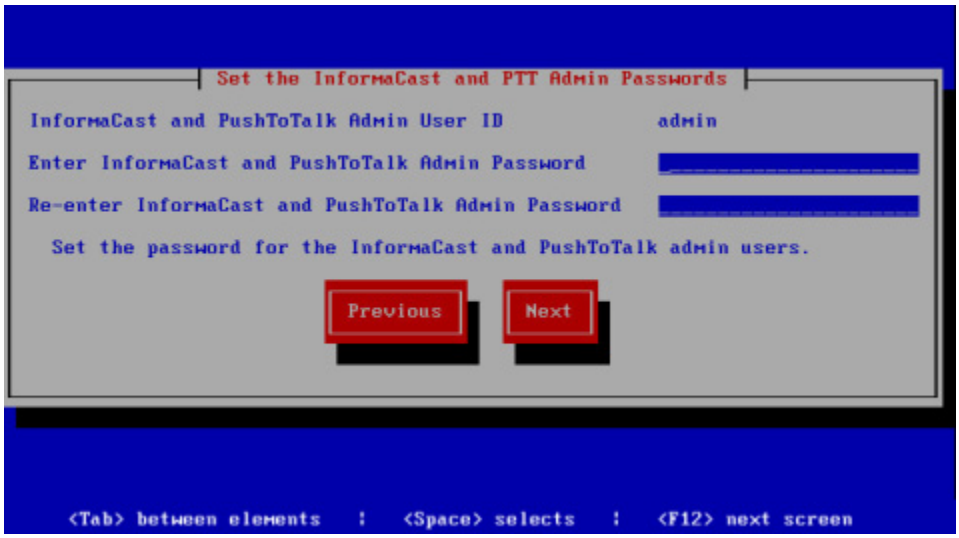
Step 19 Accept the common name of your server, which should be a combination of your hostname and your DNS domain name, or provide one of your own in the **Certificate DNS Name (hostname and domain)** field, then continue entering information for your signed certificate by entering any Subject Alternative Names (SANs) in the fields provided. 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.

Step 20 Press the **Tab** key to highlight the **Next** button, then the **Spacebar** to select it. The Singlewire InformaCast VM console window refreshes.

Step 21 Enter a password in the **Enter OS Admin Password** field, press the **Tab** key, and enter the password again in the **Re-enter OS Admin Password** field. Your OS credentials are used to enter Webmin and Control Center and when using SSH to access the InformaCast Virtual Appliance.

Note Your password must be at least six characters in length, and contain at least one lowercase letter, one number, and one of the following characters: !\"#$%"() *+,-./ :;<=>?@[]^_`. Also, when setting your password, you cannot use "changeMe."

Step 22 Press the **Tab** key to highlight the **Next** button, then the **Spacebar** to select it. The Singlewire InformaCast VM console window refreshes.



Step 23 Enter a password in the **Enter InformaCast and PTT 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 Your password must be at least six characters in length, and contain at least one lowercase letter, one number, and one of the following characters: !\"#$%"() *+,-./ :;<=>?@[\\]^_`. Also, when setting your password, you cannot use "changeMe."

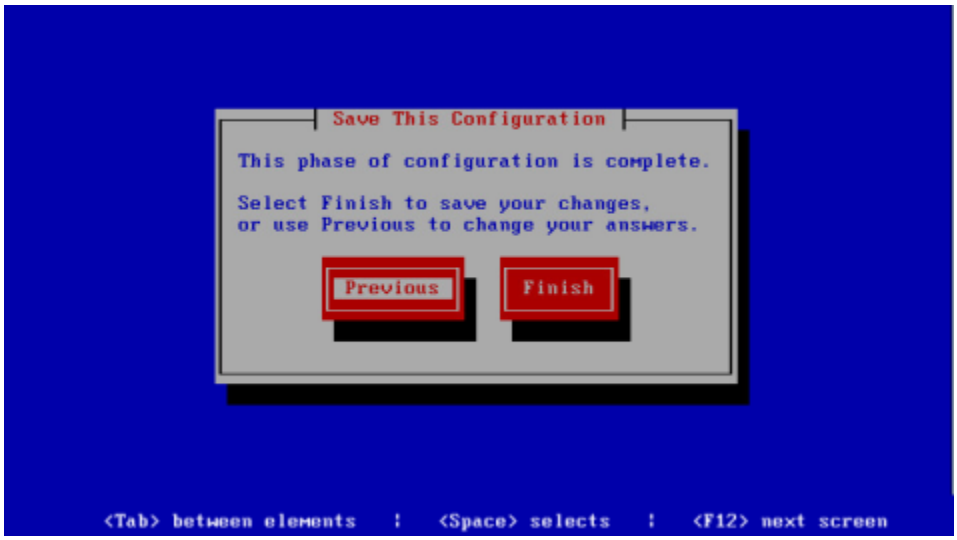
Note PushToTalk is only available to Advanced InformaCast users.

Step 24 Press the **Tab** key to highlight the **Next** button, then the **Spacebar** to select it. The Singlewire InformaCast VM console window refreshes.

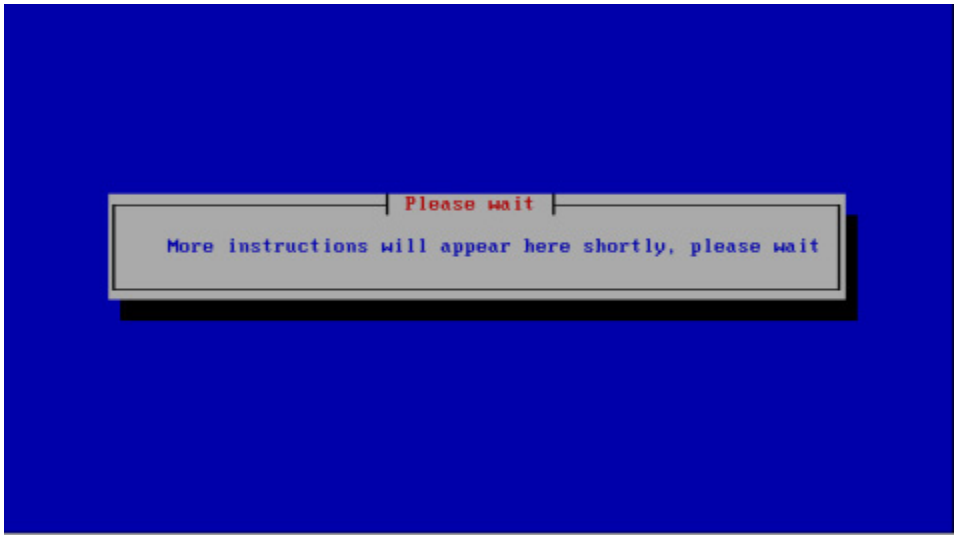
Step 25 Enter a security passphrase in the **Enter Security Passphrase** and **Re-enter Security Passphrase** fields. This passphrase is used to secure your backups of the InformaCast Virtual Appliance. You must remember this passphrase. Singlewire Support personnel cannot recover it for you if it's lost.

Note Your passphrase must follow the same character requirements as your OS admin password.

Step 26 Press the **Tab** key to highlight the **Next** button, then the **Spacebar** to select it. The Singlewire InformaCast VM console window refreshes.

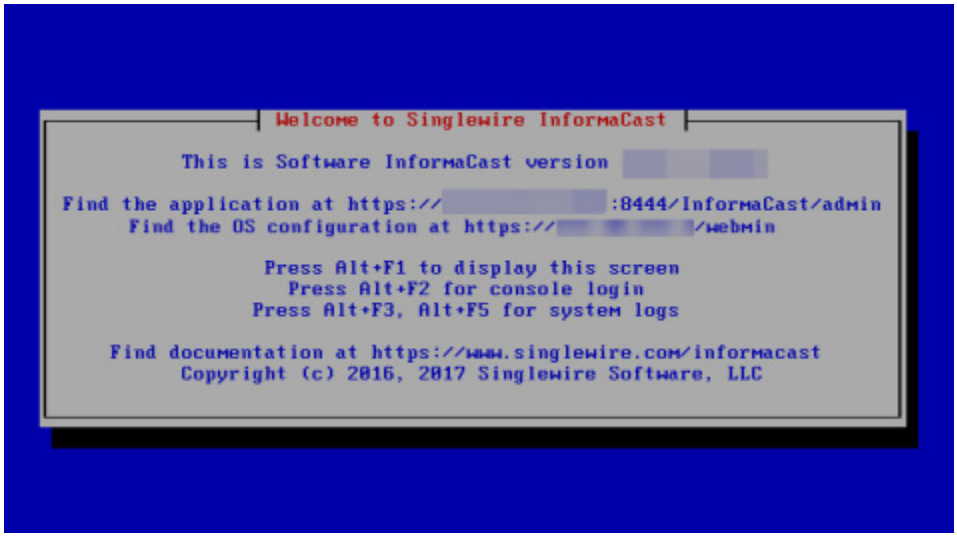


Step 27 Press the **Tab** key to highlight the **Finish** button, then the **Spacebar** to select it. The Singlewire InformaCast VM console window refreshes.



Note There may be a short wait while your changes are written to disk.

Once your changes have been saved, the Singlewire InformaCast VM console window refreshes.



Step 28 Make a note of the displayed IP address. This is the IP address of the InformaCast Virtual Appliance's landing page, which you will use to access the InformaCast Virtual Appliance, Control Center, and Webmin web user interfaces.

Step 29 Close your open console window.

Log into InformaCast Virtual Appliance's Interfaces

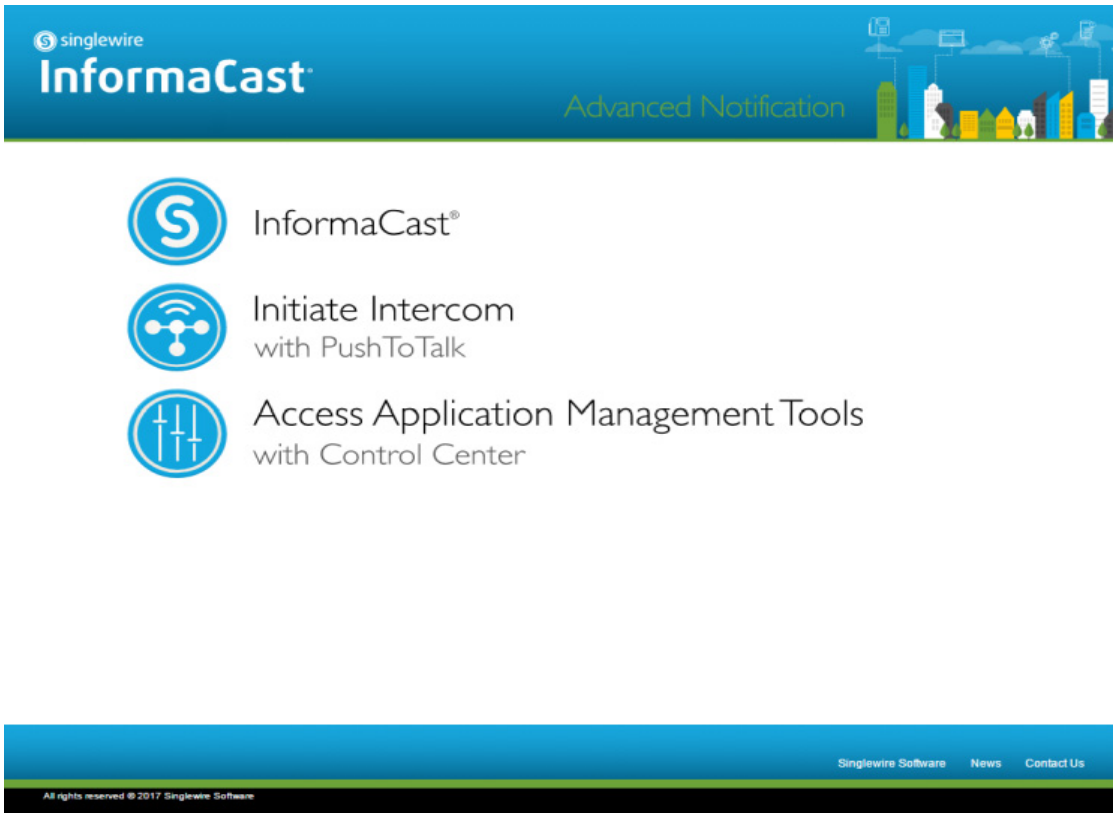
When using InformaCast Virtual Appliance, you will access it and log into its different interfaces: InformaCast, PushToTalk, the Control Center, Webmin, and the command-line interface. All of these interfaces, with the exception of the command-line interface, are accessible through the Singlewire landing 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 "Deploy InformaCast" on page 2-6, the InformaCast Virtual Appliance should be running and you can access the Singlewire landing 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 10 on page 2-22), and press the **Enter** key. The Singlewire landing page appears.



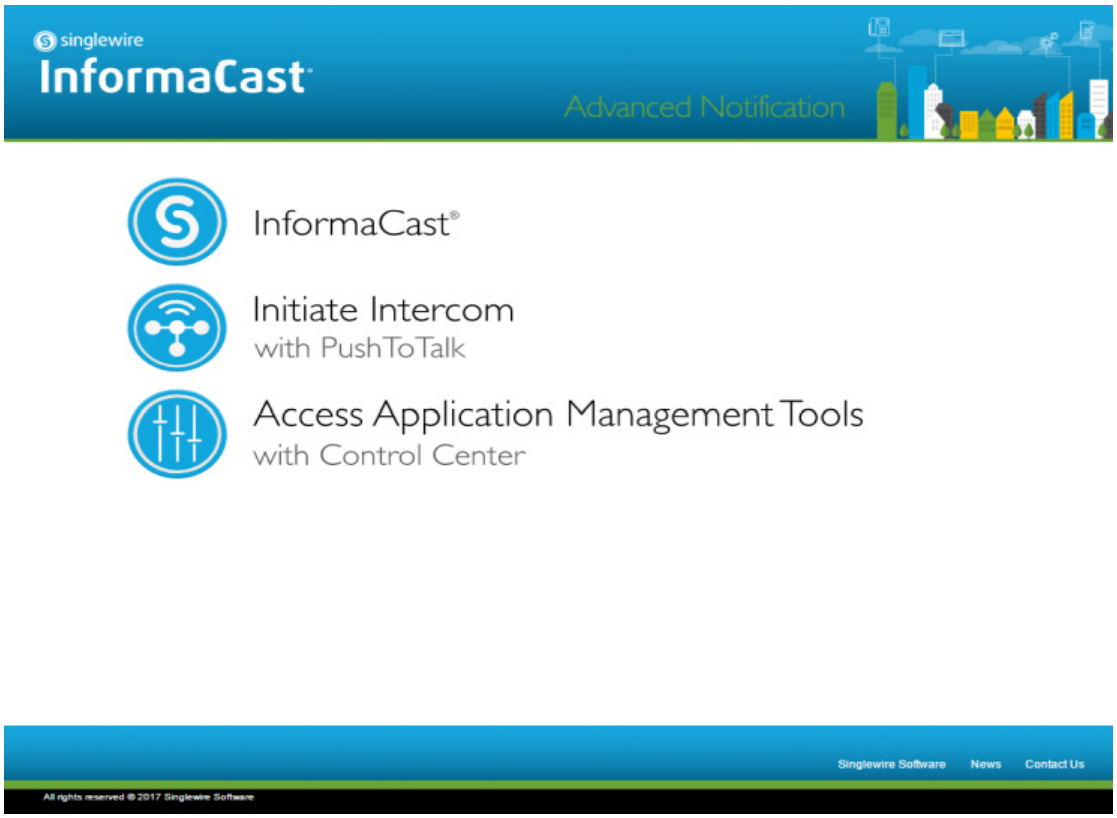
The Singlewire landing page allows you to easily access all of your Virtual Appliance user interfaces along with application- and system-level management tools. You may find it helpful to both keep this tab/window open during the time that you're working with the Virtual Appliance and bookmark it for 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 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 9-39).

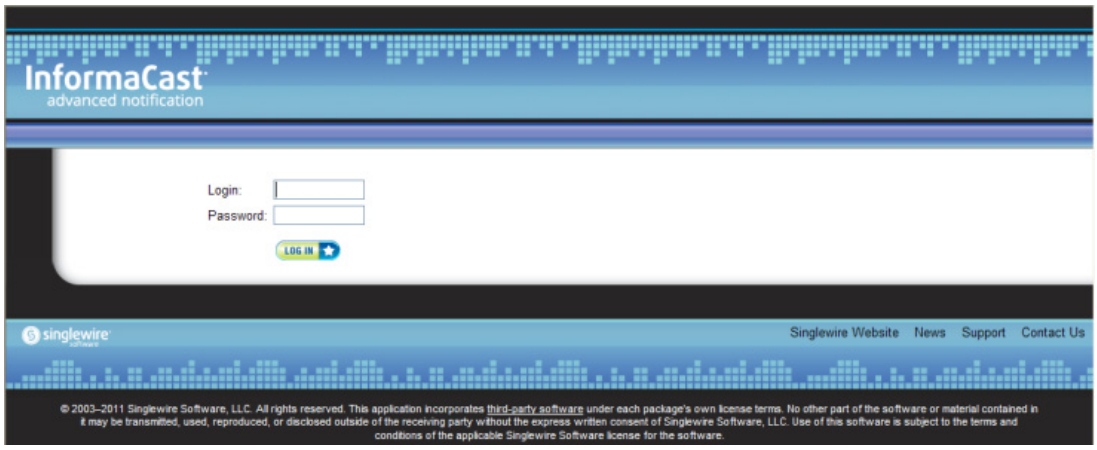
Log into InformaCast

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 landing page appears.

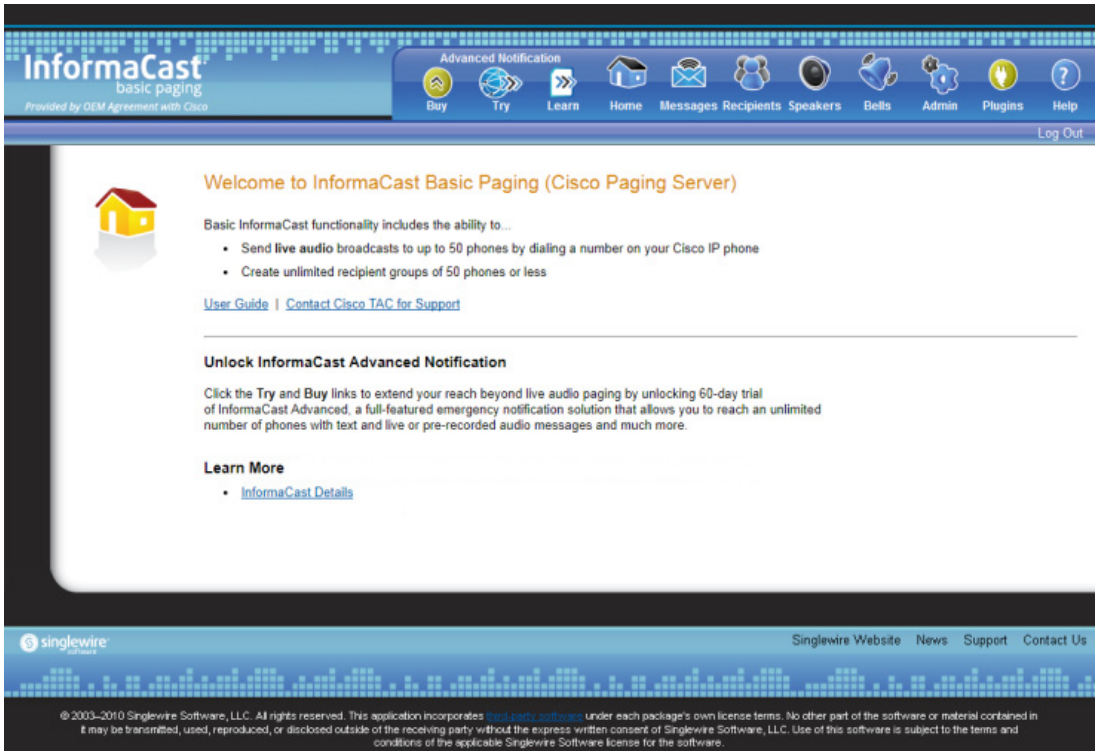


Step 2 Click the **InformaCast** link. A separate tab/window opens to InformaCast's Login page.



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

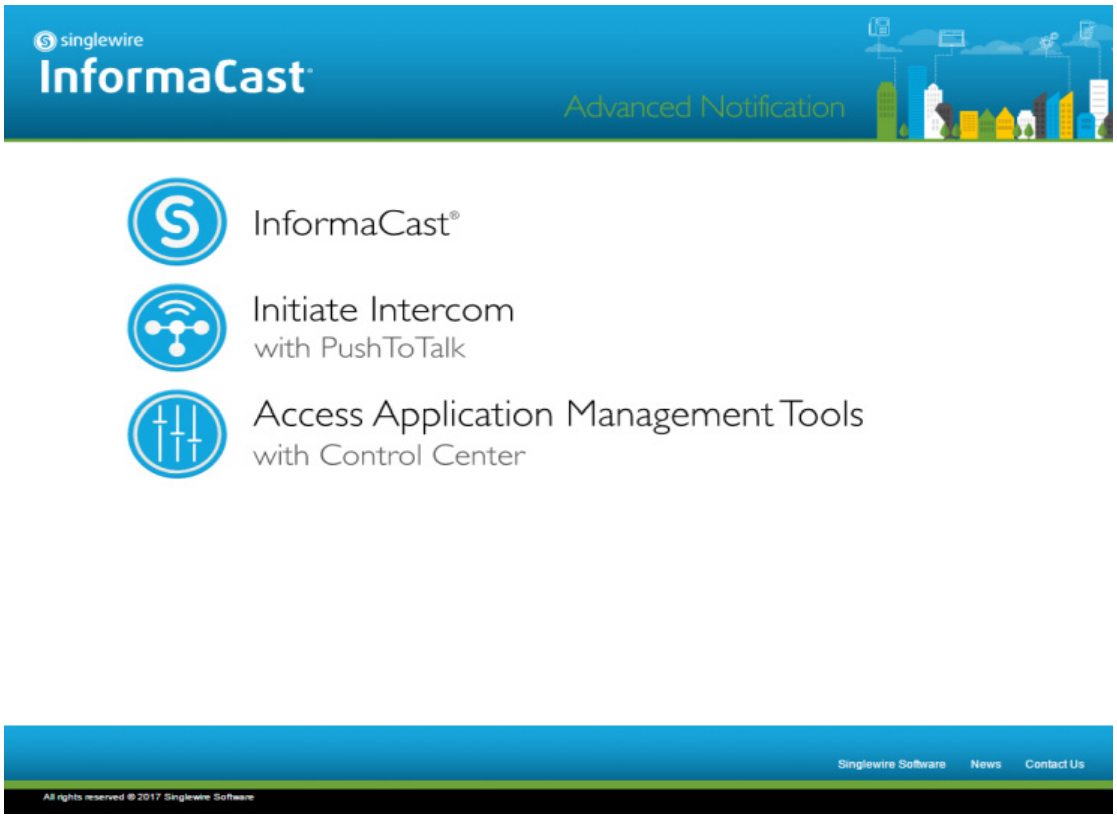
PushToTalk is designed to facilitate easy and immediate communication between multiple parties or on a one-to-one basis through talk/listen or intercom functionality. From the **Services** button on any designated phone or the side button of the 7921G wireless IP phone, you can pick from a list of phone 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.

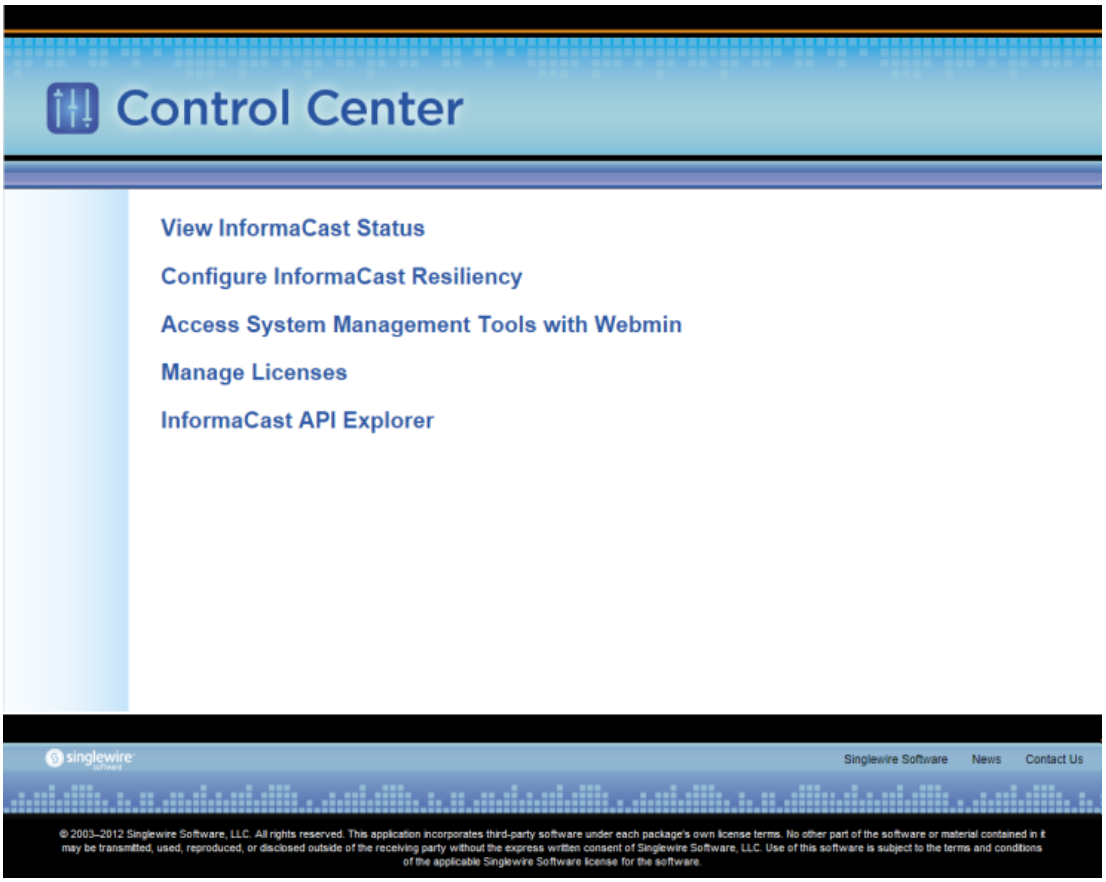
Log into the Control Center

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 landing 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.

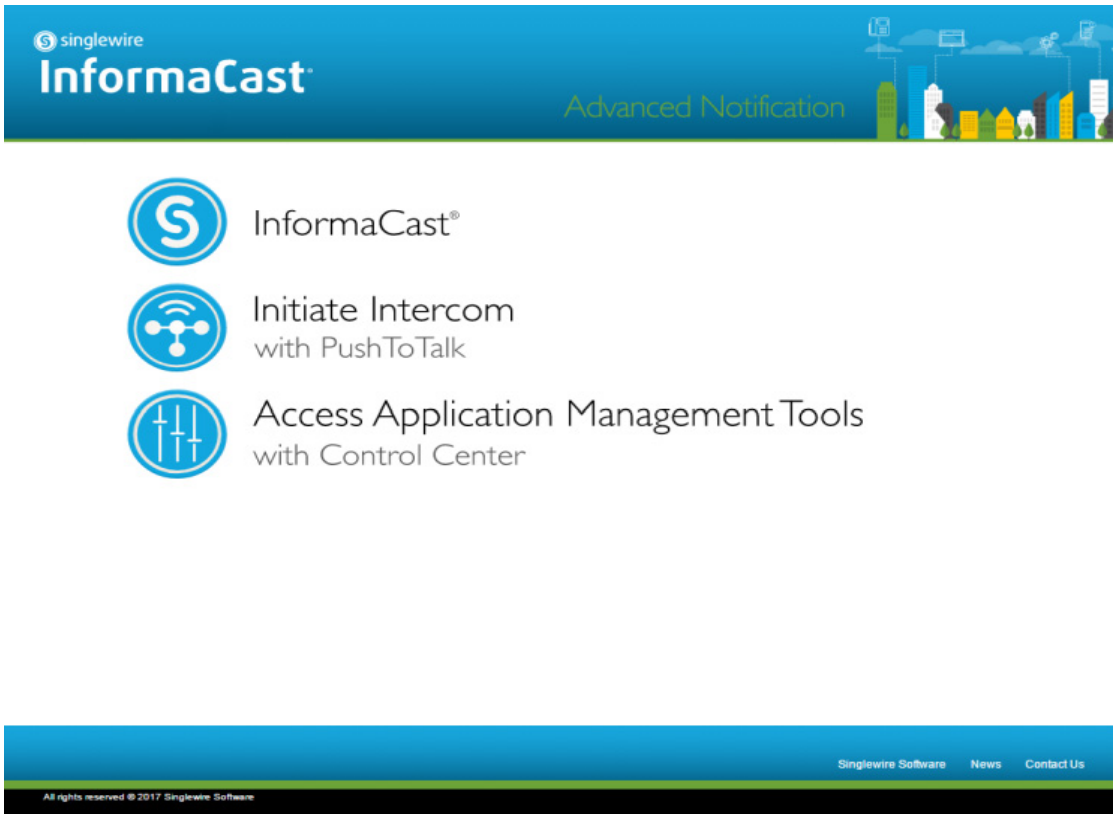
Note The **Configure InformaCast Resiliency** link is dependent upon your license containing resiliency functionality: if your license doesn't include resiliency, you won't see the link.

From the Control Center menu page, you can access Singlewire's accessory tools.

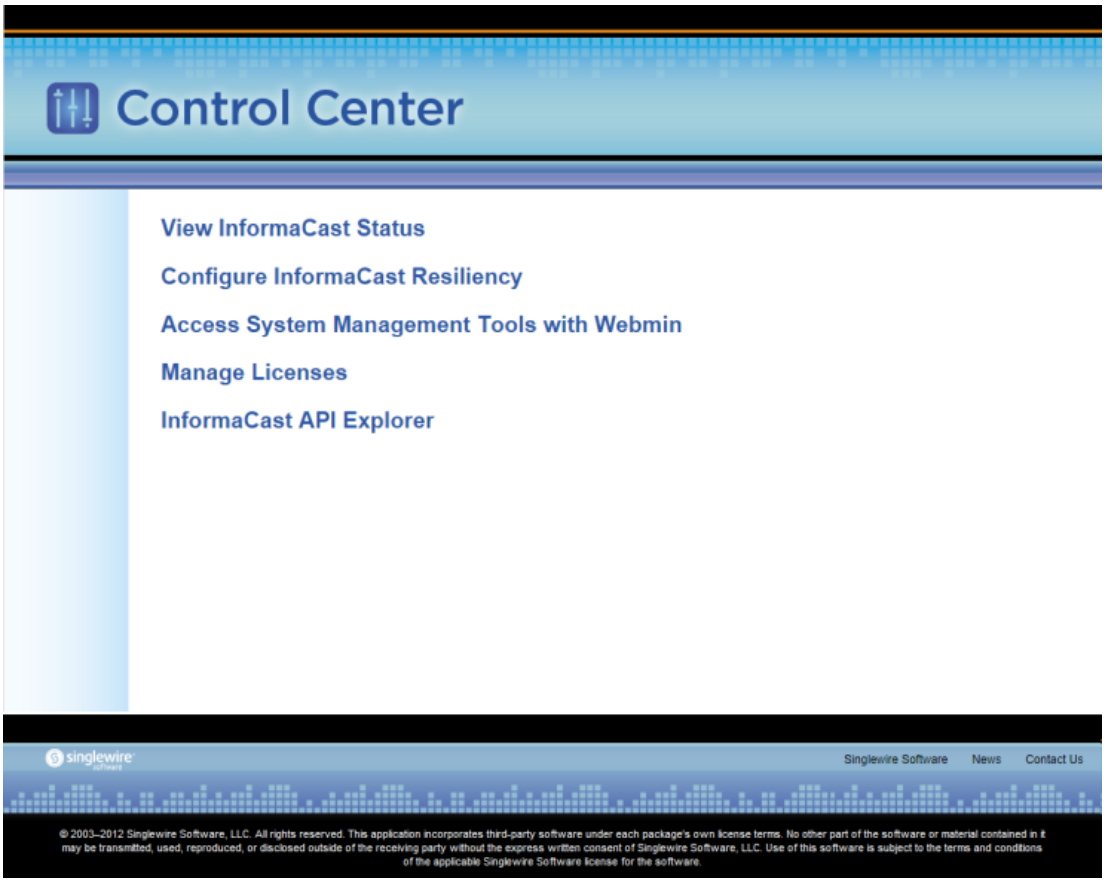
Log into Webmin

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.

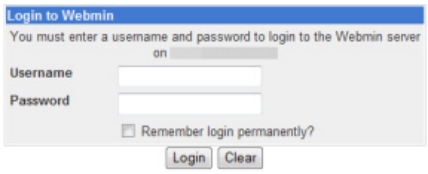
Step 1 Open a web browser, enter the IP address of the InformaCast Virtual Appliance, and press the **Enter** key. The Singlewire landing page appears.



Step 2 Click the **Access Application Management Tools with Control Center** link. A separate tab/window opens to the Control Center menu page.

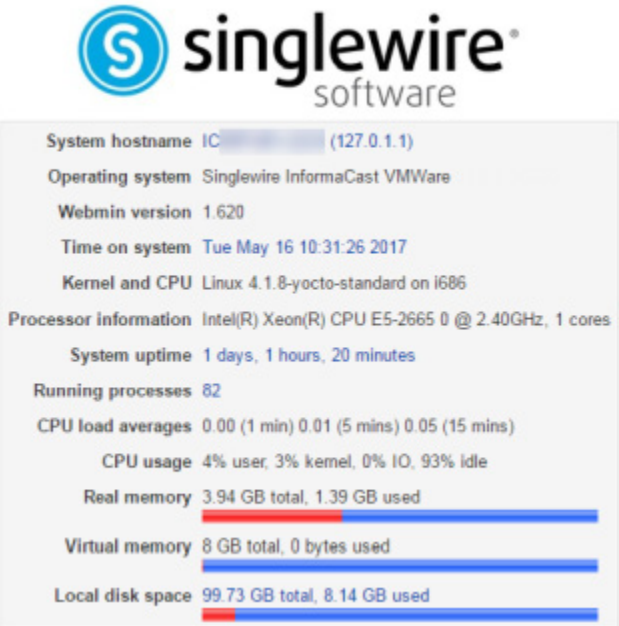


Step 3 Click the **Access System Management Tools with Webmin** link. A separate tab/window opens to the Login to Webmin page.



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

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



The Webmin homepage displays versioning information and statistics about the Virtual Appliance.

From the Webmin homepage, you can install a new software package (see "Upgrade InformaCast Pre-12.0.1" on page 9-77), 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 9-1 for more information).

Log into the Command-line Interface

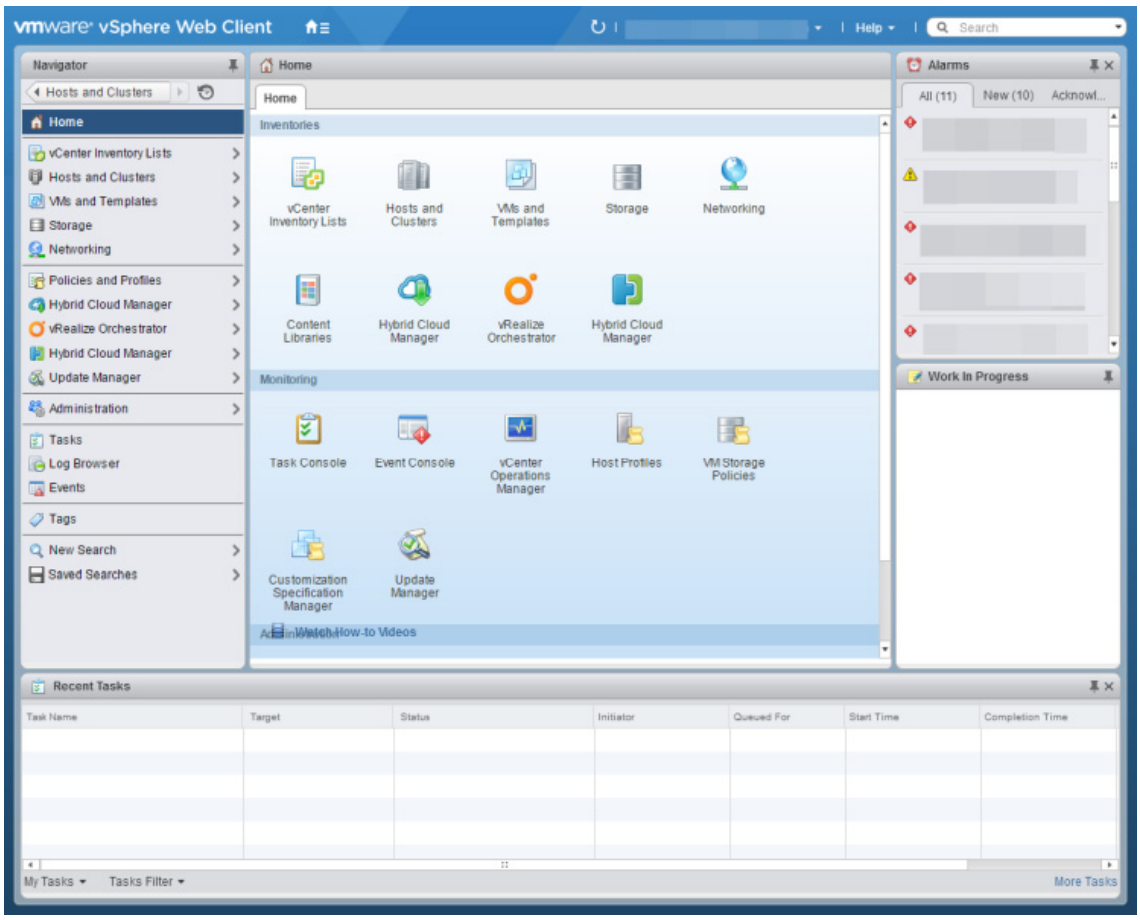
The command-line interface (CLI) is a text-based interface used for support issues and some configuration procedures (e.g. those that require manual editing of files or the running of scripts). It also allows you to perform various administrative functions such as changing the Virtual Appliance's password, restarting the server, assigning a static IP address, and collecting/viewing logs, among others. The command line interface uses the bash command line shell, and can be accessed via a virtual machine console window, such as vSphere, or over the network through the use of an SSH (Secure Shell) client like PuTTY.

Note Pictures illustrating the command-line interface will usually depict accessing a Virtual Appliance through an SSH client rather than a virtual machine console window; however, the commands are the same.

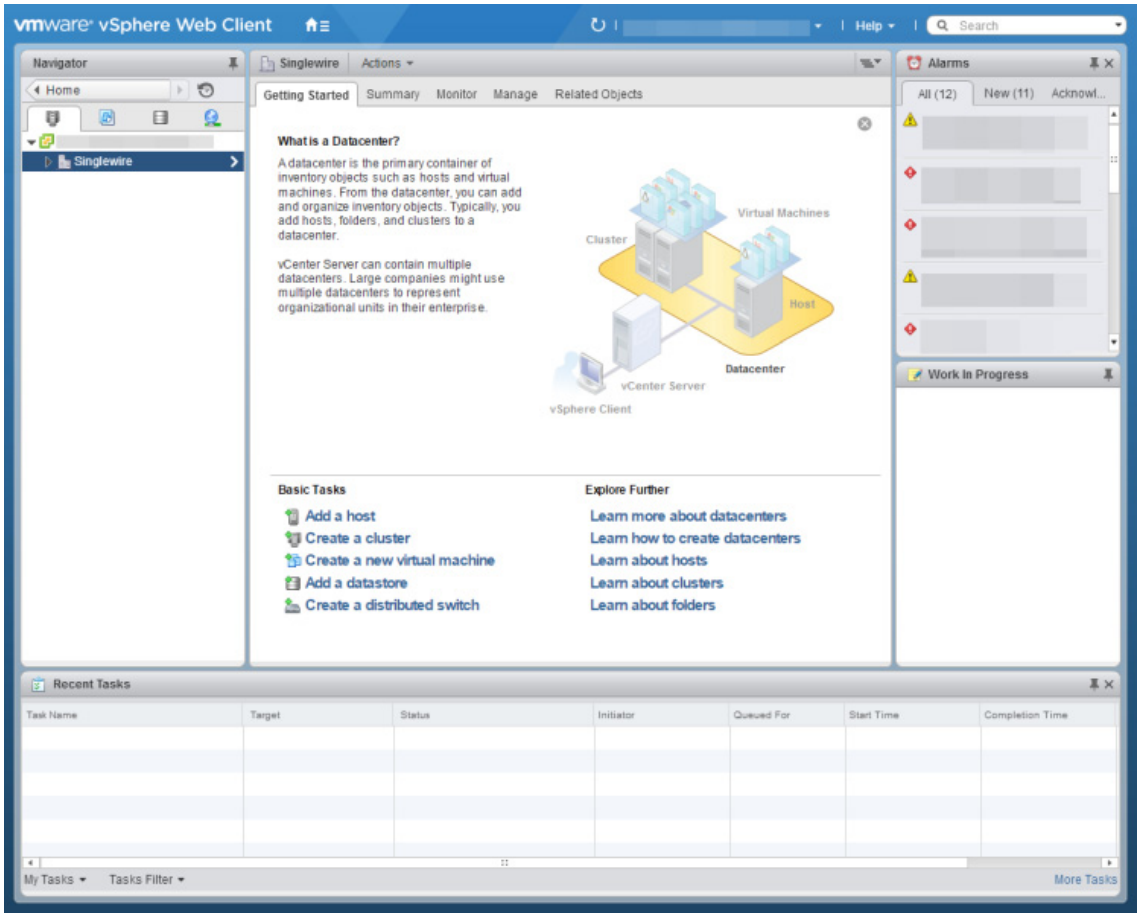
Use a Virtual Machine Console Window

Singlewire supports the Virtual Appliance on the VMware ESXi platform, which is managed through the vSphere web client.

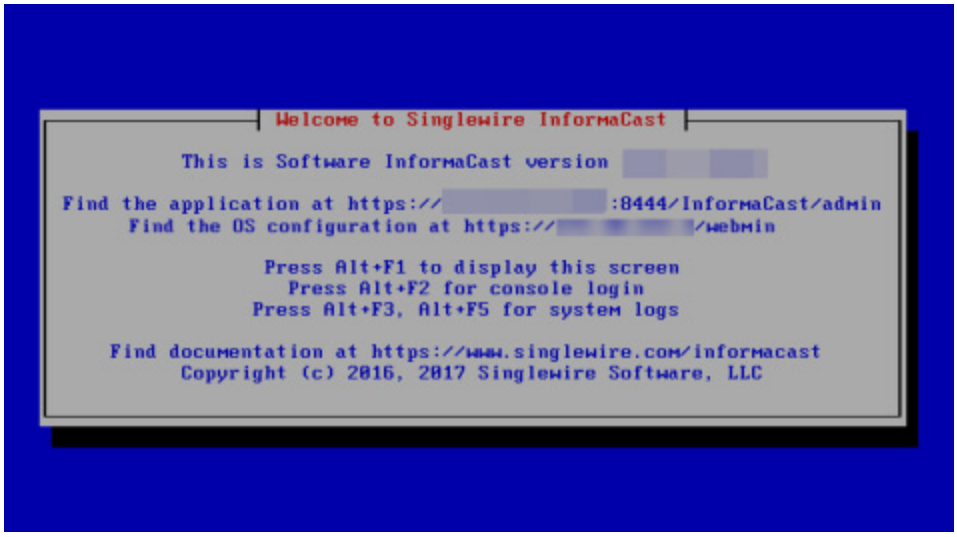
Step 1 Open a web browser and log into your vSphere web client. The vSphere Web Client page appears.



Step 2 Click the **Hosts and Clusters** icon. The vSphere Web Client page refreshes.

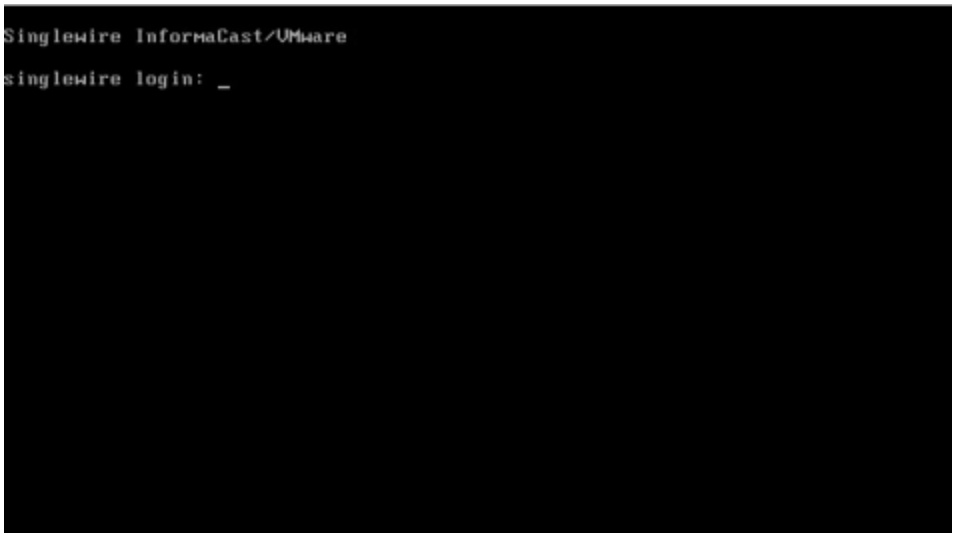


Step 3 Right click your Virtual Appliance in the left pane and select **Open Console**. A console window to your Virtual Appliance appears.



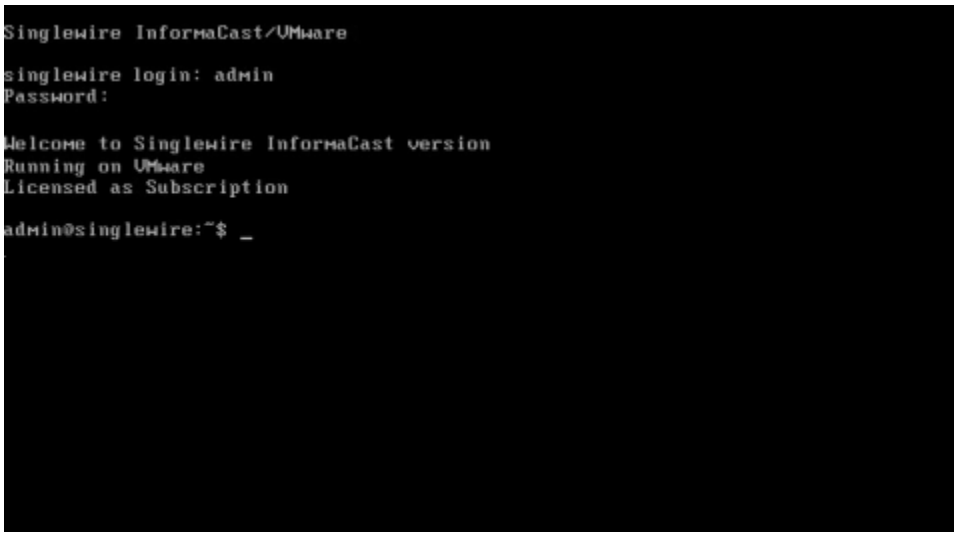
Upon opening a console, the Virtual Appliance's Status screen appears, which displays version information and interface and documentation links.

Step 4 Press the **Alt** + **F2** keys to switch to the console screen where you can enter commands.



Step 5 Enter **admin** at the prompt and press the **Enter** key.

Step 6 Enter your OS password at the prompt and press the **Enter** key. The console window refreshes, showing you that you're logged in.

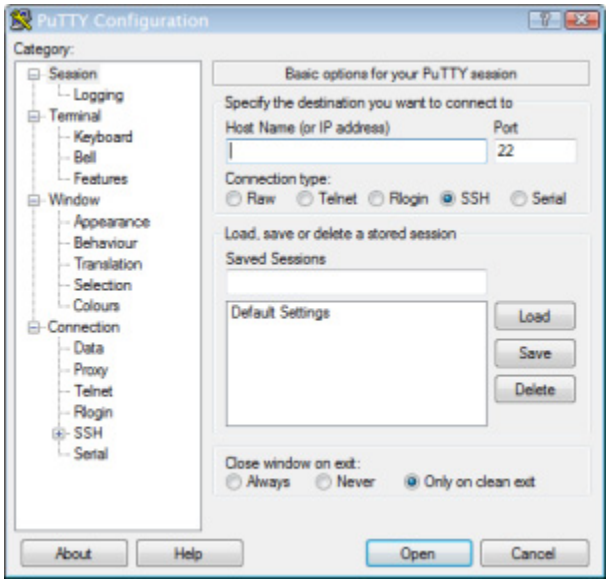


Tip Press the **Alt** + **F3** or **Alt** + **F5** keys to see the logs available through the Status screen.

Use an SSH Client

Singlewire recommends PuTTY for an SSH client, and it's available through a free download.

Step 1 Open PuTTY. The PuTTY Configuration window appears.



Step 2 Enter your Virtual Appliance's IP address in the **Host Name (or IP address)** field.

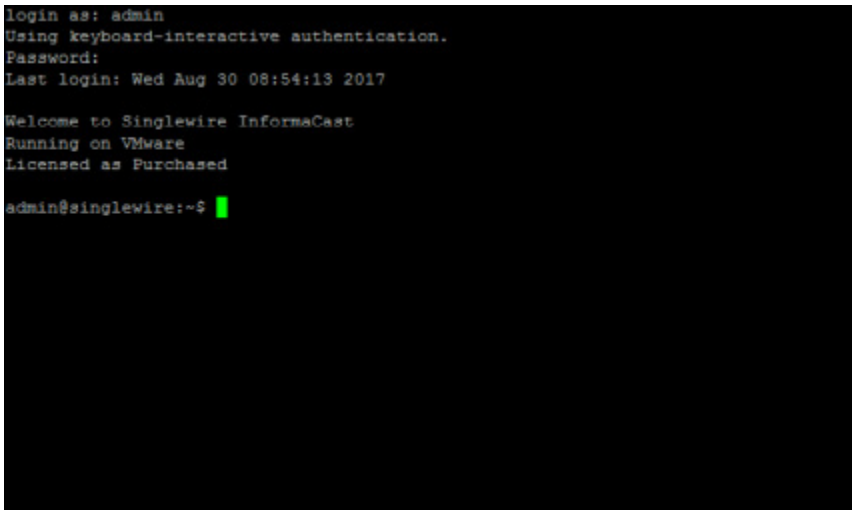
Step 3 Leave the **Port** field at its default of 22.

Step 4 Click the **SSH** radio button.

Step 5 Click the **Open** button. The command-line interface for the Virtual Appliance appears.

Step 6 Enter **admin** at the prompt and press the **Enter** key.

Step 7 Enter your OS password at the prompt and press the **Enter** key. The command-line interface refreshes, showing you that you're logged in.



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 2-43
- "Set the Default Codec to G.711" on page 2-51
- "Create a Device Pool" on page 2-53
- "Create a Route Partition" on page 2-55
- "Create a Calling Search Space" on page 2-56
- "Create CTI Ports" on page 2-58
- "Create an Access Control Group" on page 2-63
- "Create an Application User" on page 2-67
- "Enable Web Access for Cisco IP Phones" on page 2-70
- "Set Your Authentication URL" on page 2-77
- "Set the Authentication Method for API Browser Access" on page 2-79
- "Reboot Your Phones" on page 2-80
- "Test Your Phones" on page 2-82

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 5-48 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

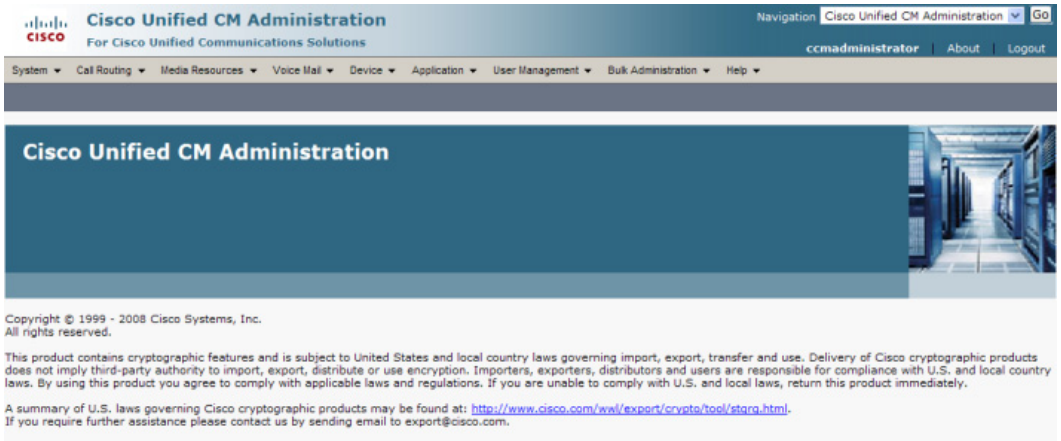
InformaCast uses SNMP to gather phone information from Unified Communications Manager. Depending on whether you are using SNMP v2 or v3, you will follow different steps:

- **SNMP v2.** Follow the steps in "Enable SNMP on Unified Communications Manager Cluster Nodes" on page 2-43 and "Create an InformaCast SNMP v2 Community String" on page 2-46.
- **SNMP v3.** Follow the steps in "Enable SNMP on Unified Communications Manager Cluster Nodes" on page 2-43 and "Create an SNMP v3 User" on page 2-48.

Enable SNMP on Unified Communications Manager Cluster Nodes

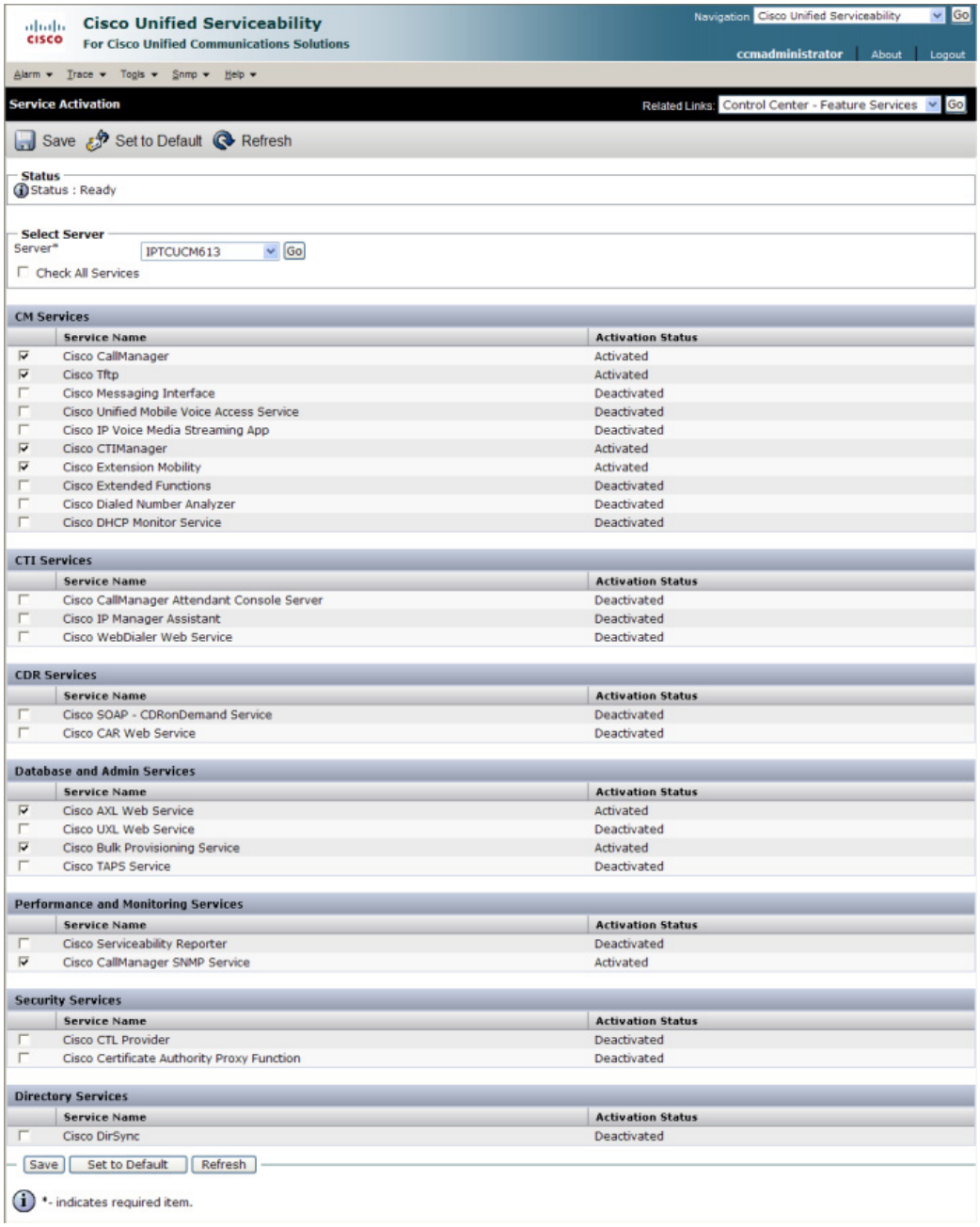
You must enable SNMP on Unified Communications Manager cluster nodes that will function with InformaCast.

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.

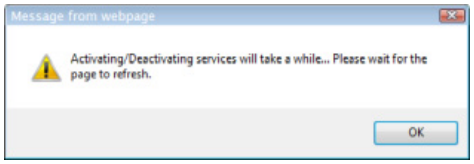


Note If you have more than one server, you'll have to select your server from the **Server** dropdown menu and click the **Go** button. The Service Activation page for that server will then appear.

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.



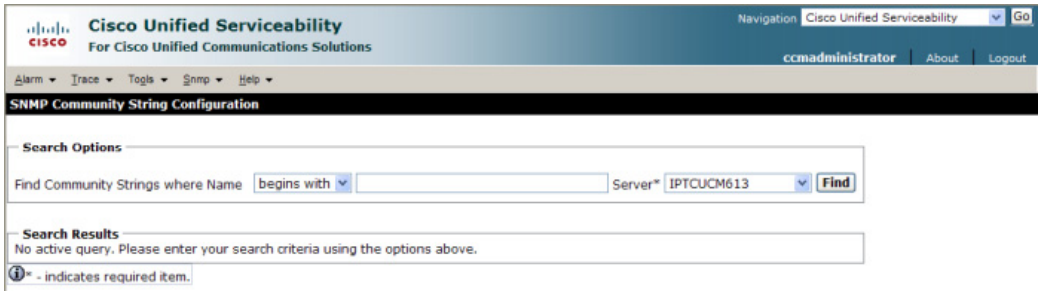
Step 7 Verify your services are running by going to **Tools | Control Center - Feature Services**. **Cisco CallManager**, **Cisco CTIManager**, **Cisco AXL Web Service**, and **Cisco CallManager SNMP Service** should say they are **Activated**. If not, click the green arrow in the top left hand corner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

Create an InformaCast SNMP v2 Community String

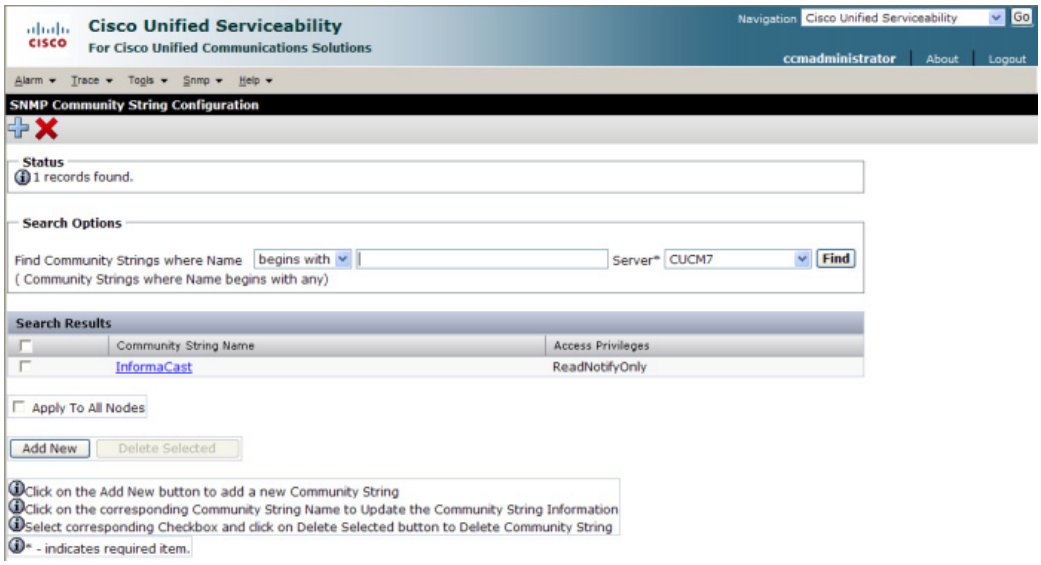
Follow these steps to create an SNMP v2 InformaCast SNMP community string.

Note Skip this section if you're using SNMP v3 and go to "Create an SNMP v3 User" on page 2-48.

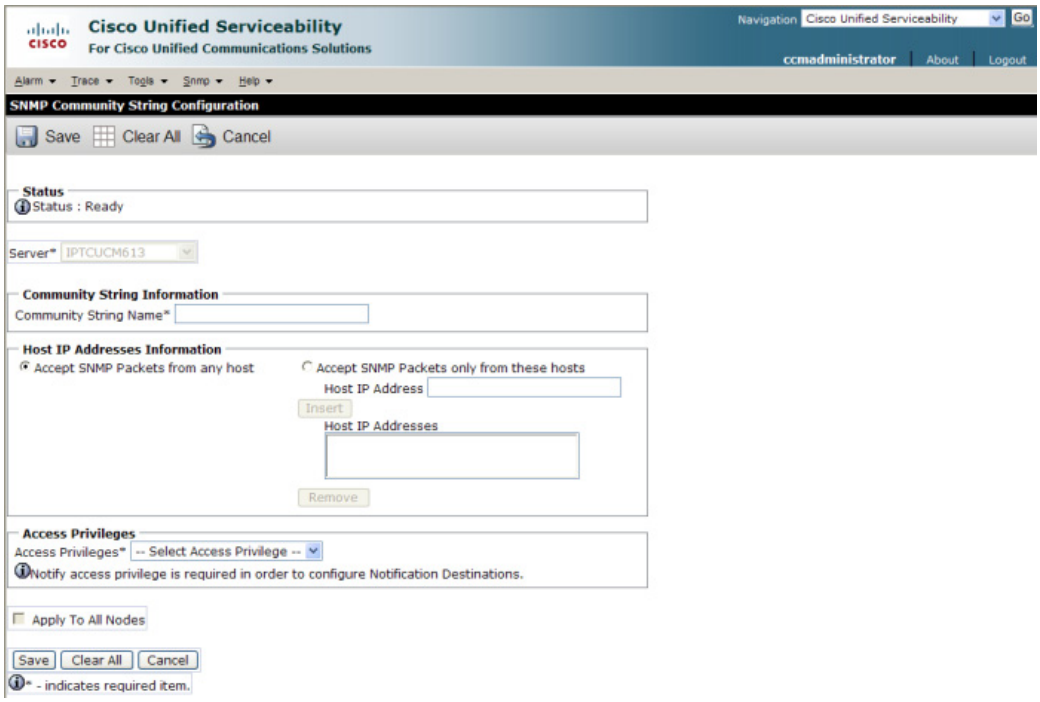
Step 1 Go to **SNMP | V1/V2c | Community String**. The SNMP Community String Configuration page appears.



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



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



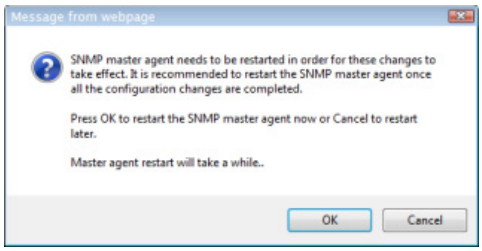
Step 4 Enter **ICVA** into the **Community String Name** field. You will need to remember this name when you edit InformaCast's SNMP configuration in "Configure Your Default Unified Communications Manager Cluster" on page 4-3.

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.

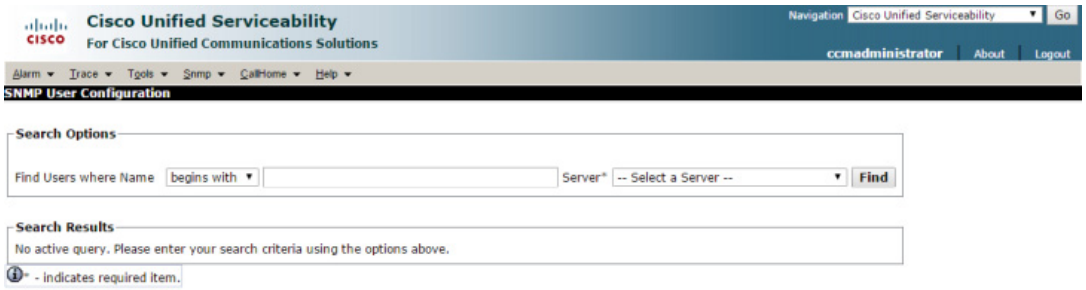


Create an SNMP v3 User

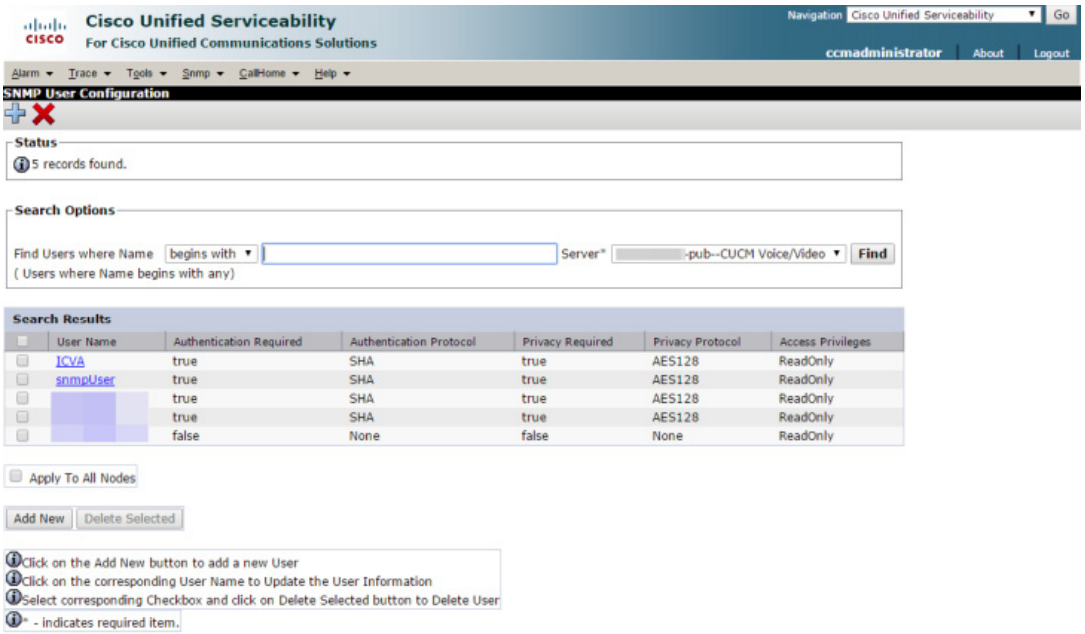
Follow these steps to create an SNMP v3 user.

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

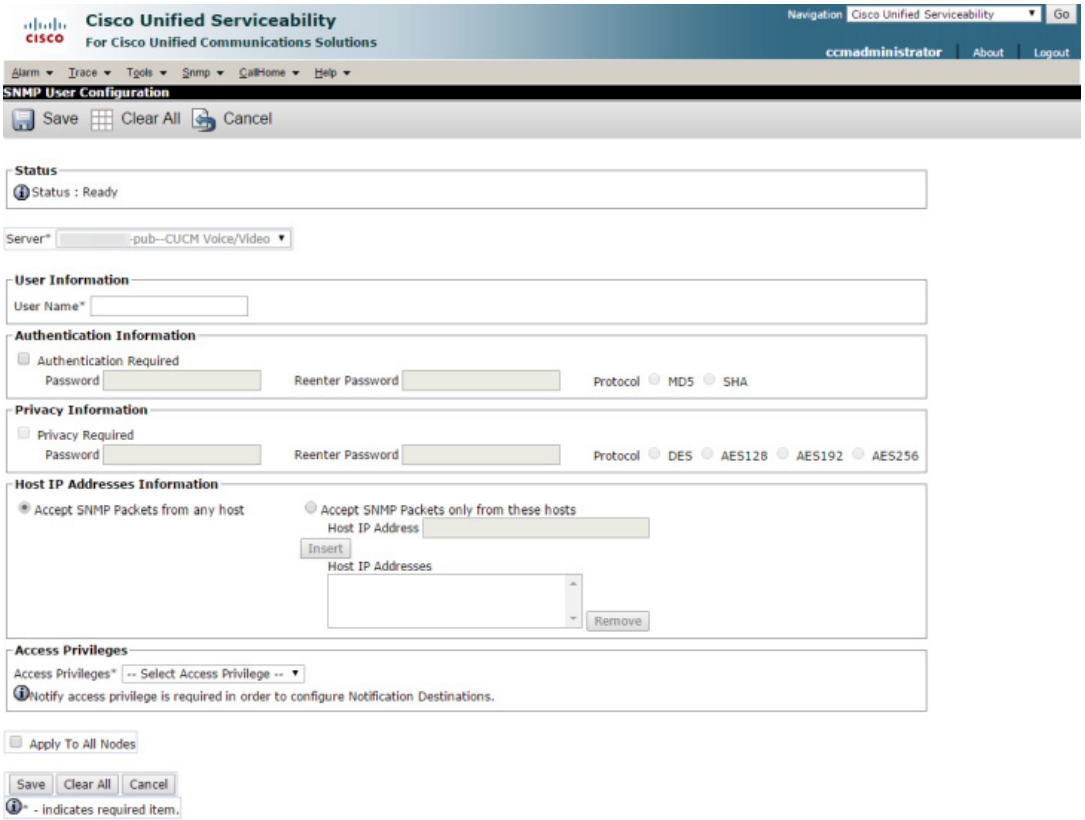
Step 1 Go to **SNMP** | **V3** | **User**. The SNMP User Configuration page appears.



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



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.

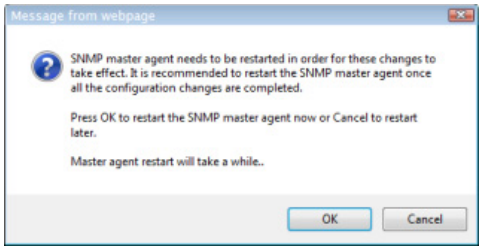
Step 9 Enter a privacy password for your user in the **Password** and **Reenter** Password fields. The password must contain at least eight characters.

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.

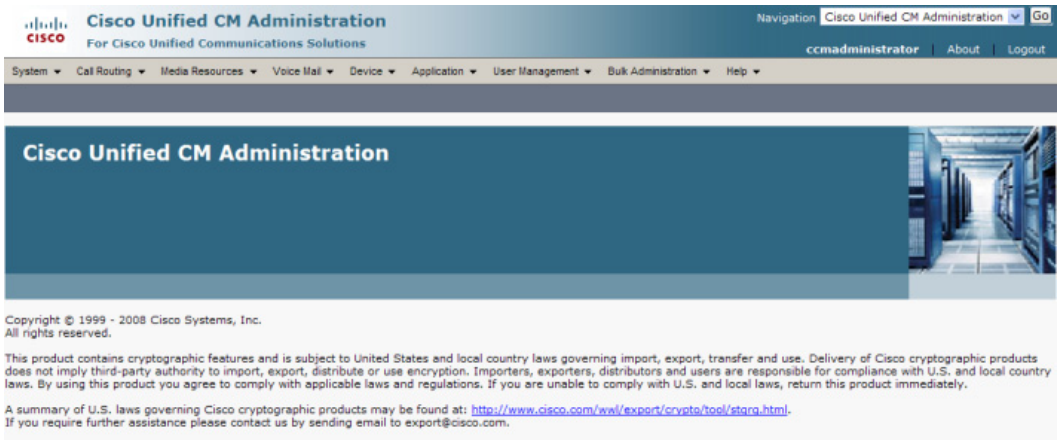
Step 13 Click the **Save** button. If you are prompted to restart the SNMP service, click the **OK** button.



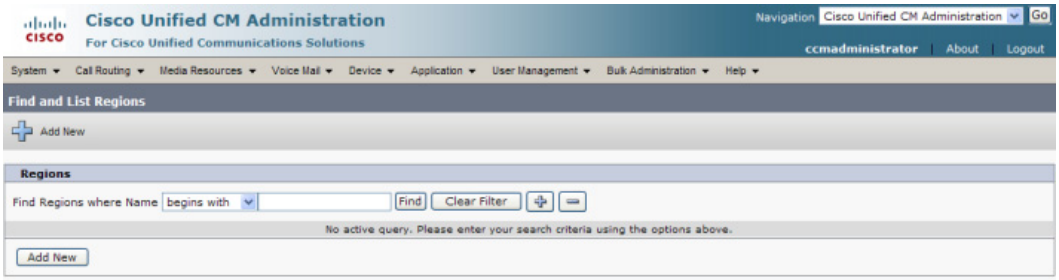
Set the Default Codec to G.711

The Virtual Appliance requires that audio streams be in G.711 µLaw 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.

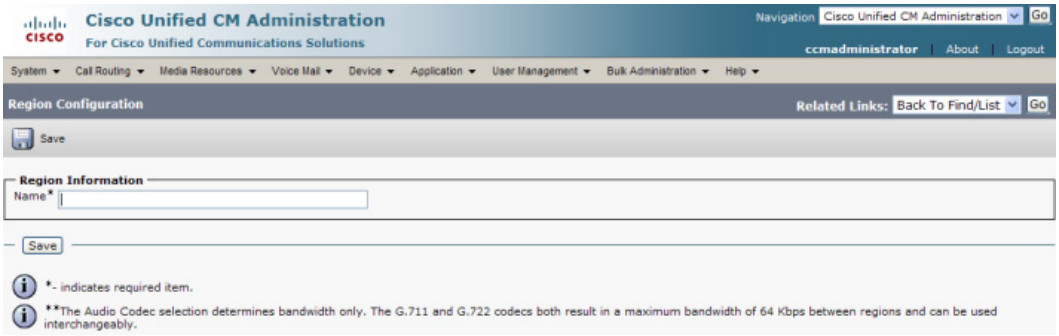
Step 1 Ensure you are in Cisco Unified CM Administration or select **Cisco Unified CM Administration** from the **Navigation** dropdown menu and click the **Go** button. The Cisco Unified CM Administration page appears.



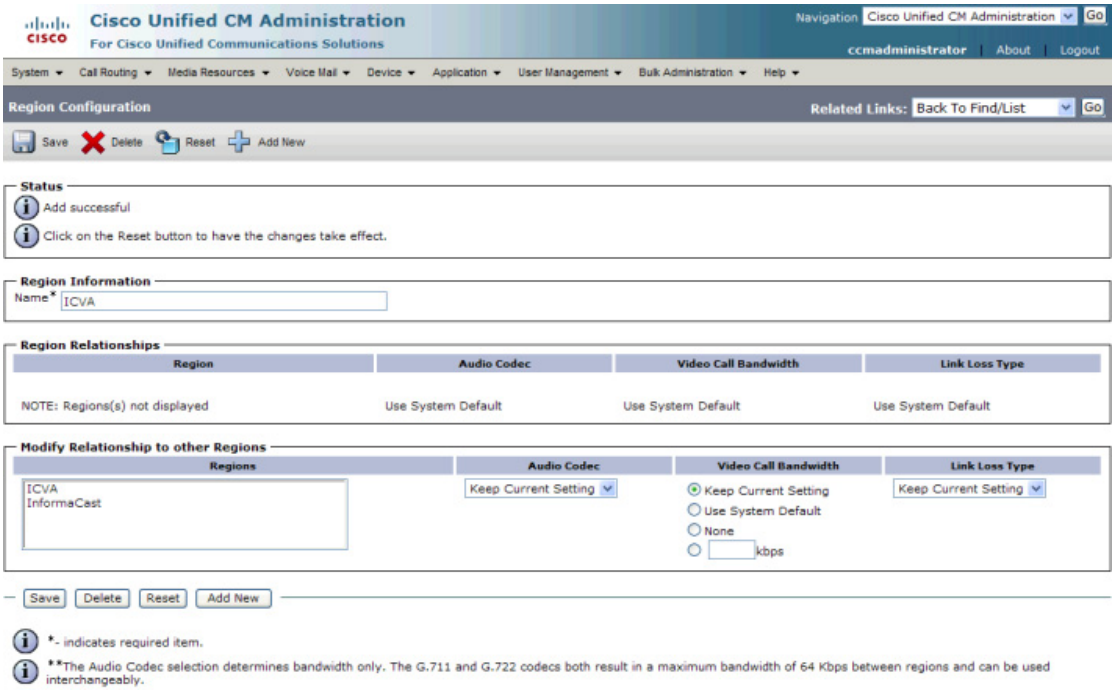
Step 2 Go to **System** | **Region Information** | **Region**. The Find and List Regions page appears.



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



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



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

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

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

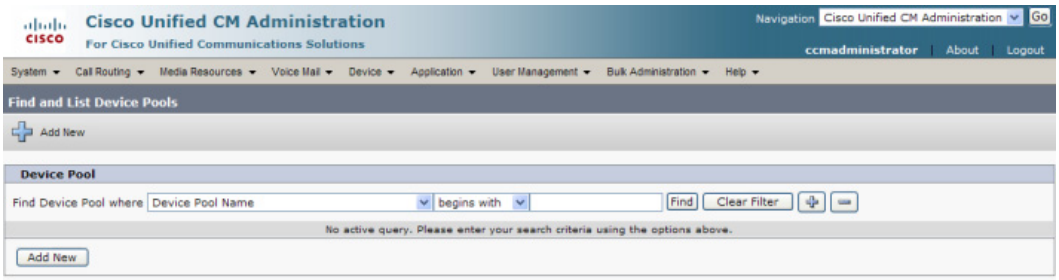
Step 8 Click the **Save** button.

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

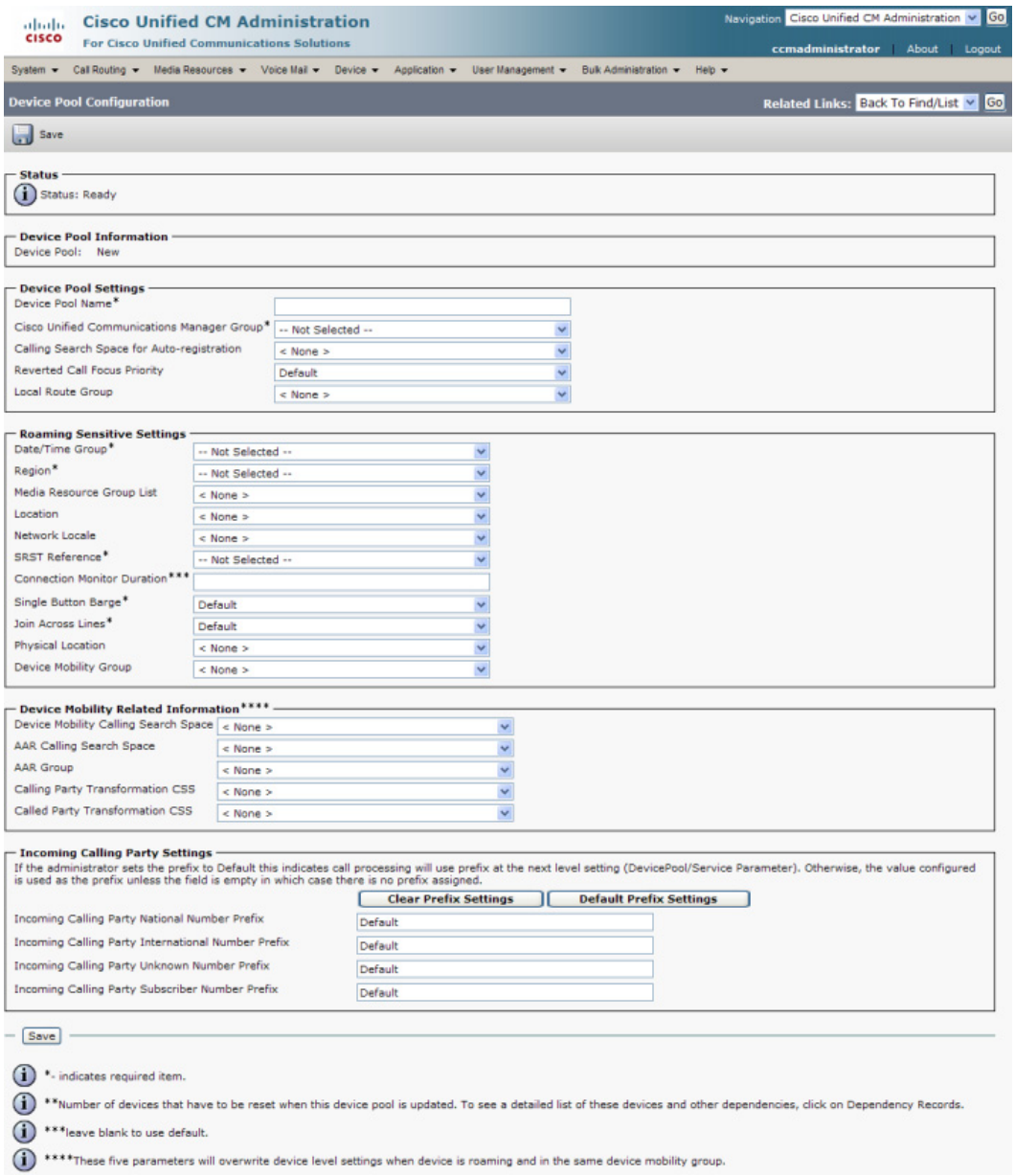
Create a Device Pool

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

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



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



Step 3 Select a 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 2-51.

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

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

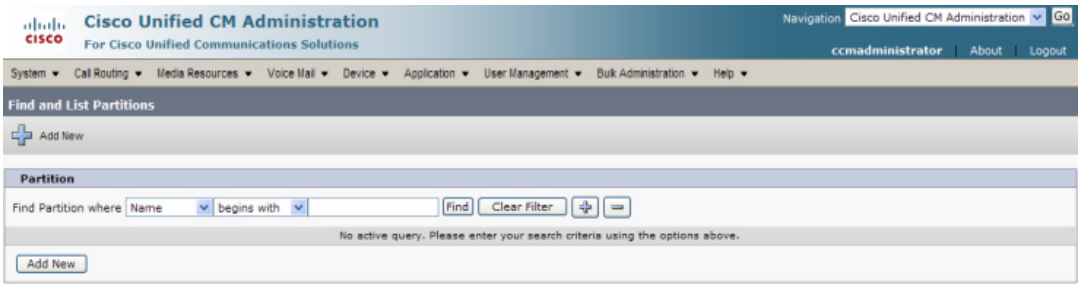
Step 8 Select/enter appropriate values for any required fields, which are marked with asterisks (*).

Step 9 Click the **Save** button.

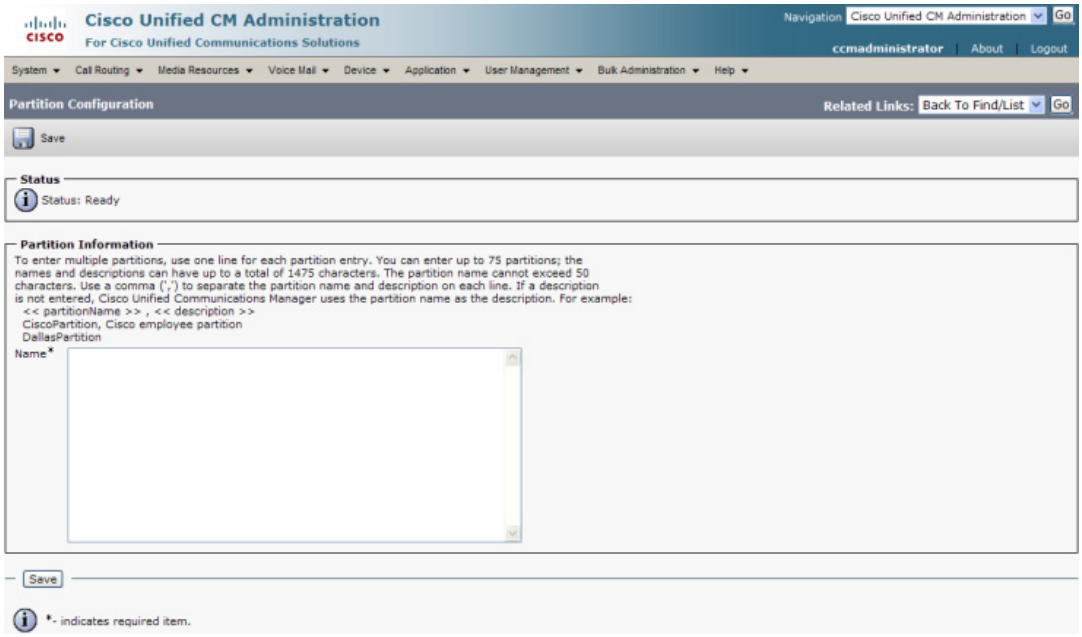
Create a Route Partition

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

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



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



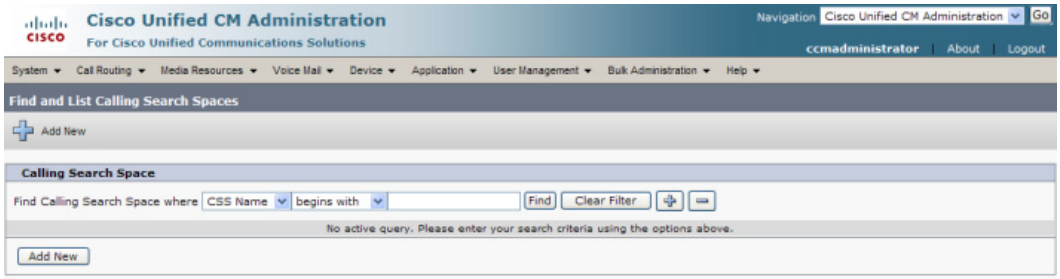
Step 3 Enter **ICVA-CTIOutbound,ICVA-Do not add to any phone CSS** in the **Name** field.

Step 4 Click the **Save** button.

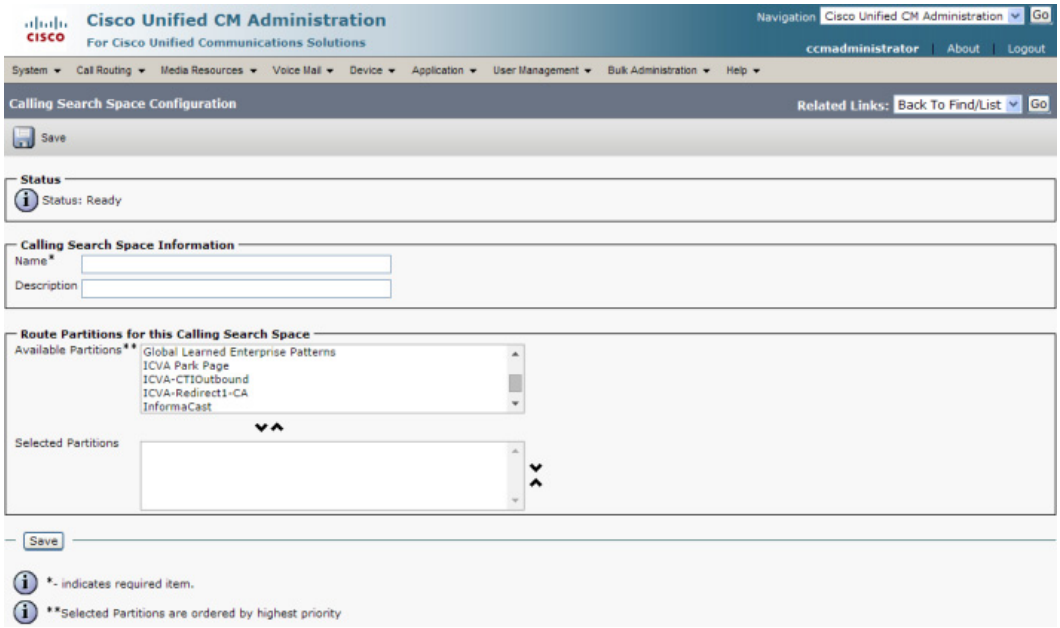
Create a Calling Search Space

InformaCast places a call to your Cisco IP phone to record the audio that will be broadcast. This is a phone call just like any other call. You must ensure that your 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.



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



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

Step 4 Select the following partition(s):

- The partition you created in "Create a Route Partition" on page 2-55
- The partition(s) housing your users' extensions

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

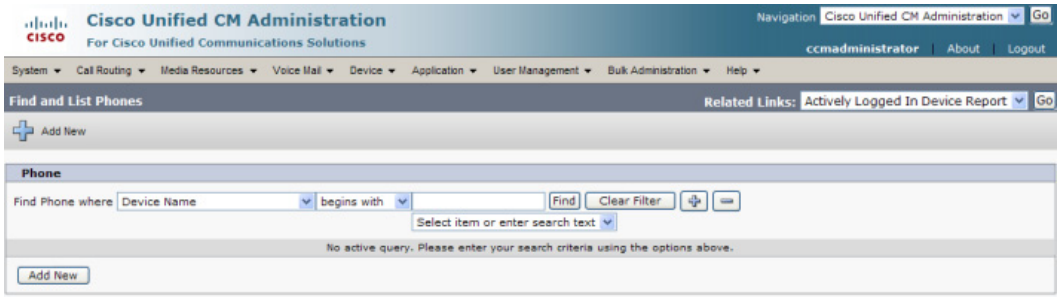
Tip Do not add your voicemail platform to the *Selected Partitions* area.

Step 6 Click the **Save** button.

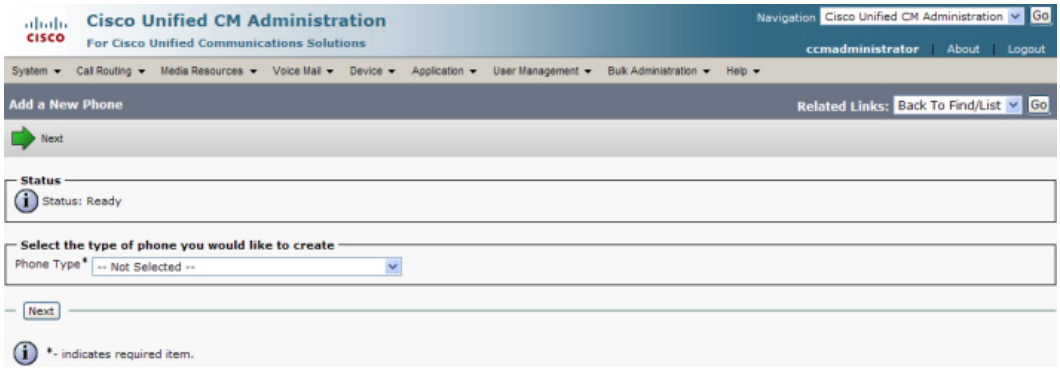
Create CTI Ports

Use the following steps to create CTI ports for InformaCast.

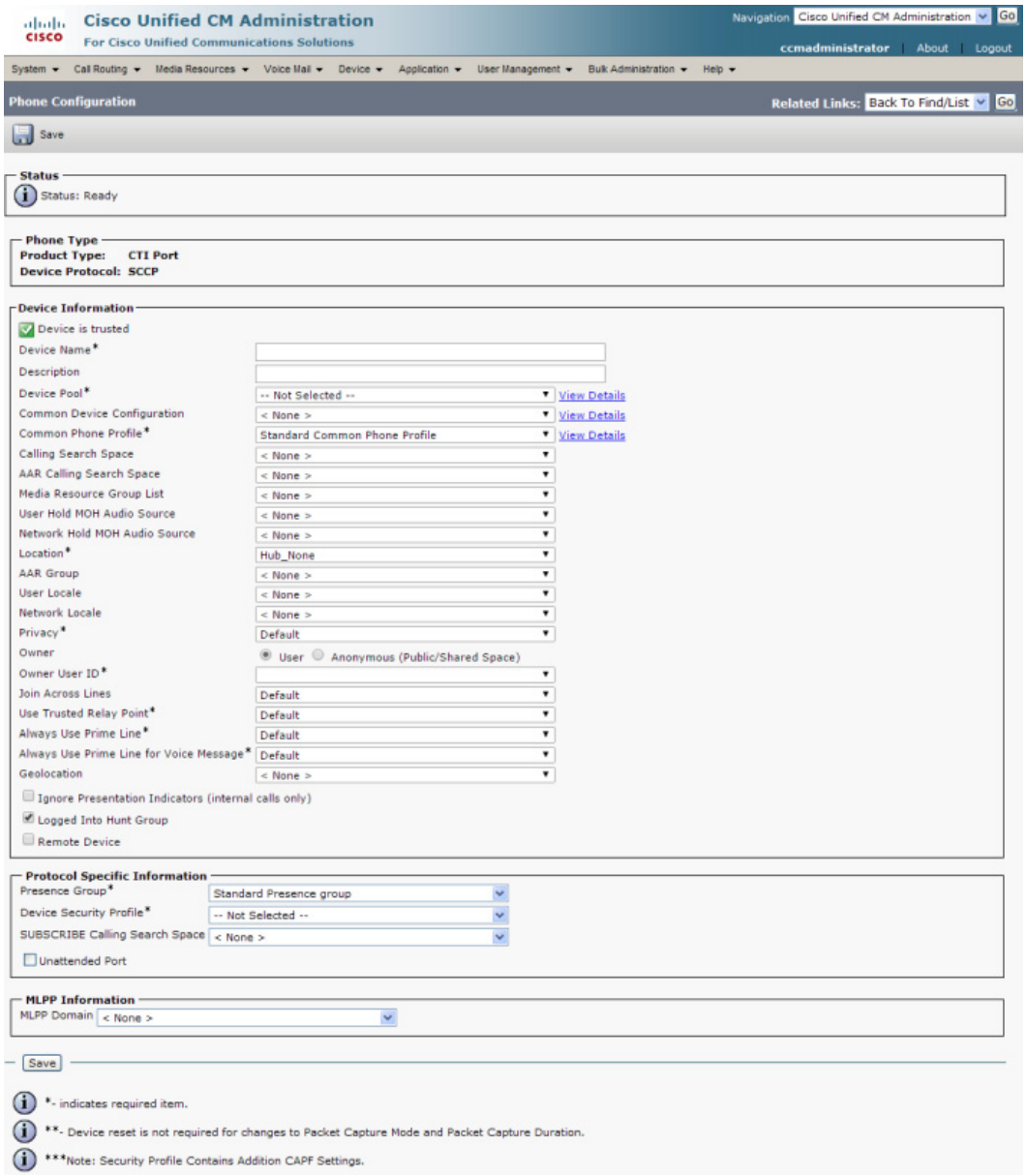
Step 1 Go to **Device | Phone**. The Find and List Phones page appears.



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



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



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

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

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

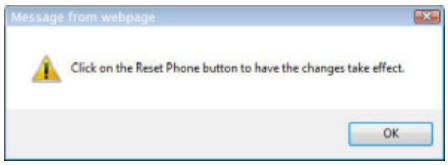
Note The device pool must use a region that will allow a G.711 µLaw call to phones.

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

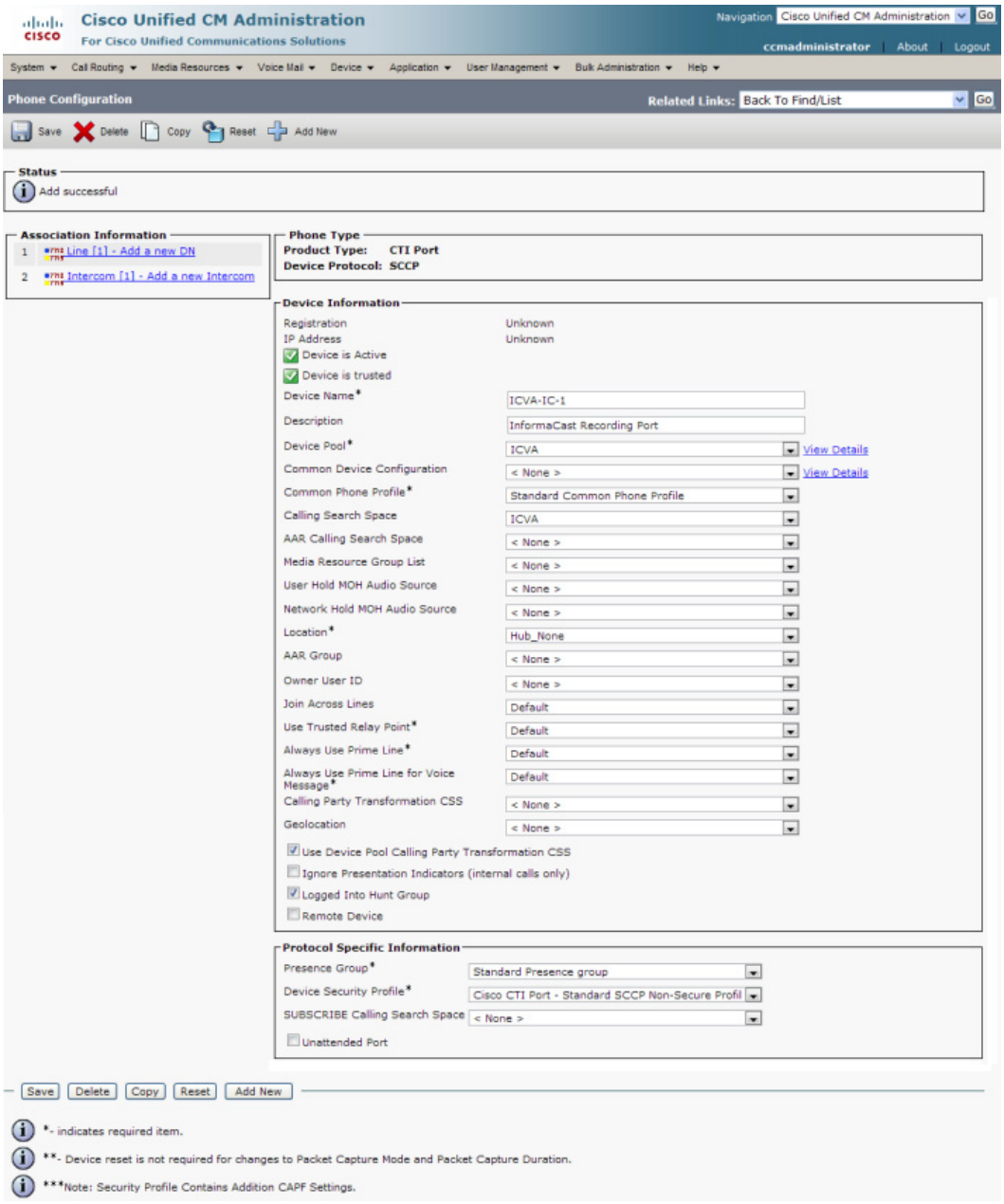
Step 8 Select the **Anonymous/Public Shared Space** radio button above the **Owner User ID** field, which will remove the required setting from the **Owner User ID** field.

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.

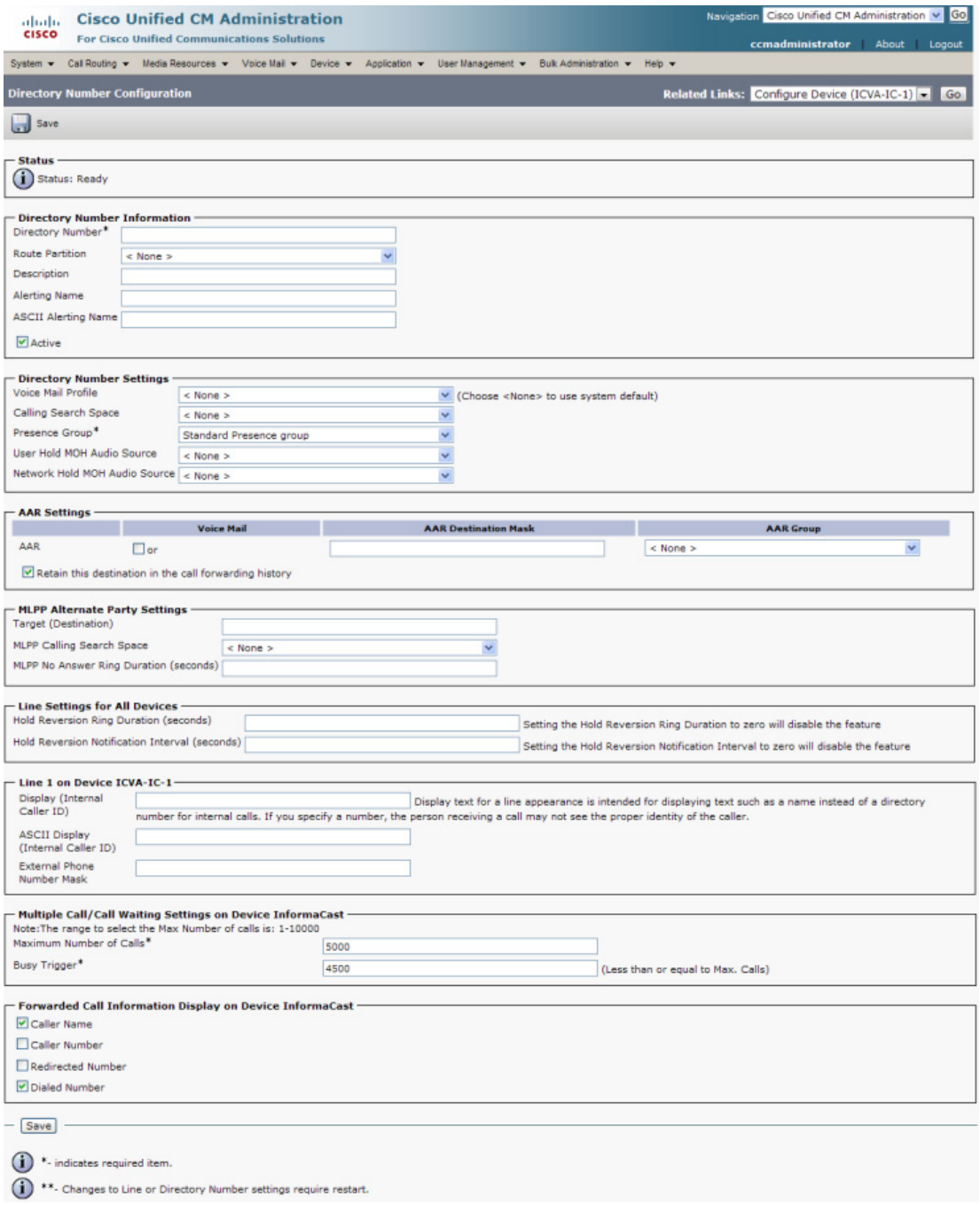
Step 10 Click the **Save** button. A warning dialog box appears.



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.



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



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.

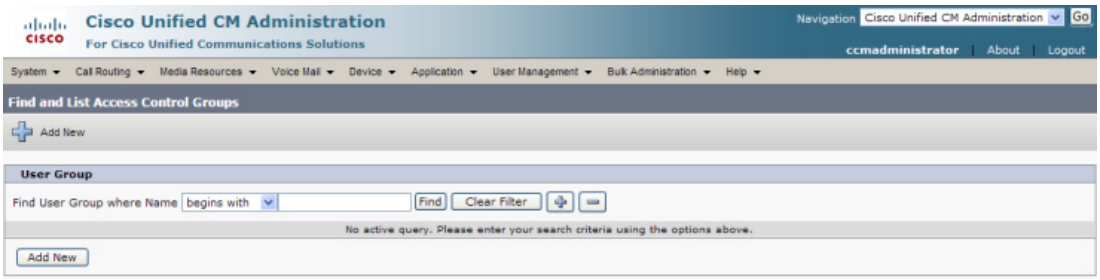
Step 17 Click the **Save** button to add the directory number.

Step 18 Repeat Steps 1 through 17 as many times as needed to create the number of CTI ports that you need (minimum two).

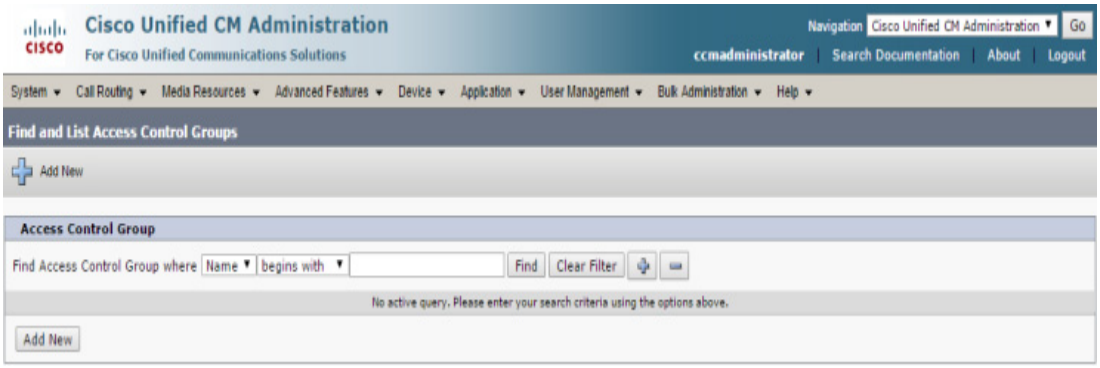
Create an Access Control Group

In "Create an Application User" on page 2-67, 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.

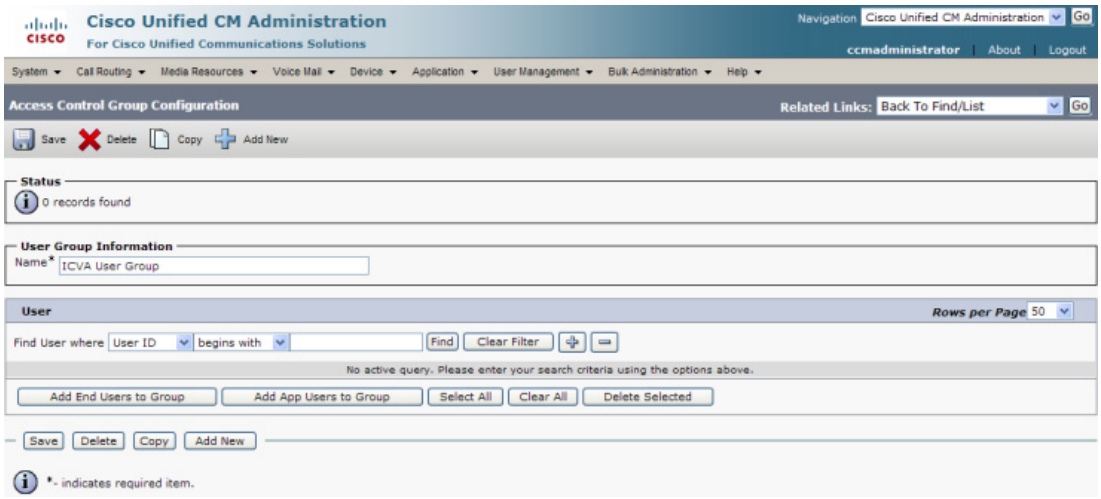
Step 1 Go to **User Management** | **User Settings** | **Access Control Group**. The Find and List Access Control Groups page appears.



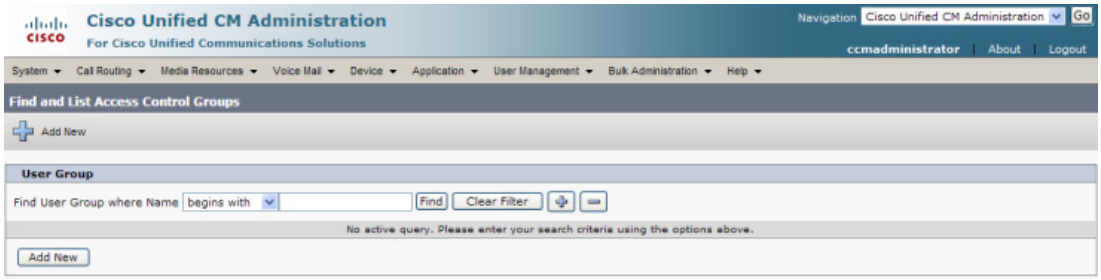
Step 2 Click the **Add New** button. The Access Control Group Configuration page appears.



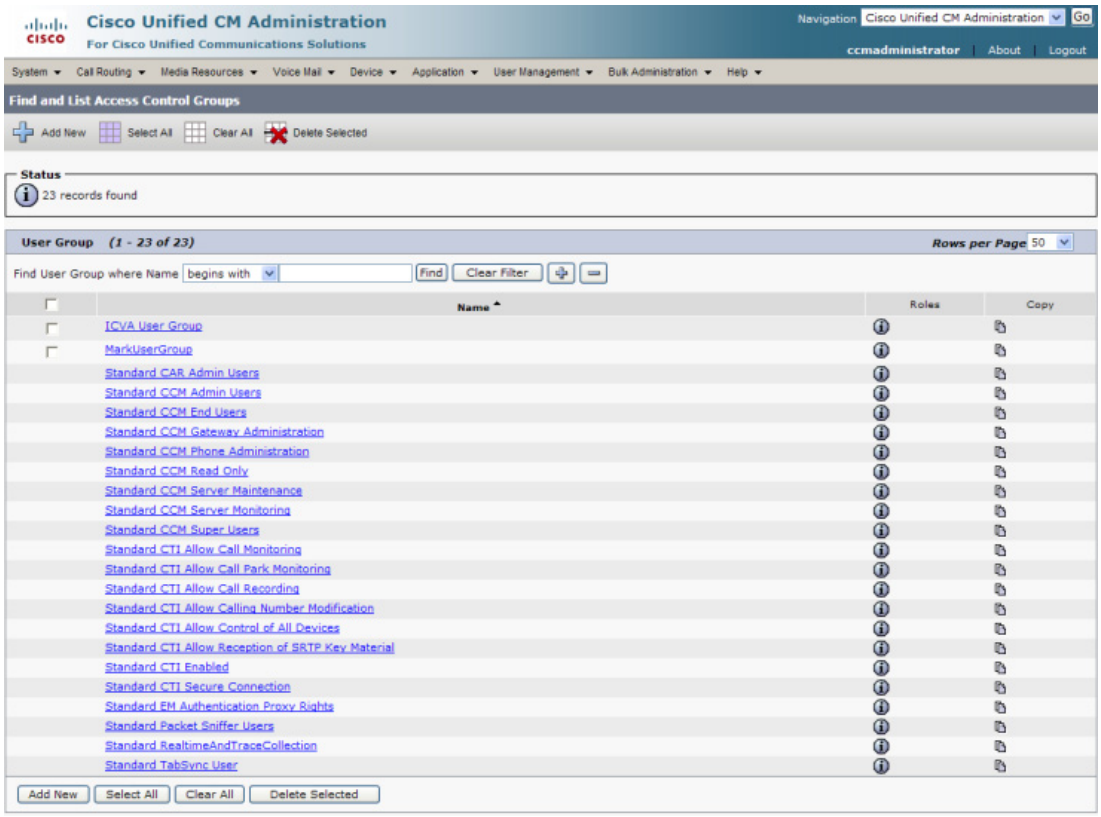
Step 3 Enter **ICVA User Group** in the **Name** field and click the **Save** button. The Access Control Group Configuration page refreshes.



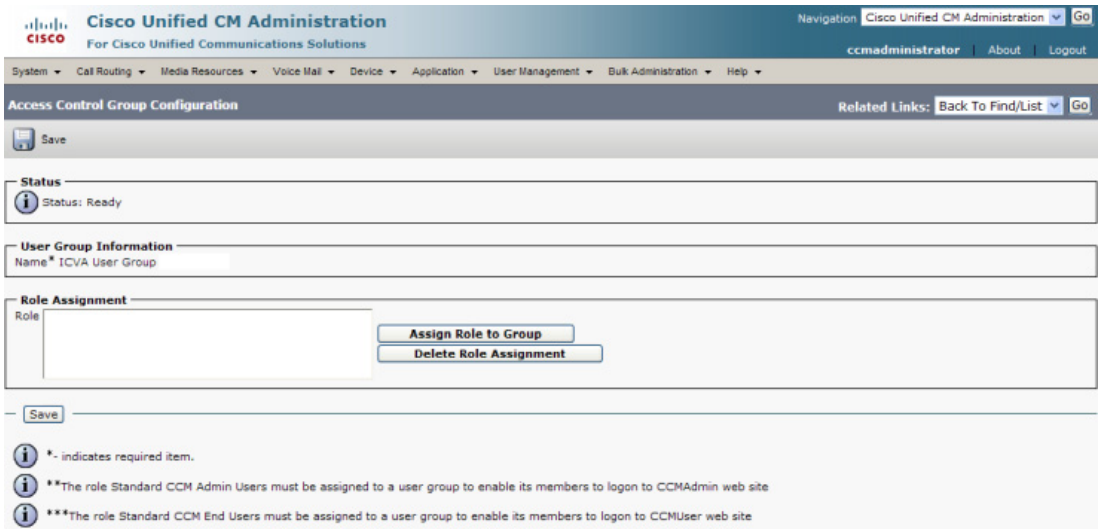
Step 4 Make sure **Back to Find/List** is selected in the **Related Links** dropdown menu and click the **Go** button. The Find and List Access Control Groups page appears.



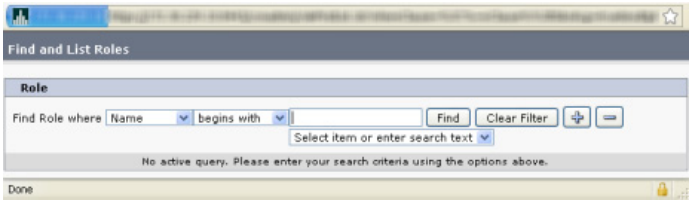
Step 5 Click the **Find** button. The Find and List Access Control Groups page refreshes and you should see your new user group.



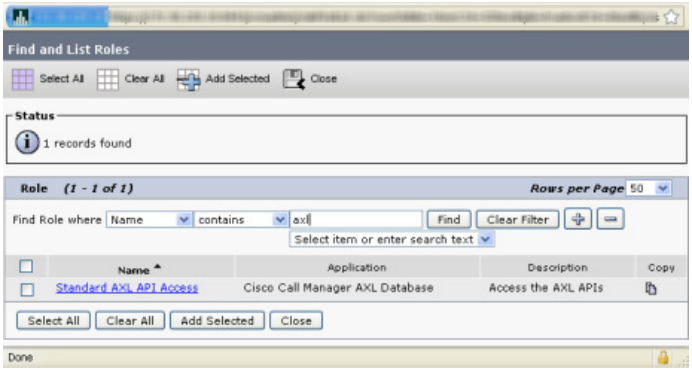
Step 6 Click the **i** icon in the Roles column next to your new user group. The Access Control Group Configuration page appears.



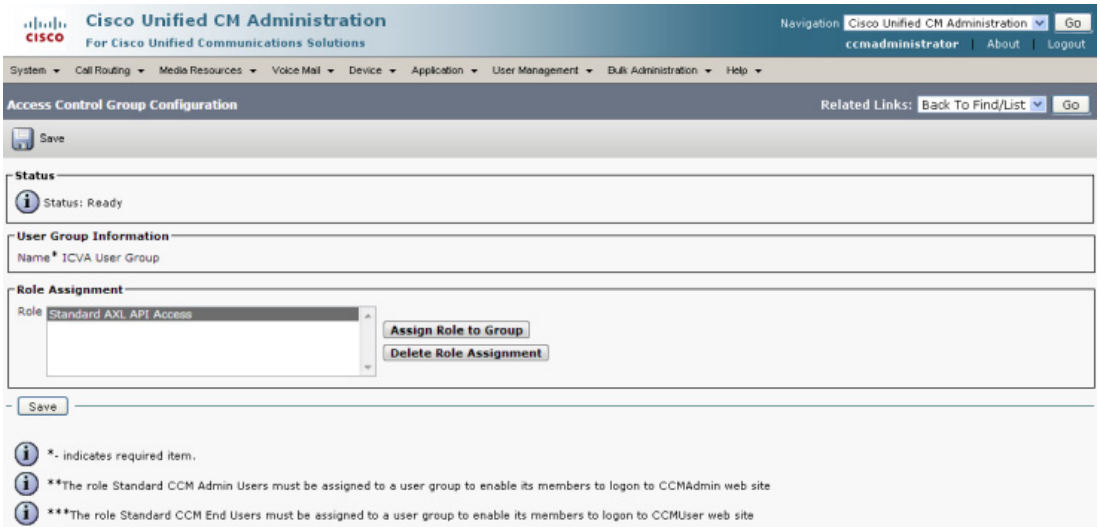
Step 7 Click the **Assign Role to Group** button. The Find and List Roles window appears.



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



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



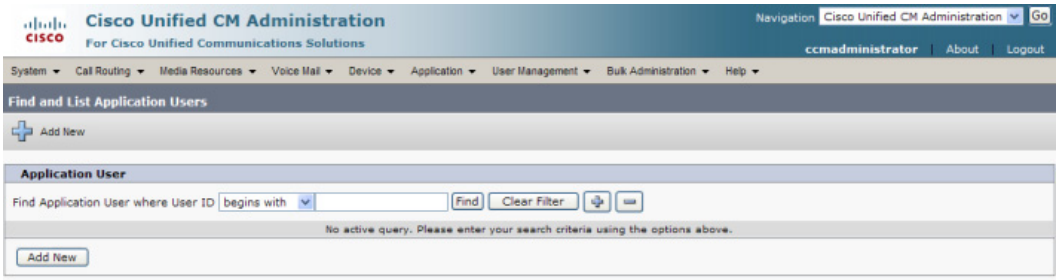
Step 10 Click the **Save** button.

Create an Application User

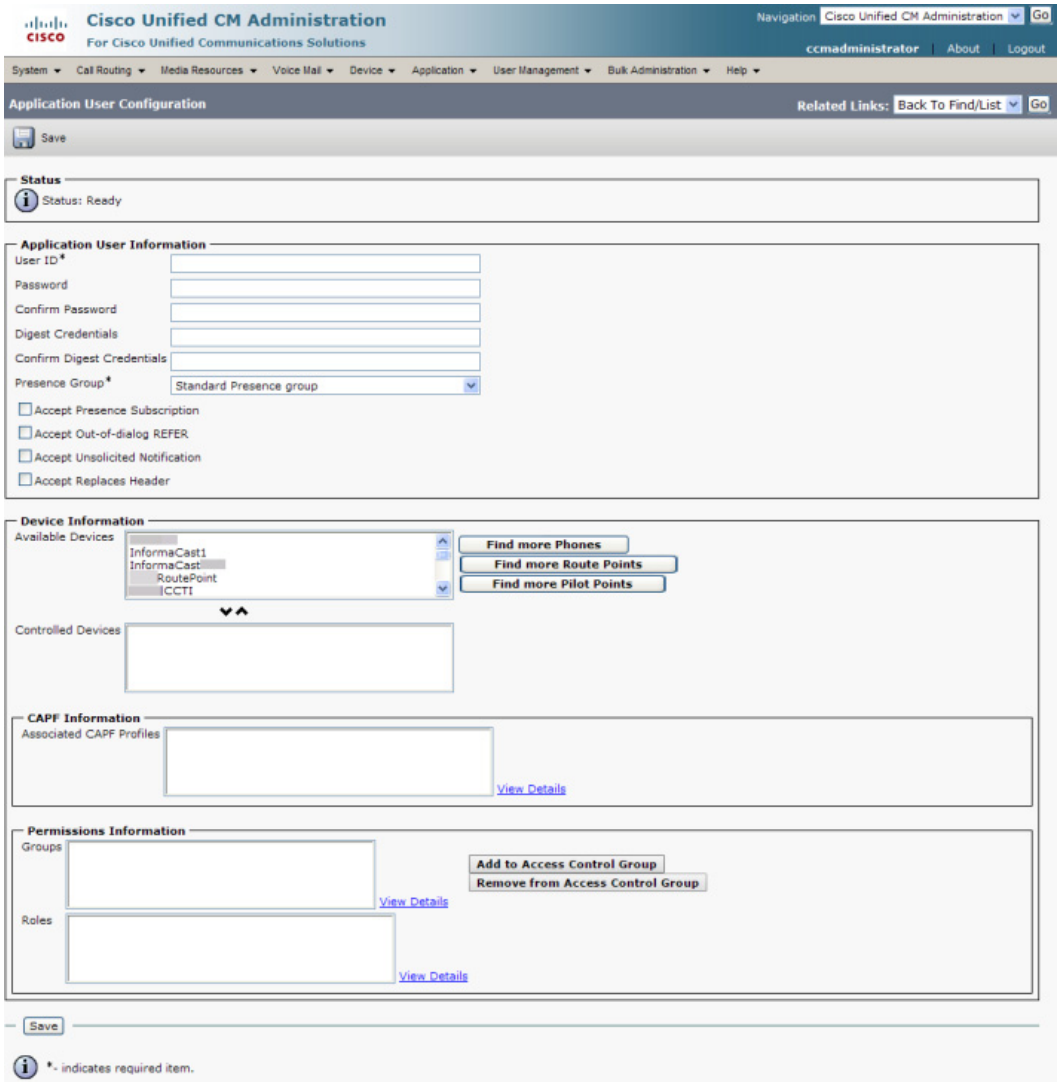
InformaCast needs an application user set in Unified Communications Manager so that it can establish a CTI connection and gain access to the telephony features Unified Communications Manager offers (e.g. making phone calls, using JTAPI to determine the busy status of a phone, etc.). You also need an 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 2-63.
- **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 the **Send Commands to Phones by JTAPI** checkbox on the Broadcast Parameters page (see "Manage Broadcast Parameters" on page 4-49), it allows you to communicate using JTAPI instead of HTTP. If you add this role, you can skip "Enable Web Access for Cisco IP Phones" on page 2-70.
- **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.



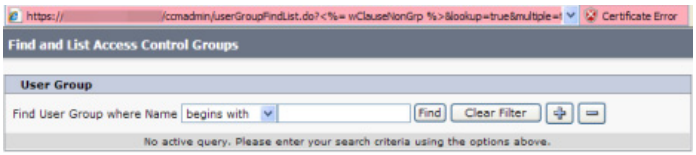
Step 3 Enter an appropriate user ID in the **User ID** field, e.g. ICVA InformaCast.

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

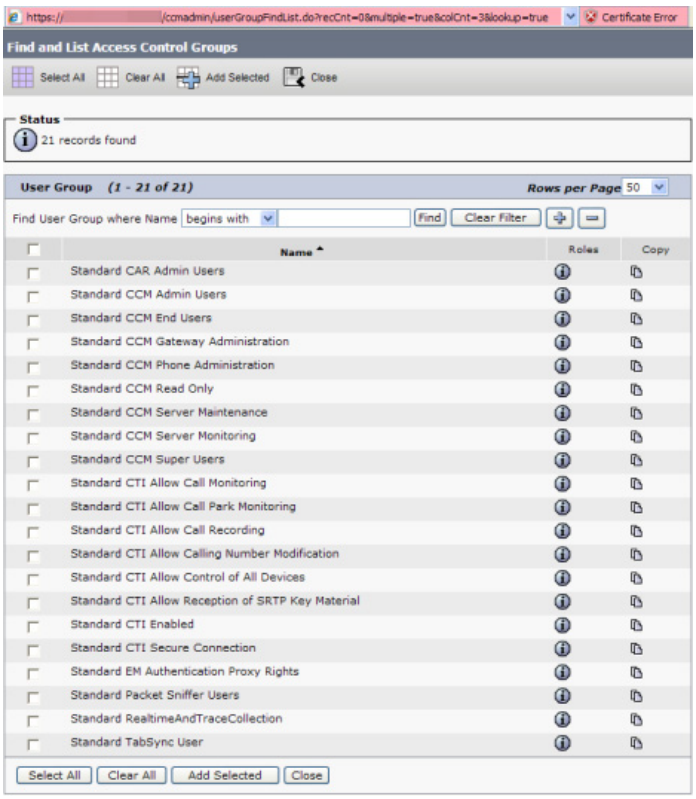
You will need to remember the user ID and password values because you will enter them into InformaCast's own Edit Telephony Configuration page once you install InformaCast (see "Configure Your Default Unified Communications Manager Cluster" on page 4-3).

Step 5 Select the CTI ports (created in "Create CTI Ports" on page 2-58) 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

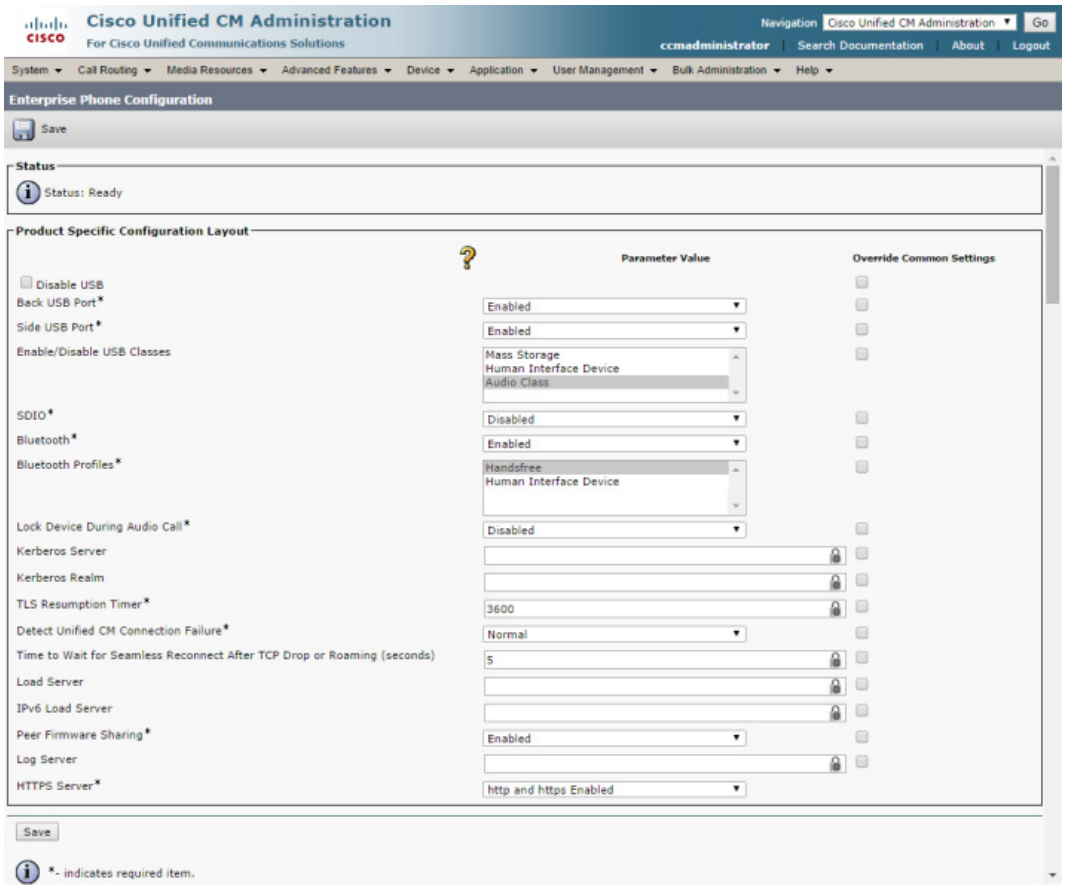
You must enable web access for all phones to which InformaCast will broadcast. To enable web access, you can:

- 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.

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



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

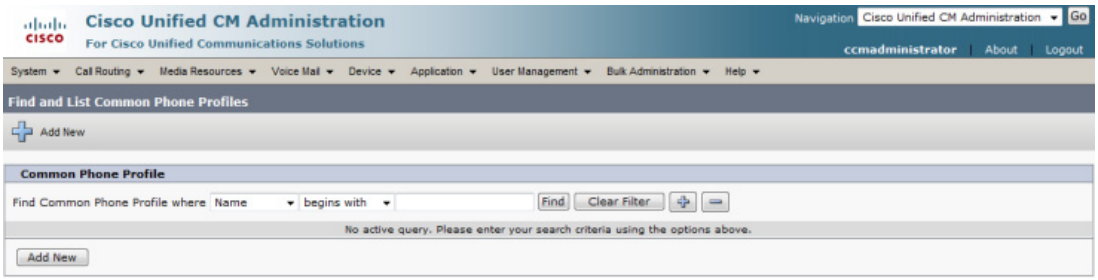
Step 3 Click the **Save** button.

Note You will need to reboot your phones for this change to take effect; however, you will also need to reboot your phones after performing the steps in "Set Your Authentication URL" on page 2-77. 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 2-80.

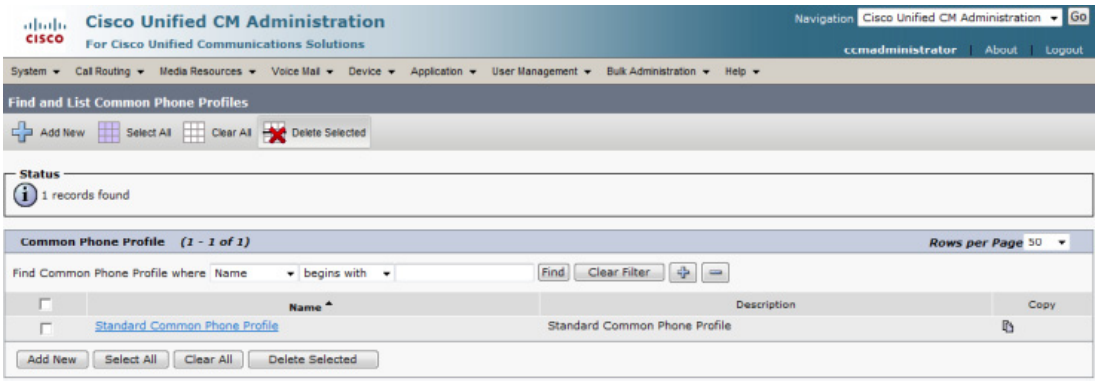
Enable Web Access for Multiple Phones by Changing Their Profiles

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

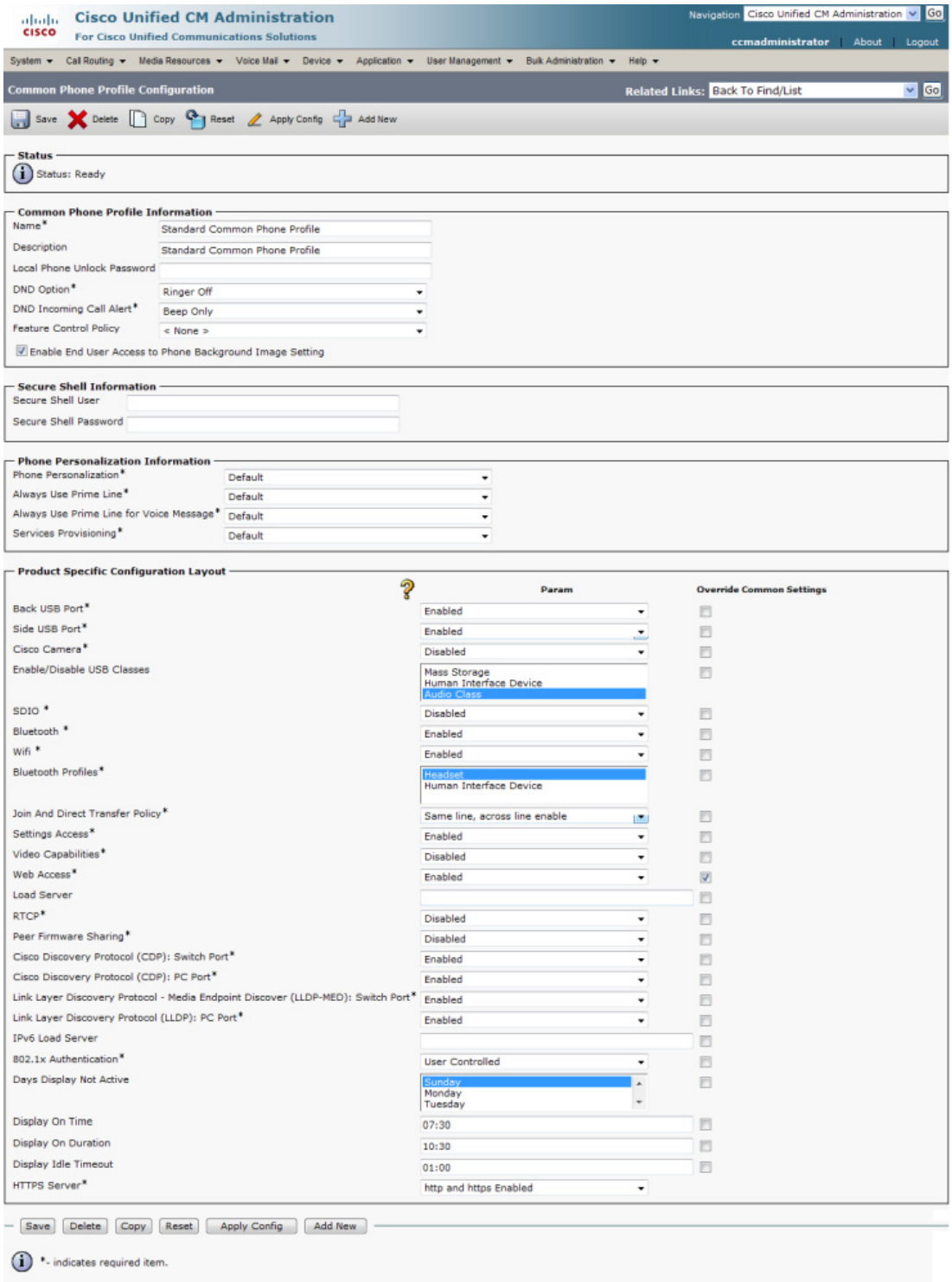
Step 1 Go to **Device** | **Device Settings** | **Common Phone Profile**. The Find and List Common Phone Profiles page appears.



Step 2 Click the **Find** button to display all the phone profiles of which 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.



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



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

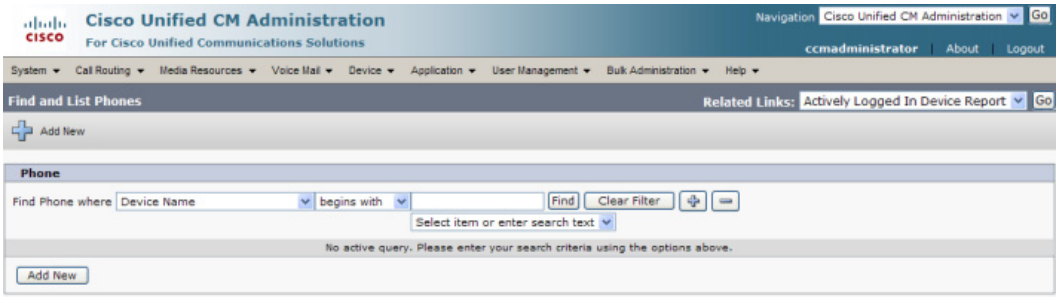
Step 5 Click the **Save** button.

Note You will need to reboot your phones for this change to take effect; however, you will also need to reboot your phones after performing the steps in "Set Your Authentication URL" on page 2-77. 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 2-80.

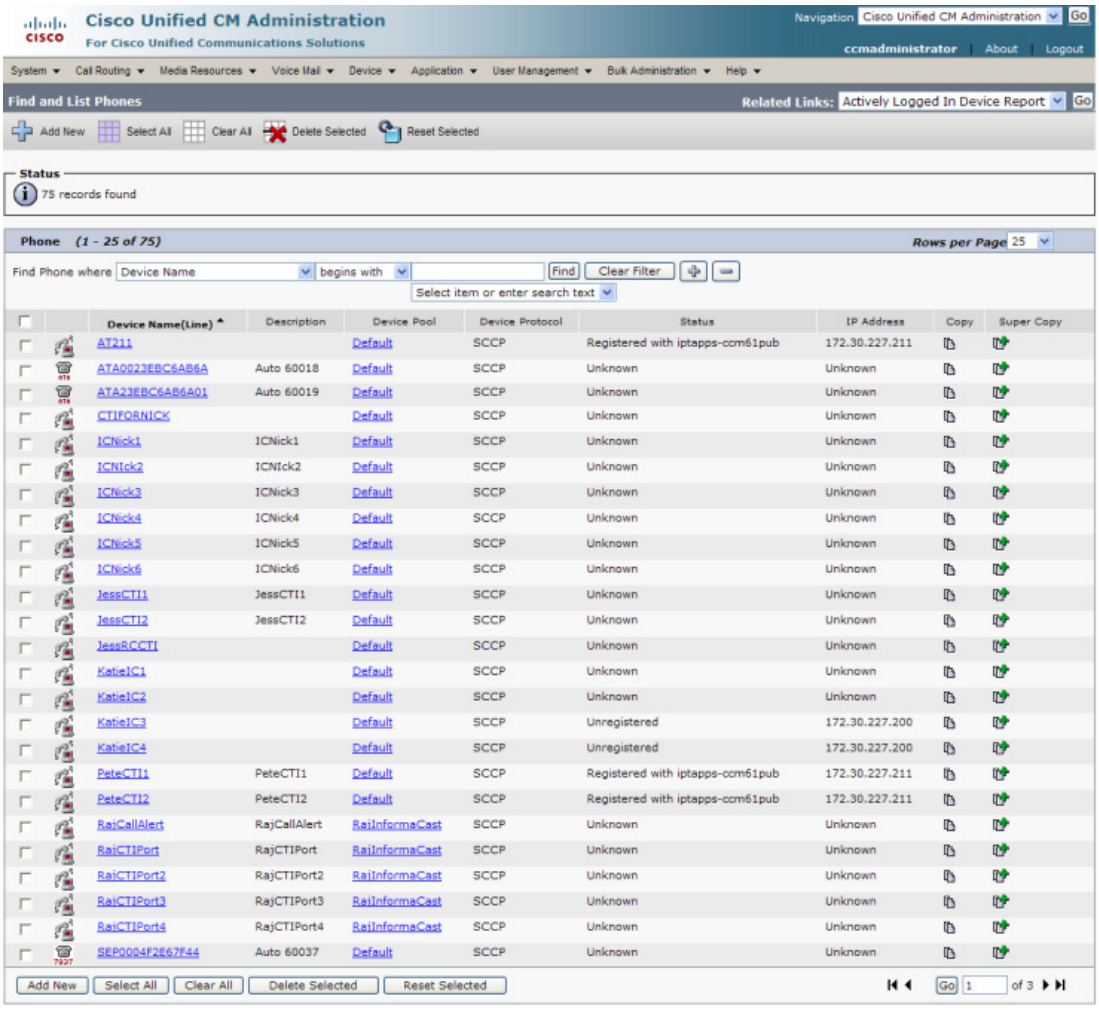
Enable Web Access for Individual Phones

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

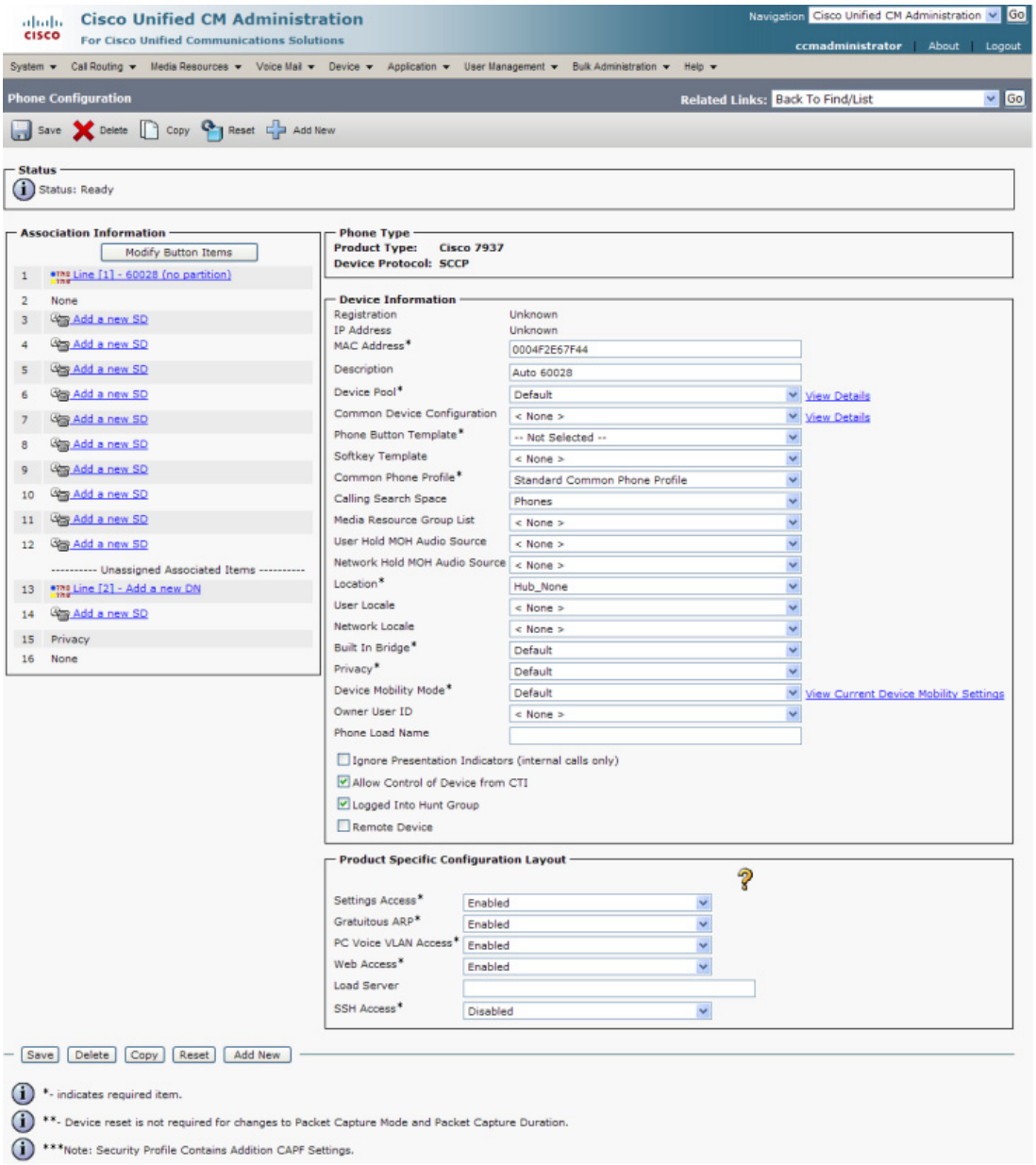
Step 1 Go to **Device** | **Phone**. The Find and List Phones page appears.



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



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



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

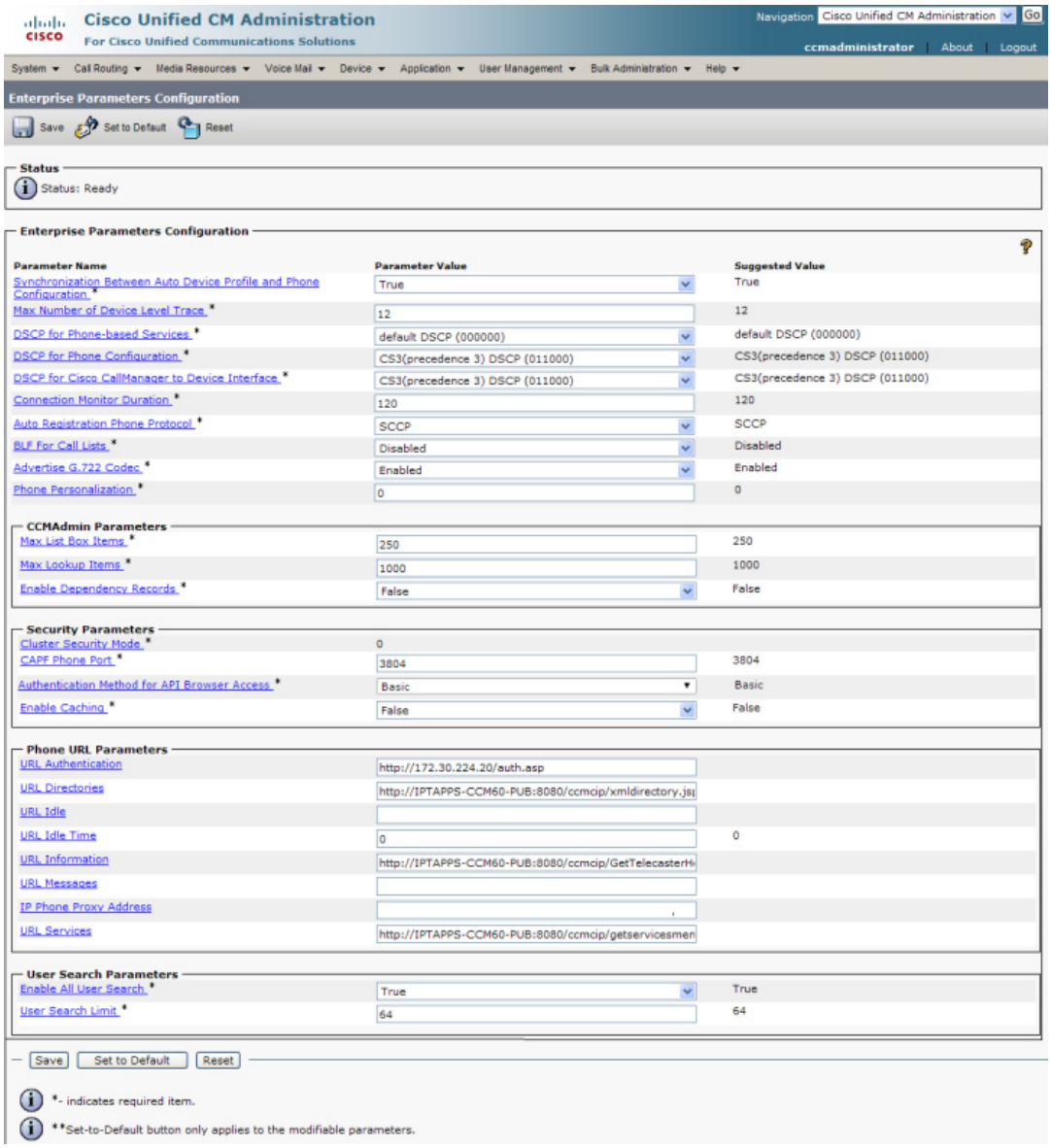
Step 5 Click the **Save** button.

Note You will need to reboot your phones for this change to take effect; however, you will also need to reboot your phones after performing the steps in "Set Your Authentication URL" on page 2-77. 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 2-80.

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.



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 4-8.

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.

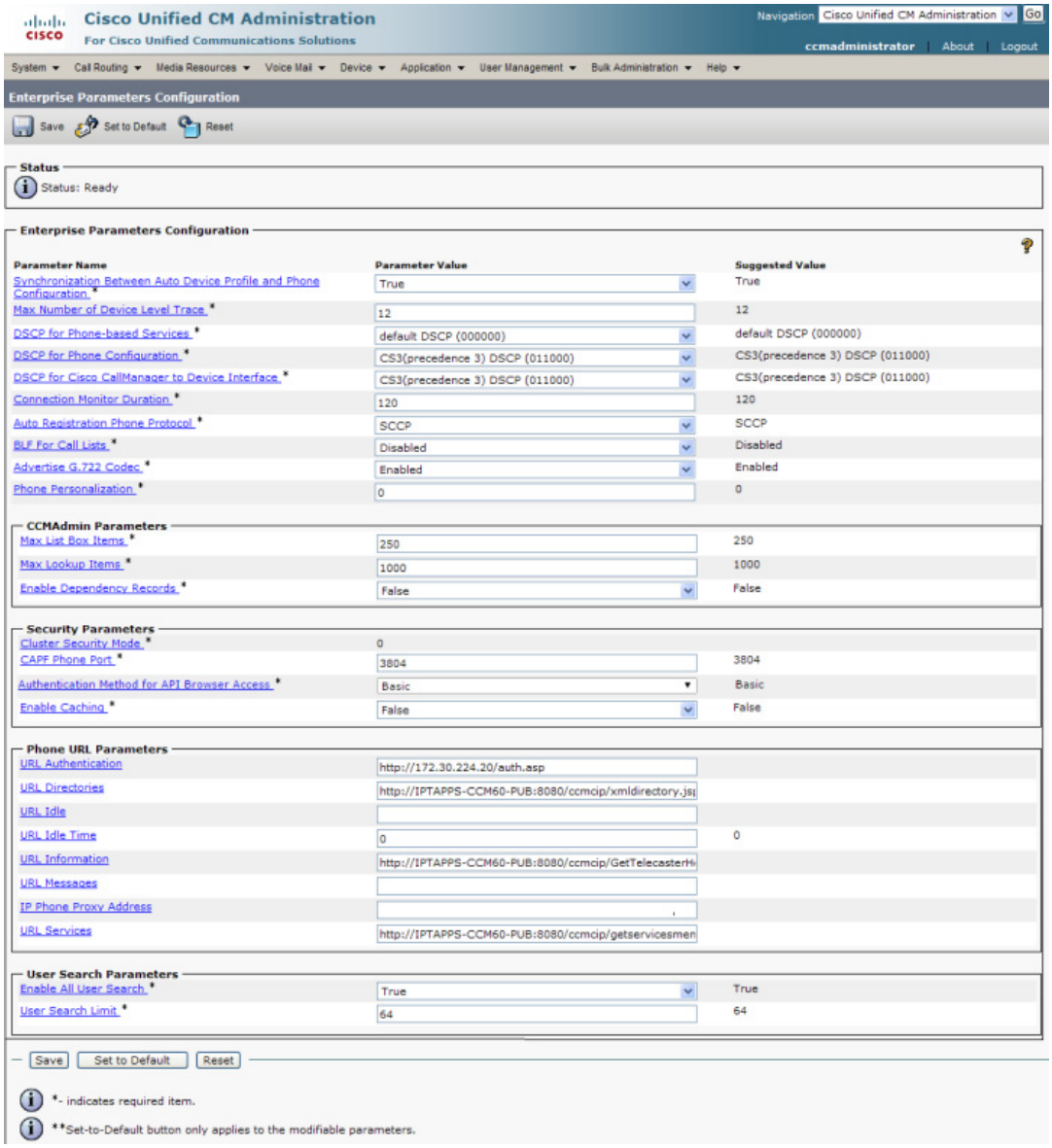
Note You must reboot your phones for the new authentication URL to take affect. See "Reboot Your Phones" on page 2-80.

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.



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

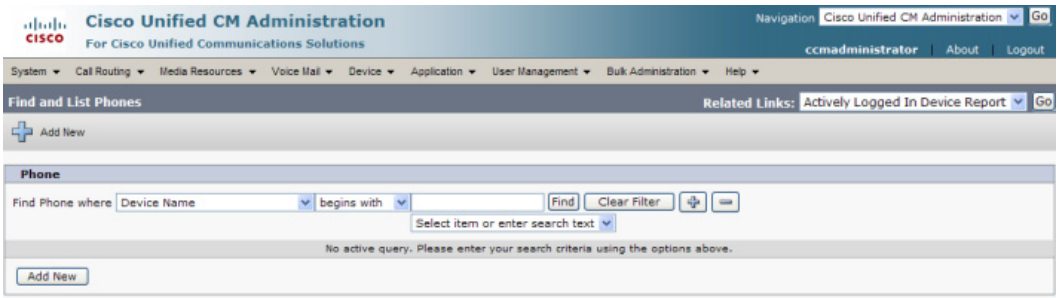
Enabling web access for your phones and setting your authentication URL both require you to reboot your phones. There are many methods that can be used to reboot your phones. Use your best judgment for how and when this can be done in your environment. Some possible options for rebooting your phones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

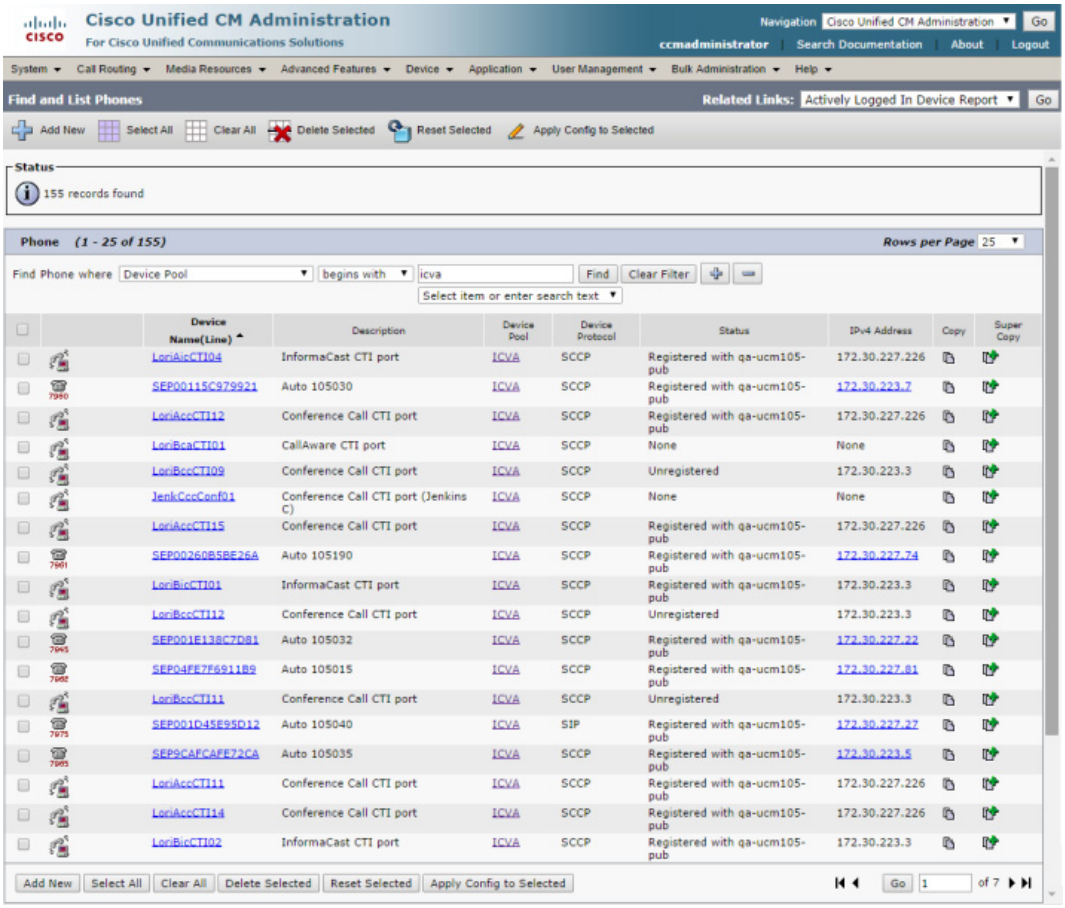
Step 1 Go to **Device** | **Phone**. The Find and List Phones page appears.



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.



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

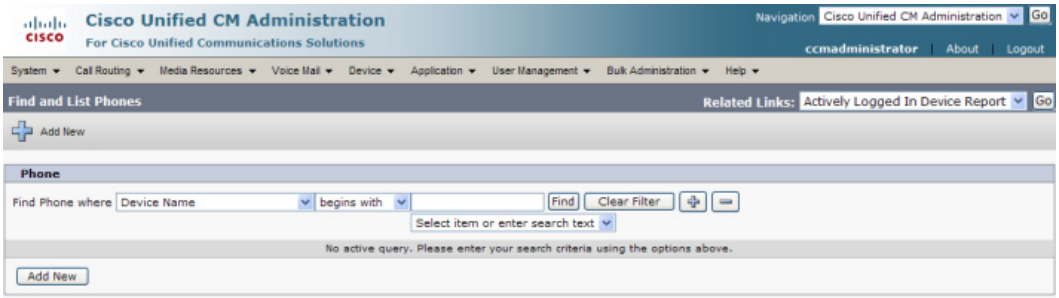
Step 6 Click the **Reset Selected** button. The Device Reset dialog box appears.

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

Test Your Phones

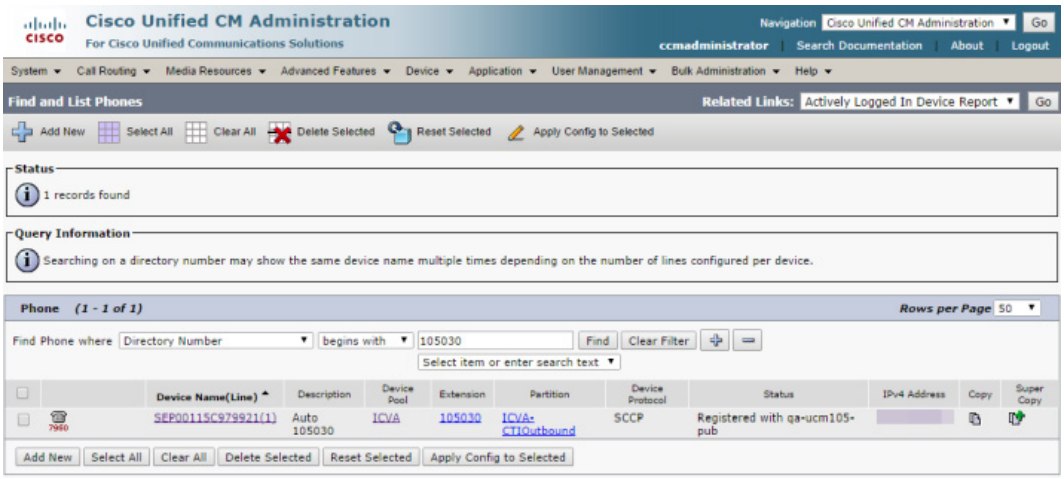
Rebooting your phones should have caused them to pick up their new settings. You can verify their new settings through a web browser.

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

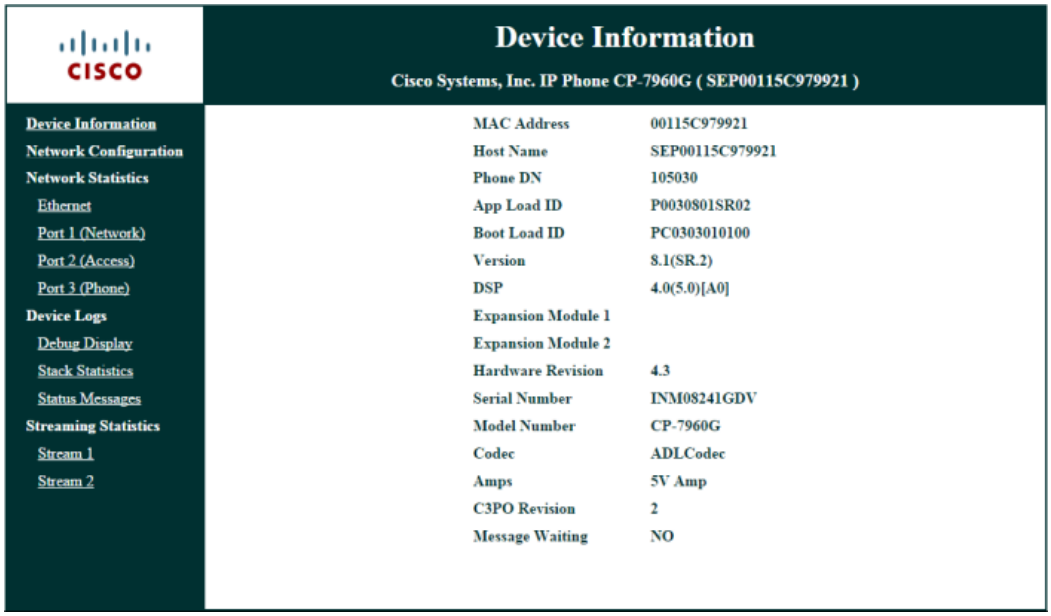


Step 2 Use the dropdown menus and fields to filter for a phone that should have picked up your new settings.

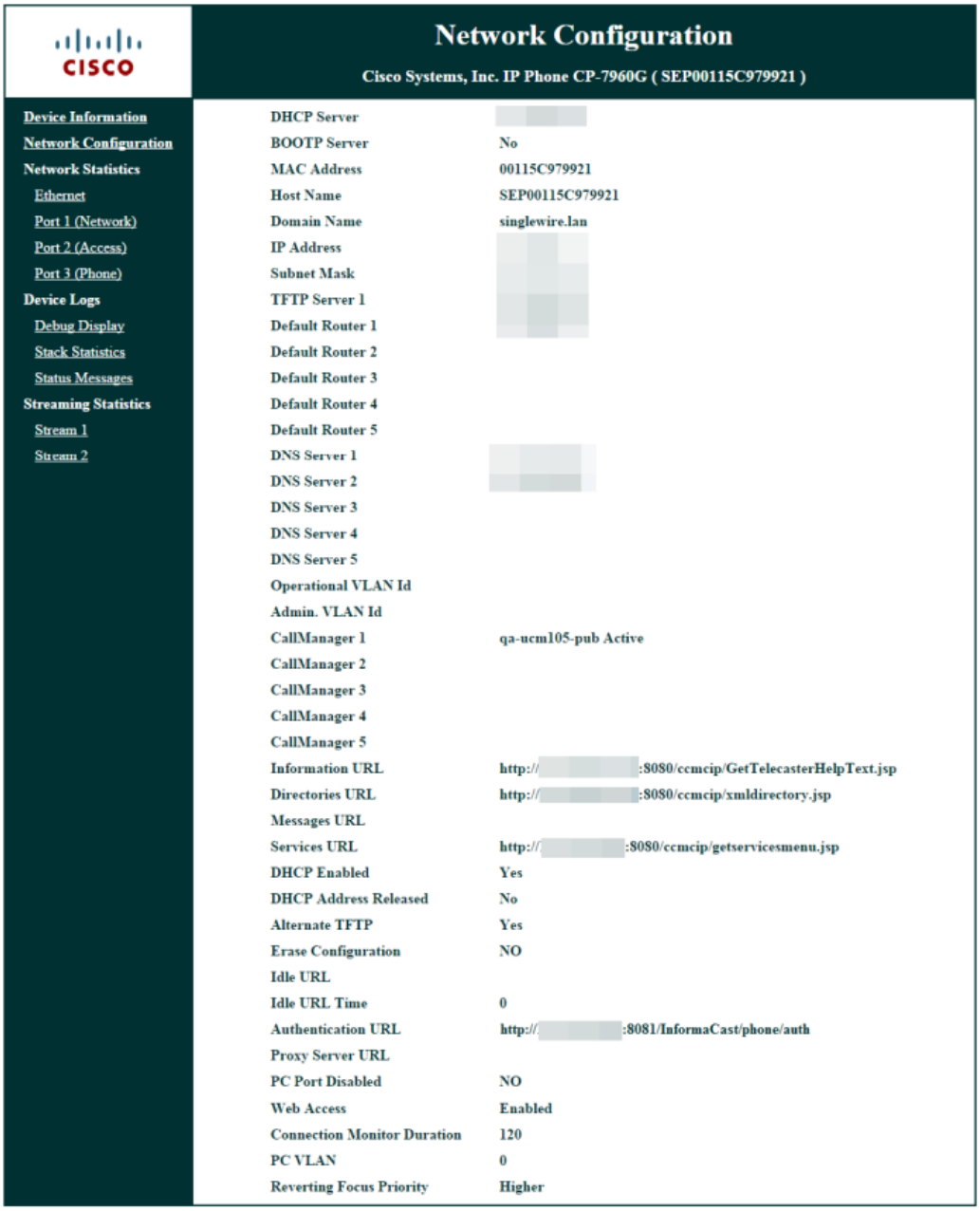
Step 3 Click the **Find** button. The Find and List Phones page refreshes with your search results.



Step 4 Click the **IP address** link in the IPv4 Address column. The Device Information page should open in a new window/tab. If 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 2-70 for more information).



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



Step 6 Scroll down the page until you come to Authentication URL. It should list the IP address you entered in the **URL Authentication** field in Step 4 on page 2-78. If it does not, see "Set Your Authentication URL" on page 2-77.

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

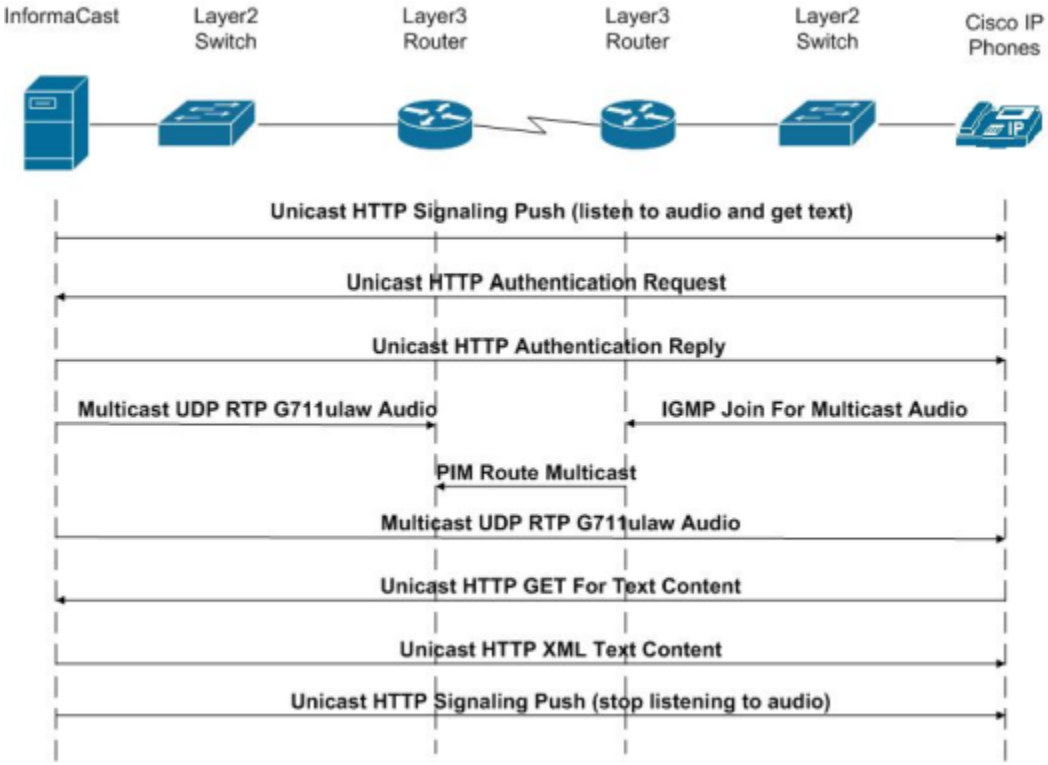
Multicast must be configured in order for InformaCast broadcasts to properly play on your recipients. The following recommendations can also apply:

- 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.



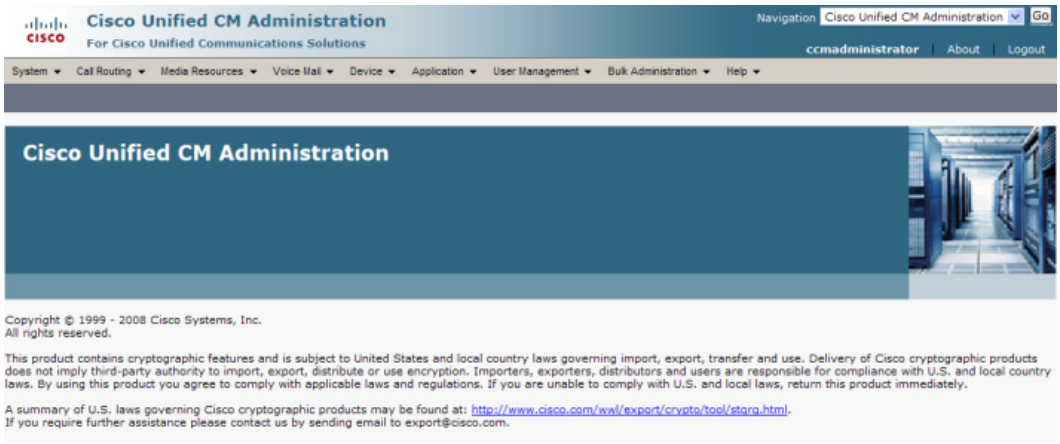
Now that you are familiar with the traffic flow created by InformaCast, you can use a protocol analyzer, such as Wireshark, to sniff the traffic on the network to see that multicast is enabled.

Obtain a Network Traffic Capture

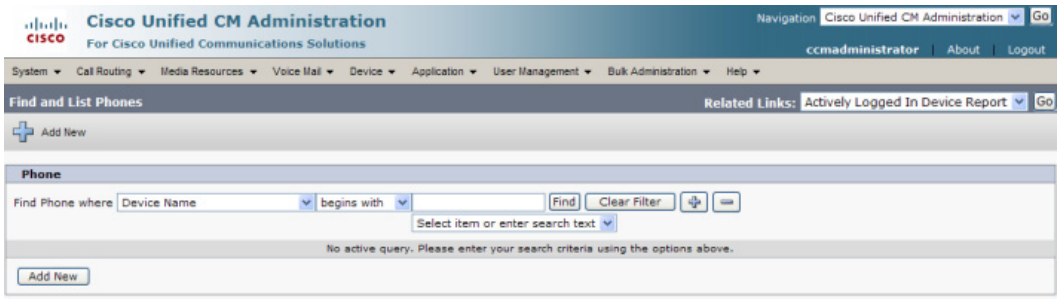
Use the following steps to obtain a network traffic capture from a phone to determine if multicast traffic is routing to that network segment.

Step 1 Download and install a protocol analyzer like Wireshark on a PC that's attached to a phone on your network on which you want to obtain a traffic capture.

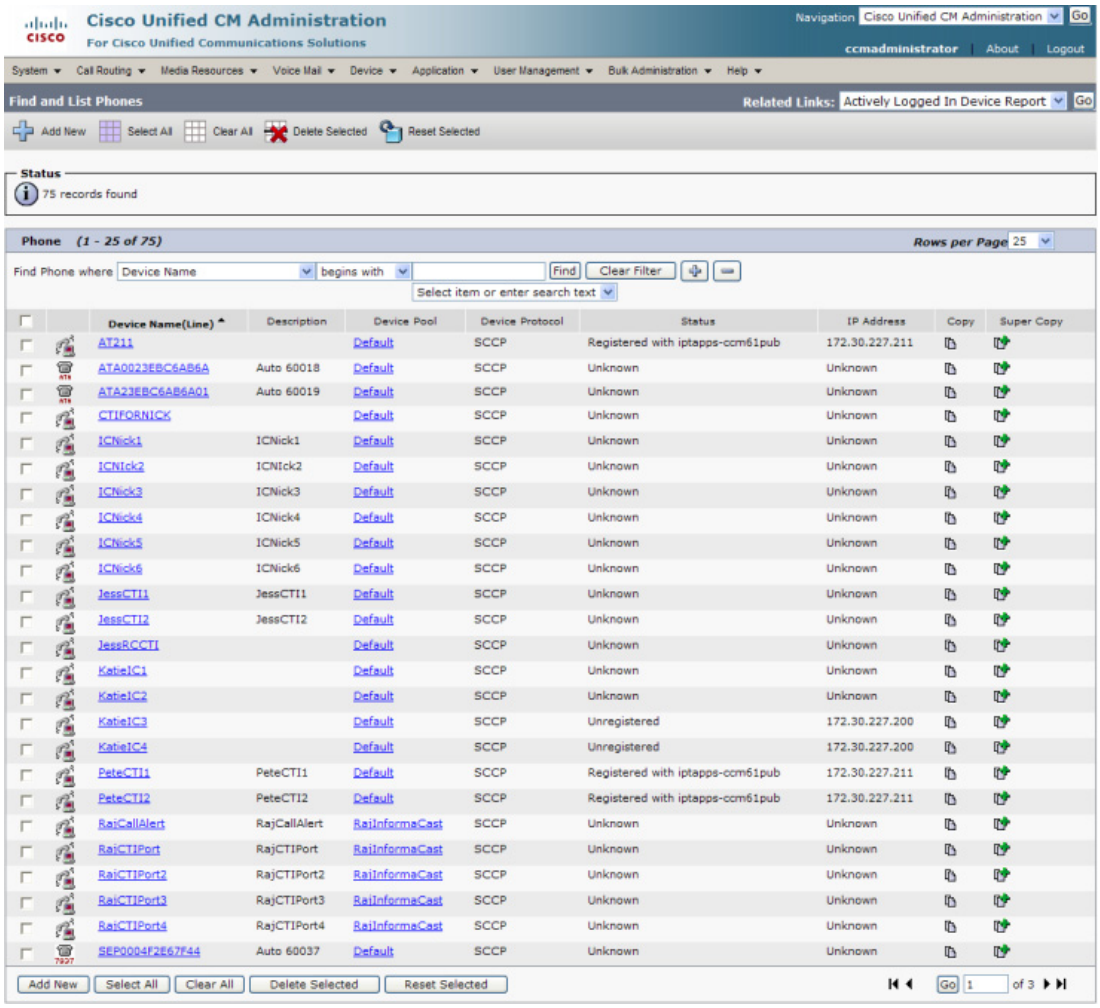
Step 2 Open and log into your Unified Communications Manager's administrative interface. The Cisco Unified CM Administration page appears.



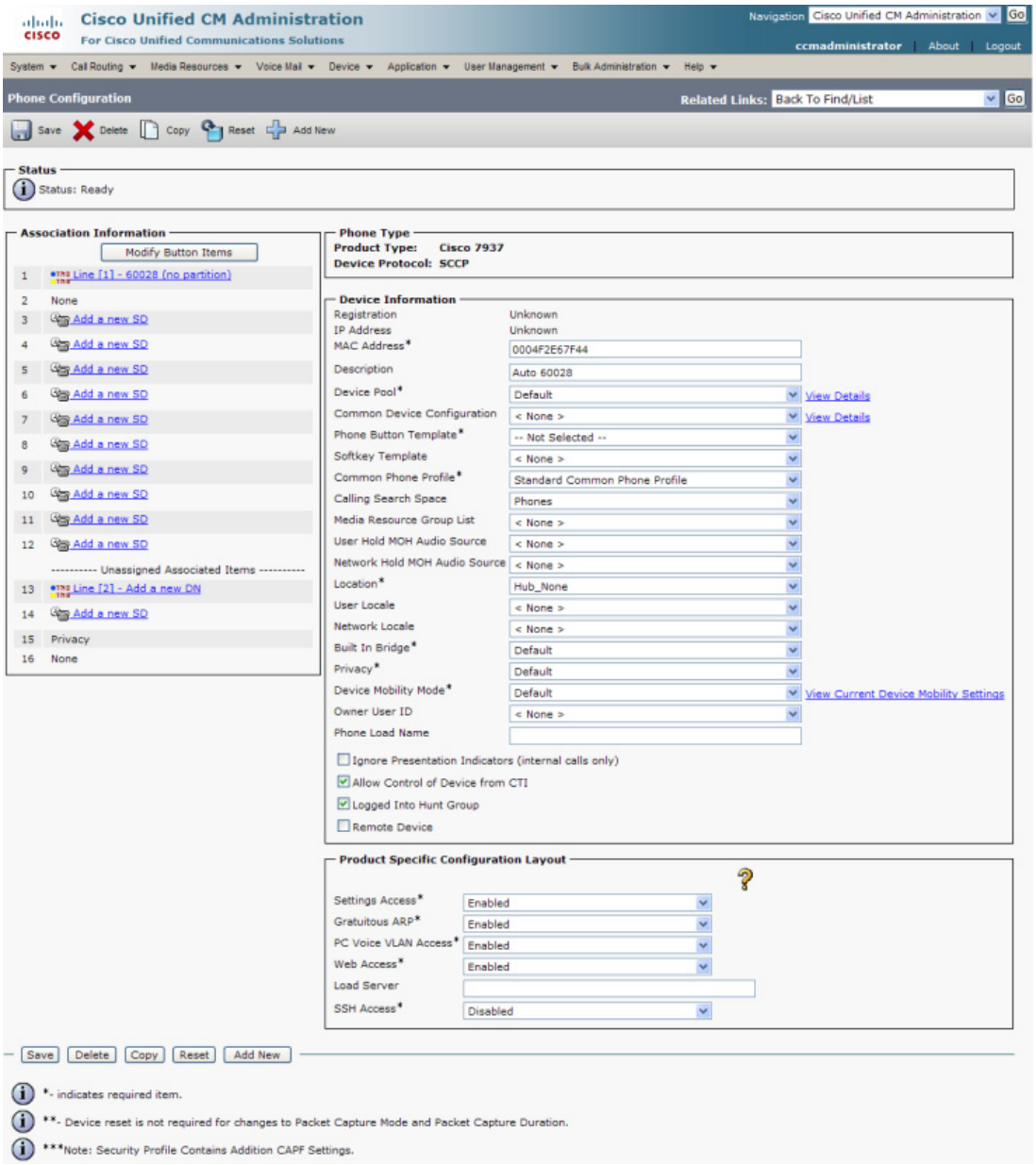
Step 3 Go to **Device** | **Phone**. The Find and List Phone page appears.



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.



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

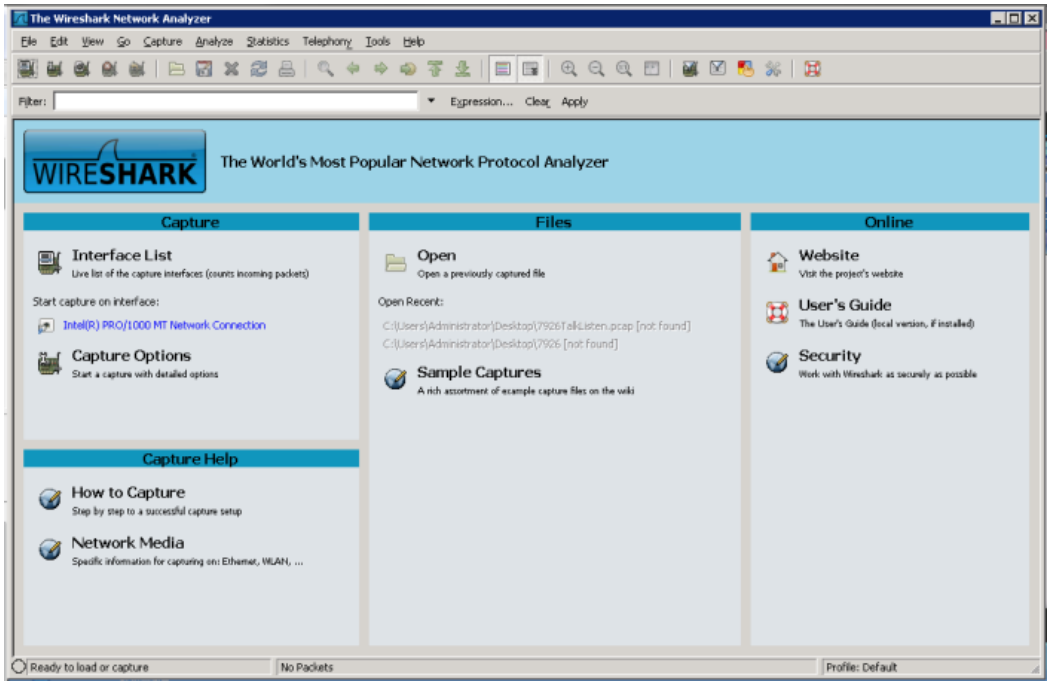


Step 6 Scroll down to the *Product Specific Configuration Layout* area.

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

Step 8 Click the **Reset** button.

Step 9 Start Wireshark. The Wireshark window appears.



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

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

Read a Network Traffic Capture

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

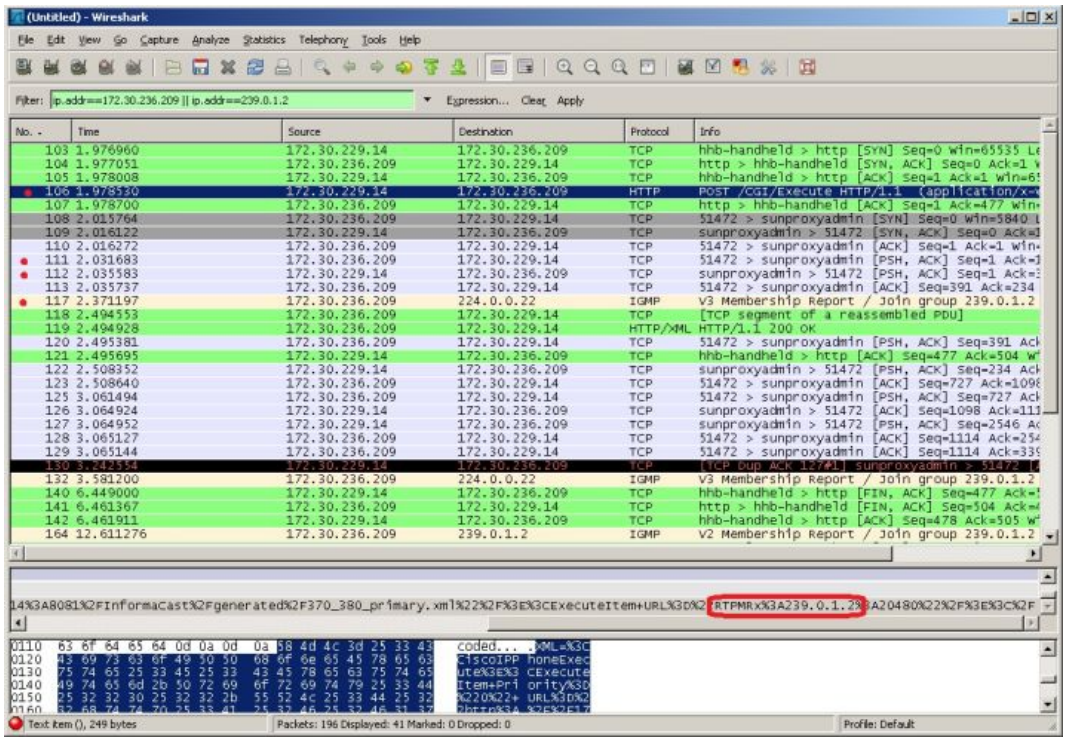
- A unicast HTTP command from InformaCast to the recipient to join the multicast group
- Successful authentication
- An IGMP join from the recipient to the multicast group
- A multicast audio stream

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

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

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

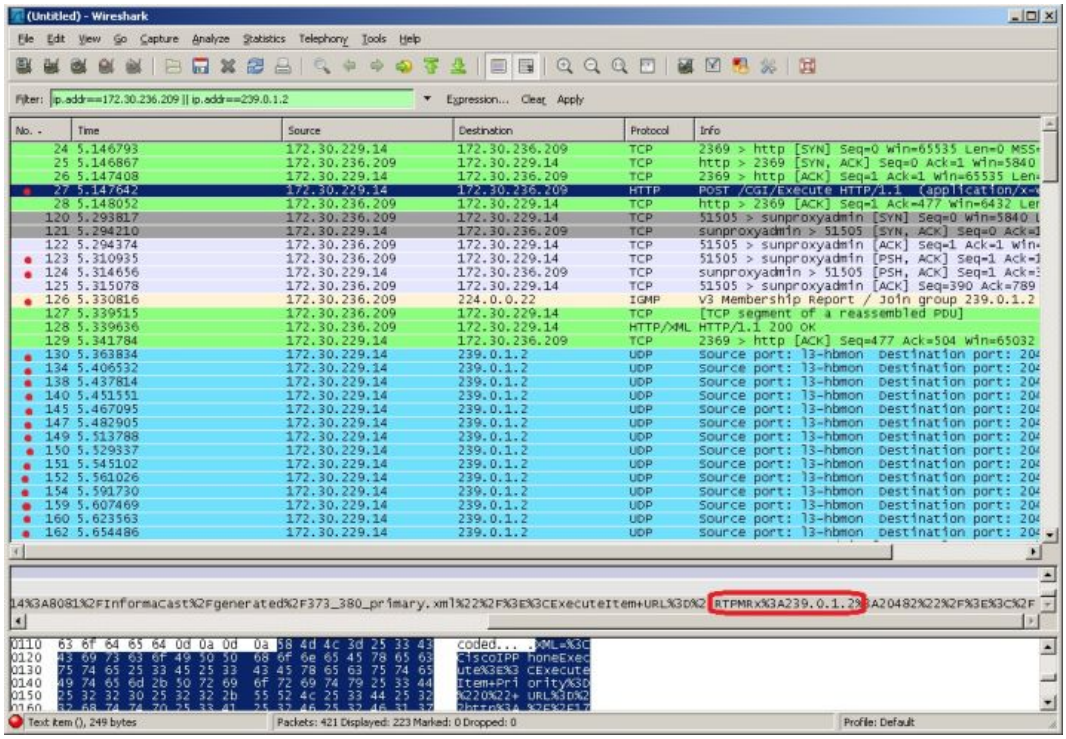
Each of the things to look for are marked with red in the following graphic.



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

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

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

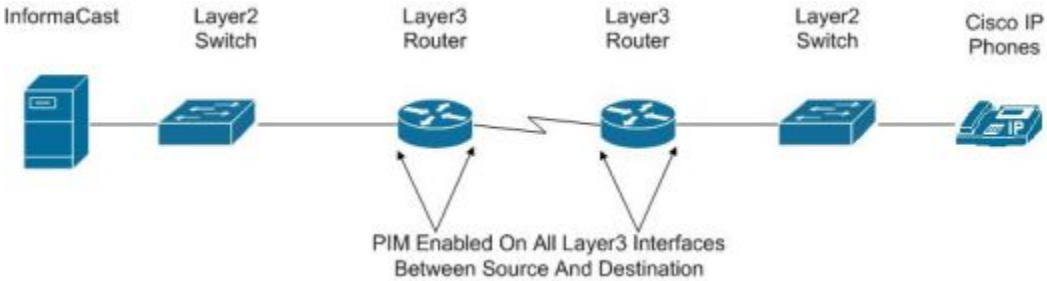


If multicast isn't working, troubleshoot the problems singly by frame(s). Work with your network administrator to configure multicast appropriately.

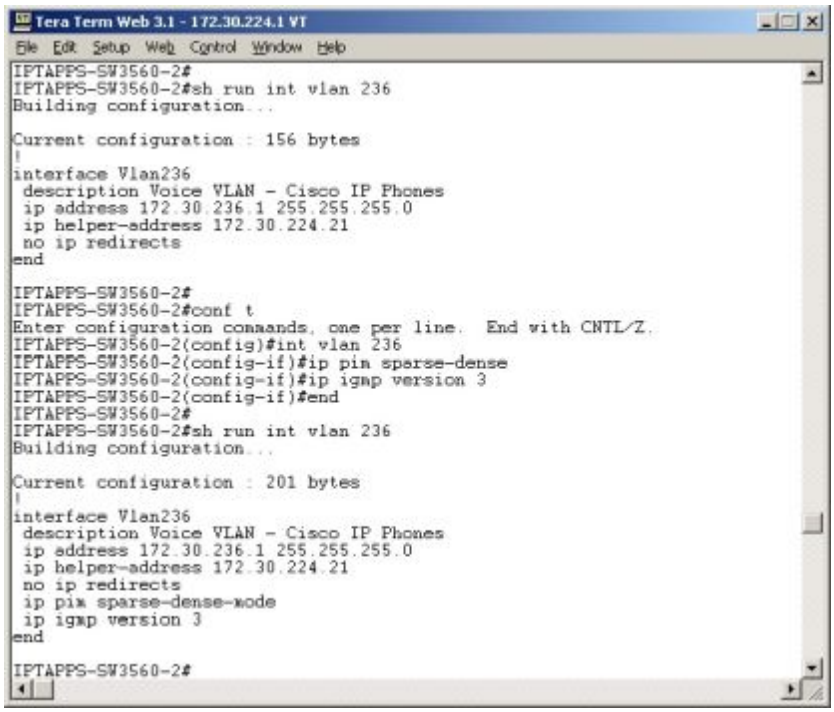
Verify PIM is Configured on All Layer 3 Interfaces

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

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



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



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

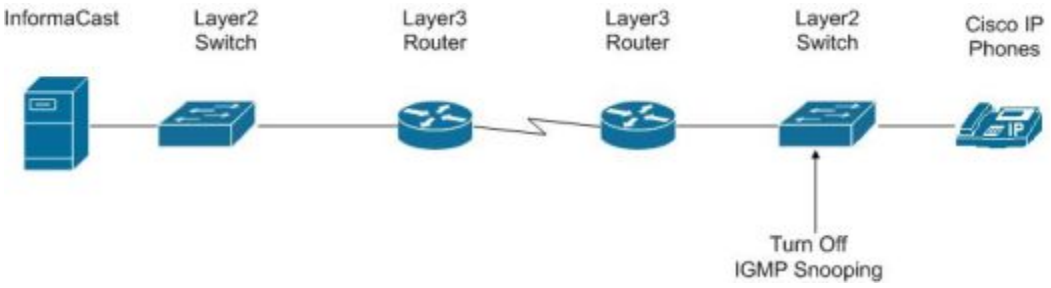
Verify your MPLS Provider Routes Multicast

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

For WAN links where your circuit provider will not route your multicast, you can use GRE tunnels, which carry your multicast traffic from the location where InformaCast is located to its recipients. The only traffic that needs to traverse these GRE tunnels is the multicast traffic you might want to route. The tunnels do not need to create a full mesh between sites; they only need to be configured from the hub location to the spoke location(s). Please see Cisco's sample configuration for multicasting over a generic routing encapsulation (GRE) tunnel for details.

Test Whether IGMP Snooping is Interrupting Multicast

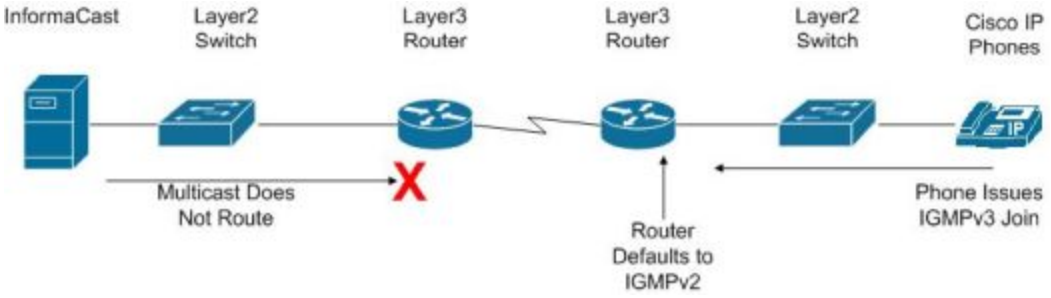
IGMP snooping has been seen to cause issues with Layer 2 switches. For this reason, if there are issues receiving the multicast audio stream at the phones, it would be worth testing if turning off IGMP snooping on the switches where phones are connected solves the problem. The following graphic illustrates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

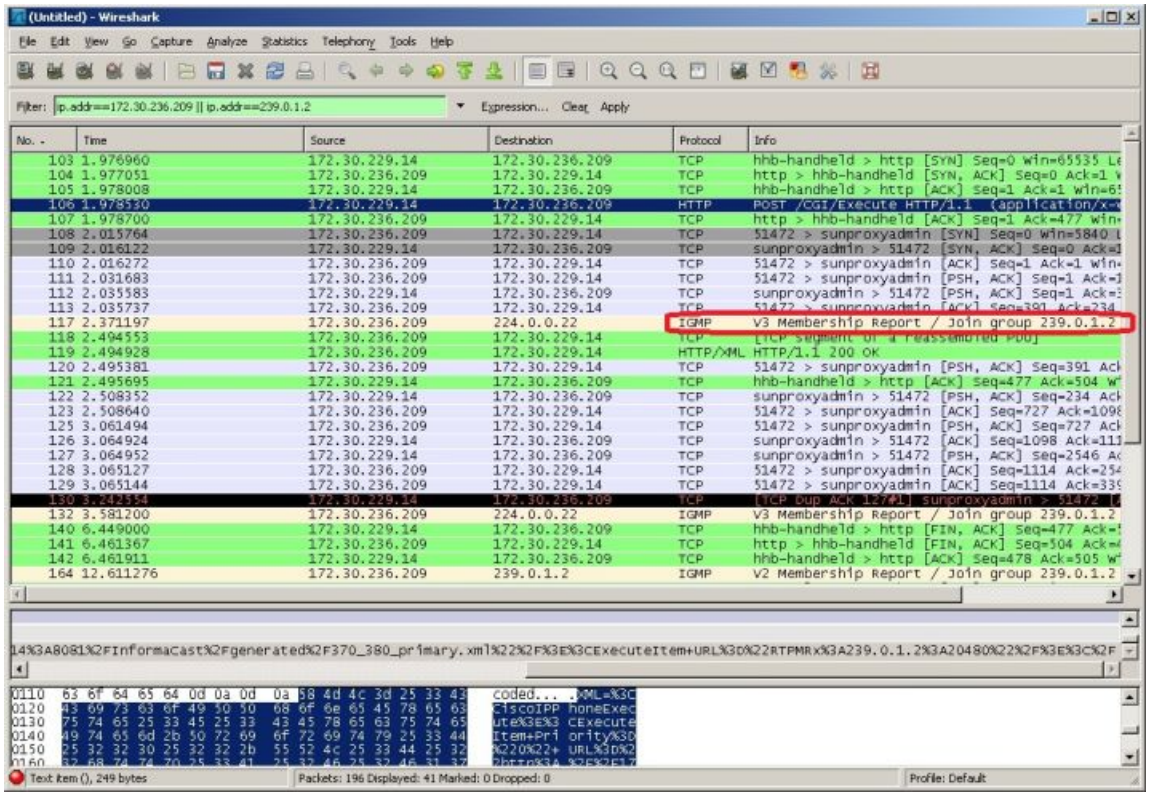
Ensure IGMPv3 is Enabled for Newer Phone Models

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.

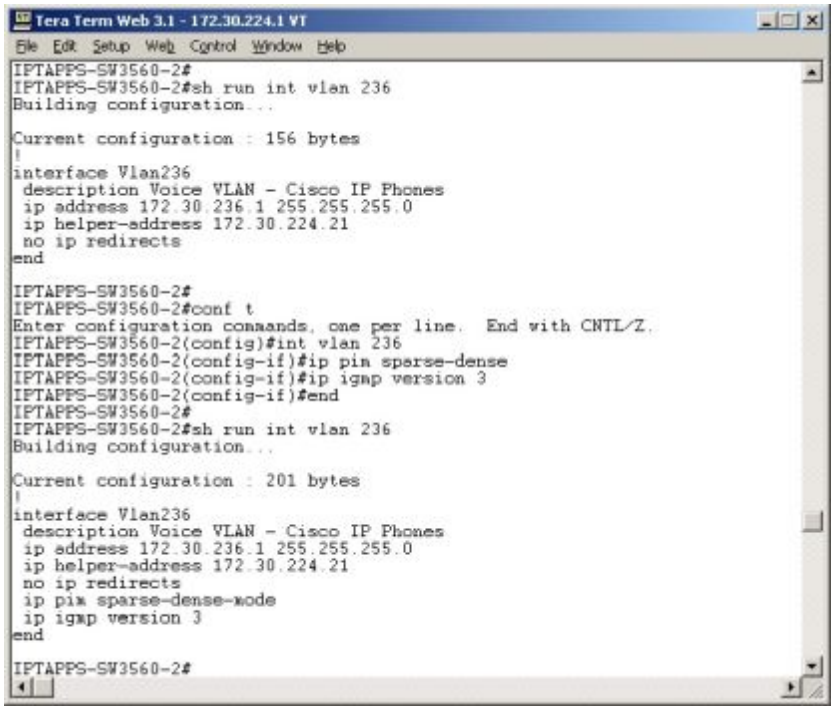


To verify if your phone(s) are using IGMPv3, you can take a network traffic capture using a protocol analyzer like Wireshark (see "Verify Multicast with a Network Traffic Capture" on page 2-86). In the capture, the phone will issue an IGMP join to listen to the multicast audio.

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



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



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

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 "Deploy InformaCast" on page 2-6). Do not continue with configuring InformaCast until you have completed these steps.

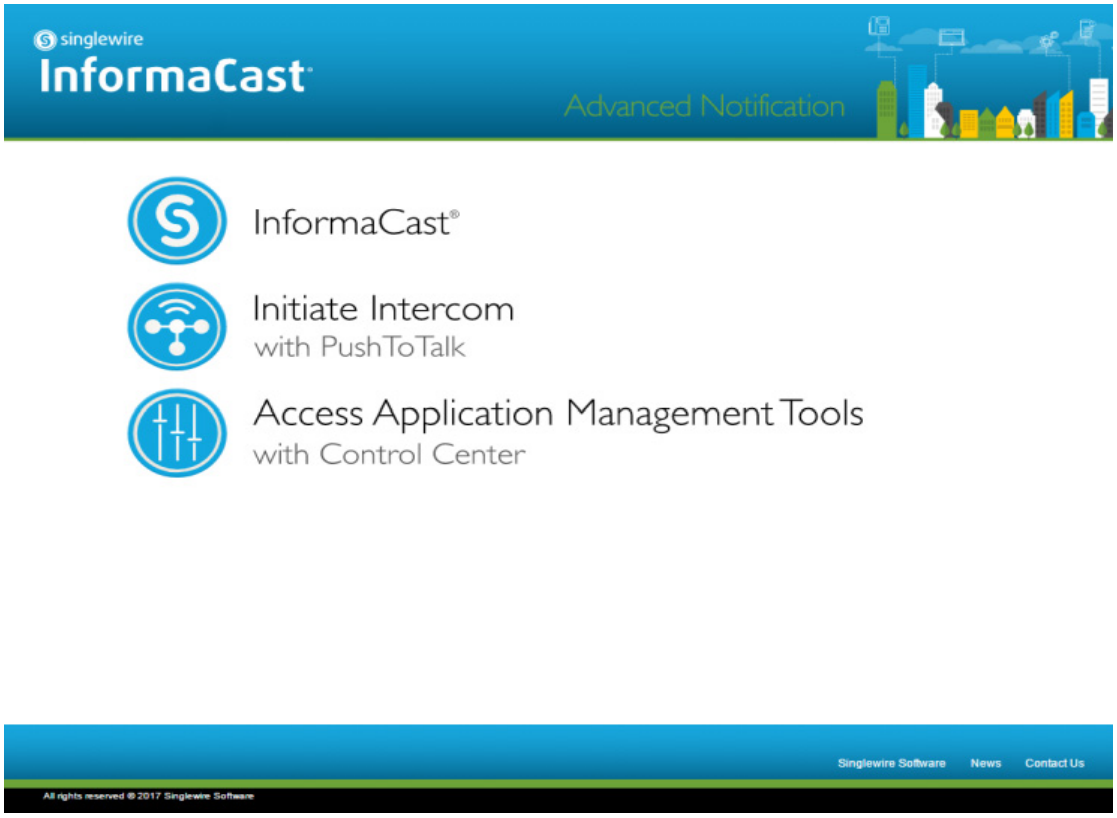
InformaCast's web interface—where you will set up your InformaCast environment, e.g. recipient groups, SIP functionality, DialCasts, etc.—is accessed through the Singlewire landing page. When first accessing InformaCast, you will want to:

- "Log into InformaCast for the First Time" on page 3-2
- "View Your License Key" on page 3-6

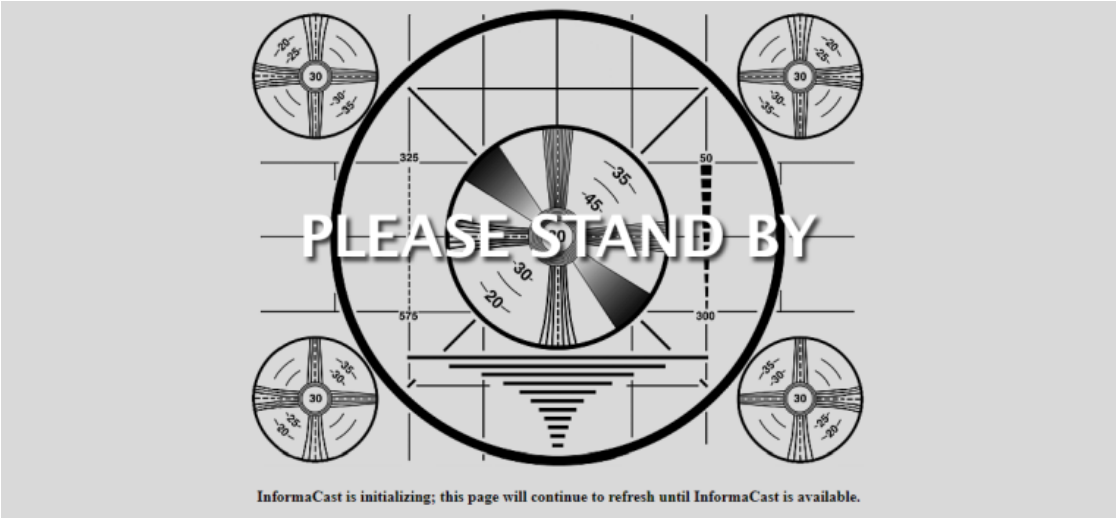
Log into InformaCast for the First Time

Once the Virtual Appliance is started and you've accessed the Singlewire landing 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 landing page appears.

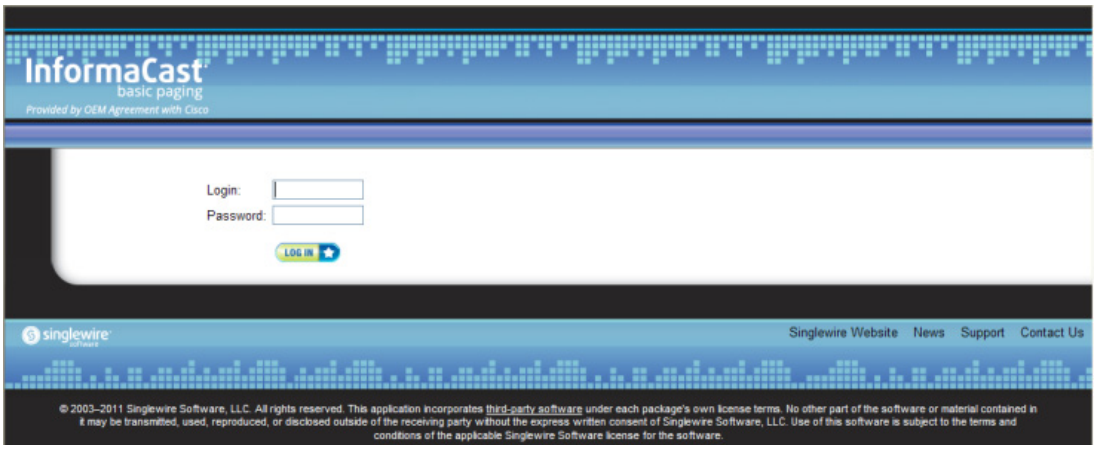


Step 2 Click the **InformaCast** link. A separate tab/window opens to InformaCast's Startup page. Depending on your system, there may be a delay of several minutes while InformaCast initializes.



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.

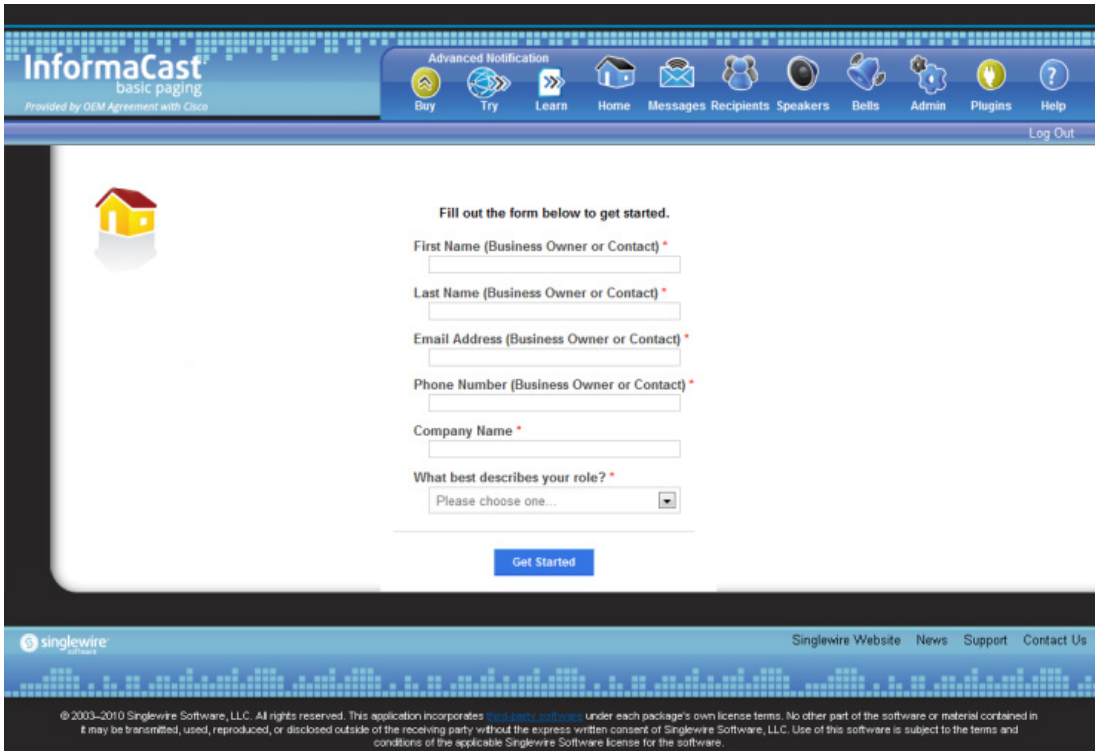


Step 3 Enter **admin** in the **Login** field. The **Login** field is case sensitive.

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

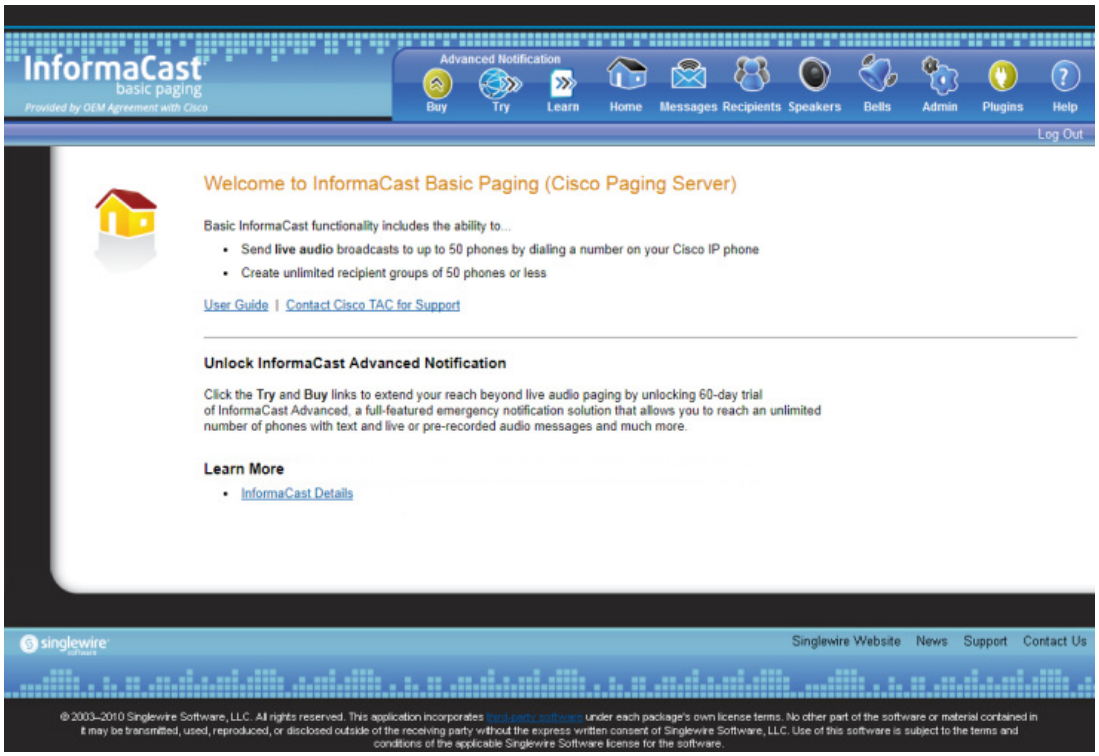
Note These are your default credentials. "Change the Application Administrator's Password" on page 6-2 will show you how to change your credentials, which will make your InformaCast installation more secure.

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.

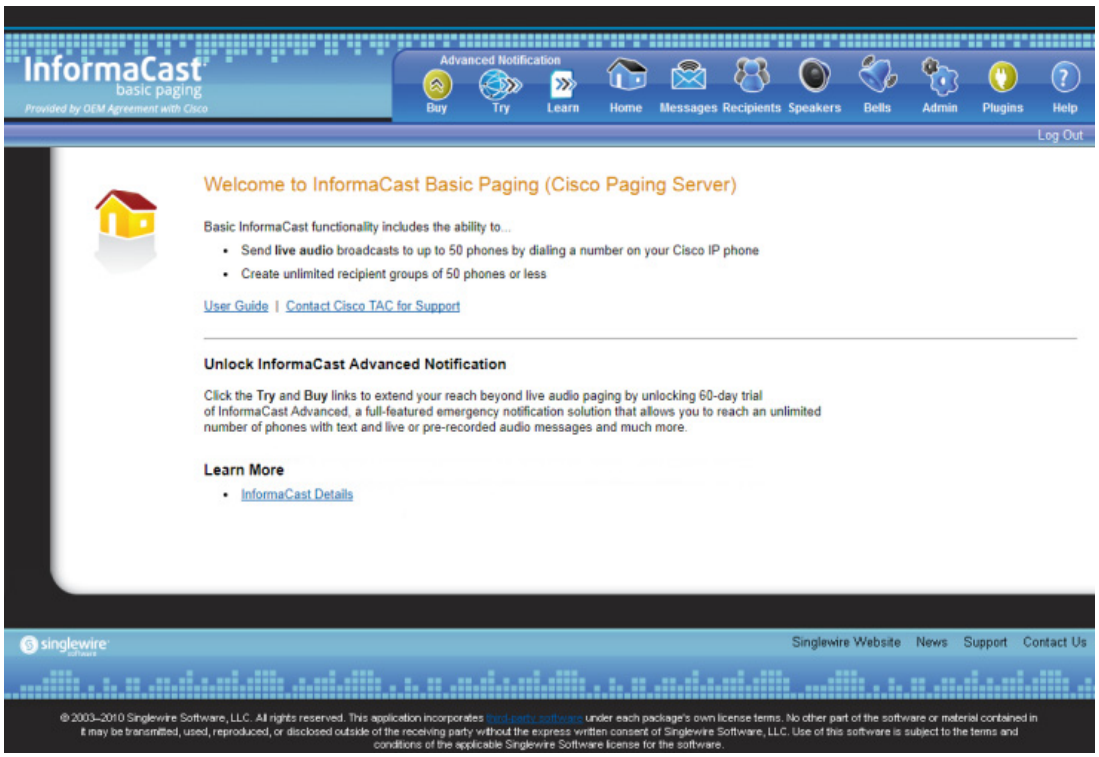


Note Completing this form is required in order to access InformaCast's functionality.

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:

Configure Host Trust

Similarly to a web browser, the Java virtual machine (JVM) on which InformaCast runs has a trust store, which is a collection of root certificates from trusted Certificate Authorities (CAs) like DigiCert or Symantec, that it uses to establish trust with hosts with which it talks via SSL or TLS. The InformaCast trust store is seeded with root certificates included by Oracle in the JVM.

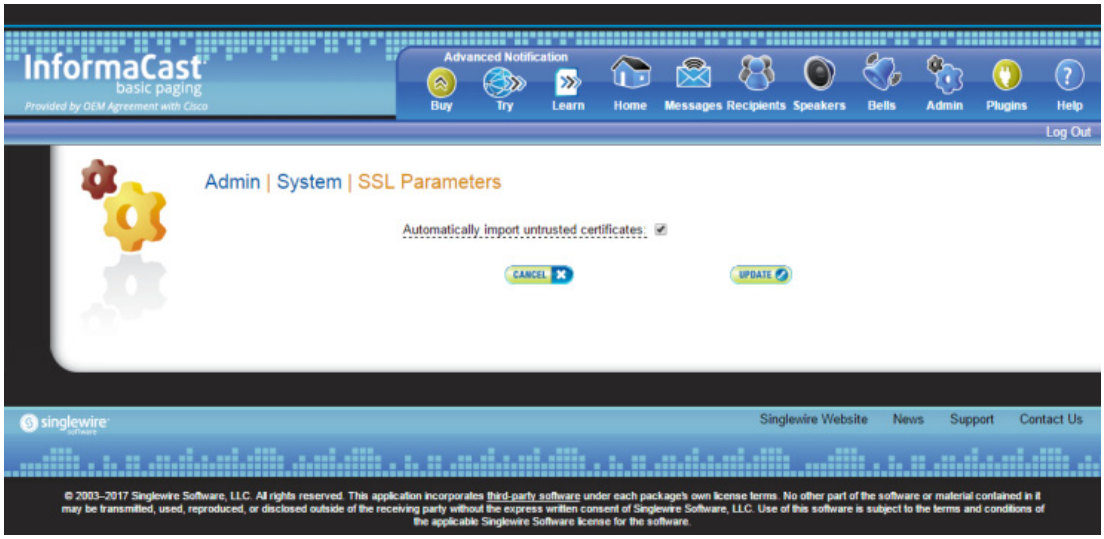
On the SSL Parameters page (**Admin | System | SSL Parameters**), you can configure InformaCast to blindly trust the hosts with which it communicates, i.e. automatically import all SSL certificates presented to it by other hosts, or you can require InformaCast to validate certificates for all outbound communication via SSL and TLS. If you choose to validate certificates, for each SSL or TLS secured host you connect to, InformaCast will reject connections to that host until you import the certificate that host presents.

There are several areas within InformaCast where certificates can be imported:

- **The Cisco Unified Communications Manager cluster.** You can see which Unified Communications Manager certificates are currently trusted, whether automatic certificate importation is enabled/disabled, and select which certificates should be imported for use in future SSL/TLS communications between InformaCast and Unified Communications Manager.
- **SIP certificates.** SIP functionality is handled separately within InformaCast and unaffected by the SSL Parameters page.

Note InformaCast will only negotiate an SSL session with a host that supports AES cipher suites; negotiation with hosts that support only 3DES will fail.

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



Step 2 Decide how you want InformaCast to interact with hosts during outbound communication via SSL and TLS:

- **Automatically Import SSL Certificates.** Leave the **Automatically import untrusted certificates** checkbox selected. The checkbox is selected by default, and if you were running InformaCast prior to InformaCast 12.0.1, this is how InformaCast worked previously.
- **Manually Import SSL Certificates.** Deselect the **Automatically import untrusted certificates** checkbox. If you deselect this checkbox, you will need to explicitly trust the SSL certificate supplied by your Unified Communications Manager cluster (see "Configure Your Default Unified Communications Manager Cluster" on page 4-3).

Step 3 Click the **Update** button to save your changes (if necessary).

Manage InformaCast's Telephony

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

Configure Your Default Unified Communications Manager Cluster

When configuring InformaCast:

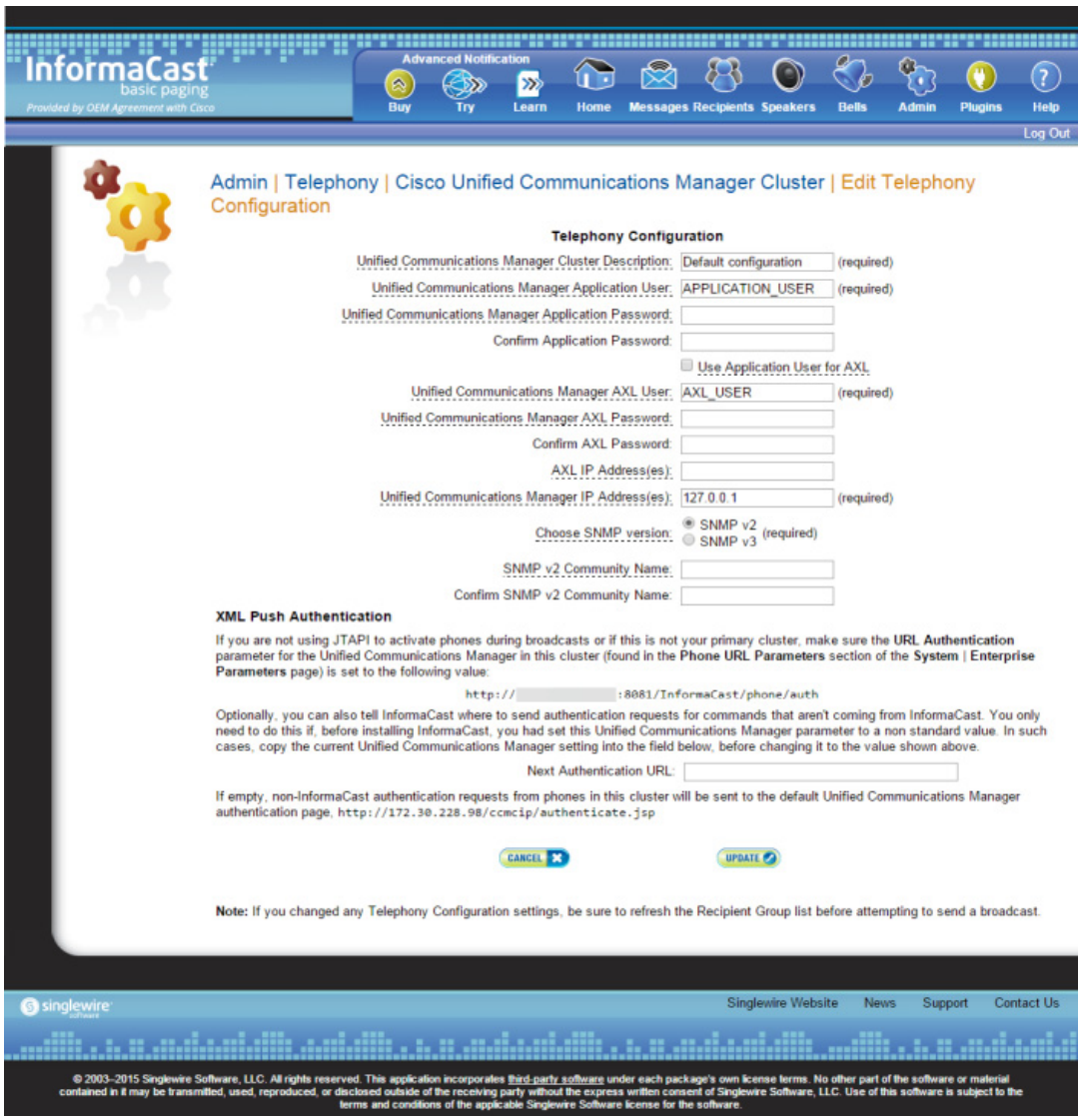
- Basic installations are limited to one cluster; however, Advanced installations can be run with multiple clusters (contact Singlewire for details)
- Neither Cisco nor Singlewire supports combining both Basic and Advanced InformaCast instances

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.

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



Step 3 Change name of your cluster (if necessary) in the **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 2-68).

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 2-68). 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 4-6.

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.

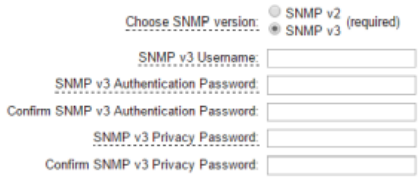
Step 7 Enter your AXL IP address(es) in the **AXL IP Address(es)** field. Separate addresses with commas. If you leave this field blank, InformaCast will attempt to find a server running the AXL service among those servers running the CallManager service.

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.

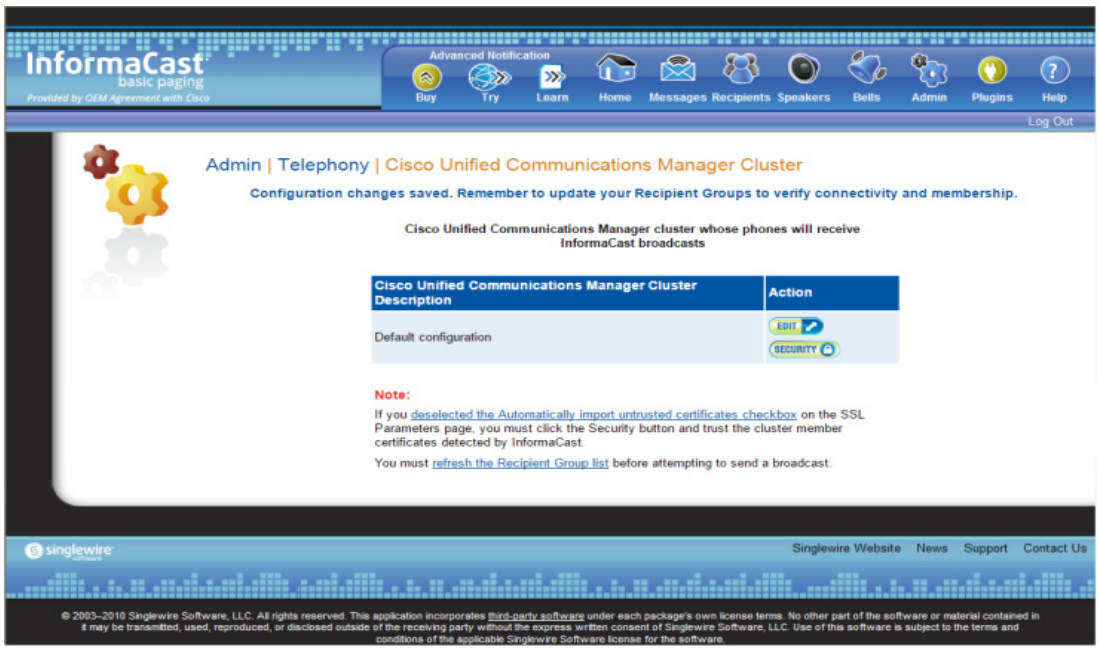


Step 10 Enter the correct information depending on your version of SNMP:

- **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 2-46. 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 2-48.

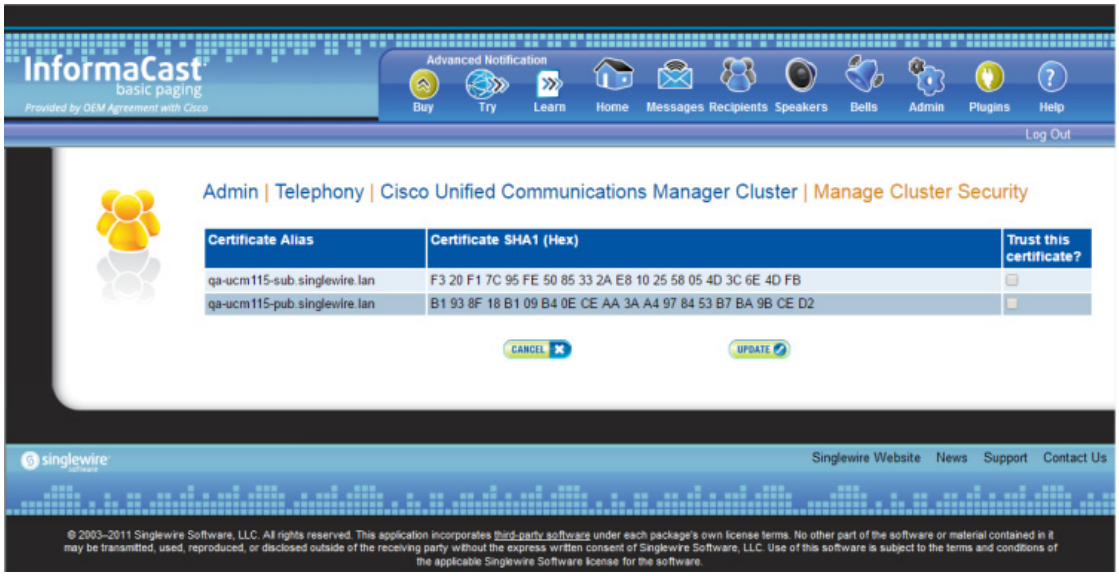
Step 11 Enter the original value of Unified Communications Manager's **URL Authentication** field in the **Next Authentication URL** field. You made note of this in Step 3 on page 2-78.

Step 12 Click the **Update** button. You will be redirected to the Cisco Unified Communications Manager Cluster page.



Note If you deselected the **Automatically import untrusted certificates** checkbox on the SSL Parameters page, you must click the **Security** button and trust the cluster members' certificates detected by InformaCast. Proceed to Step 13 on page 4-9. If you left the **Automatically import untrusted certificates** checkbox selected, skip to Step 15 on page 4-9.

Step 13 Click the **Security** button in the Action column of the table. The Manage Cluster Security page appears.



The table on the Manage Cluster Security page has all of the cluster members' hostnames that InformaCast has been able to detect and successfully contact, along with their downloaded SSL certificates. When the automatic import of certificates is enabled, they will be automatically stored in the trust store that InformaCast uses for SSL/TLS communication with Unified Communications Manager. Since you have deselected the **Automatically import untrusted certificates** checkbox, you will have to choose which of the certificates should be imported into InformaCast's trust store.

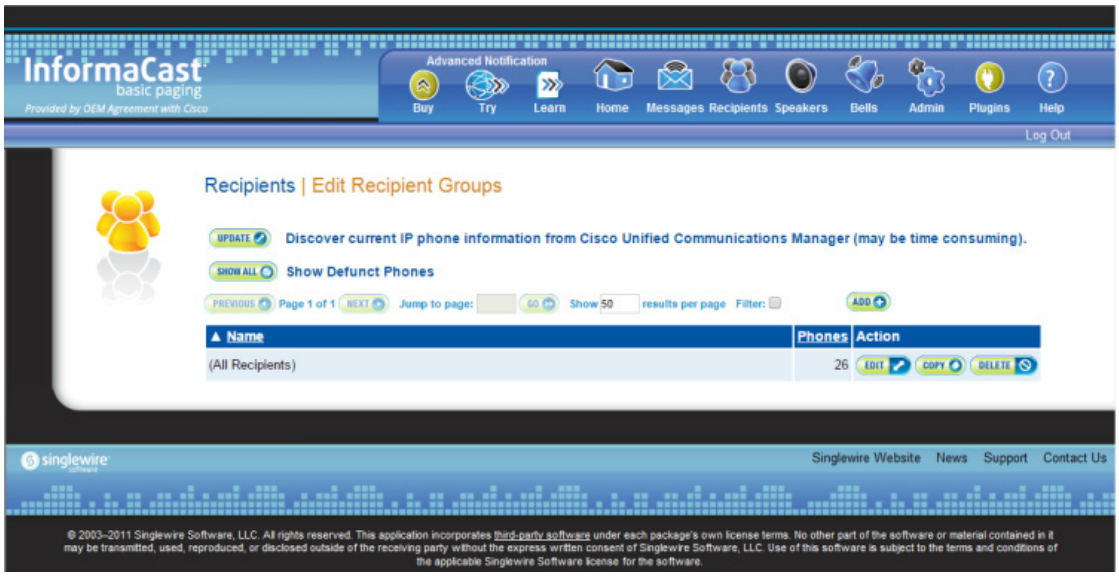
Step 14 Verify that the SHA1 fingerprints displayed in the table match the SHA1 fingerprints of the actual certificates provided by the Unified Communications Manager cluster members and click the **Trust this certificate?** checkbox for each match.

Note Viewing certificate SHA1 fingerprints can be done through a browser and the steps for viewing them are browser dependent. For example, in Chrome, go to **Settings** | **More tools** | **Developer tools** | **Security** tab | **View certificate** button | **Details** tab.

Step 15 Click the **Update** button to save these certificates in InformaCast's trust store. By default, InformaCast stores its Unified Communications Manager certificates in /usr/local/singlewire/InformaCast/certs/cucm.bcf.

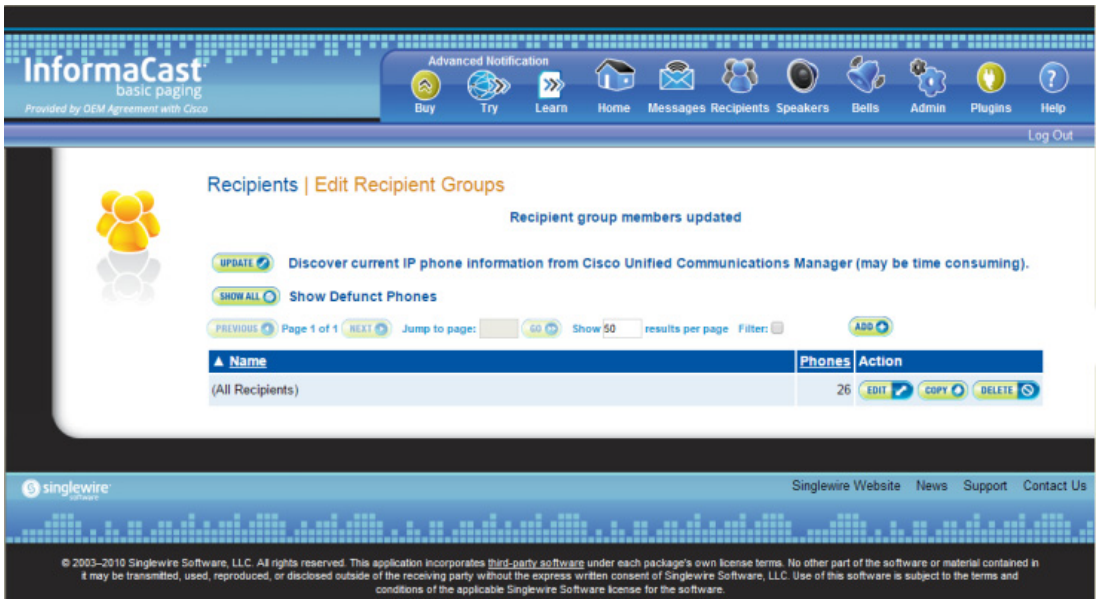
Note If your Unified Communications Manager cluster members change, you will need to return to the Manage Cluster Security page and mark the changed member as trusted.

Step 16 Click the **refresh the Recipient Group list** link. You will be redirected to the Edit Recipient Groups page.



Step 17 Click the **Update** button to refresh InformaCast's information pertaining to recipient groups. You will be redirected to the Discover Recipient Groups page.

Step 18 Click the **Update** button again. You will be redirected to the Edit Recipient Groups page that will now have a note that recipient group members have been updated.



Edit Your Default Cluster

Once you've configured your default 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.

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

Step 3 Edit the information for that cluster.

Step 4 Click the **Update** button.

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

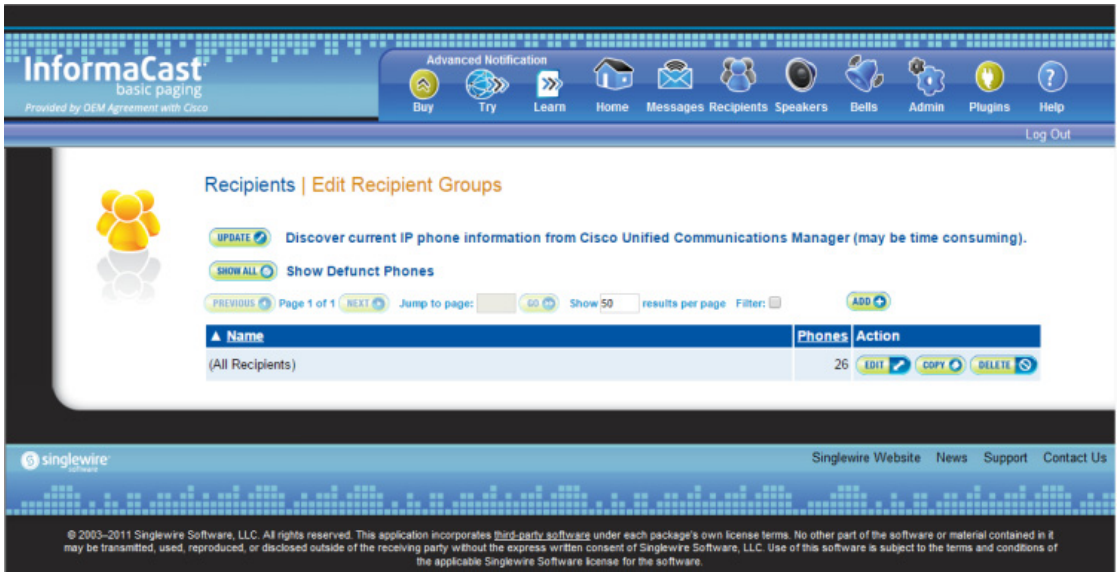
Once you've added recipients by selecting multiple existing recipient groups and/or constructing rules, you can also create exclusions, which allow recipients that had been included in a recipient group by a certain rule or through a recipient group to now be excluded.

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

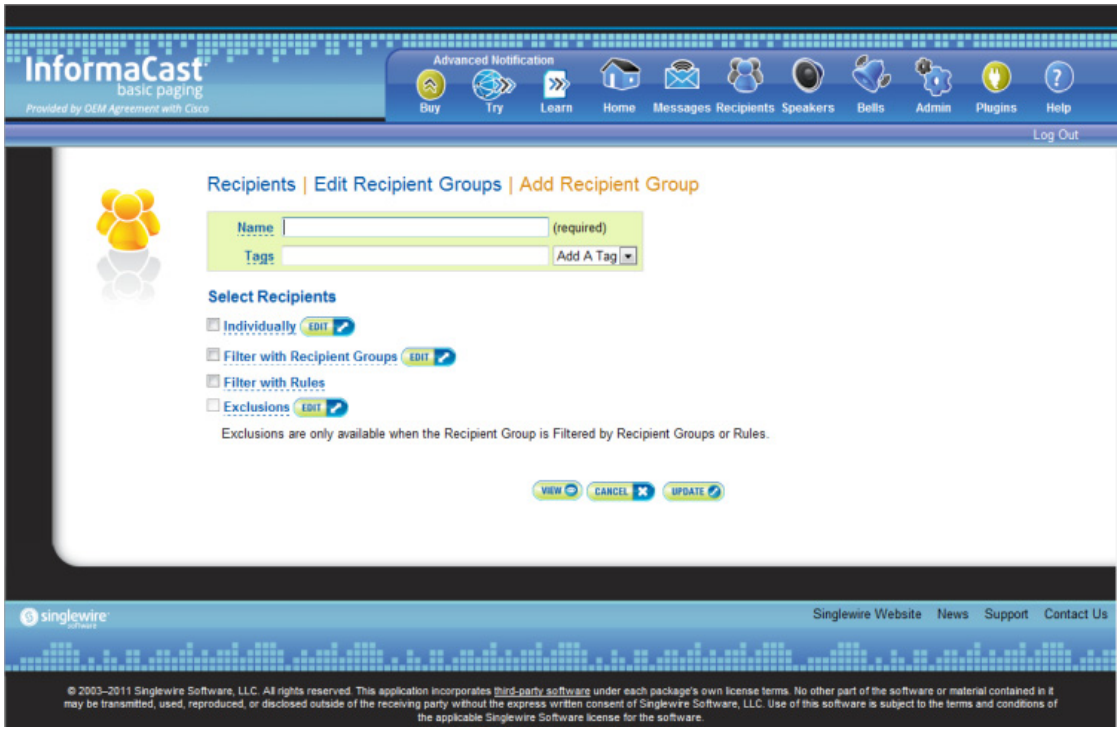
Add a Recipient Group

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.



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



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

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

Note You can also create recipient group tags by going to **Recipients** | **Edit Tags** (see "Configure Recipient Group Tags" on page 4-39). 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:

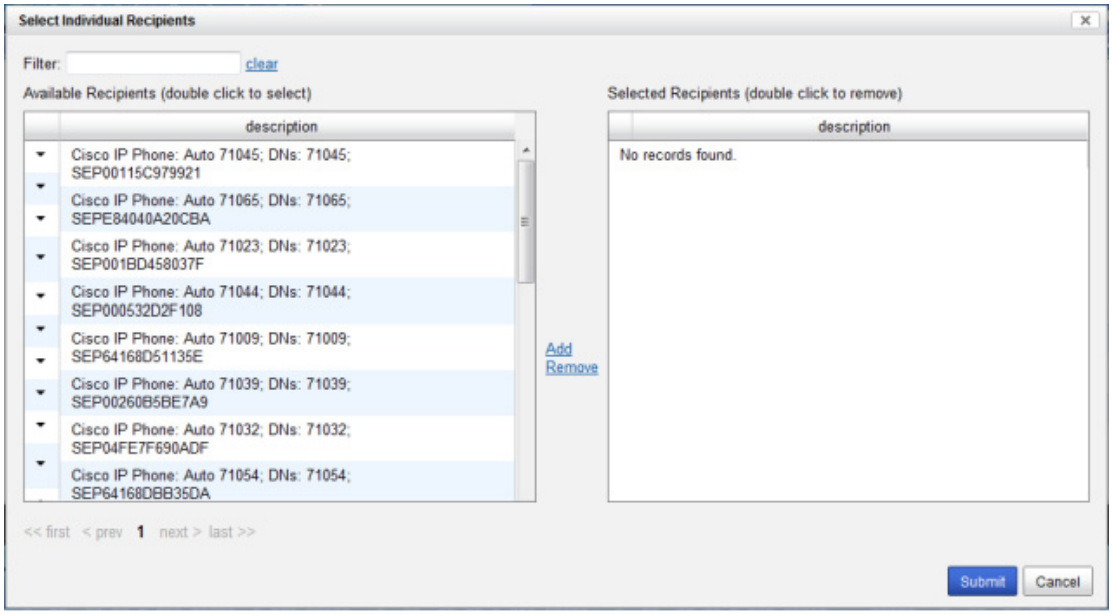
- If you have chosen to select recipients, continue with Step 2 in "Create a Recipient Group by Selecting Individual Recipients" on page 4-15.
- If you have chosen to select existing recipient groups, continue with Step 2 in "Create a Recipient Group by Selecting Multiple, Existing Recipient Groups" on page 4-17.
- If you have chosen to make rules, continue with Step 2 in "Create a Recipient Group Using Rules" on page 4-20.

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 4-13.

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:

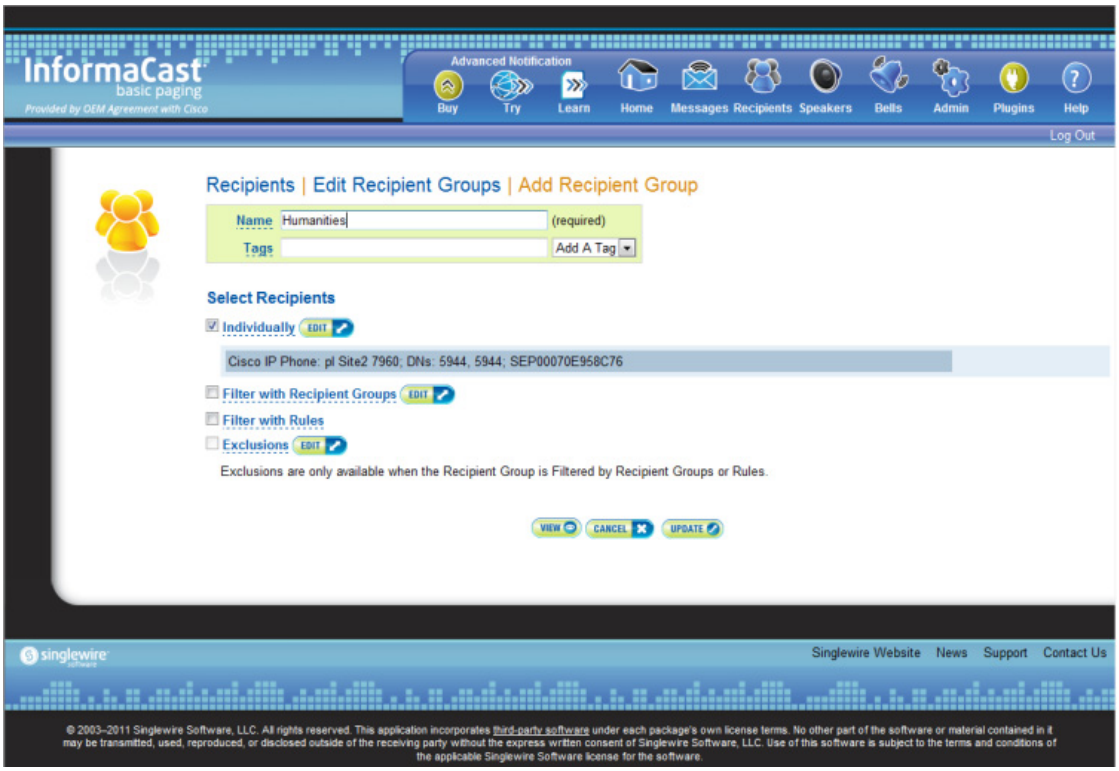
Matching Parameter	Description
Communications Manager Calling Search Space	Phones that match the specified search space.[a]
Communications Manager Cluster Name	Phones that match the specified Unified Communications Manager cluster name.
Communications Manager Device Pool	Phones that match the specified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

Matching Parameter	Description
Description	Recipients that match the supplied description value. This is often a useful grouping tool because you have control over the description of the recipients in your system, so you can set up your descriptions in ways that facilitate grouping. The text you enter will be compared against the Device Description entries of phones registered with your 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.
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 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 4-17 and/or "Create a Recipient Group Using Rules" on page 4-20.

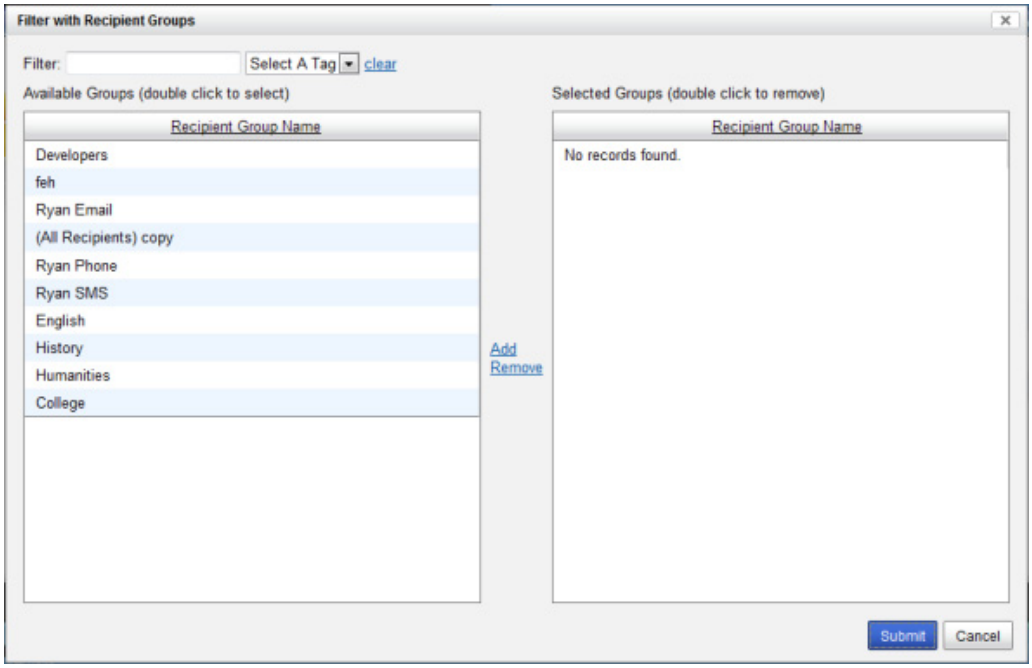
Create a Recipient Group by Selecting Multiple, Existing Recipient Groups

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 4-13.

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

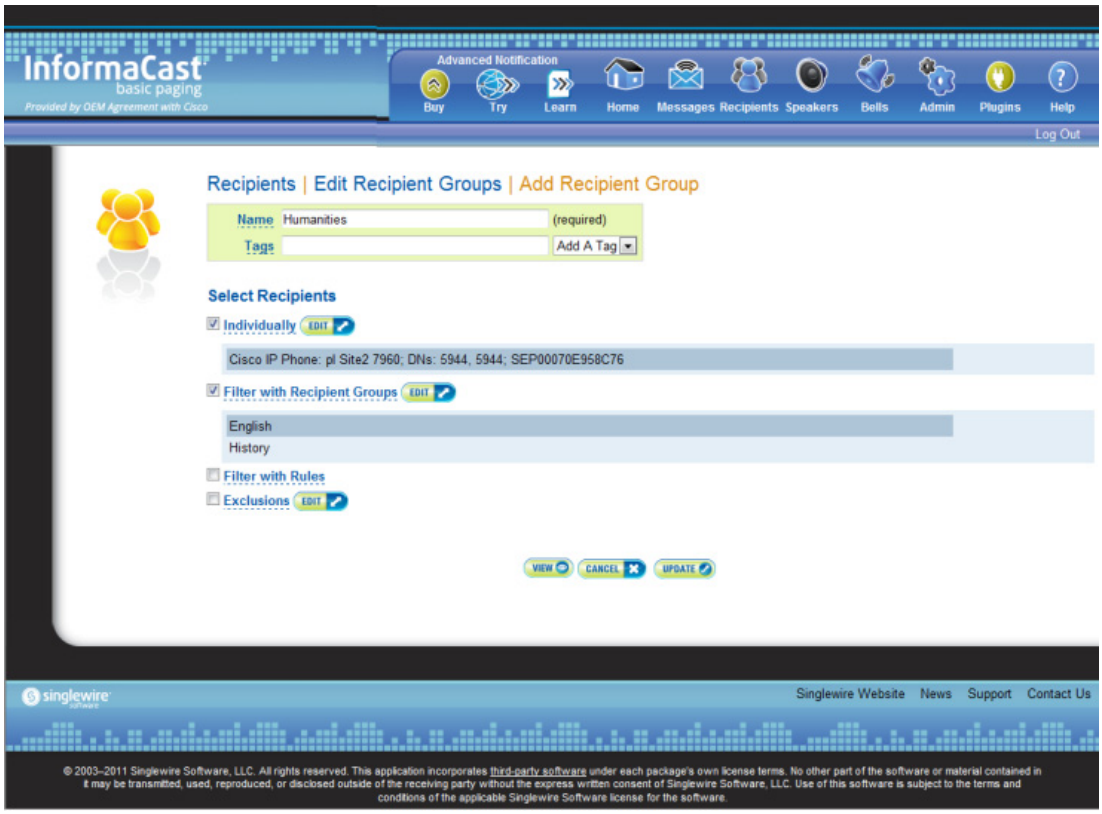


Step 3 Filter the results of your existing recipient groups by entering partial or full recipient group names in the **Filter** field or by selecting a particular recipient group tag from the **Select a Tag** dropdown menu.

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

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

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



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

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

If you would like to further refine your recipient group, continue with "Create a Recipient Group by Selecting Individual Recipients" on page 4-15, "Create a Recipient Group Using Rules" on page 4-20, and/or "Add Exclusions to a Recipient Group" on page 4-23.

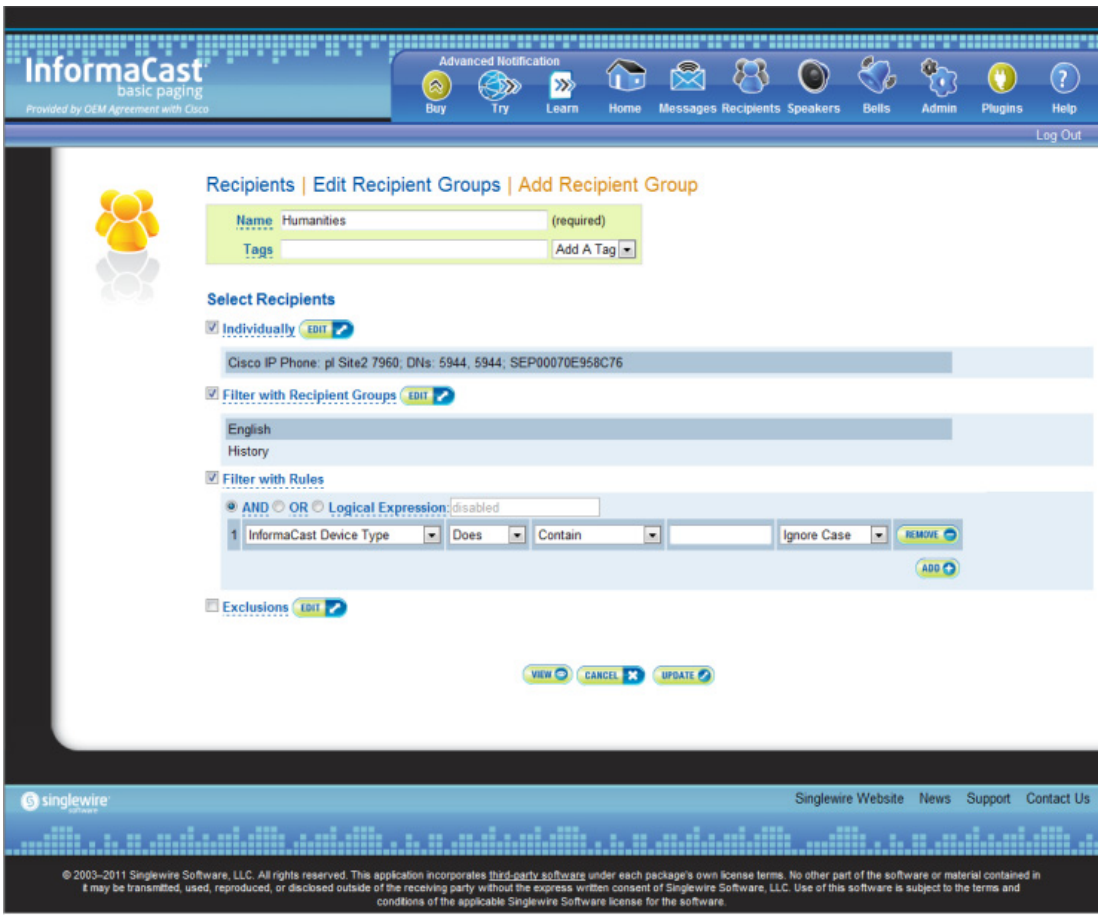
Create a Recipient Group Using Rules

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 4-17).

Step 1 Complete the steps in "Add a Recipient Group" on page 4-13.

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



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

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

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

Matching Parameter	Description
Communications Manager Calling Search Space	Phones that match (or don't match) the specified search space.[a]
Communications Manager Cluster Name	Phones that match (or don't match) the specified 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	Recipients that match (or don't match) the supplied description value. This is often a useful grouping tool because you have control over the description of the recipients in your system, so you can set up your descriptions in ways that facilitate grouping. The text you enter will be compared against the Device Description entries of phones registered with your Unified Communications Manager server Any recipients whose descriptions match with the rule you've specified will be considered part of the recipient group.
Directory Numbers	Phones that match (or don't match) the supplied phone number(s) assigned to them in the 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 4-42 for more information about this approach.
InformaCast Device Type	Recipients that match (or don't match) in their functionality as an IP phone.
Location	Recipients that match (or don't match) the supplied location value.
MAC Address	Recipients that match (or don't match) the supplied network hardware address of the recipient, which is guaranteed to be unique across your network.
Name	Recipients that match (or don't match) the supplied name. Like the **Description** parameter, you have control over names, so they may useful for grouping, but should be concise.
Partition Names	Phones that match (or don't match) the supplied dial plan partition assigned to each directory number, a.k.a. phone number, assigned to an IP phone in 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 4-42 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 4-15, "Create a Recipient Group by Selecting Multiple, Existing Recipient Groups" on page 4-17, and/or "Add Exclusions to a Recipient Group" on page 4-23.

Add Exclusions to a Recipient Group

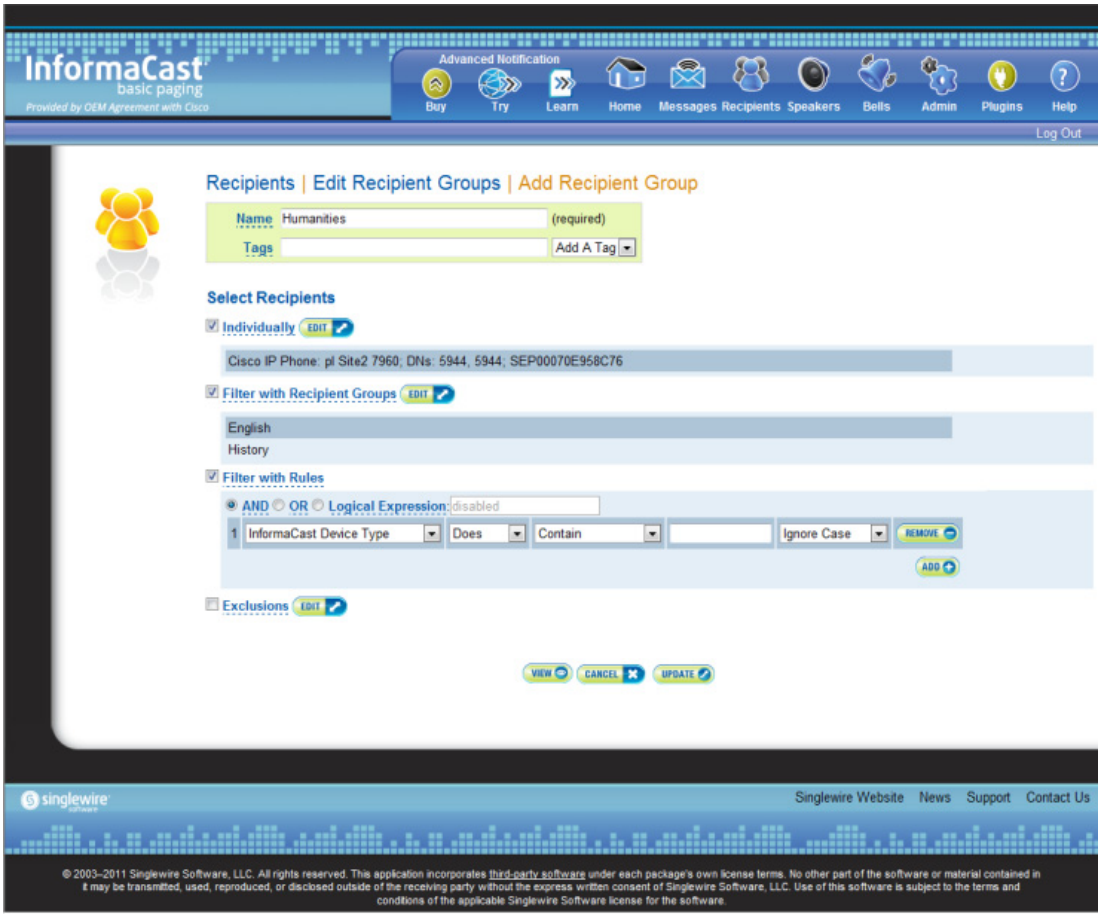
Use the steps in the following section to add exclusions to a recipient group, which allow recipients that had been included in a recipient group by a certain rule or through a recipient group to now be excluded.

Step 1 Complete the steps in "Add a Recipient Group" on page 4-13.

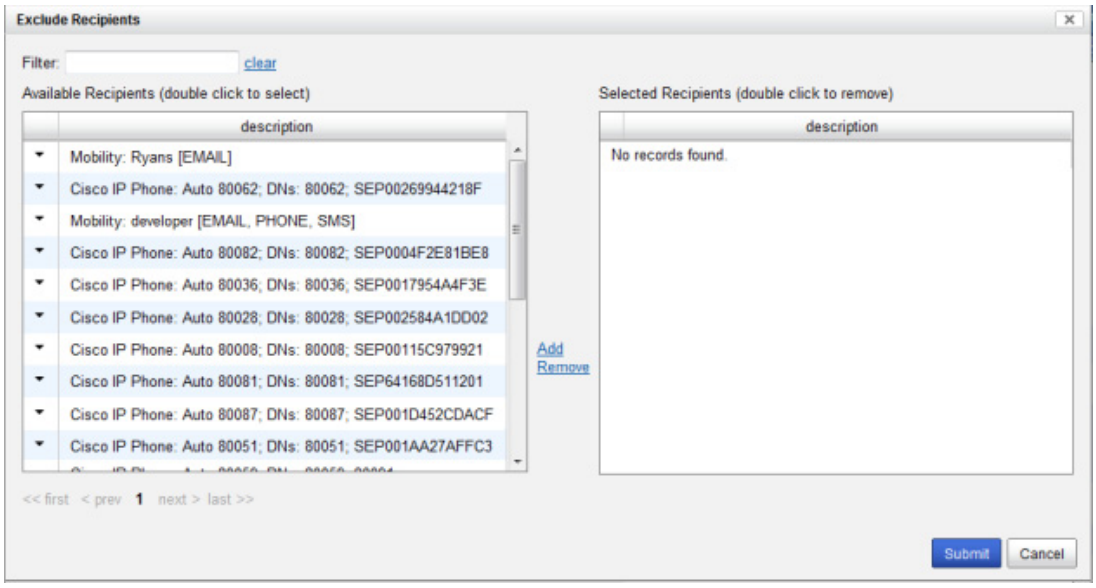
Step 2 Complete the steps in either "Create a Recipient Group by Selecting Multiple, Existing Recipient Groups" on page 4-17 or "Create a Recipient Group Using Rules" on page 4-20 (or both).

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	Recipients that match the supplied description value. This is often a useful grouping tool because you have control over the description of the recipients in your system, so you can set up your descriptions in ways that facilitate grouping. The text you enter will be compared against the Device Description entries of phones registered with your Unified Communications Manager server
Directory Numbers	Phones that match the supplied phone number(s) assigned to them in the Unified Communications Manager server.

Matching Parameter	Description
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.

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.

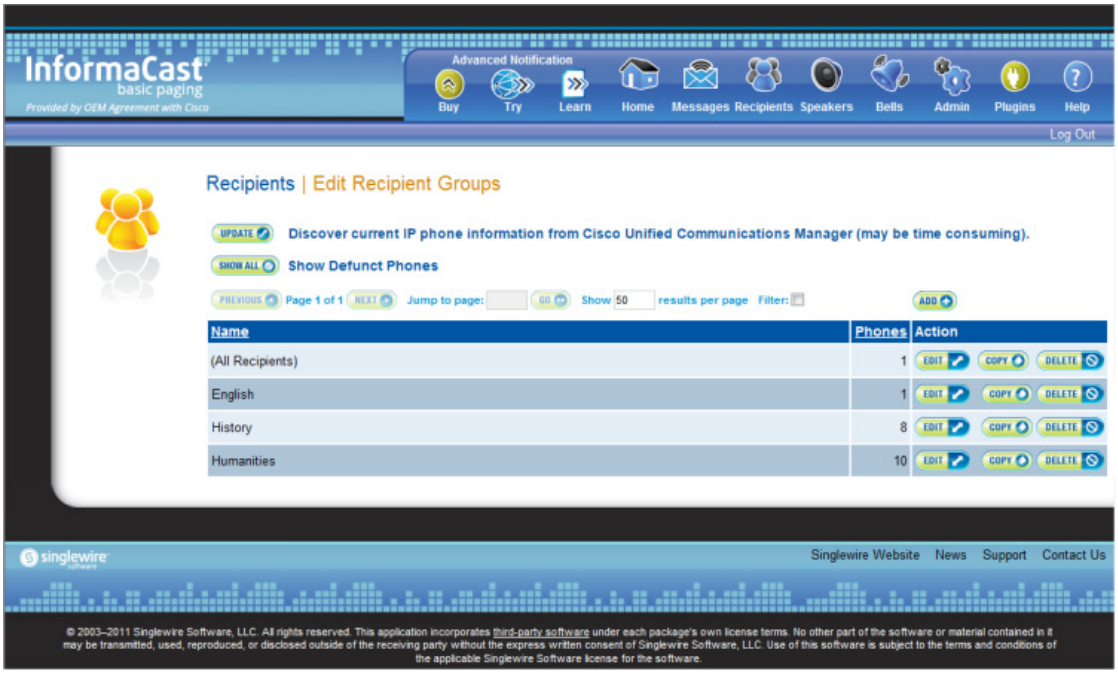
If you would like to further refine your recipient group, continue with "Create a Recipient Group by Selecting Individual Recipients" on page 4-15, "Create a Recipient Group by Selecting Multiple, Existing Recipient Groups" on page 4-17 and/or "Create a Recipient Group Using Rules" on page 4-20.

Edit a Recipient Group

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

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

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



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

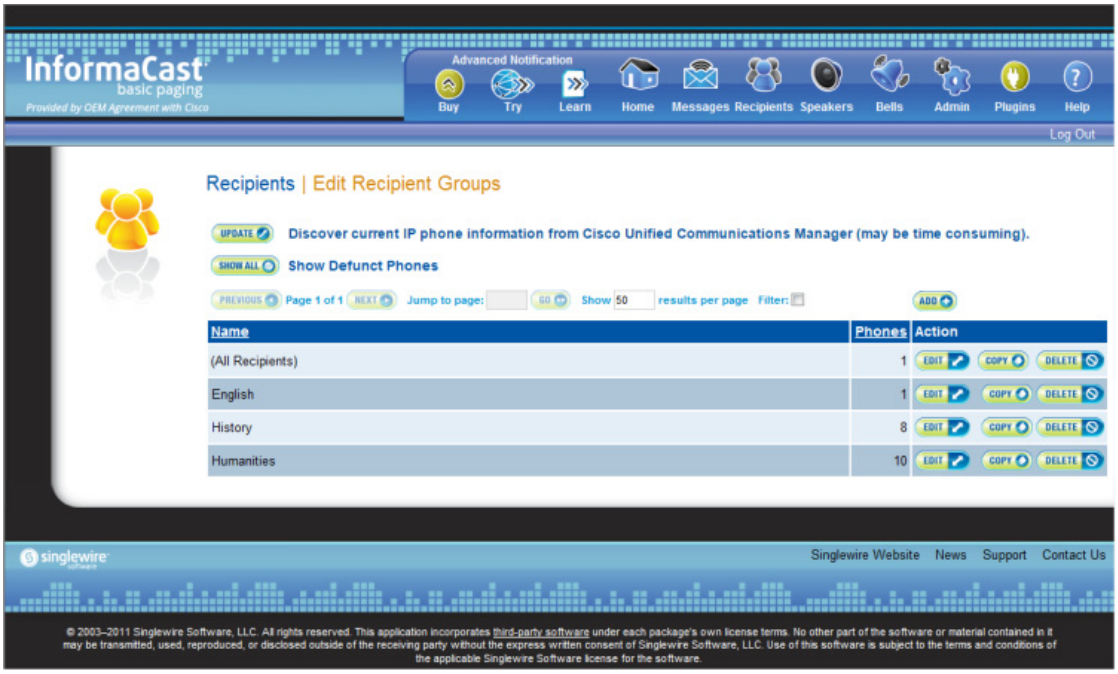
Step 3 Make your desired changes. See "Create a Recipient Group by Selecting Individual Recipients" on page 4-15, "Create a Recipient Group by Selecting Multiple, Existing Recipient Groups" on page 4-17, "Create a Recipient Group Using Rules" on page 4-20, or "Add Exclusions to a Recipient Group" on page 4-23 for more information on recipient group creation.

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

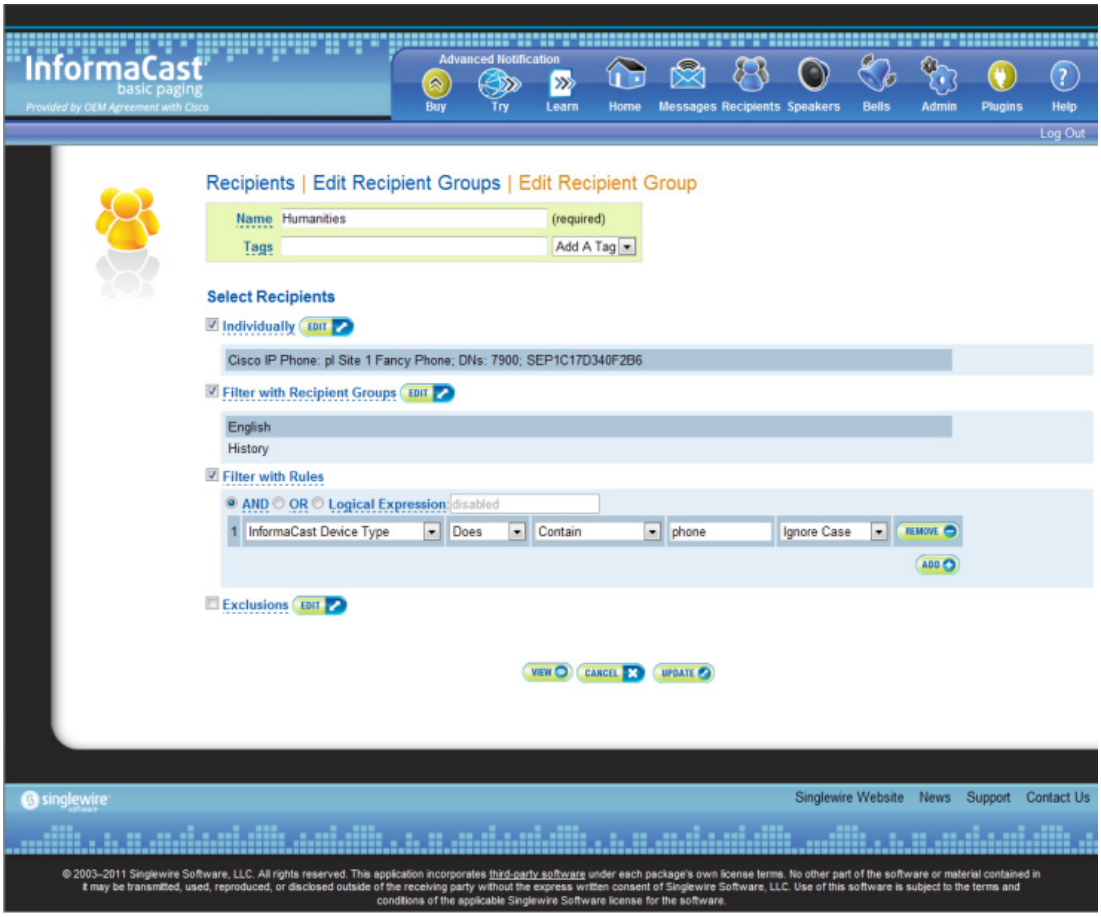
View Recipients in a Recipient Group

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

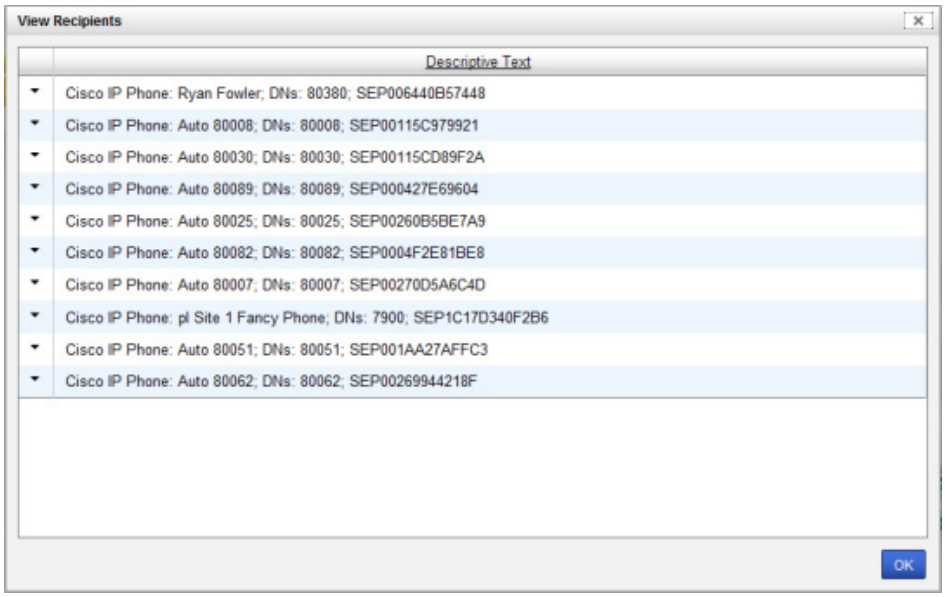
Step 1 Go to **Recipients** | **Edit Recipient Groups**. The Edit Recipient Groups page appears.



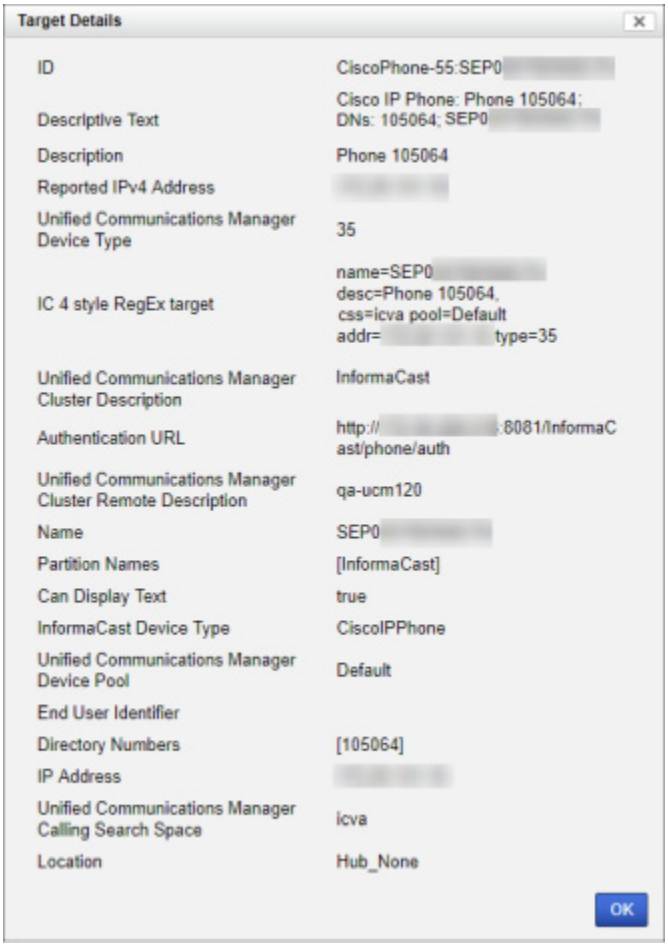
Step 2 Click the **Edit** button of the recipient group you want to view. The Edit Recipient Group page appears.



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



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



Target Details

ID	CiscoPhone-55:SEP0
Descriptive Text	Cisco IP Phone: Phone 105064; DNs: 105064; SEP0
Description	Phone 105064
Reported IPv4 Address	
Unified Communications Manager Device Type	35
IC 4 style RegEx target	name=SEP0 desc=Phone 105064, css=icva pool=Default addr= type=35
Unified Communications Manager Cluster Description	InformaCast
Authentication URL	http:// :8081/InformaCast/phone/auth
Unified Communications Manager Cluster Remote Description	qa-ucm120
Name	SEP0
Partition Names	[InformaCast]
Can Display Text	true
InformaCast Device Type	CiscoIPPhone
Unified Communications Manager Device Pool	Default
End User Identifier	
Directory Numbers	[105064]
IP Address	
Unified Communications Manager Calling Search Space	icva
Location	Hub_None

OK

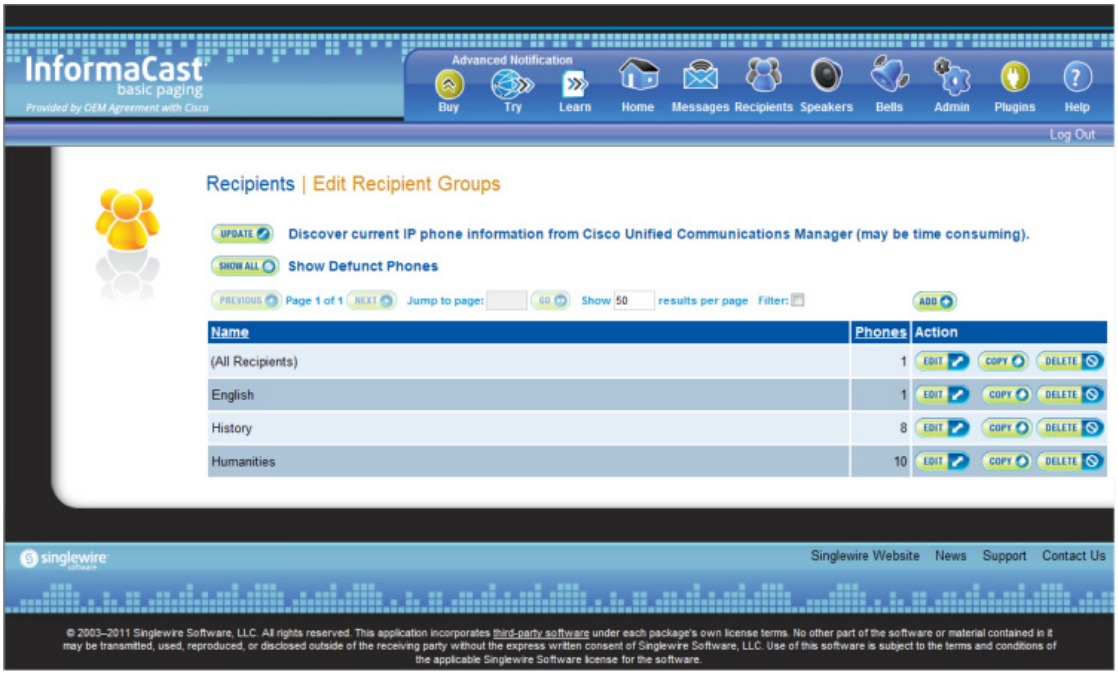
Step 5 Click the **OK** buttons in the Target Details and View Recipients pop-up windows to close them.

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

Copy a Recipient Group

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

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



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

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

Step 3 Make your desired changes. See "Create a Recipient Group by Selecting Individual Recipients" on page 4-15, "Create a Recipient Group by Selecting Multiple, Existing Recipient Groups" on page 4-17, "Create a Recipient Group Using Rules" on page 4-20, or "Add Exclusions to a Recipient Group" on page 4-23 for more information on recipient group creation.

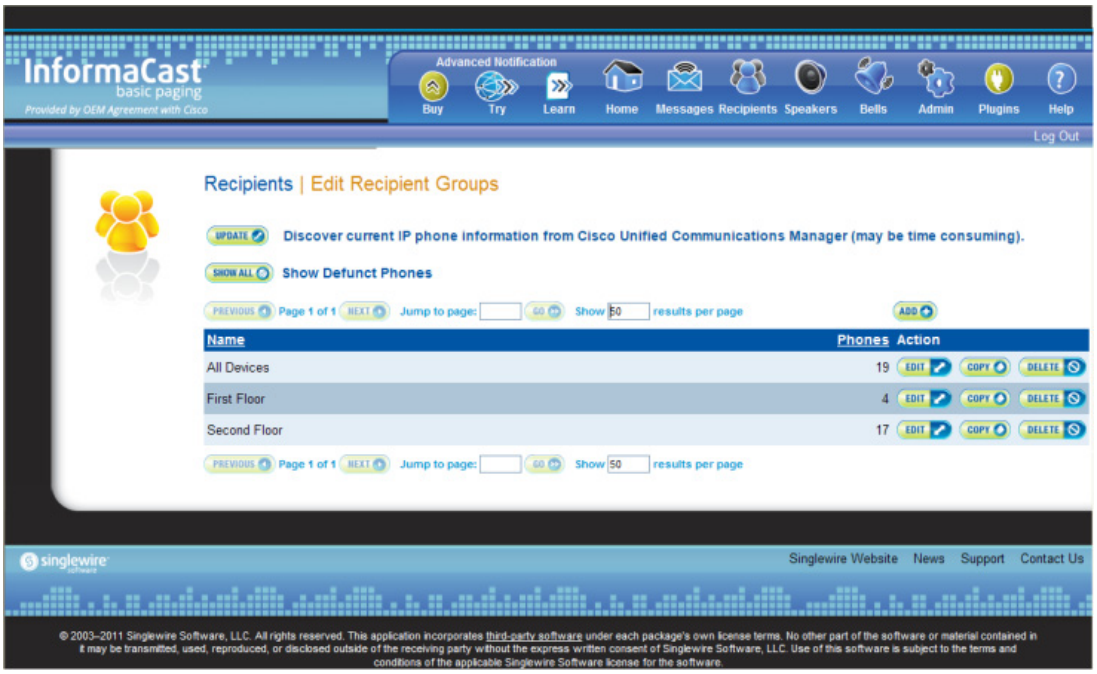
Step 4 Click the **Update** button when you are finished.

Remove Defunct Phones from Recipient Groups

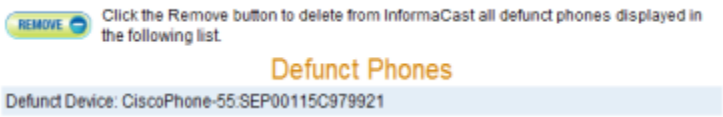
Defunct phones are recipients that are no longer available to Unified Communications Manager when the regular polling interval occurs. Recipients can become defunct if they lose power and/or are accidentally unplugged. A large number of defunct phones can degrade InformaCast's performance, and they should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

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



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



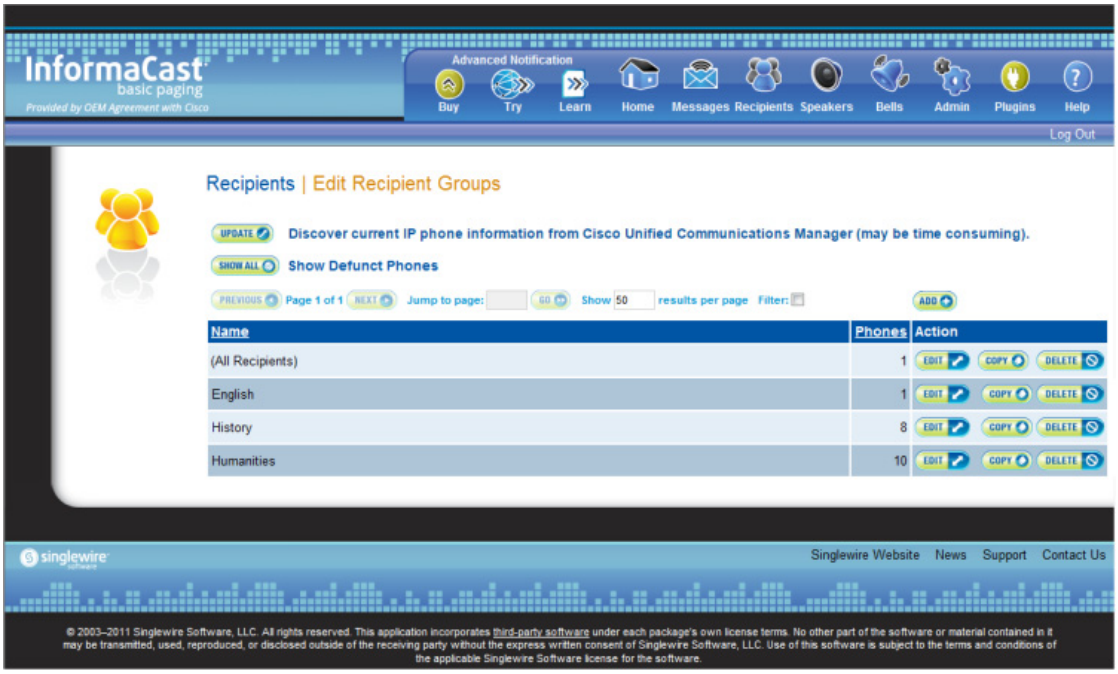
Step 3 Click the **Remove** button. Your defunct phones are removed from any recipient group to which they had been manually included or excluded.

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

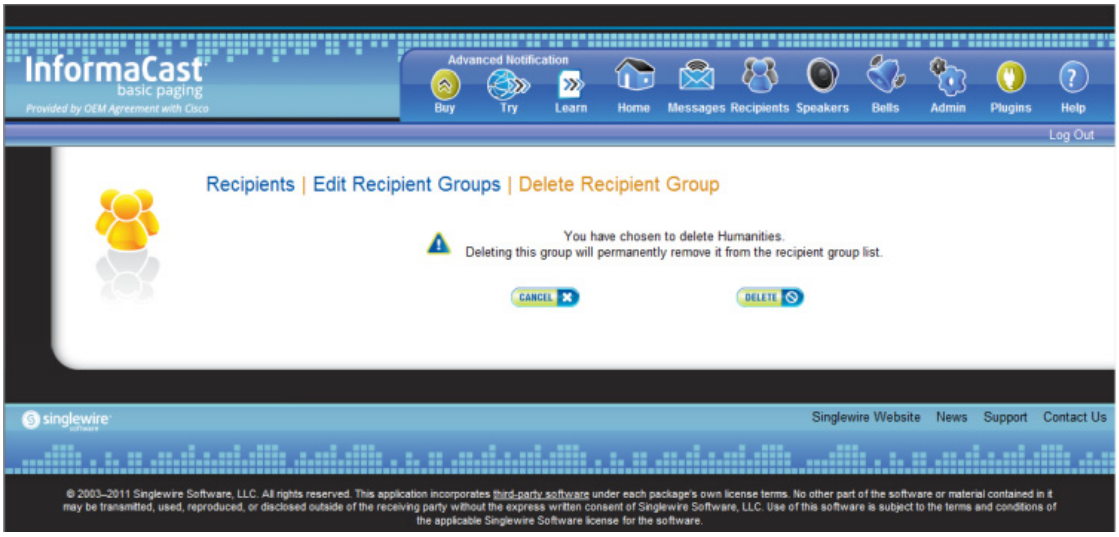
Delete a Recipient Group

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

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



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



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

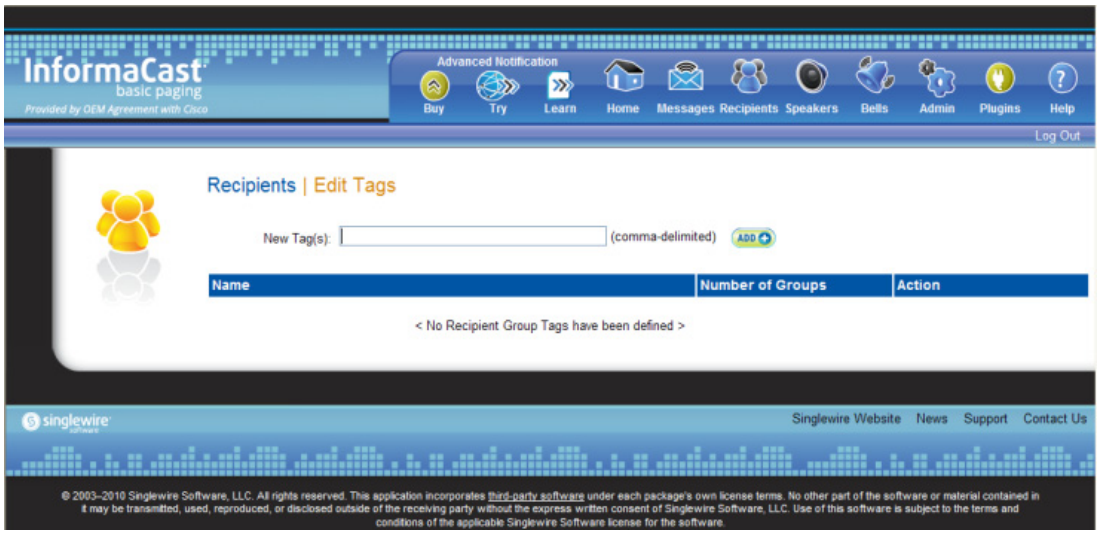
Configure Recipient Group Tags

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

Add a Recipient Group Tag

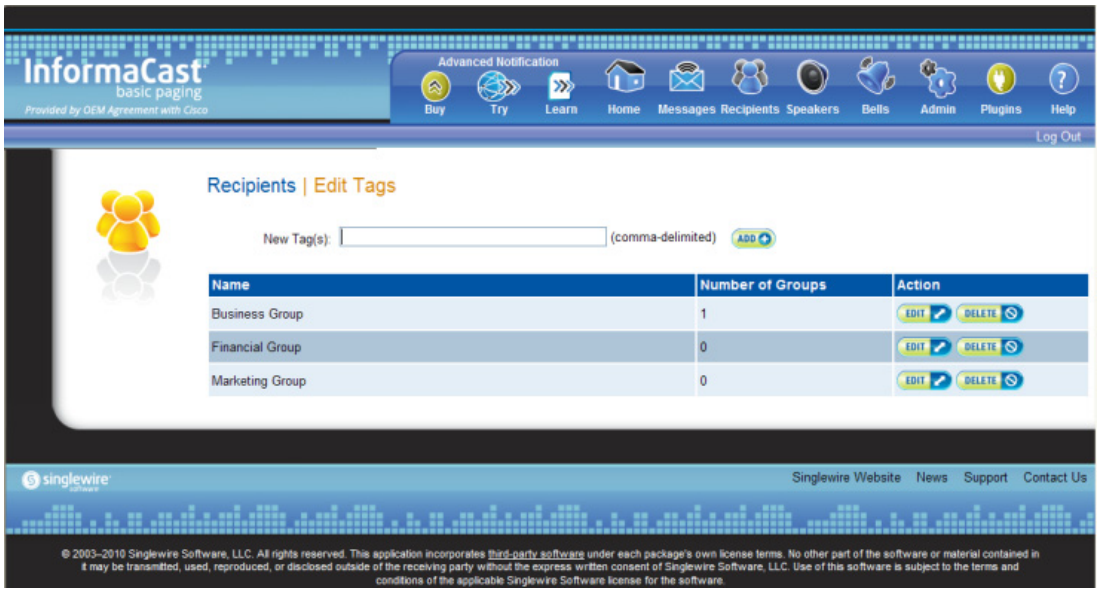
Before you can filter recipient groups through tags, you need to add them to InformaCast.

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



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

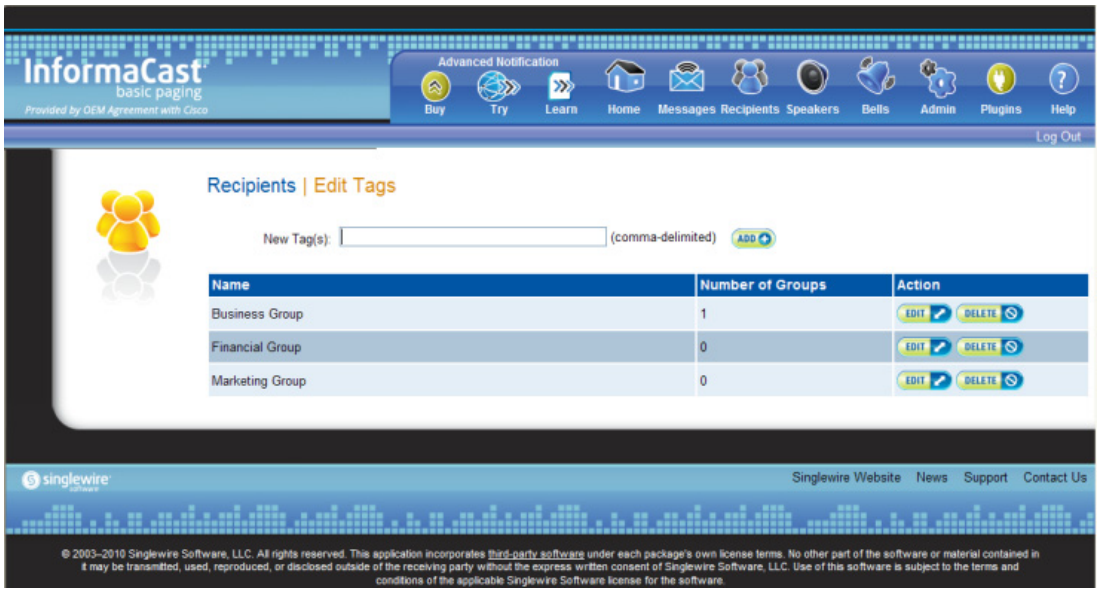
Step 3 Click the **Add** button. The Edit Tags page now shows the tag(s) you added. When you assign your tags to recipient groups, the number of recipient groups assigned to that tag will appear in the table.



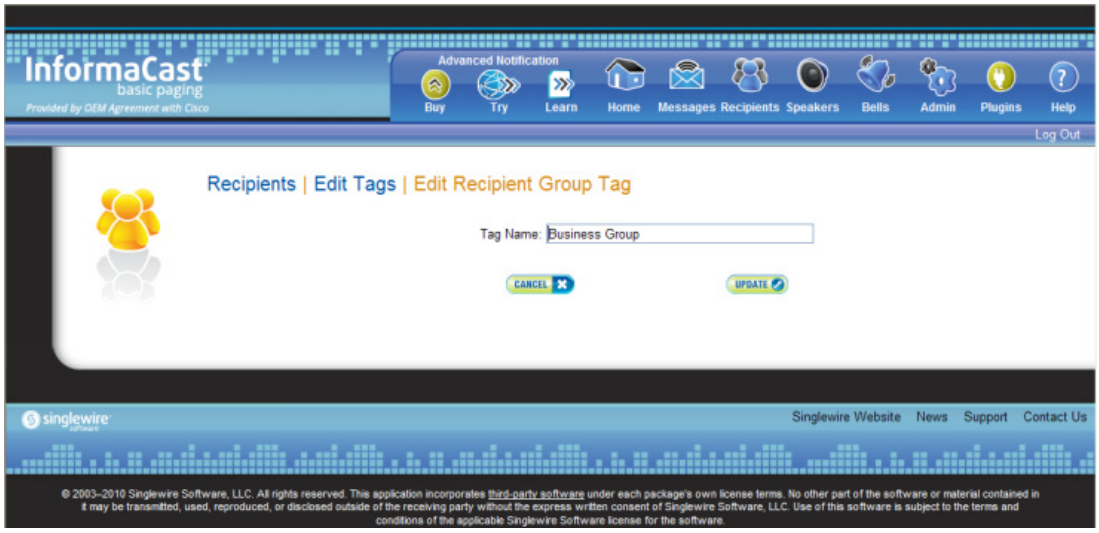
Edit a Recipient Group Tag

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

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



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



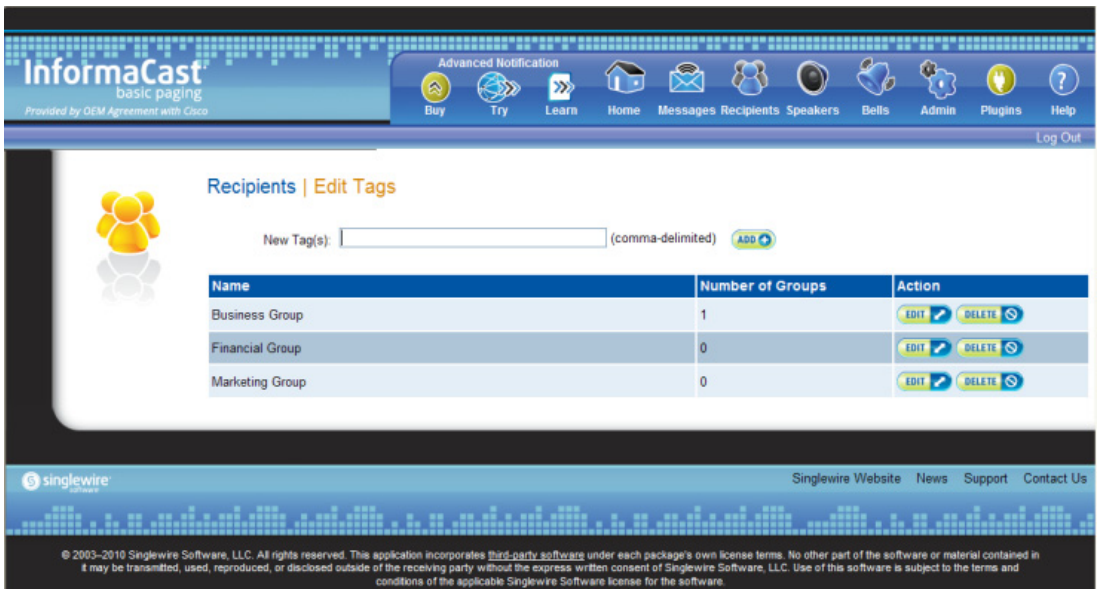
Step 3 Make your changes.

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

Delete a Recipient Group Tag

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

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



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

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

Manage Recipient Administration

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

Configure Advanced Matching for Recipient Groups

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

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

Subnet Matching

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

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

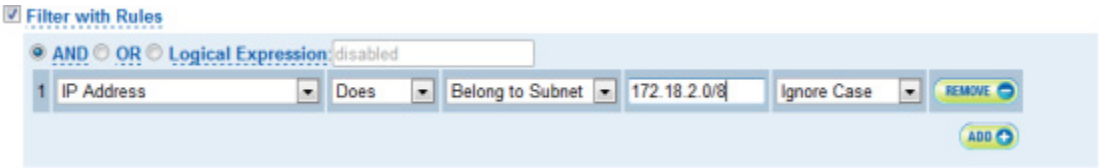
To specify a subnet within InformaCast, supply an address and the number of "host bits" that should be ignored in that address. For example, look at how you'd match a very common style of LAN, which uses what is known as "Class C" addressing. In a Class C network, there are 24 bits of network address,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

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

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

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

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



Regular Expressions

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

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

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

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

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

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

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

```
m/pattern/i
```

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

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

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

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

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

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

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

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

Manage Phone Updates

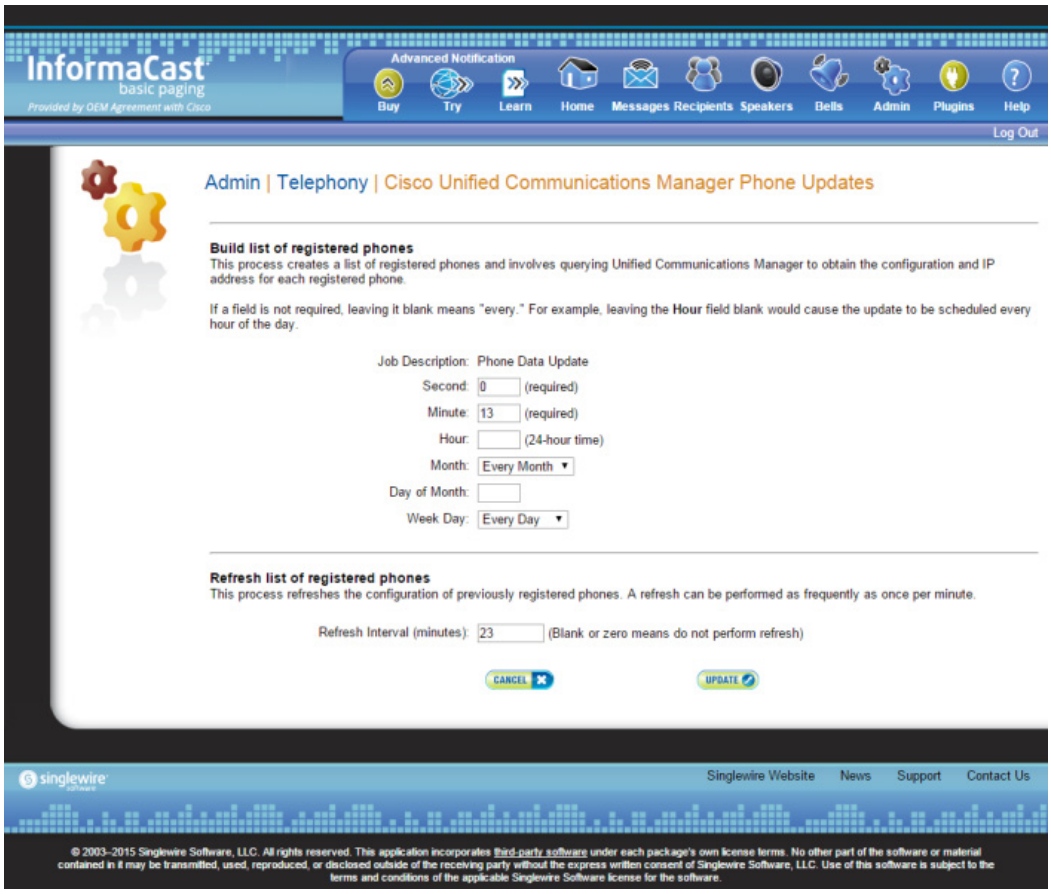
Phone updates allow you to configure the timing for two scheduled jobs of how often InformaCast will update its phone information: build a list of registered phones and refresh a list of registered phones.

The time it takes for InformaCast to *rebuild* a list of phones is directly related to the number of phones you have. During a build of registered phones, 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.



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.

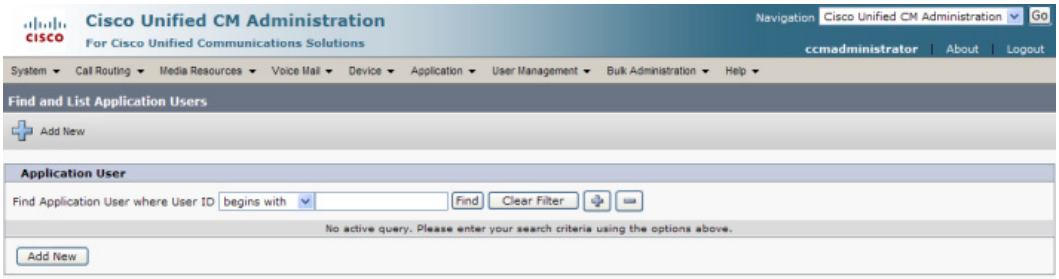
Step 7 Click the **Update** button. On the Overview page, you can see your changes reflected in the *Phone Updates* section.

Determine the Busy State of a Phone with JTAPI

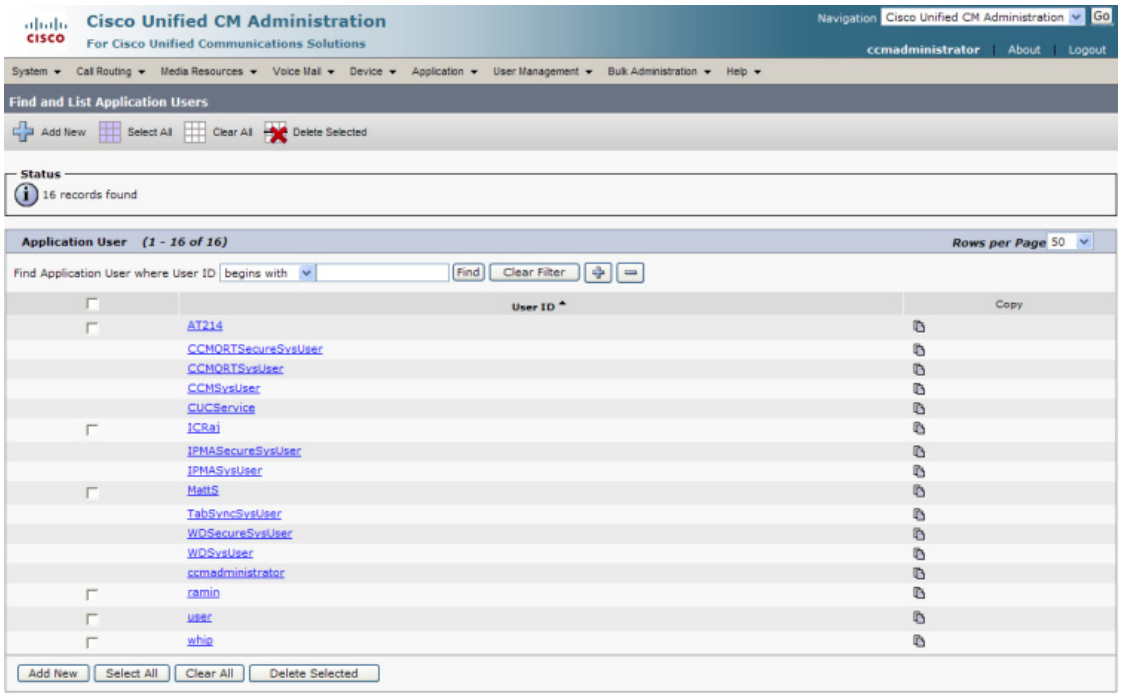
Cisco IP phones have become progressively less reliable at reporting whether they are in use during a broadcast. For those small number of phones where it is very important to be sure that message audio is always and only delivered if the phone is idle (a requirement for Basic InformaCast), it is now 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.

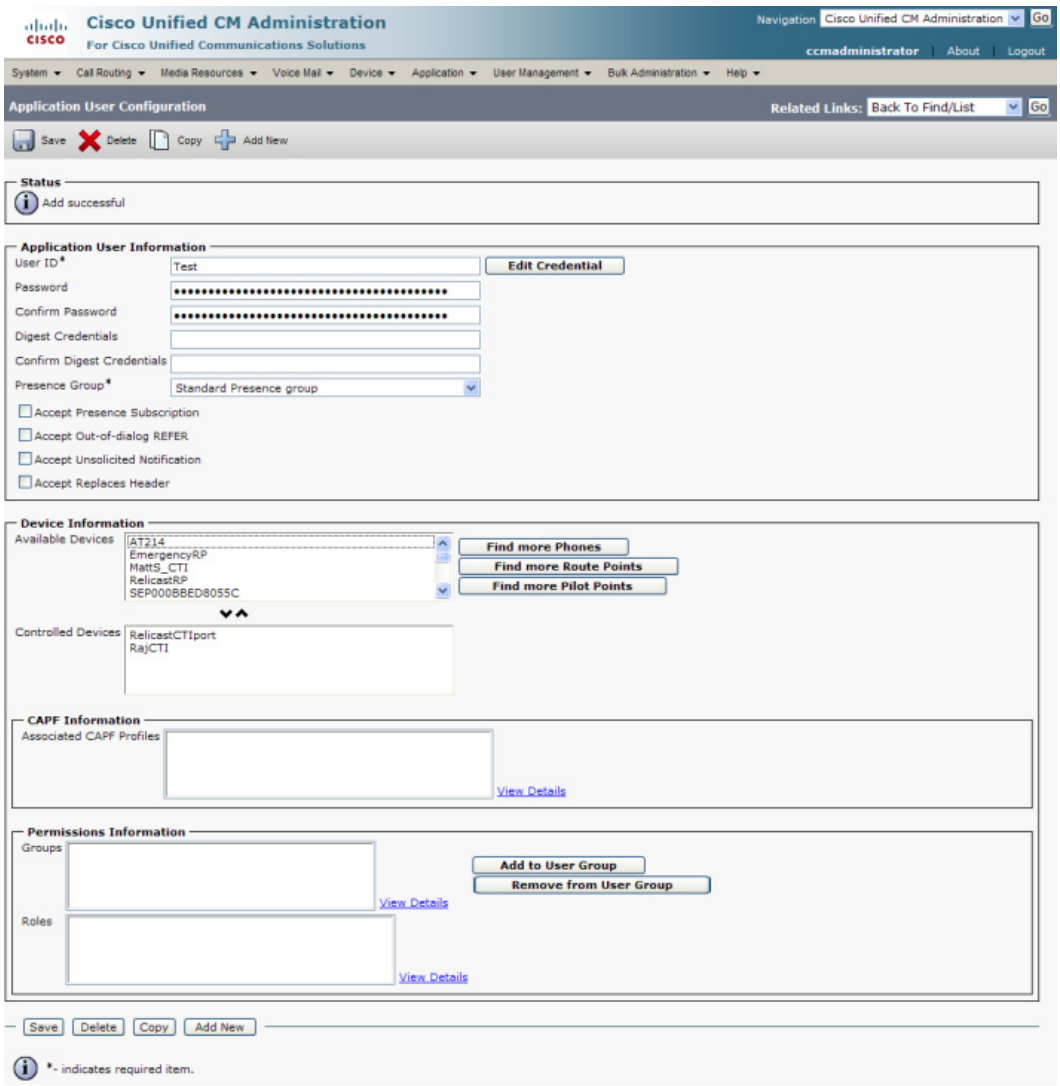
Step 1 Log into your Unified Communications Manager's administrative interface and go to **User Management** | **Application User**. The Find and List Application Users page appears.



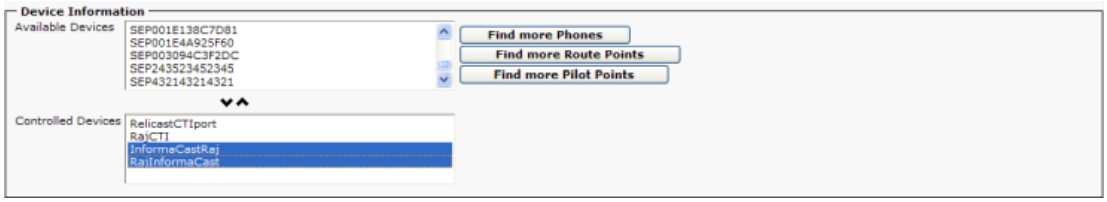
Step 2 Use the filters to search for the name of the application user you are using. Click the **Find** button. The Find and List Application Users page refreshes with your results.



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



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

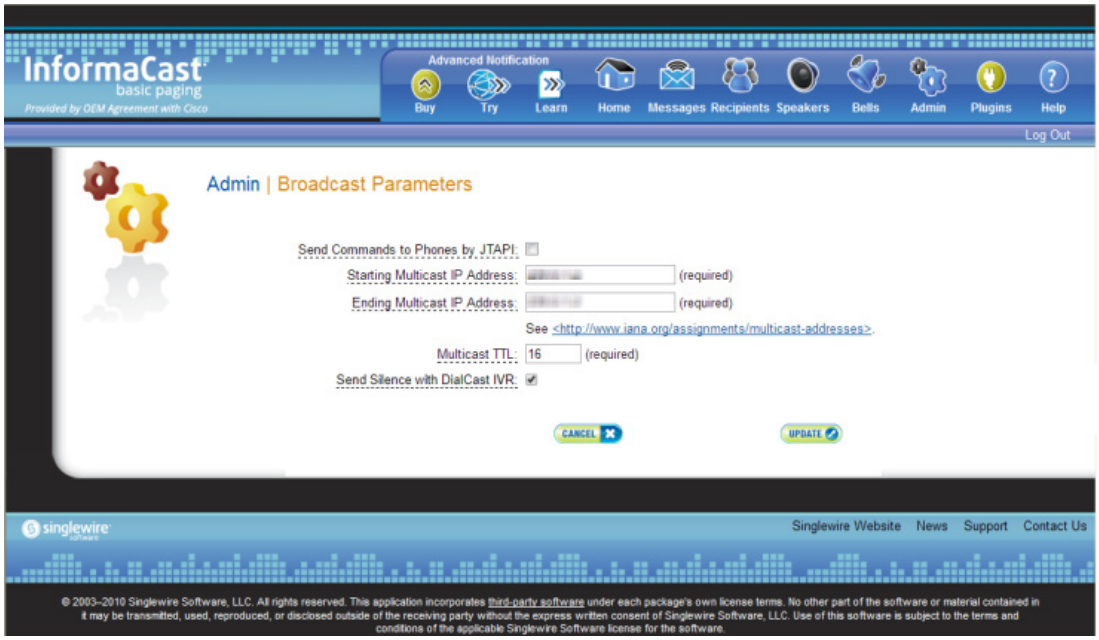


Step 5 Click the **Save button** to save your changes.

Manage Broadcast Parameters

Set whether InformaCast uses JTAPI or HTTP when communicating with Unified Communications Manager and ensure that there is a valid multicast address (or range of addresses) for InformaCast's use.

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



Step 2 Determine how InformaCast will communicate with your IP phones:

- If you leave the **Send Commands to Phones by JTAPI** checkbox unselected, InformaCast communicates directly with your IP phones over HTTP. Each time InformaCast sends a broadcast to a phone, it shares a unique, one-time token to validate its communication. One-time passwords enhance the security of the HTTP communication between InformaCast and Unified Communications Manager by pairing your device's name with an ever-changing password instead of static application user credentials. If you leave the **Send Commands to Phones by JTAPI** checkbox unselected, you must have also enabled web access for your phones.
- If you select the **Send Commands to Phones by JTAPI** checkbox, InformaCast uses JTAPI to communicate with your Unified Communications Manager cluster, which then uses SCCP or SIP to pass on the actual activation commands to your IP 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).

See this article for more information on the pros and cons of JTAPI vs. HTTP.

If 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 https://www.iana.org/assignments/multicast-addresses/multicast-addresses.xhtml 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 18 Select the **Send Silence with DialCast IVR** checkbox to allow the DialCast IVR to send RTP packets that contain silence to the caller after the IVR has finished interacting with it.

A DialCast call consists of two audio streams: one contains the audio sent by the calling party to InformaCast and heard during the broadcast, and the other contains the audio sent by the DialCast IVR and heard by the caller. Sending silent RTP packets is necessary in some circumstances when the party making a DialCast call needs to receive audio during the entire call in order to prevent it from terminating the call due to perceived inactivity. Without enabling this checkbox, the DialCast IVR will

only send audio to the caller when welcoming the caller, authenticating the caller, etc. For the rest of the call, no audio will be sent, and callers may interpret silence as indicating the call is over and terminate the call.

Step 19 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

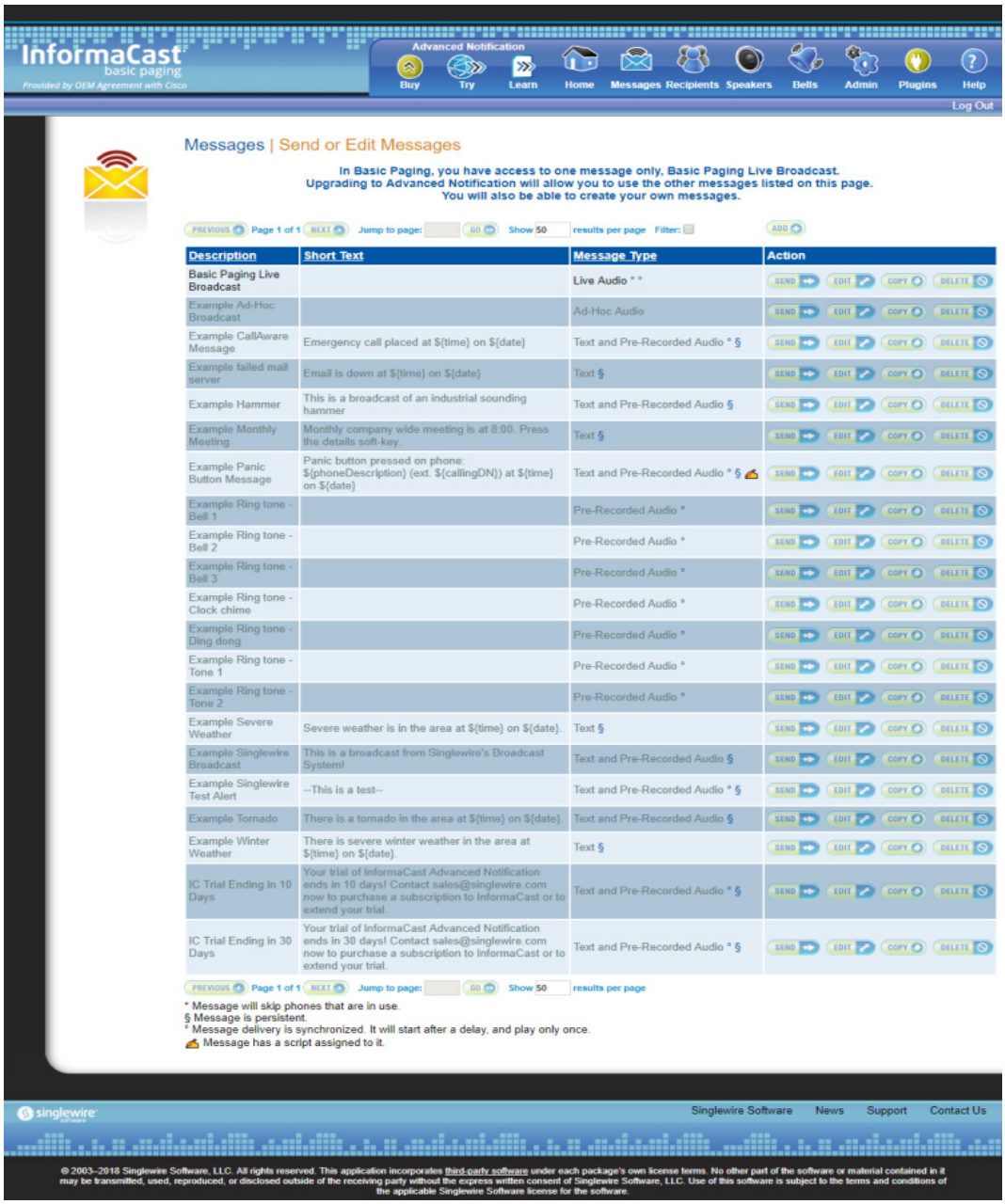
Messages are the basis of any InformaCast broadcast. A message predefines the characteristics of the broadcast.

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 can be sent immediately after the audio is recorded or they can be entered into a queue and sent when a predetermined percentage of recipients are available to play the broadcast. Outside of a queue, these broadcasts are used to rapidly respond to unpredictable events. In a queue, these broadcasts offer a high degree of confidence that they will be heard by their recipients even during times of high broadcast traffic.
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 can be sent immediately after the audio is recorded or they can be entered into a queue and sent when a predetermined percentage of recipients are available to play the broadcast. Outside of a queue, these broadcasts are used to rapidly respond to unpredictable events. In a queue, these broadcasts offer a high degree of confidence that they will be heard by their recipients even during times of high broadcast traffic.
Talk and Listen	Talk and Listen messages allow any phone in a recipient group to speak, in real time ("live"), to all the other phones receiving the broadcast by pressing a **Talk** softkey. Other listeners can respond by pressing the **Talk** softkey on their own phones.

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



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

Aside from viewing potential InformaCast messages, you can also view active broadcasts by clicking the **View** button (only visible on the Send or Edit Messages page when there is an active broadcast) and cancel any ongoing broadcasts (see "Cancel a DialCast/Broadcast" on page 5-54).

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 5-38).

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 5-38).

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 Profile" on page 5-8
- "Add a SIP Trunk" on page 5-11
- "Add a Route Pattern" on page 5-33

For a secure SIP trunk, follow these steps:

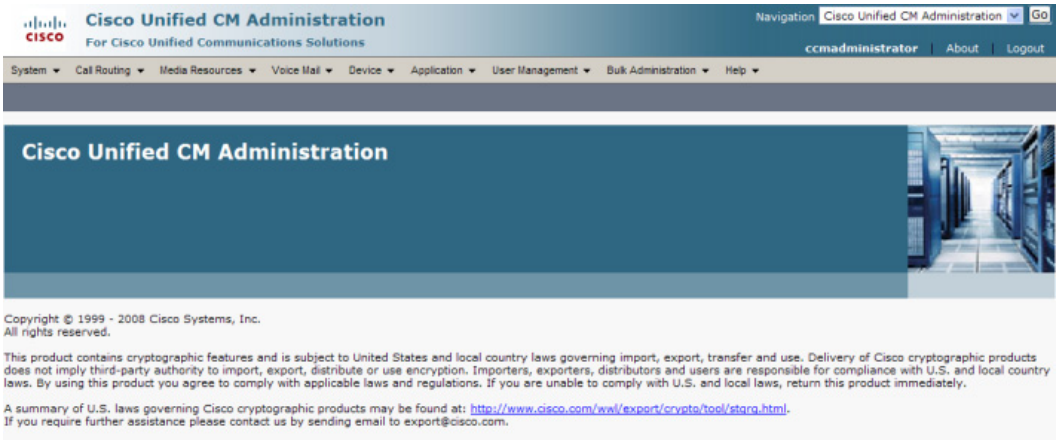
- "Manage SIP Certificates to Facilitate TLS Protocol" on page 5-13
- "View the InformaCast SIP Certificate" on page 5-14
- "Install the InformaCast SIP Certificate on Unified Communications Manager" on page 5-15
- "Add a SIP Trunk Security Profile That Uses TLS" on page 5-21
- "Add a SIP Profile" on page 5-8
- "Add a SIP Trunk That Uses TLS" on page 5-24
- "Install Unified Communications Manager Certificates on InformaCast" on page 5-27
- "Add a Route Pattern" on page 5-33

Add a SIP Trunk Security Profile

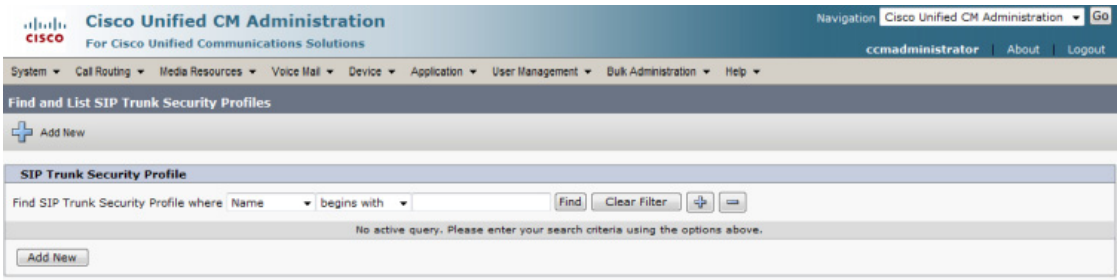
A SIP trunk security profile specifies things such as the transport protocol to be used, whether digest authentication should be performed, etc.

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 5-21.

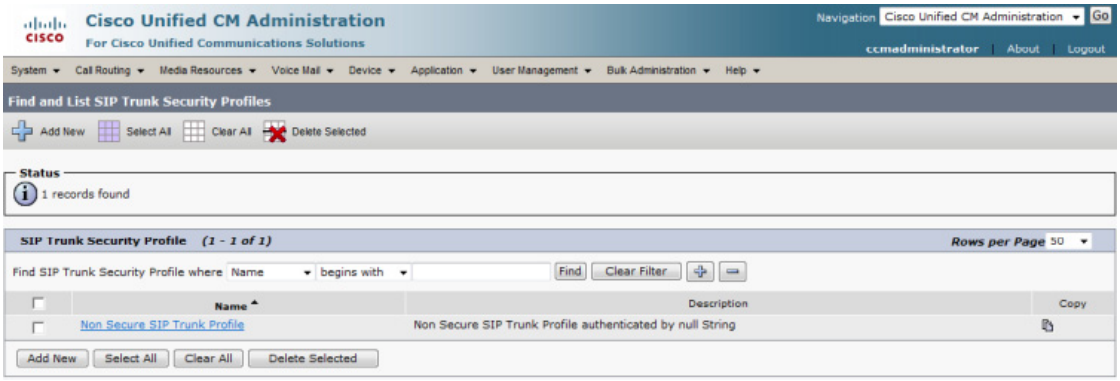
Step 1 Open a web browser and log into the administration interface of the Unified Communications Manager server (the address will be similar to https://<Unified Communications Manager IP Address>/ccmadmin). The Cisco Unified CM Administration page appears.



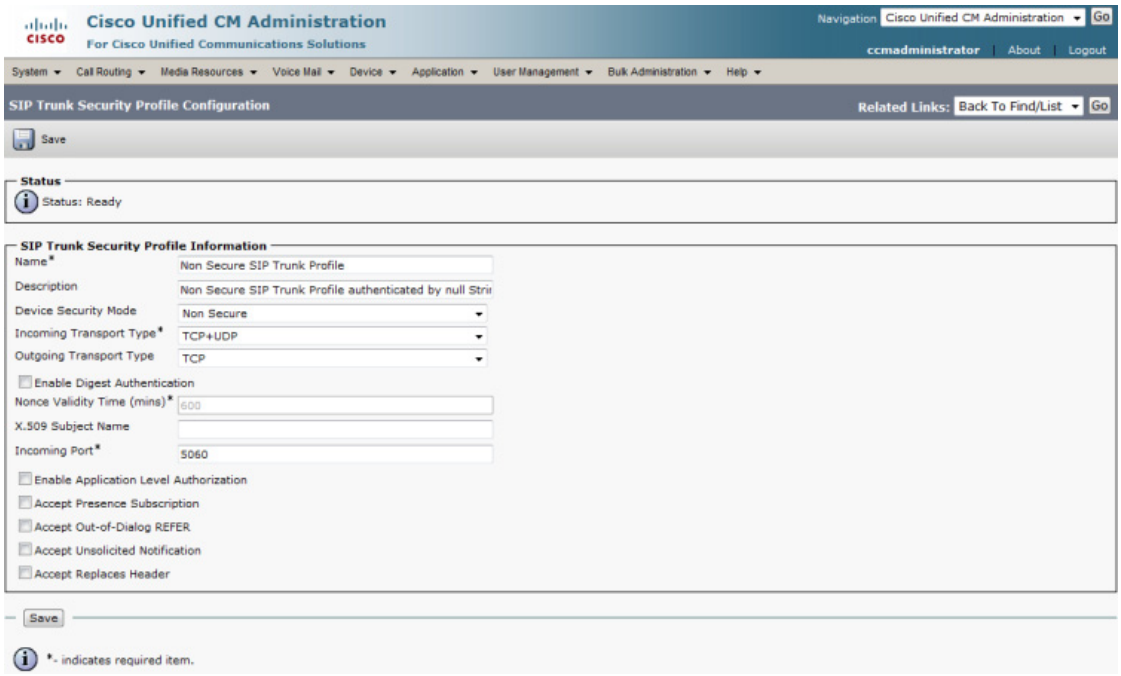
Step 2 Go to **System | Security | SIP Trunk Security Profile**. The Find and List SIP Trunk Security Profiles page appears.



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.



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**.

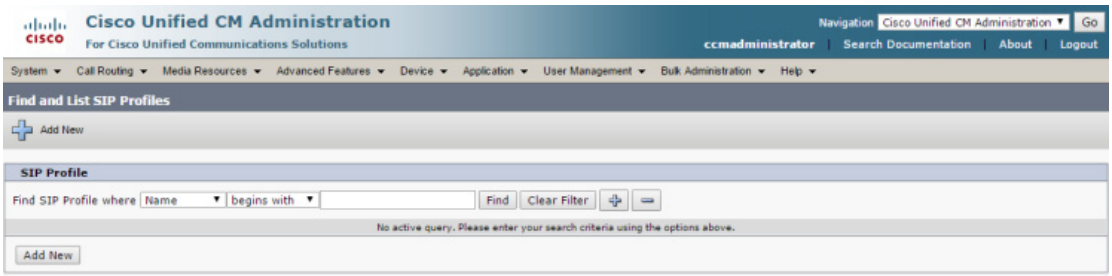
Step 10 Select the **Accept Unsolicited Notification** checkbox.

Step 11 Click the **Save** button.

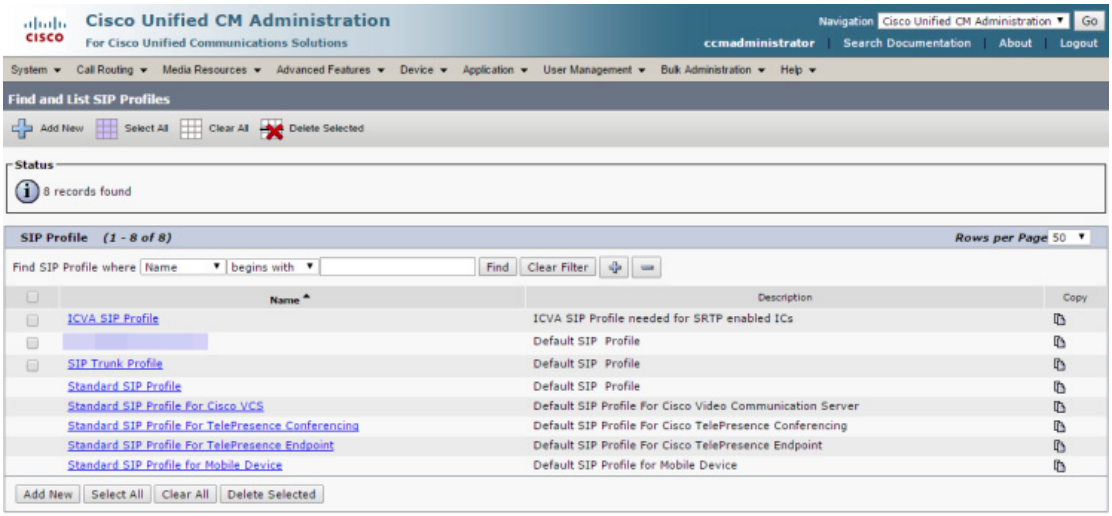
Add a SIP Profile

The **Early Offer support for voice and video calls** parameter, available through a SIP profile, should be set to **Best Effort (no MTP inserted)** or enabled (depending on your version of Unified Communications Manager) to ensure efficient SIP call setup and media routing.

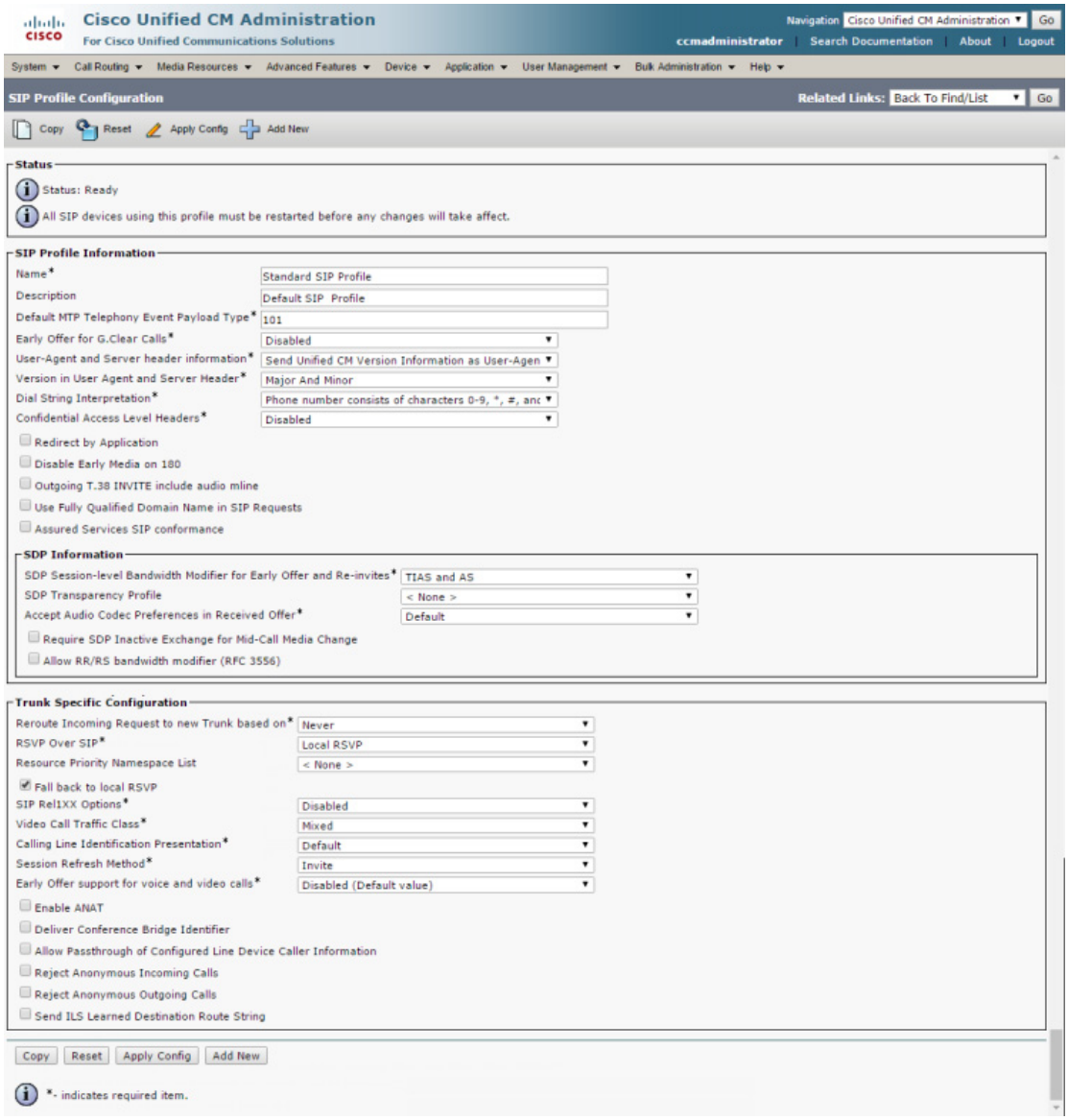
Step 1 Go to **Device** | **Device Settings** | **SIP Profile**. The Find and List SIP Profiles page appears.



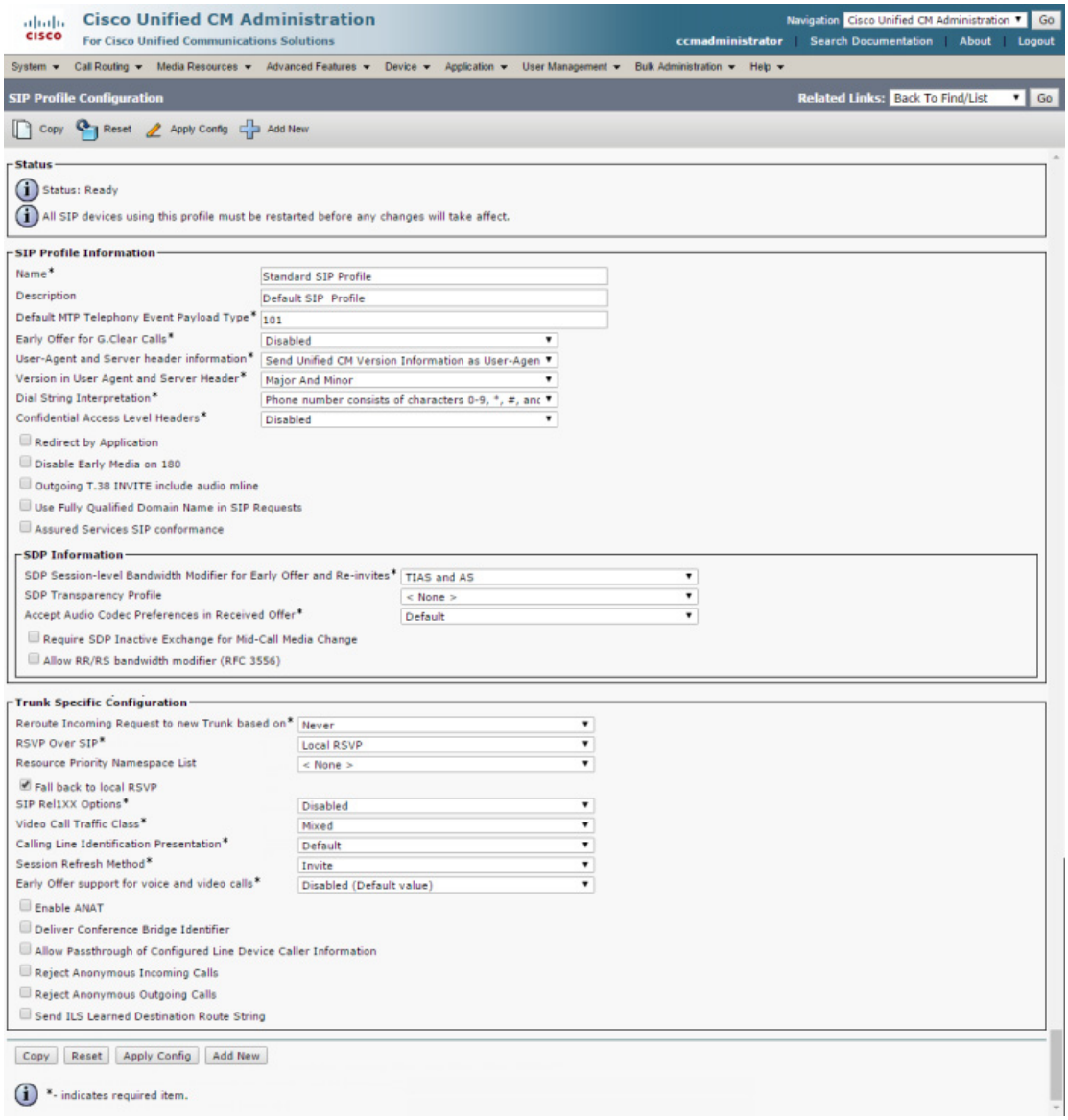
Step 2 Click the **Find** button. The Find and List SIP Profiles page refreshes.



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



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



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, the dropdown menu is a checkbox: select the **Early Offer support for voice and video calls (insert MTP if needed)** checkbox.

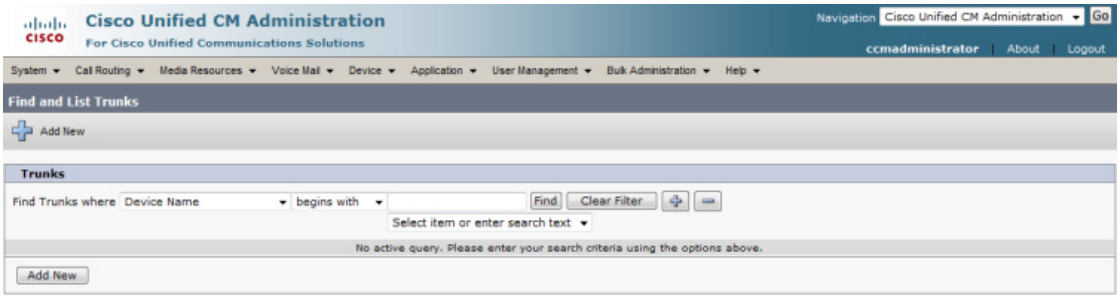
Step 8 Click the **Save** button.

Add a SIP Trunk

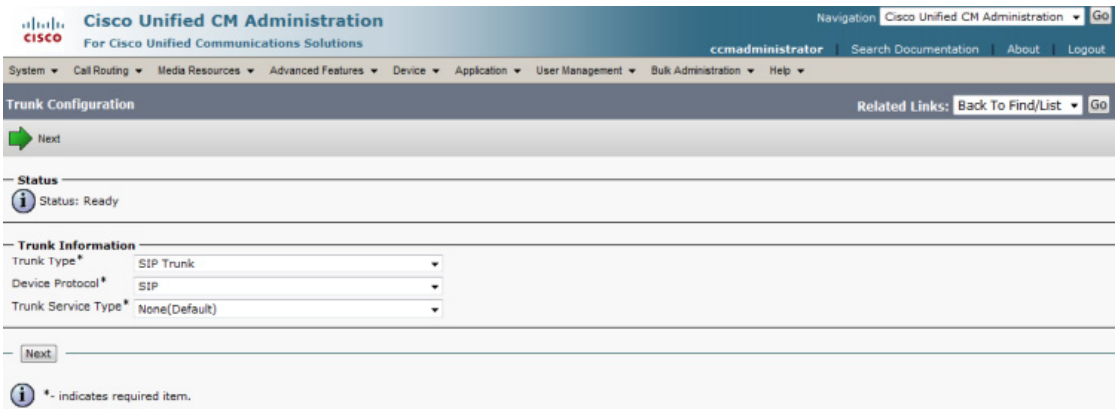
Use the following steps to create a SIP trunk that uses the security profile you just created.

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.

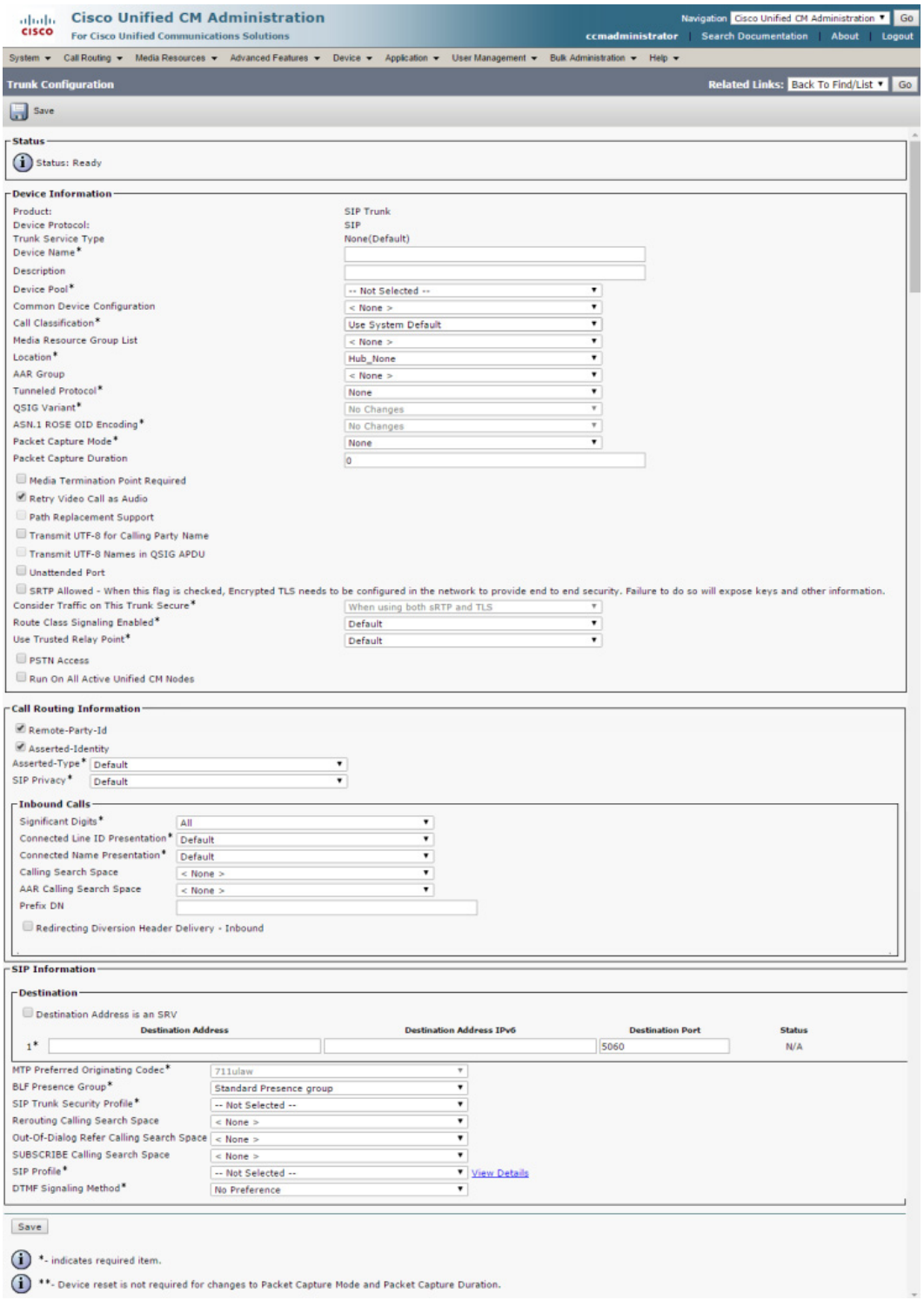


Step 3 Select **SIP Trunk** from the **Trunk Type** dropdown menu.

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.



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 2-53 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 2-56 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 the SIP profile you created in "Add a SIP Profile" on page 5-8 from the **SIP Profile** dropdown menu.

Step 15 Click the **Save** button.

Step 16 Proceed to "Add a Route Pattern" on page 5-33.

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.

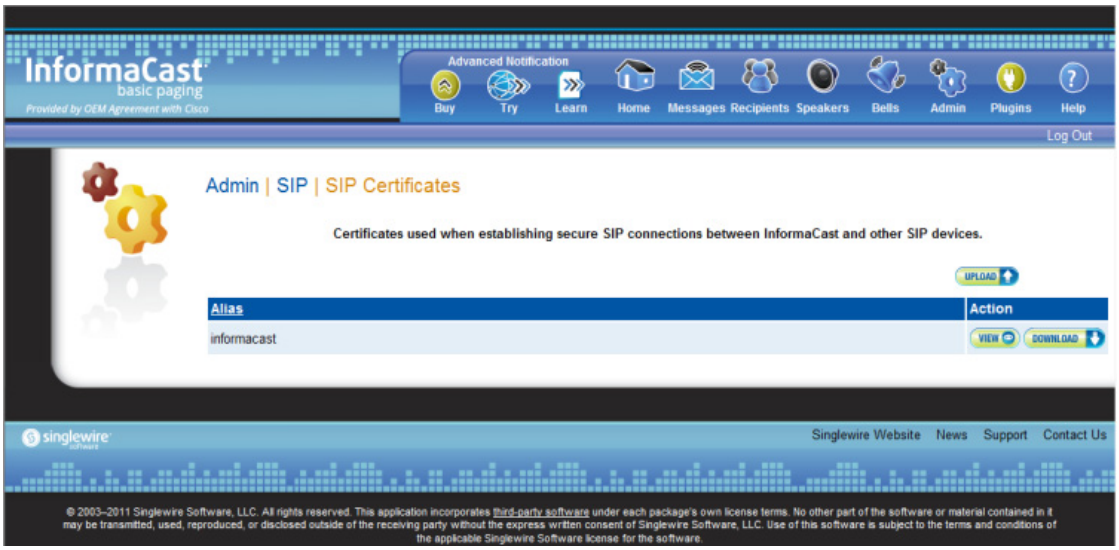
It is essential that the InformaCast certificate be downloaded and installed at each host that expects to use TLS as its SIP transport protocol with InformaCast. It is also essential that a certificate from each of those same hosts be uploaded to InformaCast. You will also need to modify it and its security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

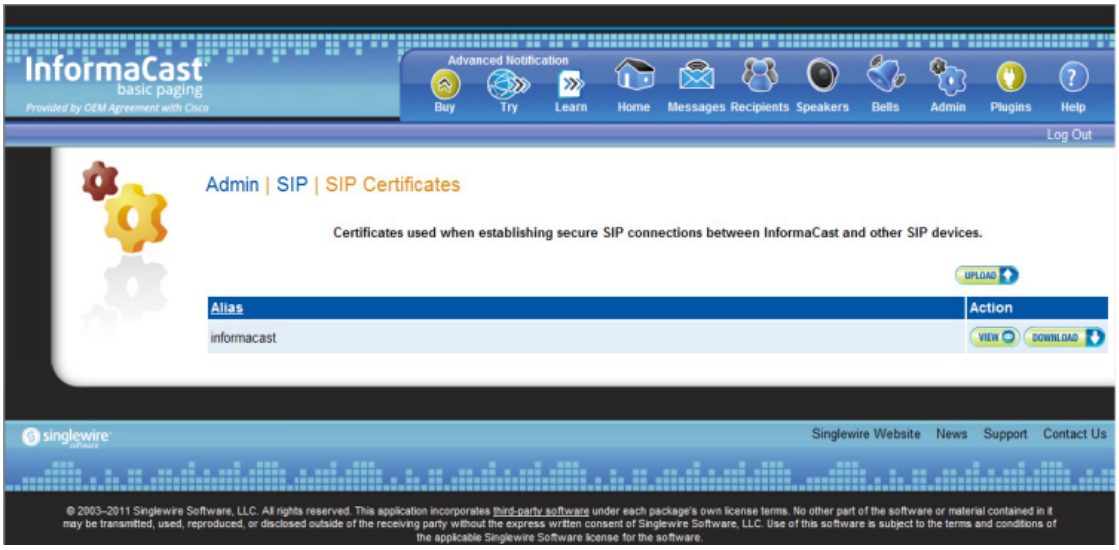
Step 3 Click the **Done** button to return to the SIP Certificates page.

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.

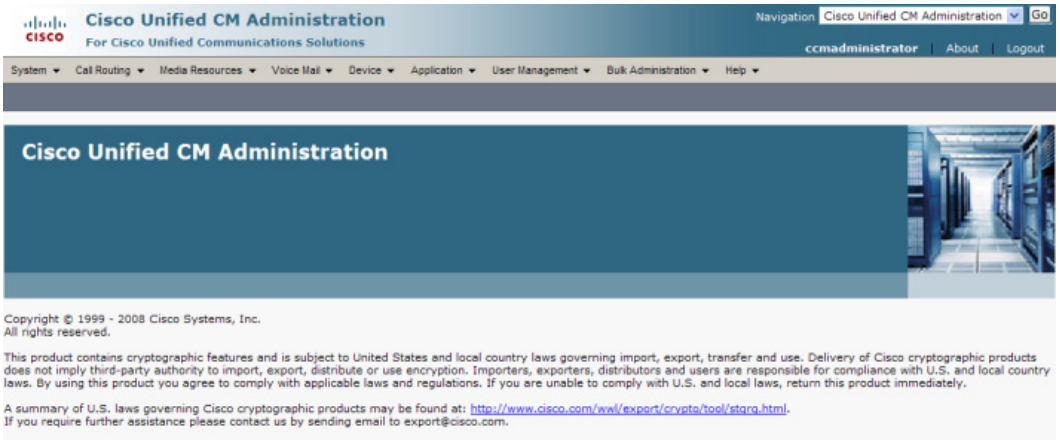


Step 2 Click the **Download** button.

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.

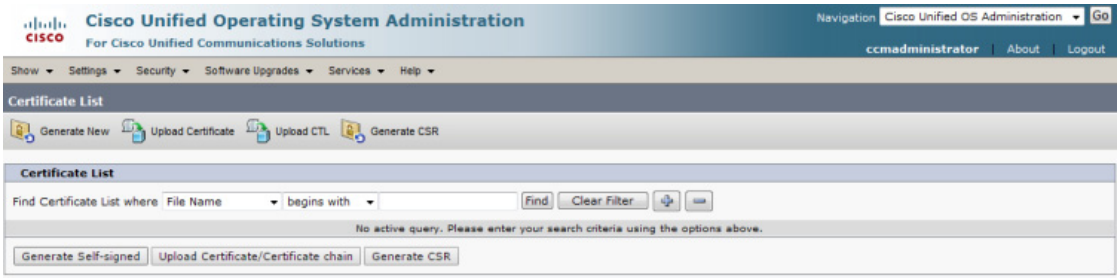
Step 4 Open a web browser and log into the administration interface of the Unified Communications Manager server (the address will be similar to https://<Unified Communications Manager IP Address>/ccmadmin). The Cisco Unified CM Administration page appears.



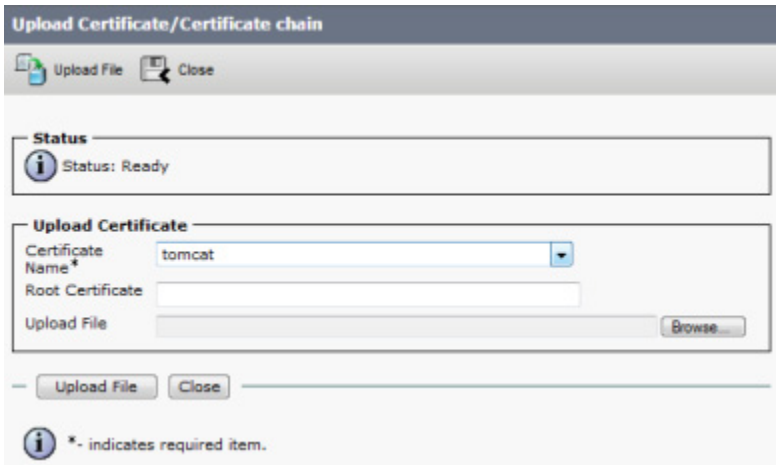
Step 5 Select **Cisco Unified OS Administration** from the **Navigation** dropdown menu and click the **Go** button. The Cisco Unified Operating System Administration page appears.

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.

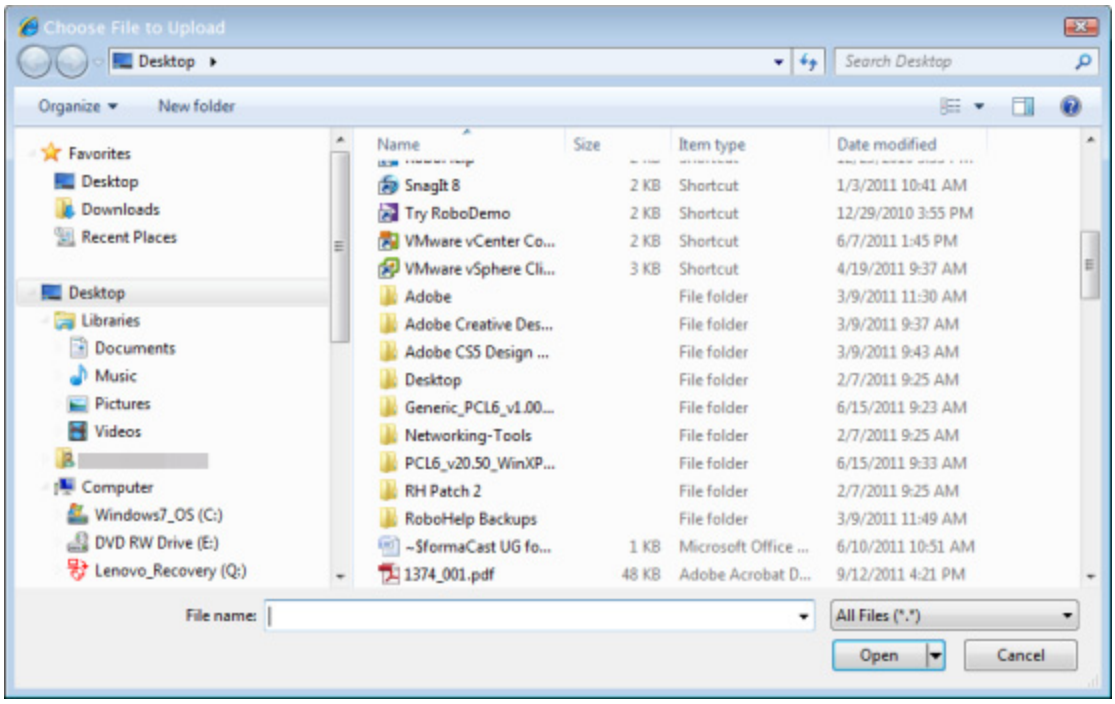


Step 8 Click the **Upload Certificate/Certificate chain** button. The Upload Certificate/Certificate chain window appears.



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.

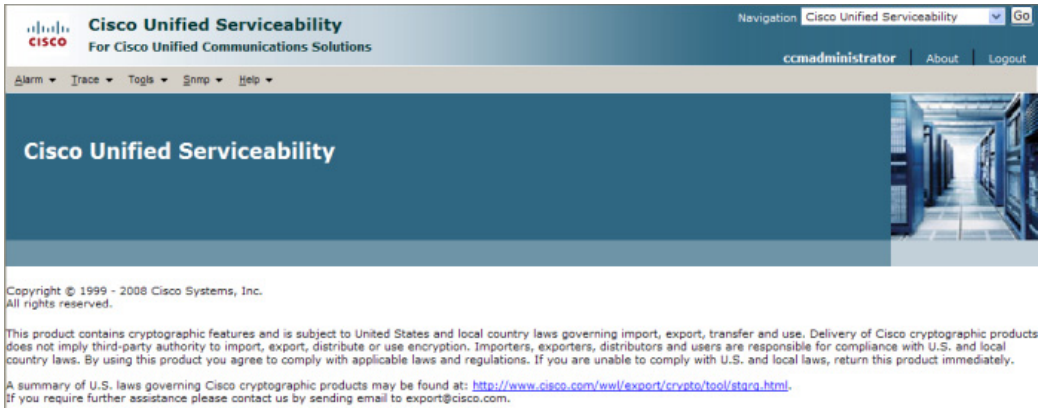
Step 13 Click the **Close** button to close this window.

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 5-21.

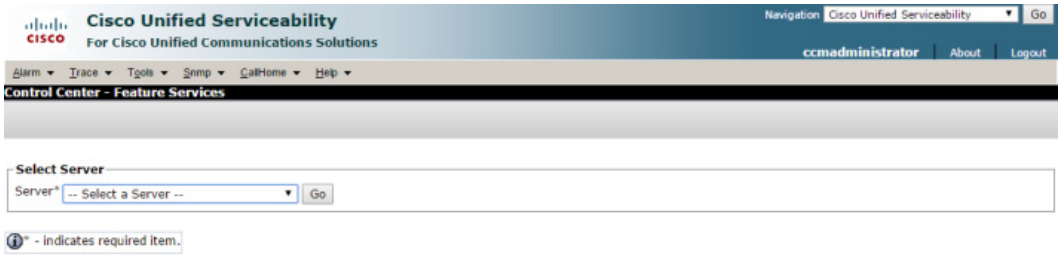
If you are using the 11.5.1 version of Unified Communications Manager or later, you will also need to perform Steps 15 through 22. Since these steps include restarting Unified Communications Manager, you should plan to perform these steps during a maintenance window to avoid disrupting your users.

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

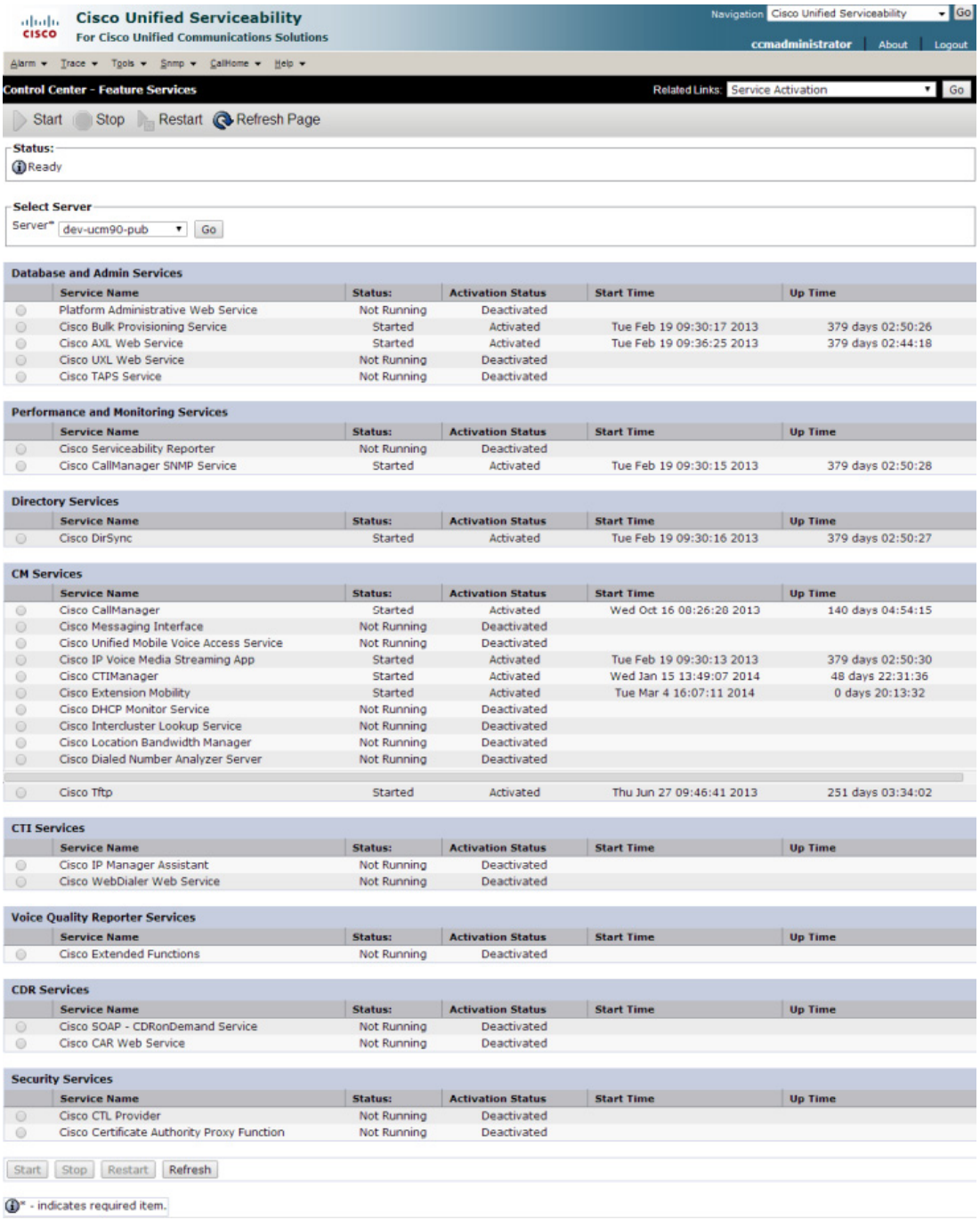


Note You may have to log into Unified Communications Manager again.

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.



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.

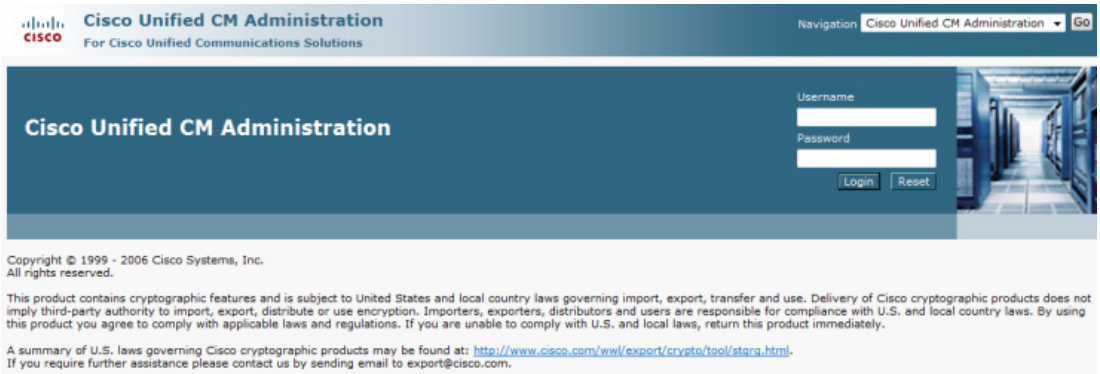
Step 21 Click the **OK** button to accept any warnings. The service will restart.

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.

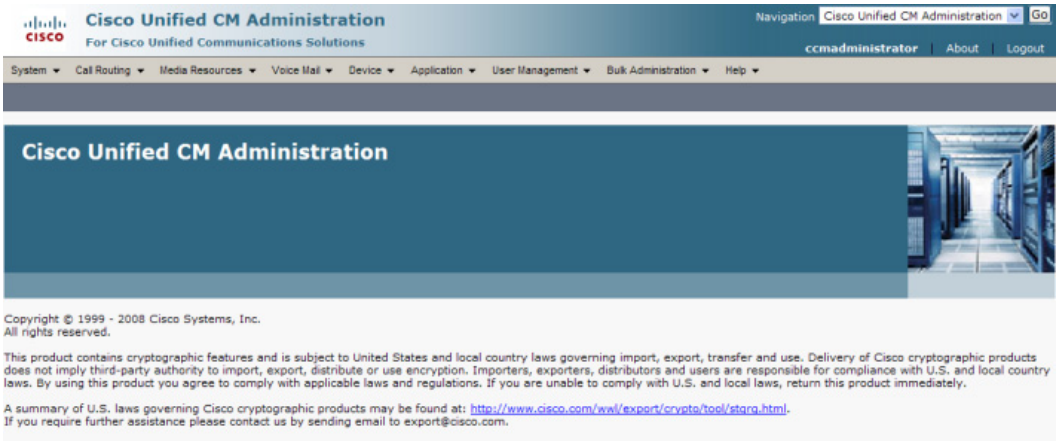
Add a SIP Trunk Security Profile That Uses TLS

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

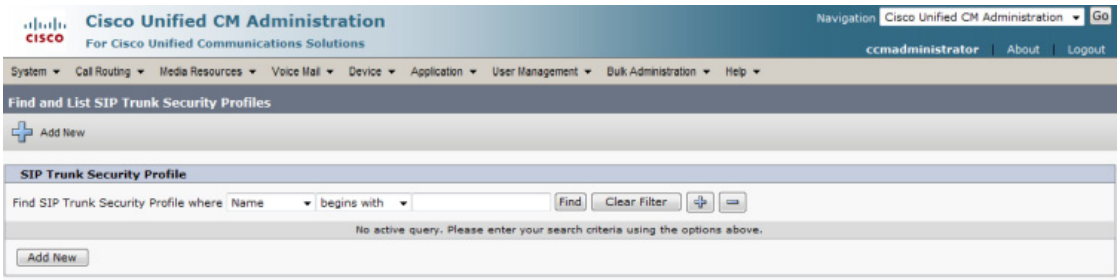
Step 1 Select **Cisco Unified CM Administration** from the **Navigation** menu and click the **Go** button. The Cisco Unified CM Administration page appears.



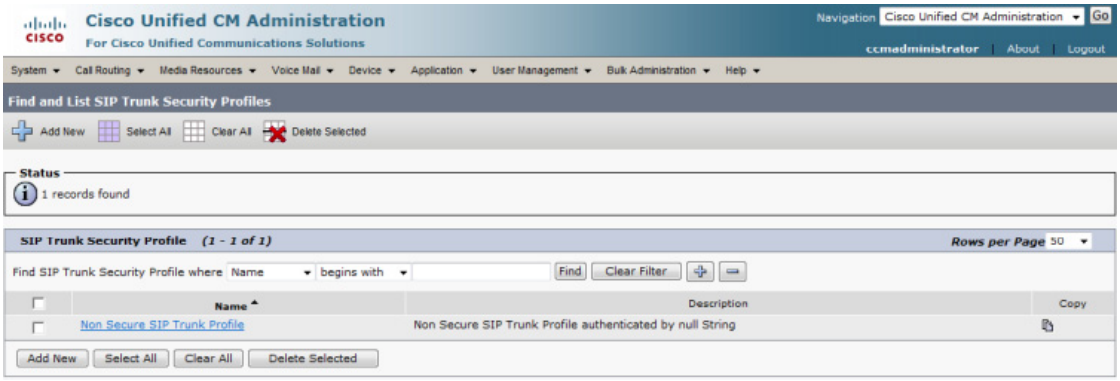
Step 2 Enter your administrative username and password in the **Username** and **Password** fields, respectively, and click the **Login** button. The Cisco Unified CM Administration page refreshes.



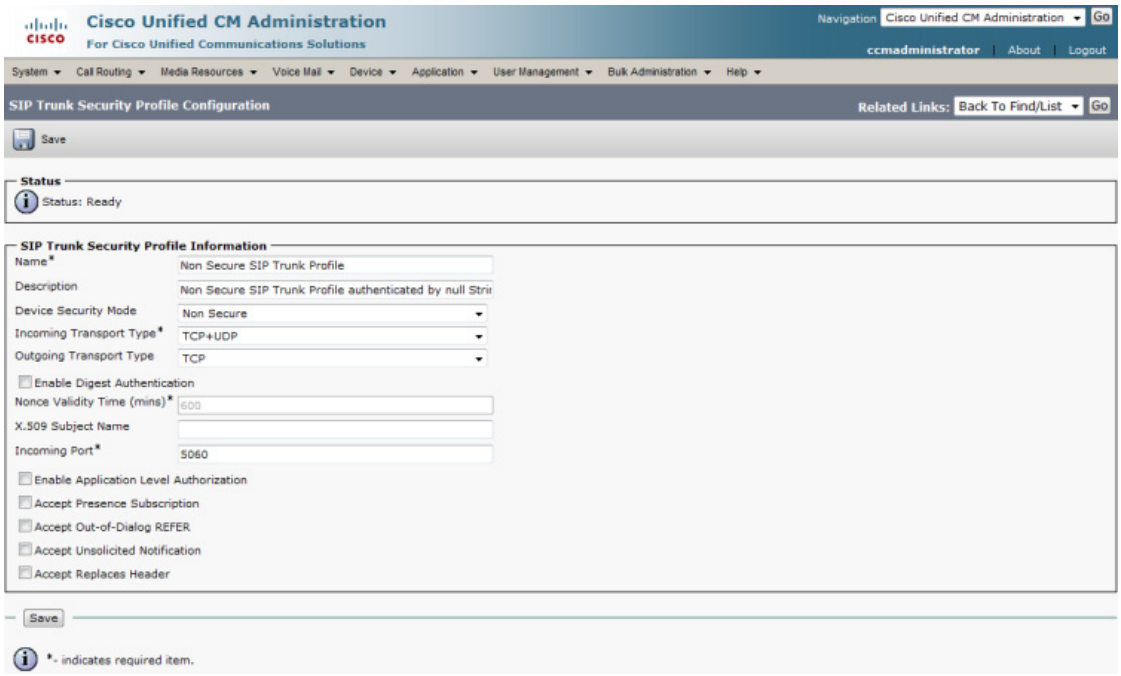
Step 3 Go to **System | Security | SIP Trunk Security Profile**. The Find and List SIP Trunk Security Profiles page appears.



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.



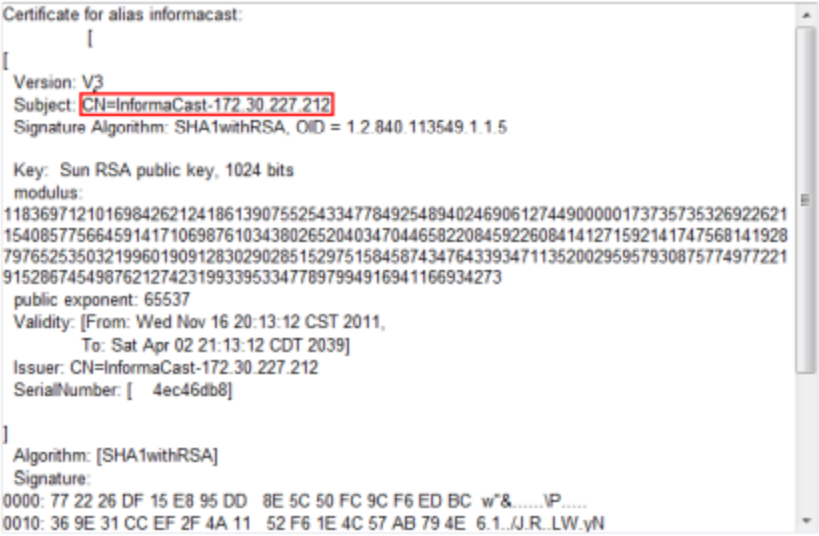
Step 6 Enter a unique name for your SIP trunk security profile in the **Name** field, e.g. InformaCastTLS.

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

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

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

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



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

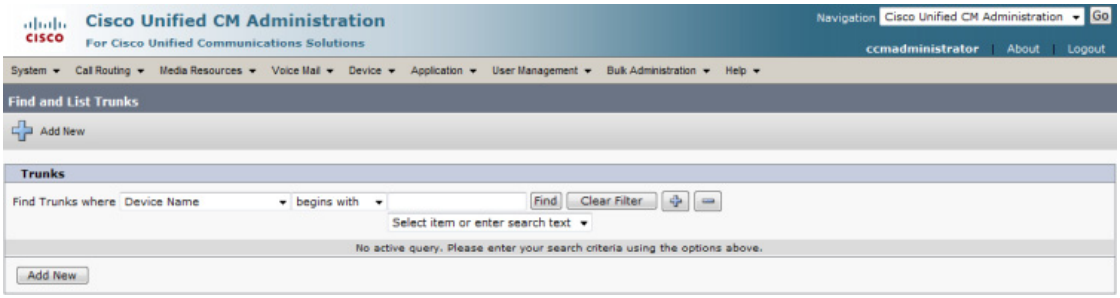
Step 12 Select the **Accept Unsolicited Notification** checkbox.

Step 13 Click the **Save** button.

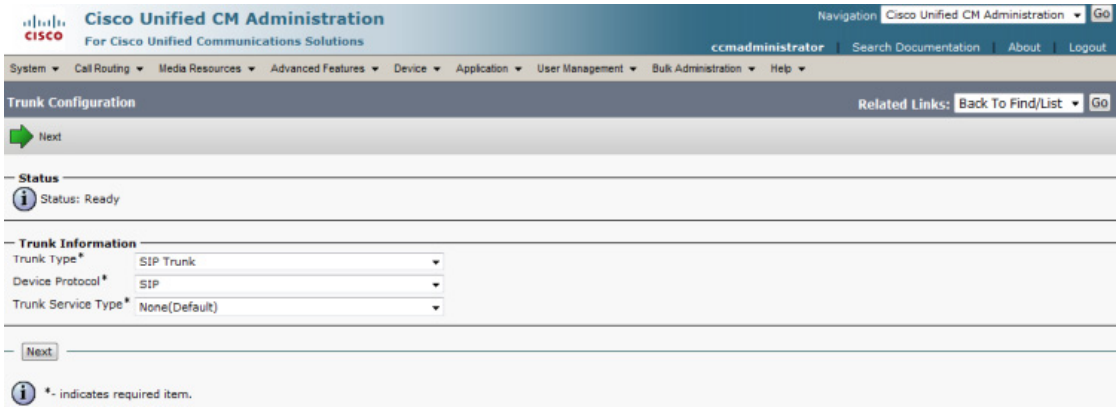
Add a SIP Trunk That Uses TLS

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 5-21.

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*			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. InformaCastTLS.

Step 8 Select the device pool you created in "Create a Device Pool" on page 2-53 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 2-56 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 5-24).

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 5-21 from the **SIP Trunk Security Profile** dropdown menu.

Step 14 Select the SIP profile you created in "Add a SIP Profile" on page 5-8 from the **SIP Profile** dropdown menu.

Step 15 Click the **Save** button.

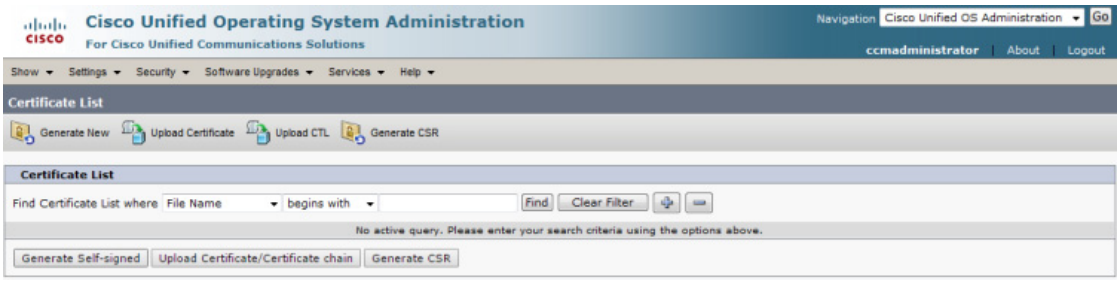
Install Unified Communications Manager Certificates on InformaCast

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

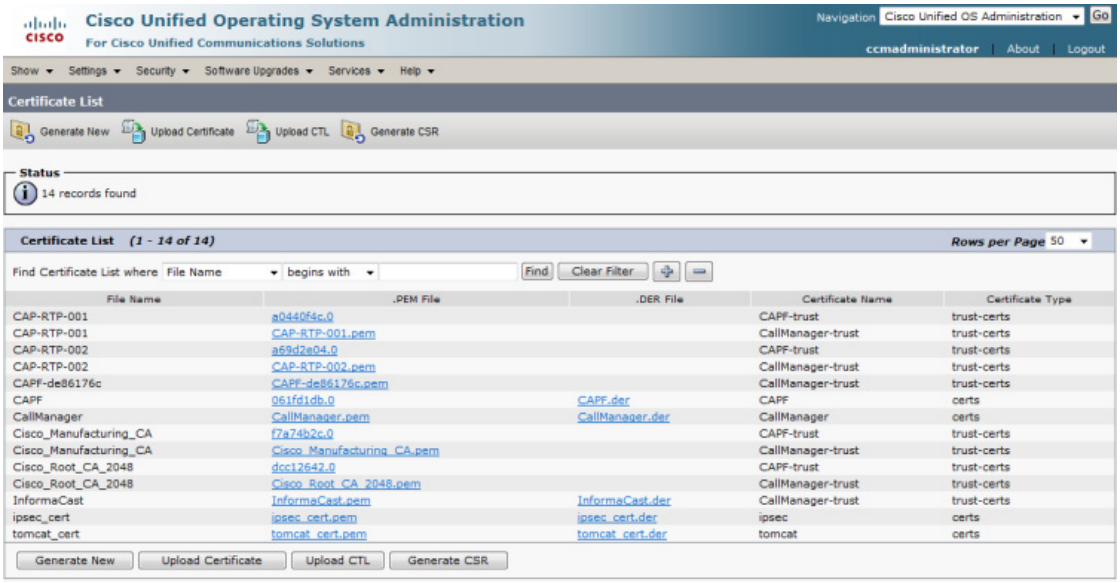
Step 1 Select **Cisco Unified OS Administration** from the **Navigation** dropdown menu and click the **Go** button. The Cisco Unified Operating System Administration page appears.

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.

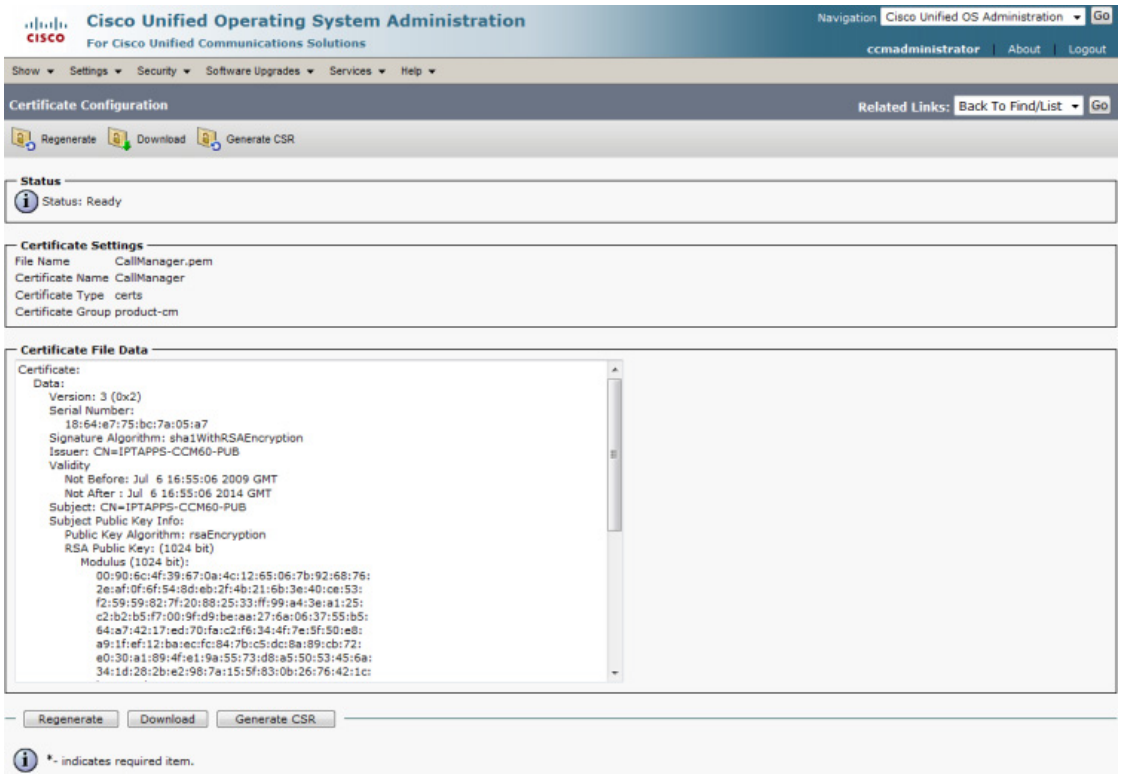
Step 3 Go to **Security** | **Certificate Management**. The Certificate List page appears.



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

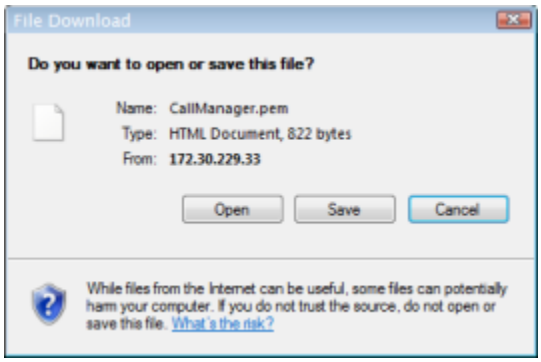


Step 5 Click the **CallManager.pem** link in the .PEM File column. The Certificate Configuration page appears.

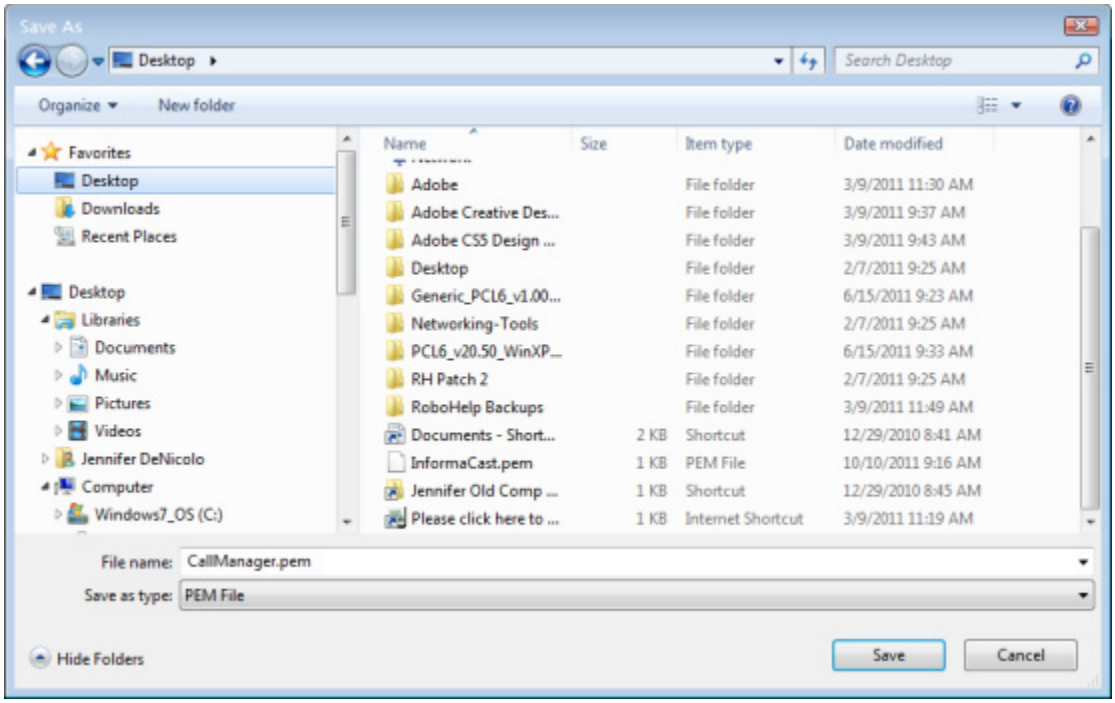


Note If you are using Unified Communications Manager 10.5 and later, you will click the **Common Name** link of the certificate that displays "CallManager" in the **Certificate** column of the Certificate List table.

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



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

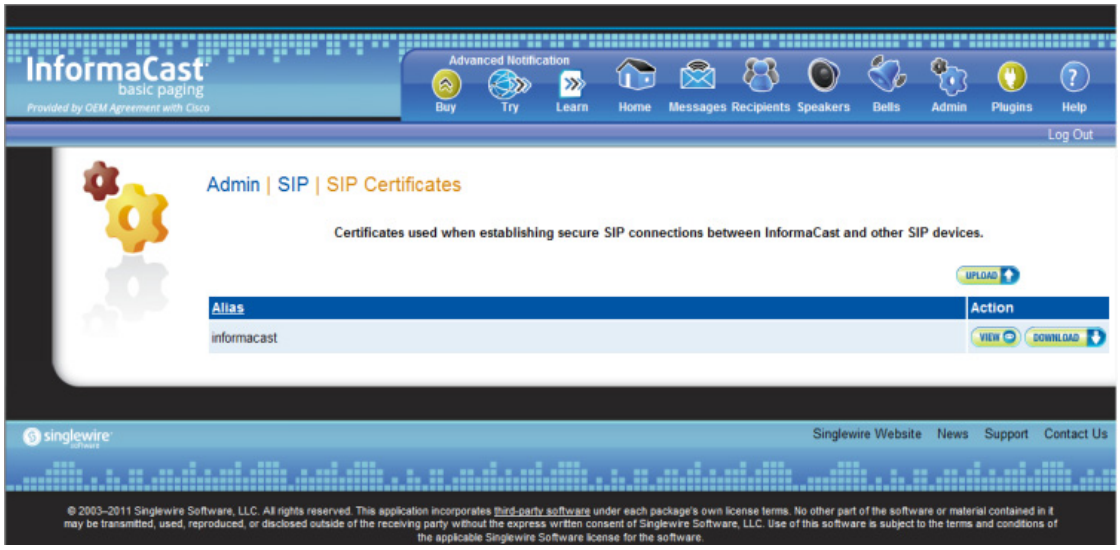


Step 8 Select a location accessible to InformaCast and click the **Save** button.

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

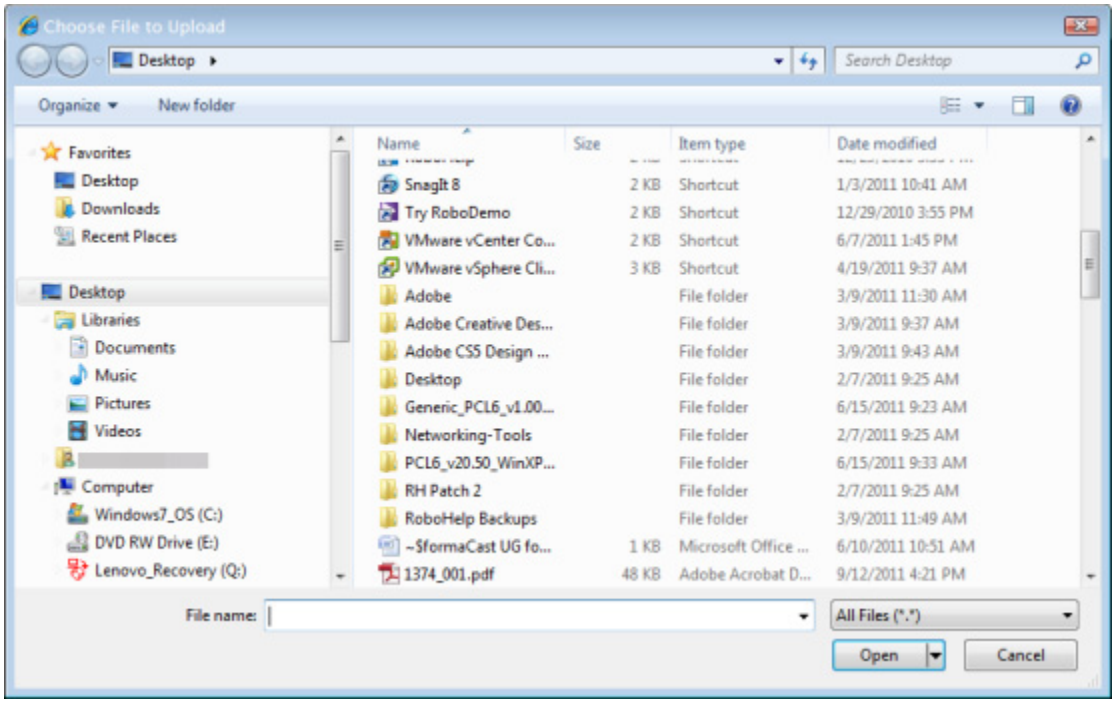
Step 9 Go back to your InformaCast window.

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.



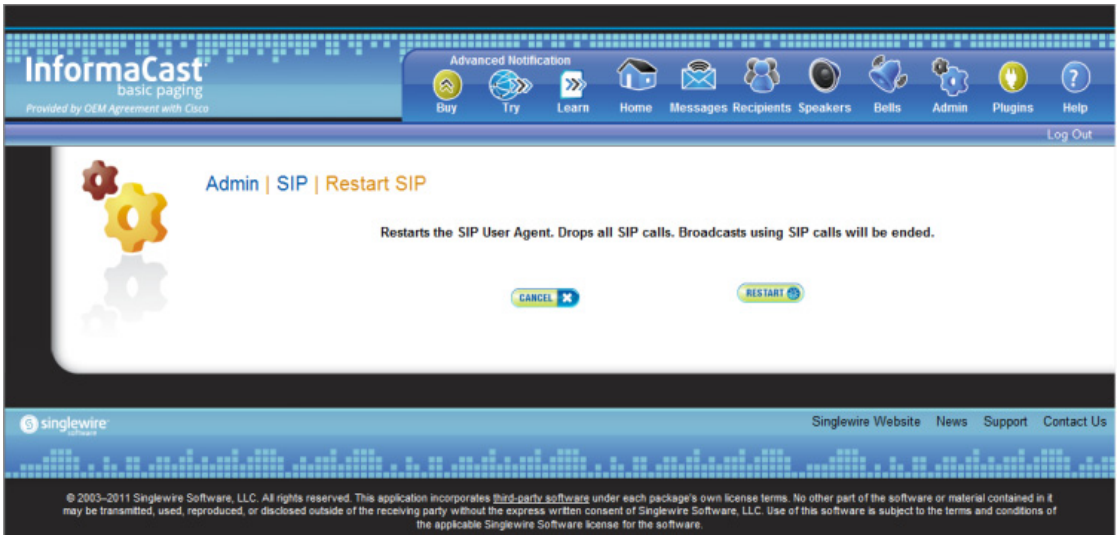
Step 13 Navigate to where you saved your CallManager.pem file, select it, and click the **Open** button.

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.



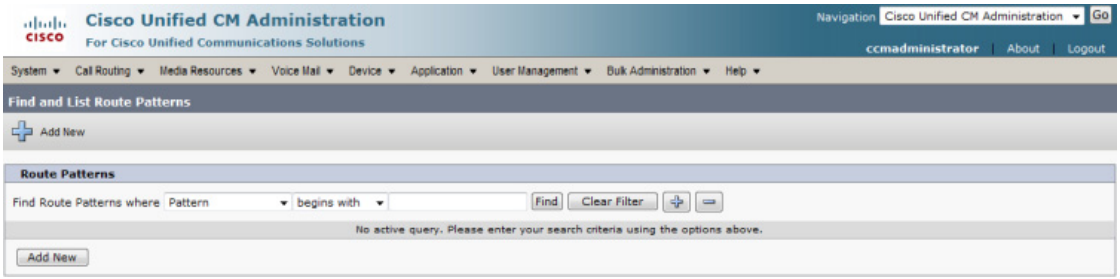
Step 17 Click the **Restart** button. It may take a few moments for SIP to restart.

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.

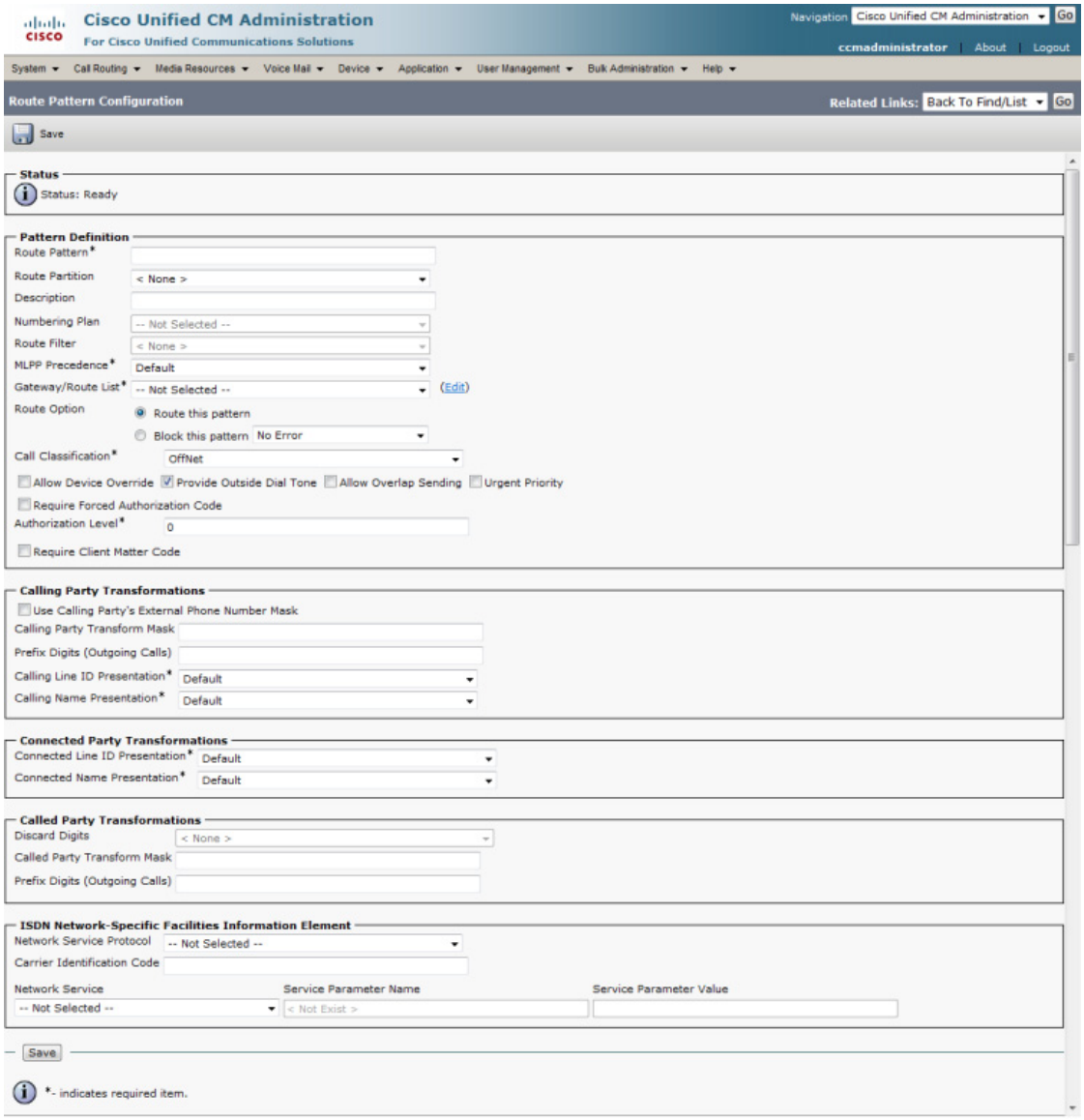
Add a Route Pattern

Use the following steps to create a route pattern that uses the SIP trunk you created in "Add a SIP Trunk" on page 5-11 or "Add a SIP Trunk That Uses TLS" on page 5-24. In your route pattern, specify a range of DNs that, when called, use the SIP trunk. Another option would be to use wild card patterns to match a range 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.



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 5-11 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.

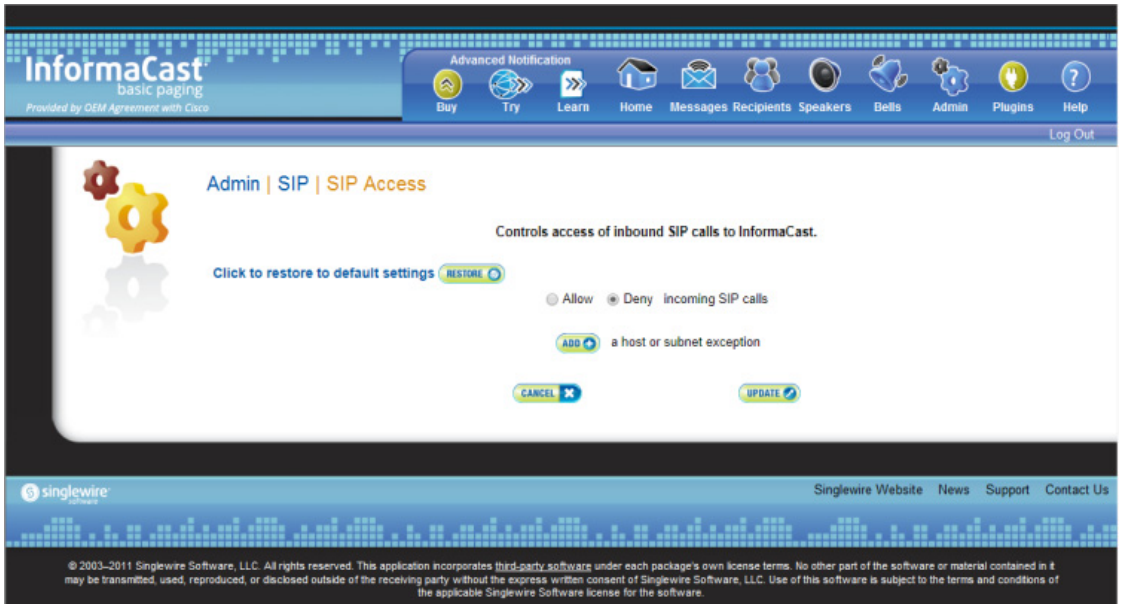
Allow/Deny SIP Access to InformaCast

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 the hosts or subnets specified in them. On the other hand, when all incoming SIP calls are allowed, exceptions serve to reject calls from the hosts or subnets specified in 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 or subnet's address is added to the request when the client sends the INVITE message.... Via headers are used by SIP to ensure that responses are routed back to the caller through the same hosts or subnets that participated in sending the request. InformaCast uses the host or subnet in the top Via header when determining if the INVITE should be accepted or denied. The top Via header represents the last host or subnet 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.

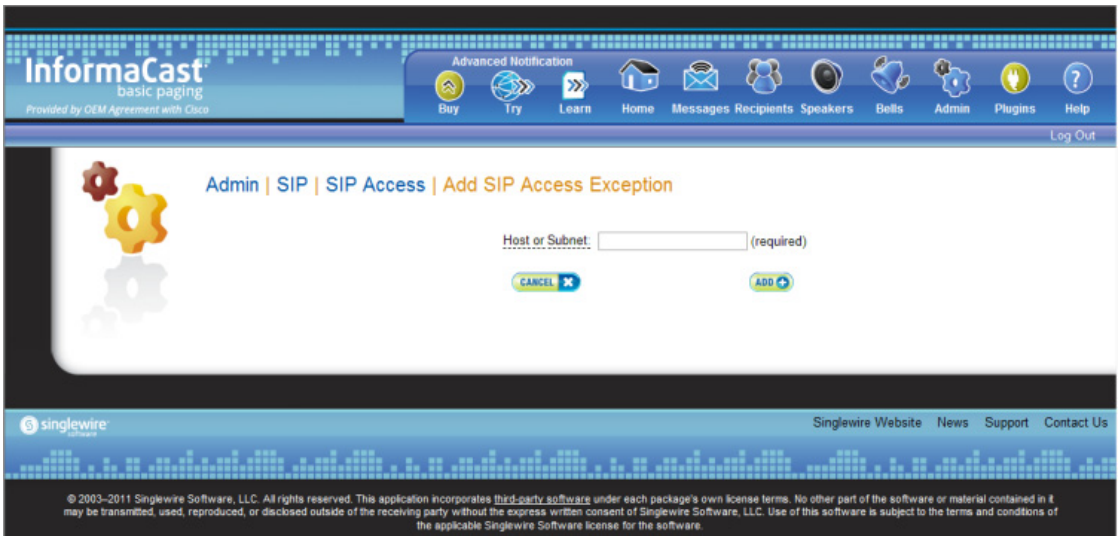
Step 1 Go to **Admin** | **SIP** | **SIP Access**. The SIP Access page appears.



Note By default, SIP access is denied.

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

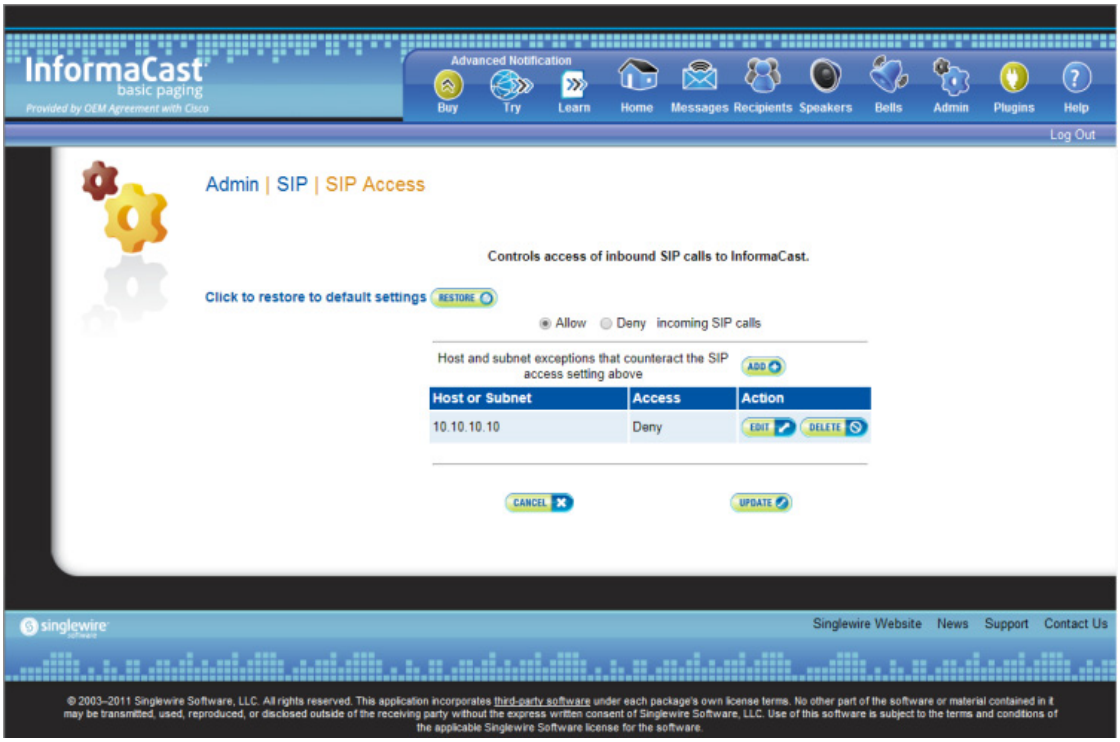
Step 3 Leave the **Deny** radio button selected and click the **Add** button to add exceptions to the SIP calls that are denied. The Add SIP Access Exception page appears.



Step 3 Enter the IP address, fully qualified domain name, or subnet (in CIDR notation) of the host you want to include in the **Host or Subnet** field. For example, sampleA and sampleB are the hostnames of two devices connected to a network domain named example.org with IP addresses of 192.168.100.1 and 192.168.100.2, respectively. Any of the following would include one or the other host: 192.168.100.1 or 192.168.100.2, sampleA.sample.org or sampleB.example.org, or you could enter 192.168.100.0/24 and get both.

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. The same holds true when using a subnet: make sure that it specifies hosts that directly send INVITE requests to InformaCast.

Step 4 Click the **Add** button. The SIP Access page appears with your new exception noted.



Note If you had elected to allow SIP access by selecting the **Allow** radio button, you can still deny some SIP access by adding exceptions, as was illustrated in Step 4. In that case, your SIP Access page would appear as follows:

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

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

Enable SIP Call Security

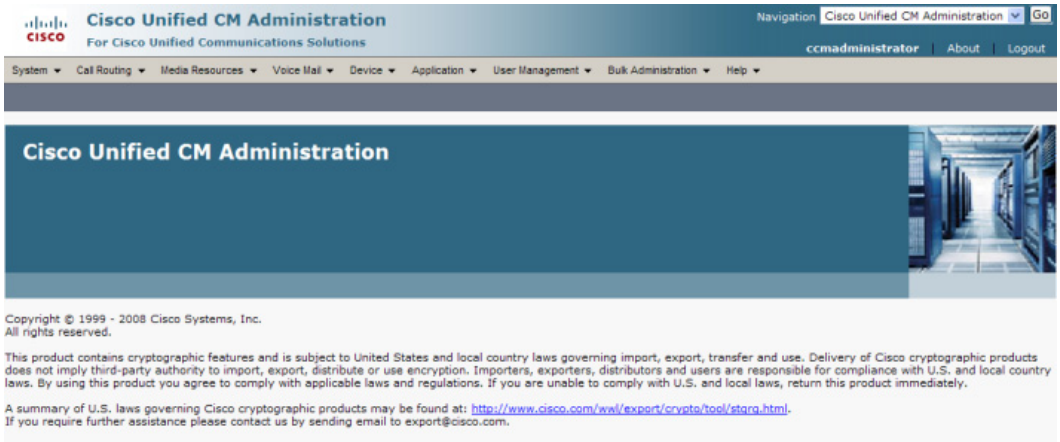
Note This section is optional depending on the security of your environment.

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:

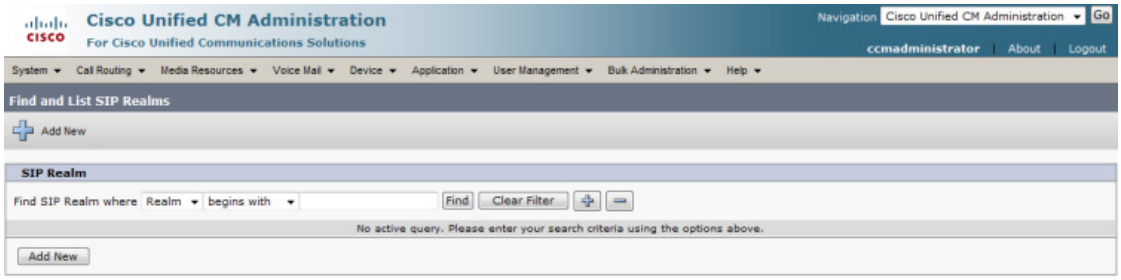
- **Default.** At this level, no encryption is used; it's just SIP over TCP or UDP.
- **Secure Signaling Required.** One level higher than the default, SIP messages are encrypted while being sent with the TLS transport protocol.
- **Secure RTP Allowed.** In conjunction with the **Secure Signaling Required** 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.

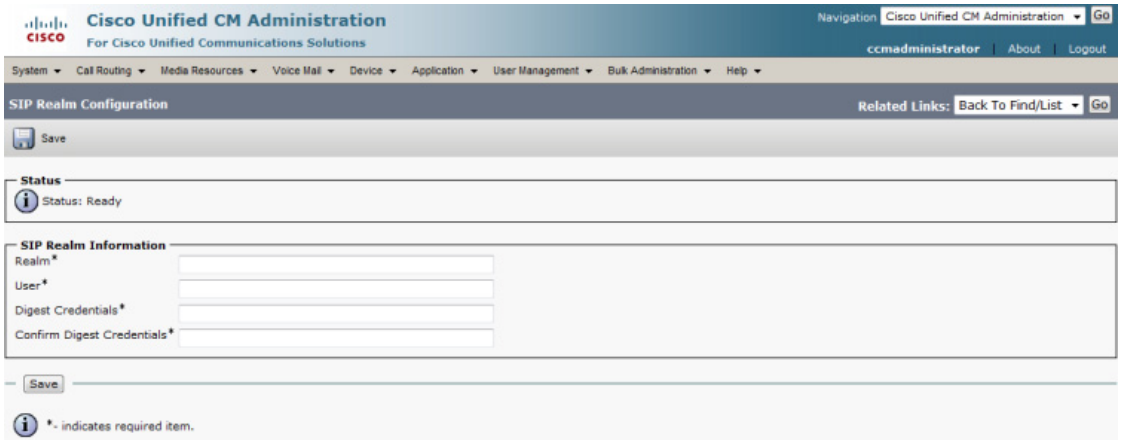
If you have a SIP realm you'd like to use, select it and make note of the values that appear in the following fields on the SIP Realm Configuration page:

- Realm
- User
- Digest Credentials

Skip to Step 10 on page 5-40.

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.

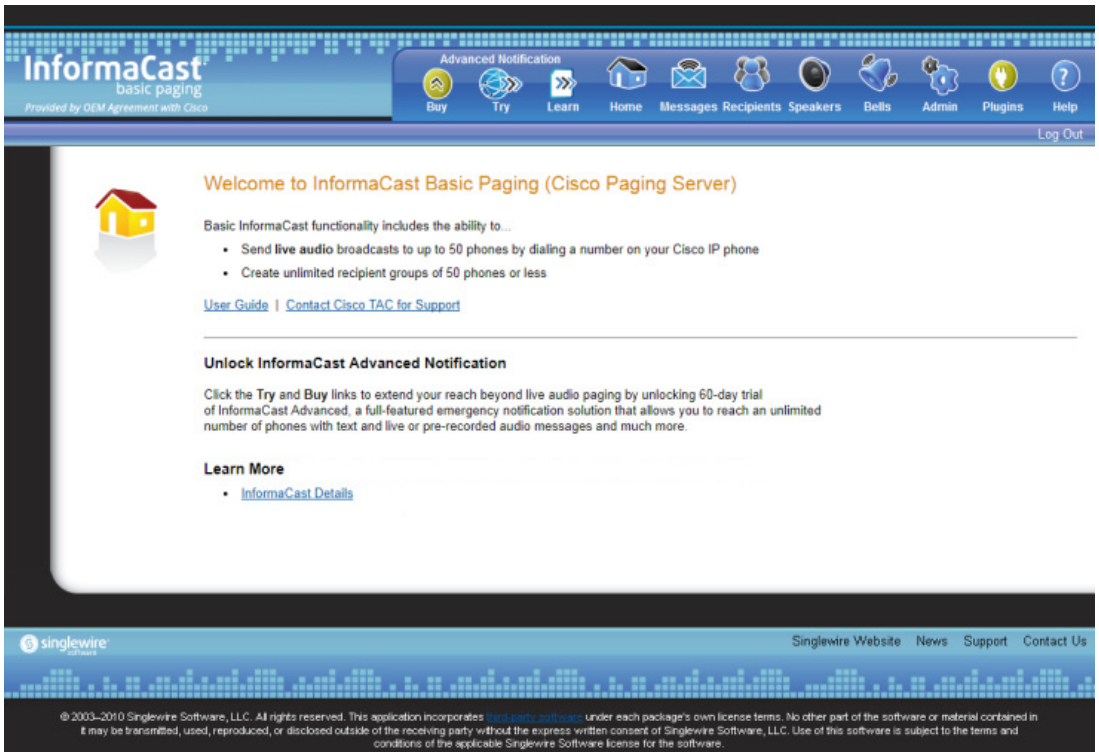
Step 6 Enter **sipuser** in the **User** field.

Step 7 Enter a secure password in the **Digest Credentials** field.

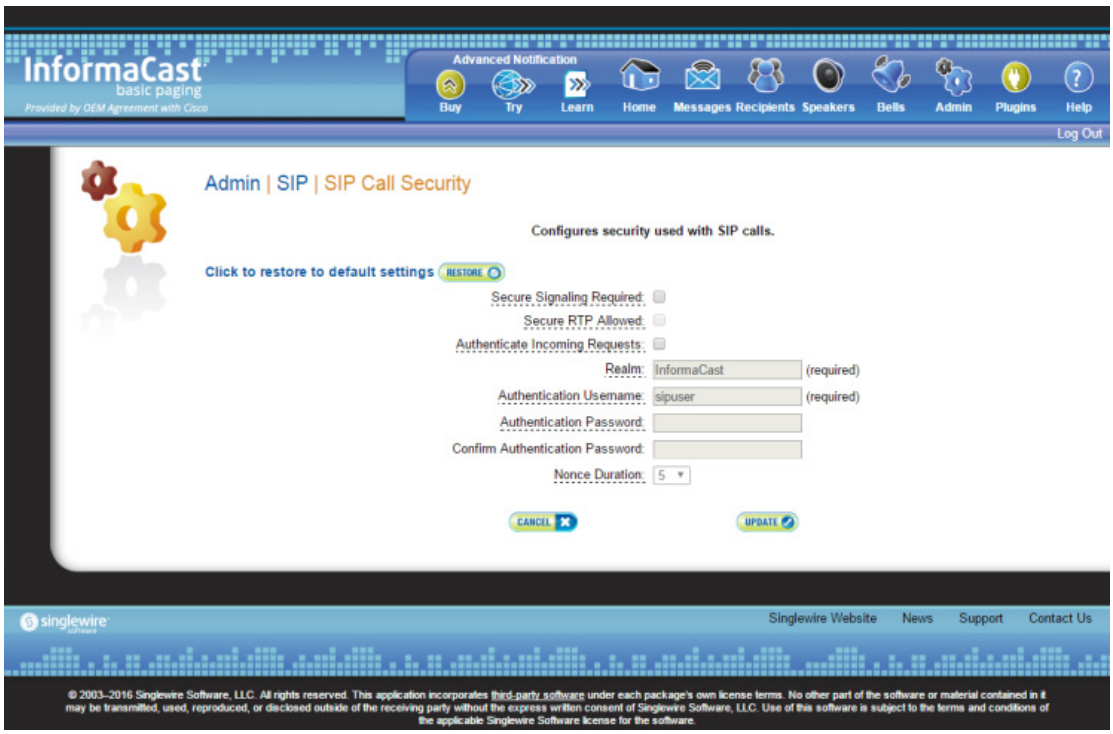
Step 8 Enter a secure password in the **Confirm Digest Credentials** field.

Step 9 Click the **Save** button.

Step 10 Log into InformaCast (see "Log into InformaCast" on page 2-31 for specific steps). The InformaCast homepage appears.



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



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

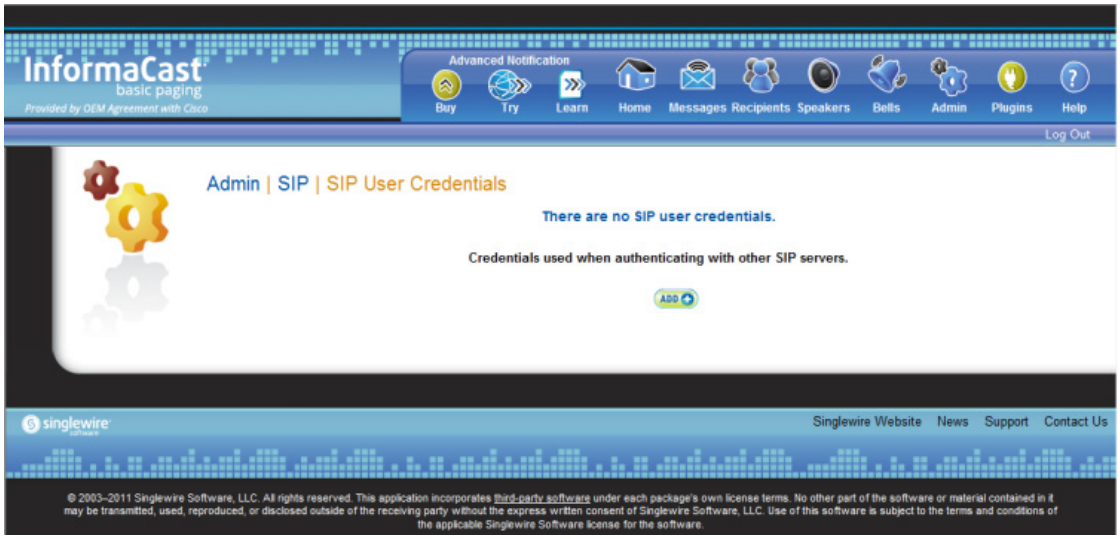
Note This section is optional depending on the security of your environment.

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.

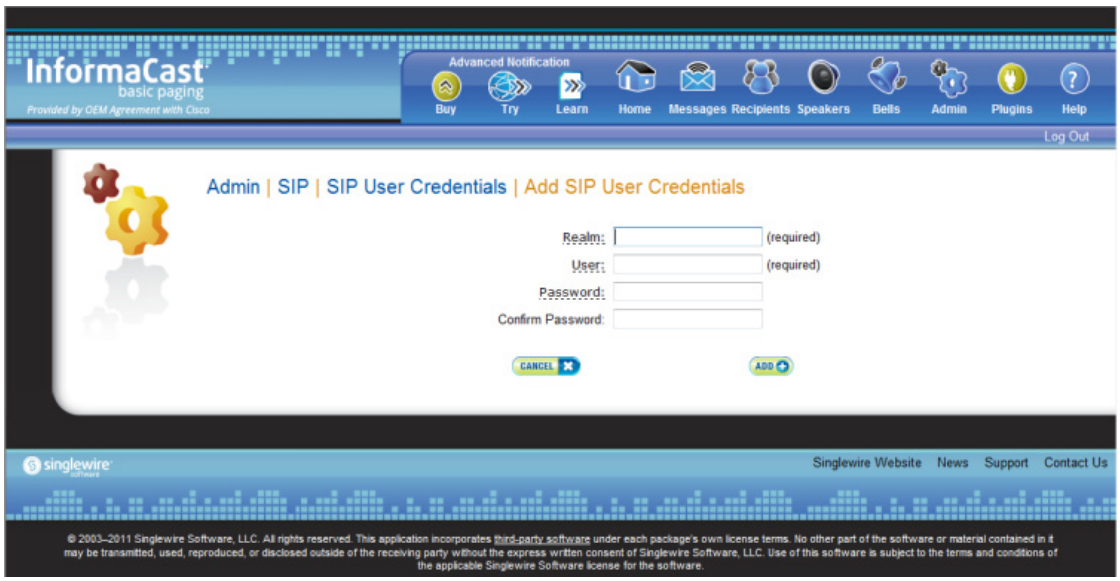
Add SIP User Credentials

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.



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.

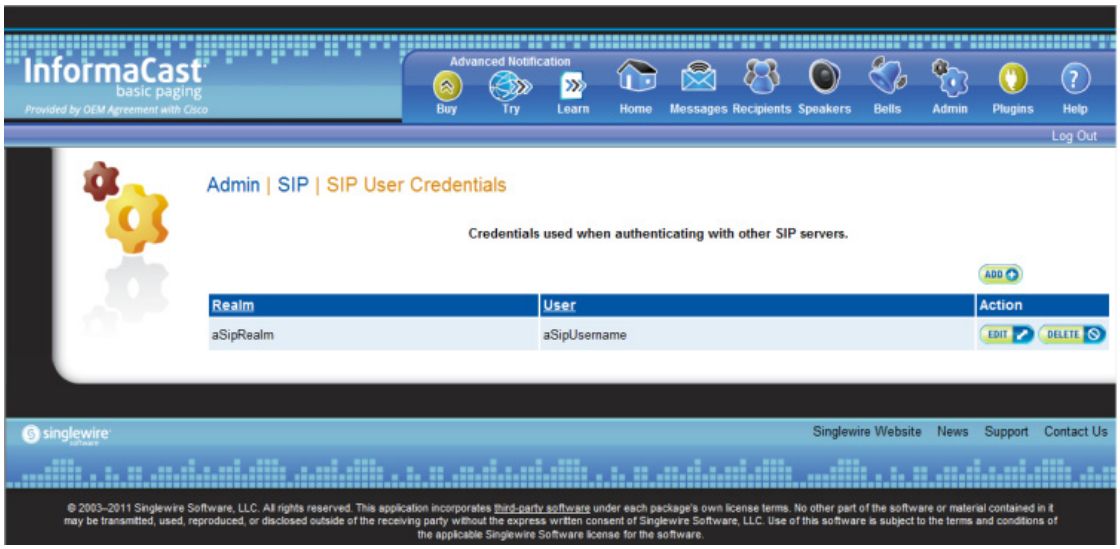
Step 5 Enter the password of the username associated with the SIP peer's SIP realm in the **Password** and **Confirm Password** fields.

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.

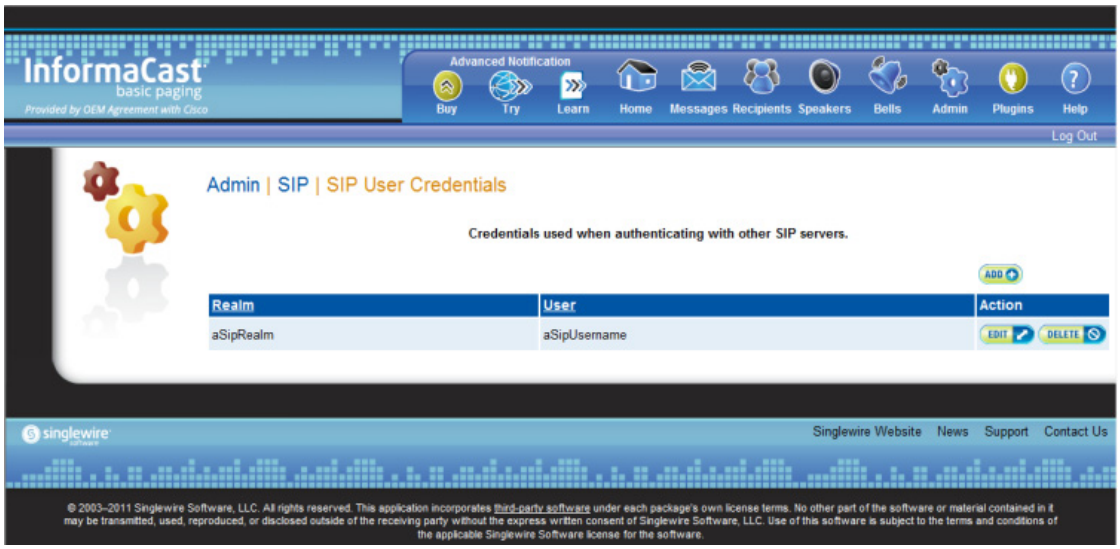
Step 3 Make your desired changes.

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

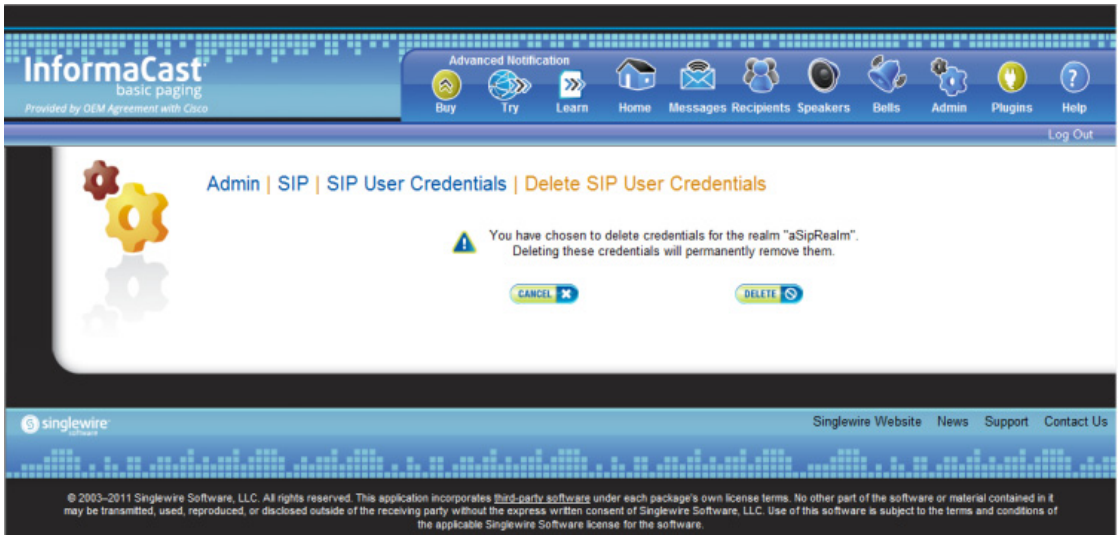
Delete SIP User Credentials

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.

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.

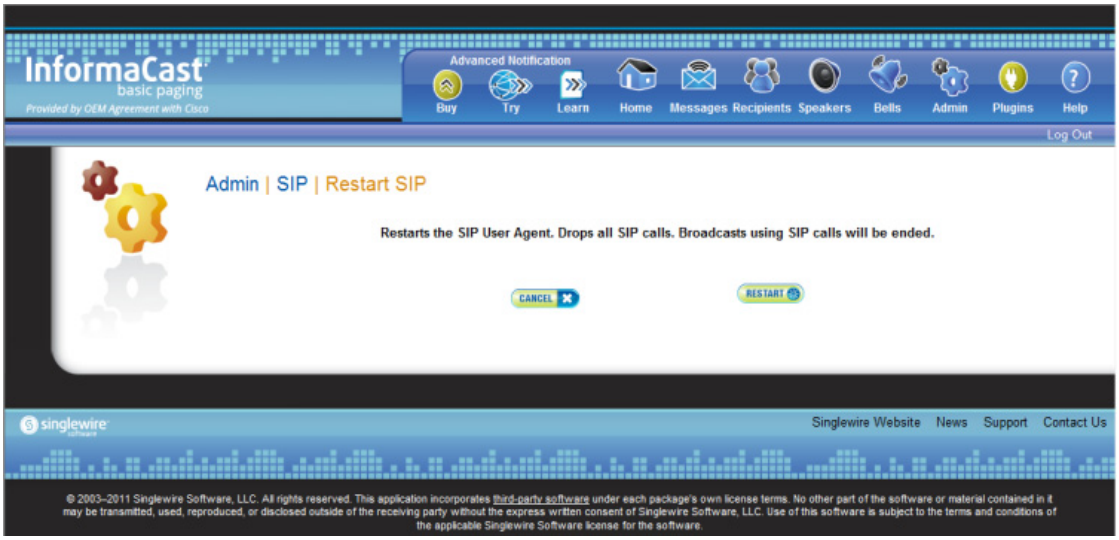
Caution You'll need to restart SIP. Restarting SIP causes all SIP calls to be dropped, i.e. any callers interacting with the DialCast IVR will have their calls dropped. Broadcasts using SIP calls will also be impacted by a restart. Live broadcasts using SIP calls will be stopped.

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.

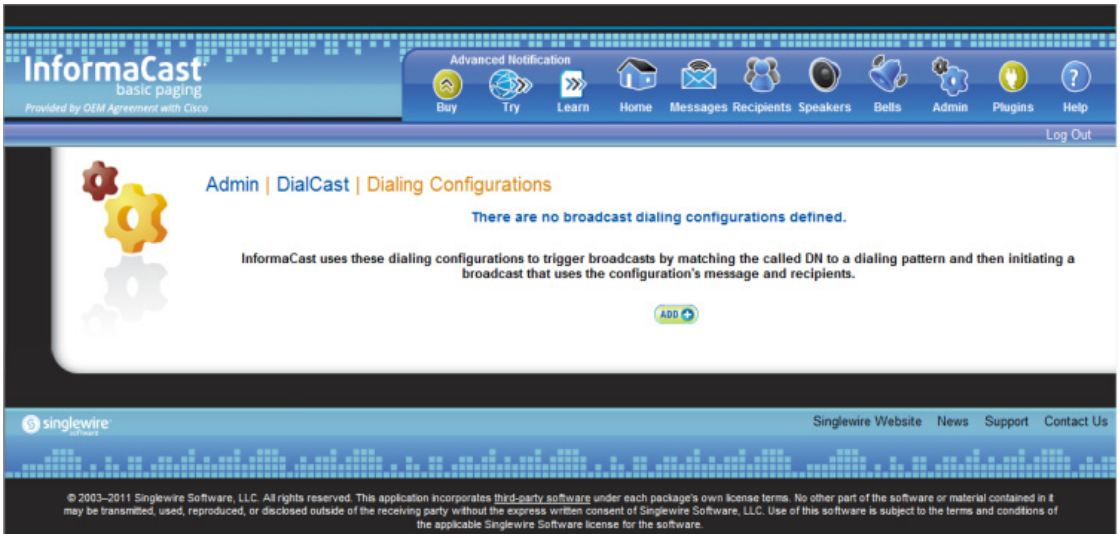
Note If you are running Unified Communications Manager in mixed mode and you want calls to and from InformaCast to use encrypted media, you must configure SRTP support (see "Enable SIP Call Security" on page 5-38).

Once you've finished configuring SIP, you can add and/or modify broadcast dialing configurations, which determine to which recipient group to broadcast based on the number that is dialed.

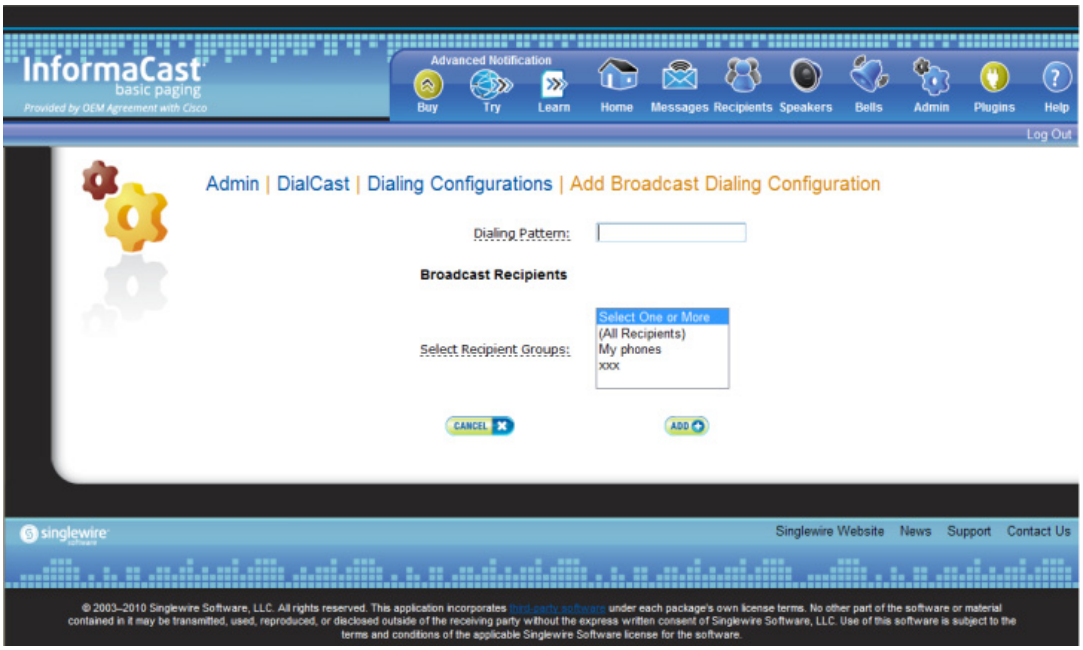
Add a Broadcast Dialing Configuration

Before you can send DialCasts, you must add broadcast dialing configurations to InformaCast.

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



Step 2 Click the **Add** button. The Add Broadcast Dialing Configuration page appears.



Step 3 Enter a dialing pattern (e.g. 8811) for a SIP trunk used with InformaCast in the **Dialing Pattern** field. You will need to add at least one dialing pattern configuration for each SIP trunk used with InformaCast.

Tip It is possible to use * or #, when setting up a dial pattern, but you must add \ before the character so that InformaCast doesn't treat it as a wildcard. For example, **1 would have a dial pattern of **1.

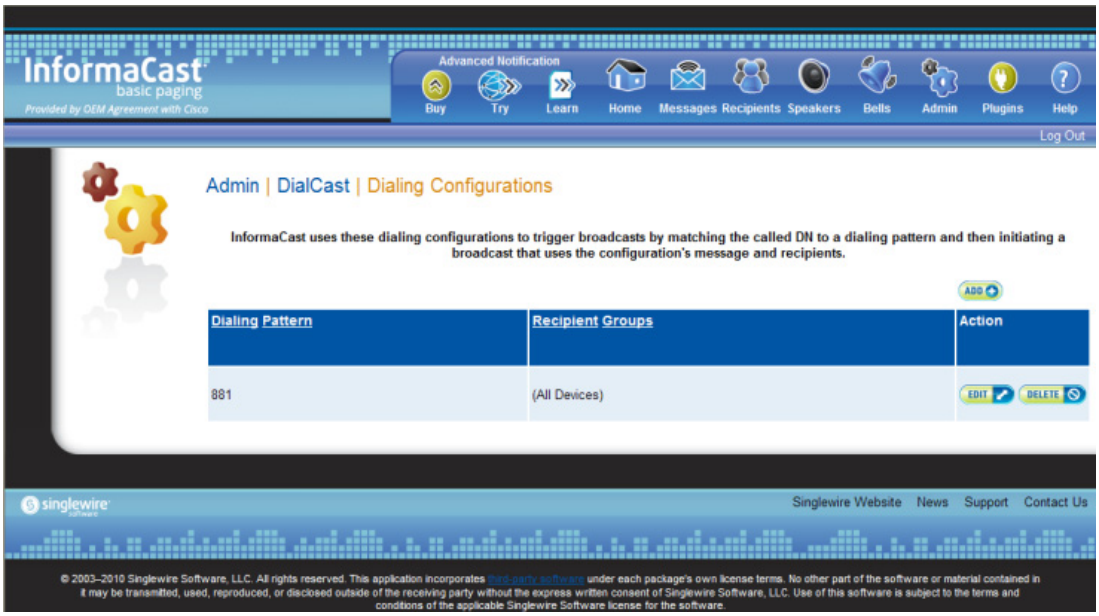
Step 4 Select a recipient group or groups from the **Select Recipient Groups** field.

Step 5 Click the **Add** button to save your current dialing pattern configuration.

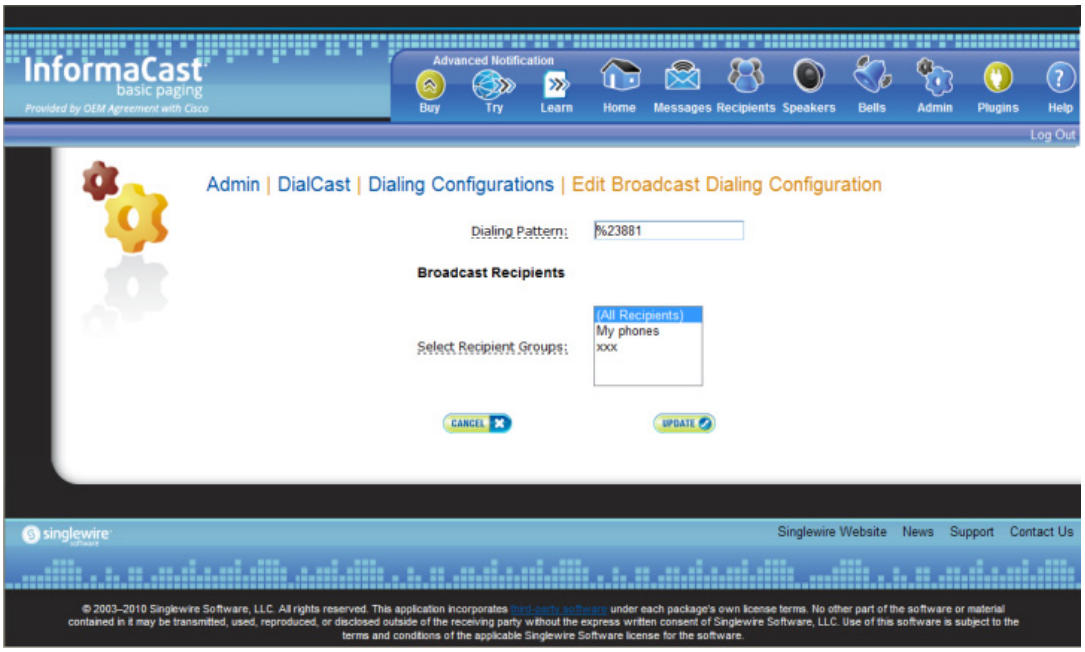
Edit a Broadcast Dialing Configuration

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

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



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



Step 3 Make your changes.

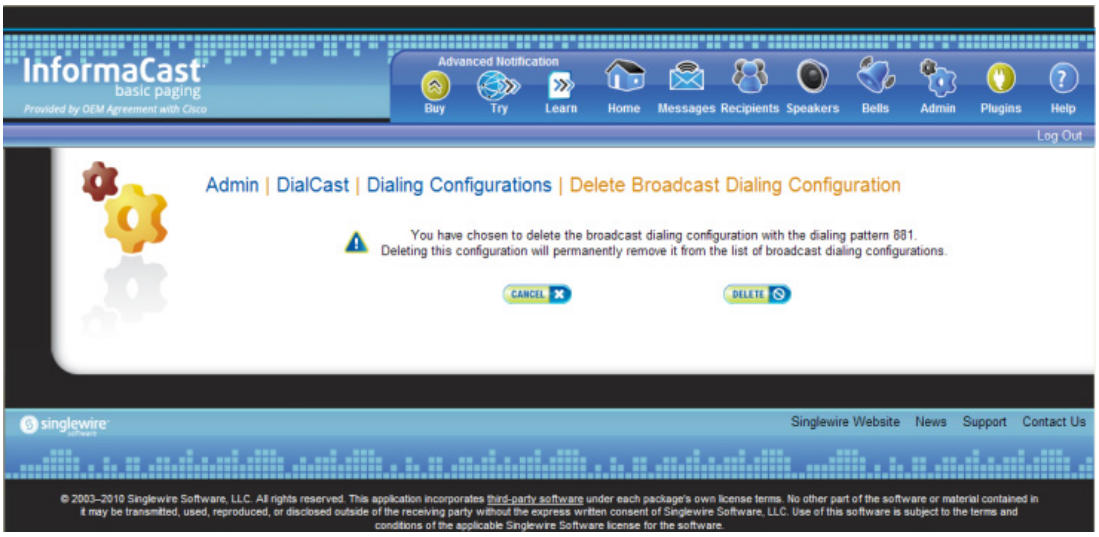
Step 4 Click the **Update** button.

Delete a Broadcast Dialing Configuration

As your needs change, you may want to delete older dialing configurations from InformaCast.

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

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



Step 3 Click the **Delete** button. Your broadcast dialing configuration is deleted.

Send a DialCast/Broadcast

With Basic InformaCast functionality, you only have the ability to send Live Audio messages through InformaCast's DialCast functionality. DialCasts are broadcasts triggered by dialing a SIP number configured with dialing pattern that determines which InformaCast message should be sent and which recipient groups should receive it.

Tip Before you can send a DialCast/broadcast, you must have a SIP trunk configured (see "Configure a SIP Trunk" on page 5-4) as well as DialCasts (see "Manage DialCasts" on page 5-48).

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 5-49), 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

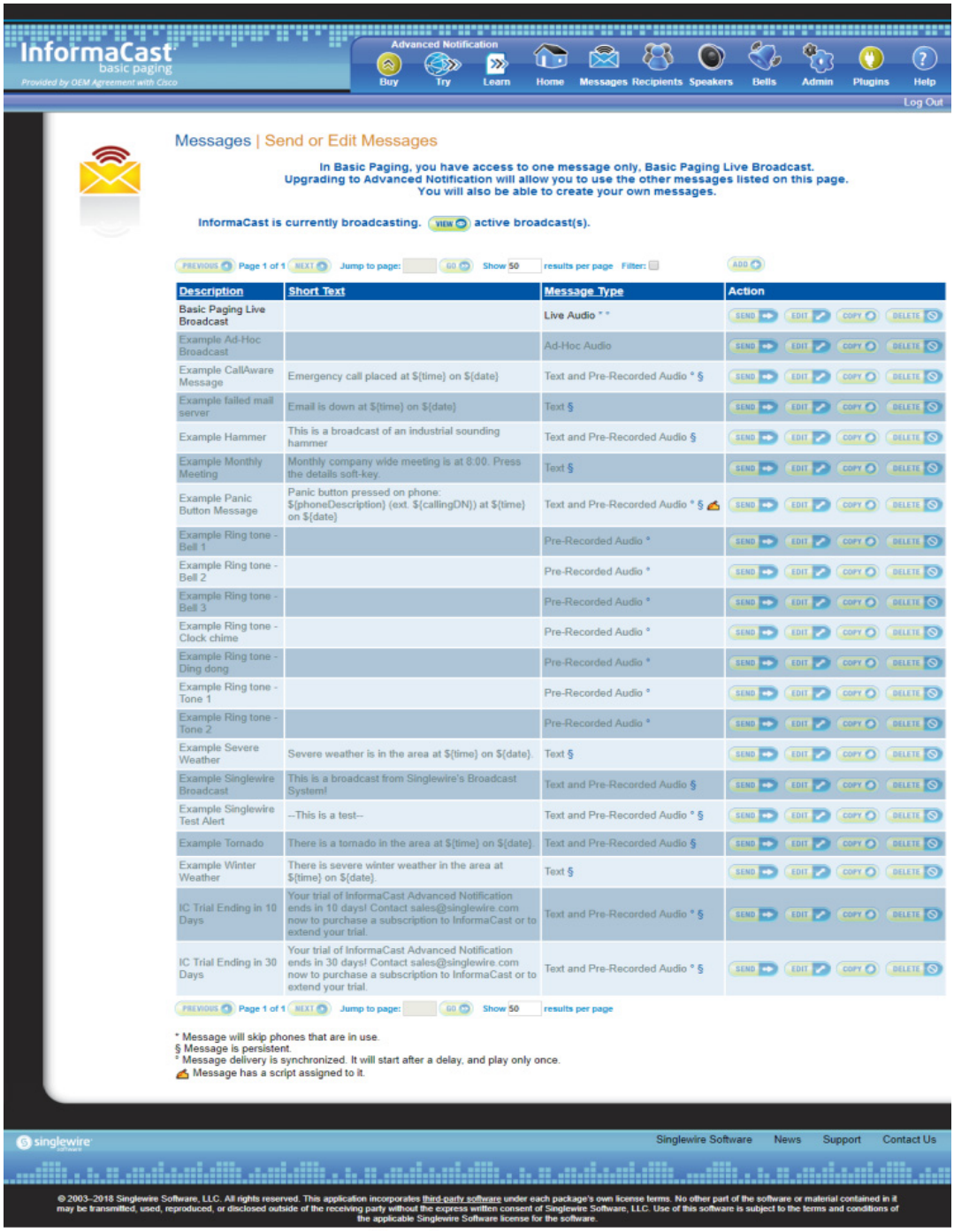
For more information on these message types, see the table in "Manage Messages" on page 5-1.

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.

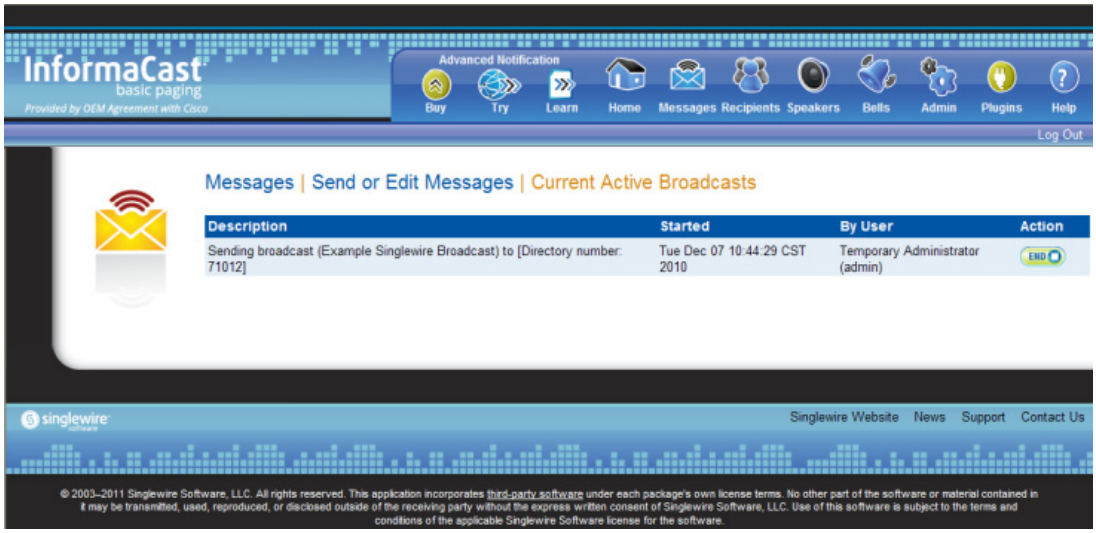
Cancel a DialCast/Broadcast

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."



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



This list offers you the ability to end any of the active broadcasts. This is particularly useful if, for example, an attempt to capture audio has been accidentally directed to a voicemail system.

Step 3 Click the **End** button of the broadcast you'd like to cancel. InformaCast displays a confirmation screen to make sure you picked the right message and that you really want to end the broadcast.

Step 4 Click the **End** button. InformaCast will stop sending the broadcast, and take you back to the Send or Edit Messages page.

If the message ends on its own or is cancelled by another administrator while you're following these steps, InformaCast will tell you that there are no active broadcasts.

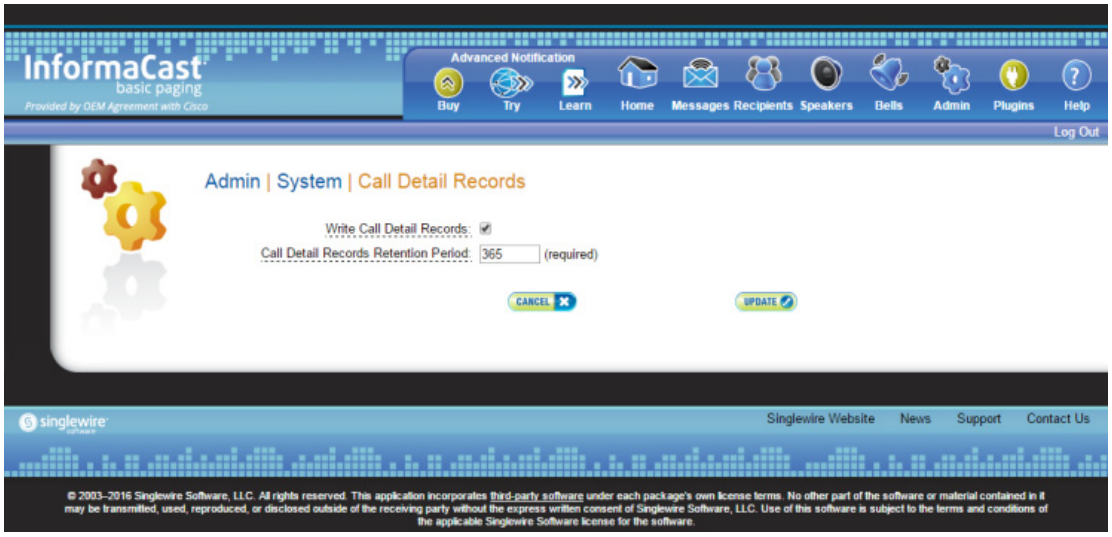
Manage Call Detail Records

When configured, InformaCast can create a call detail record for every SIP and CTI call it receives (for example, 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 or CTI calls, you may want to keep your retention period low.

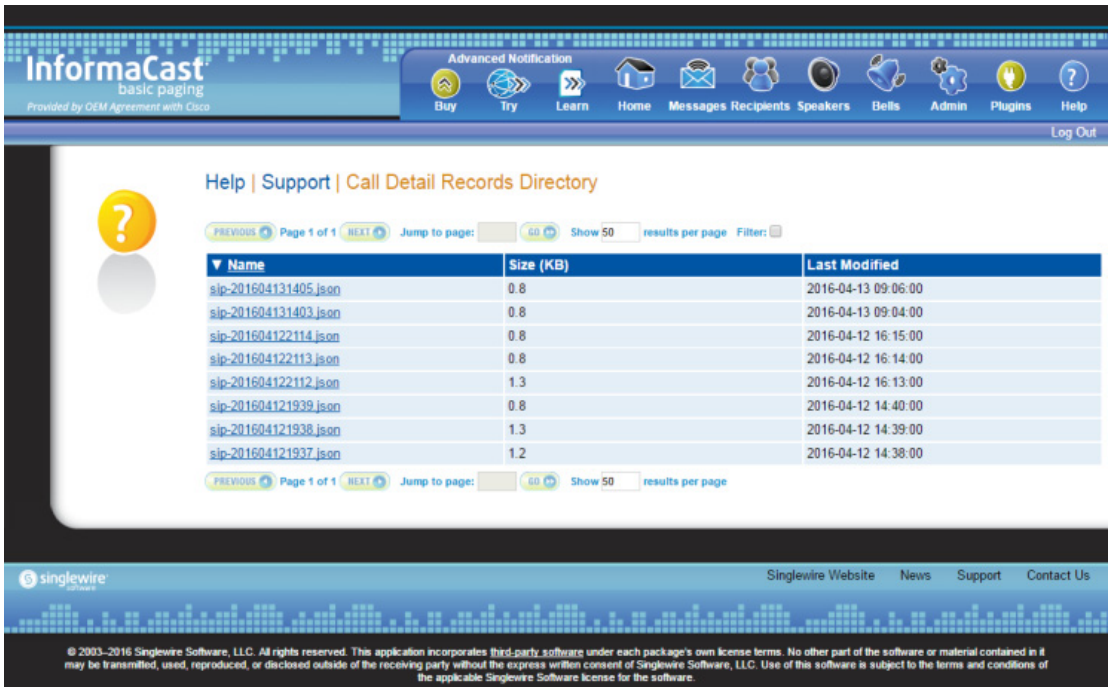
Step 4 Click the **Update** button to save your changes.

View Call Detail Records

When InformaCast is configured to collect call detail records (see "Collect Call Detail Records" on page 5-56), those records are written to a directory accessible through the **Call Detail Records Directory** link on the Support page. InformaCast collects two types of call details records: SIP and CTI.

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

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



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 SIP call detail record might look similar to the following picture.


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


Each file has the following call detail record structure:

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

Each SIP call within the record has the following structure:

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

}
```

With sessionActivity defined like this:

```
"sessionActivity" : [ { "SIP" : { <SIP-data>},  "SDP" : { <SDP-data>} }, …, {
    "RTP"

: {<RTP-data>}, "DTMF", {<DTMF-data>} }, ... ]
```

A CTI call detail record might look similar to the following picture.


```
{
    "records": [
        {
            "callID": "72008/1",
            "component": "ParkAndPage",
            "start": "2017-07-06 08:51:47,889",
            "end": "2017-07-06 08:52:19,109",
            "duration": "000:00:00:31,220",
            "callActivity": [
                {
                    "routeEvent": "RouteEvent",
                    "time": "2017-07-06 08:51:47,889",
                    "epochTime": 1499349107,
                    "terminal": "    RoutePoint1",
                    "callingTerminal": "                ",
                    "callingPartition": "InformaCast",
                    "callingDN": "105003",
                    "calledDN": "#711",
                    "lastRedirectedDN": "",
                    "modifiedCalledDN": "#711",
                    "currentCalledDN": "#711"
                },
                {
                    "info": "triggerDestination",
                    "time": "2017-07-06 08:51:47,896",
                    "epochTime": 1499349107,
                    "triggerID": "2",
                    "destinationID": "0"
                },
                {
                    "routeEvent": "RouteUsedEvent",
                    "time": "2017-07-06 08:51:47,905",
                    "epochTime": 1499349107,
                    "terminal": "    RoutePoint1",
                    "routeUsed": "#105001"
                },
                {
                    "routeEvent": "RouteEndEvent",
                    "time": "2017-07-06 08:51:47,905",
                    "epochTime": 1499349107,
                    "terminal": "    RoutePoint1",
                    "cause": "CAUSE_NO_ERROR"
                },
                {
                    "routeAction": "SelectRoute",
                    "time": "2017-07-06 08:51:47,906",
                    "epochTime": 1499349107,
                    "terminal": "    RoutePoint1",
                    "routes": "#105001,105000",
                    "css": "ROUTEADDRESS_SEARCH_SPACE"
                },
                {
                    "callEvent": "CallCtlConnOfferedEv",
                    "time": "2017-07-06 08:51:47,911",
                    "epochTime": 1499349107,
                    "connDN": "#105001",
                    "callingTerminal": "                ",
                    "callingPartition": "InformaCast",
                    "callingDN": "105003",
                    "calledDN": "#711",
                    "lastRedirectedDN": "#711",
                    "modifiedCalledDN": "#105001",
                    "currentCalledDN": "#105001"
                },
                {
                    "callEvent": "CallCtlTermConnRingingEvImpl",
                    "time": "2017-07-06 08:51:47,915",
                    "epochTime": 1499349107,
                    "termConnTerminal": "    CtiPort01",
                    "termConnDN": "#105001",
                    "callingTerminal": "SEP3037A616CD9E",
                    "callingPartition": "InformaCast",
                    "callingDN": "105003",
                    "calledDN": "#711",
                    "lastRedirectedDN": "#711",
                    "modifiedCalledDN": "#105001",
                    "currentCalledDN": "#105001"
                },
                {
                    "callEvent": "CallCtlTermConnTalkingEv",
                    "time": "2017-07-06 08:51:47,923",
                    "epochTime": 1499349107,
                    "termConnTerminal": "    CtiPort01",
                    "termConnDN": "#105001",
                    "callingTerminal": "                ",
                    "callingPartition": "InformaCast",
                    "callingDN": "105003",
                    "calledDN": "#711",
                    "lastRedirectedDN": "#711",
                    "modifiedCalledDN": "#105001",
                    "currentCalledDN": "#105001"
                },
                {
```


Each file has the following call detail record structure:

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

With callActivity defined like this:

```
"callActivity" : [ { <Route-Request>},  { <Route-Action>} ,{<Call-Event>},
   {<Call-Action>},{<Provider-Event>}, {<Terminal-Event>},
   {<Broadcast-Action>}, {<Info>},...]
```

Summary data, which applies to both SIP and CTI call detail records, 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@ xxx.xx.xxx.xxx
component	The part of InformaCast handling the call, e.g. DialCast, call recording, and/or the CallAware, Night Bell, Park and Page, and Legacy Paging Interface plugins	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

The next tables have been separated into SIP or CTI types.

SIP Data Tables

Session activity 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 the SIP message's 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

Field	Definition	Example
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
negotiatedDtmfMethod	The DTMF transport method negotiated between InformaCast and Unified Communications Manager, which is used when the LPI plugin sends an INVITE without an offer (delayed offer), 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.xxx:18270
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.xxx:18270

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

CTI Data Tables

Call action data includes the actions taken by InformaCast and its plugins to control CTI calls, as shown in the following table:

Field	Definition	Example
callAction	The call action performed, e.g. Accept, Answer, Connect, Park, Redirect, Reject, and Unpark	Park
<Time-data>	The time when the action was performed	See Time Data table
callingTerminal	The calling terminal for the Connect action	CtiPort05
callingDN	The calling DN for the Connect action	#91140
calledDN	The called DN for the Connect action	105065
parkingTerminal	The parking terminal for the Park action	CtiPort05
parkingDN	The parking DN for the Park action	#91140
parkDN	The park DN for the Park or Unpark action	105065
redirectDN	The redirect DN for the Redirect action	105098
css	The calling search space for the Redirect action, e.g. ADDRESS_SEARCH_SPACE, DEFAULT_SEARCH_SPACE, and CALLINGADDRESS_SEARCH_SPACE	ADDRESS_SEARCH_SPACE
unparkingTerminal	The unparking terminal for the Unpark action	CtiPort05
unparkingDN	The unparking DN for the Unpark action	#91140

Call event data includes the JTAPI call events received by InformaCast and its plugins during CTI calls, as shown in the following table:

Field	Definition	Example
callEvent	The name of the call event	CallCtlConnOfferedEv
<Time-data>	The time when the event was received	See Time Data table
connDN	The connection DN for a connection event, e.g. connection offered	#91140
termConnTerminal	The terminal-connection terminal for a terminal-connection event, e.g. terminal connection talking	CtiPort05
termConnDN	The terminal-connection DN for a terminal-connection event, e.g. terminal connection talking	#91140
transferToDN	The DN call a is being transferred to for a CiscoTransferStartEv or CiscoTransferEndEv event	#91140
<Call-Data>	The call data for the event	See Call Data table

Call data includes the data common to both JTAPI call and route events received by InformaCast and its plugins during CTI calls, as shown in the following table:

Field	Definition	Example
callingTerminal	The calling terminal	SEP3037A616CD9E
callingPartition	The partition of the calling DN	InformaCast
callingDN	The calling DN	105065
calledDN	The called DN	#771
lastRedirectedDN	The last DN that redirected the call	#771
modifiedCalledDN	The modified called DN	#771
currentCalledDN	The current called DN	#771

Provider event data includes the JTAPI provider events received by InformaCast and its plugins during CTI calls, as shown in the following table:

Field	Definition	Example
providerEvent	The name of the provider event	CiscoProvCallParkEv
<Time-data>	The time when the event was received	See Time Data table
parkDN	The park DN for a call park event	80100
parkPartition	The partition of the park DN for a call park event	InformaCast

Field	Definition	Example
parkedParty	The parked DN for a call park event	105065
parkedPartyPartition	The partition of the parked DN for a call park event	InformaCast
parkingPartyDN	The parking DN for a call park event	#91137
parkingPartyPartition	The partition of the parking DN for a call park event	InformaCast
reason	The reason for a call park event, e.g. REASON_CALLPARK, REASON_CALLPARKREMINDER, and REASON_CALLUNPARK	REASON_CALLPARKREMINDER
state	The park state for a call park event, e.g. PARK_STATE_ACTIVE and PARK_STATE_IDLE	PARK_STATE_ACTIVE
duration	The parked duration for a call park event in the format of ssss,mmm	0029,139

Route action data includes the actions taken by InformaCast and its plugins to route CTI calls, as shown in the following table:

Field	Definition	Example
routeAction	The route action performed, e.g. SelectRoute and EndRoute	SelectRoute
<Time-data>	The time when the action was performed	See Time Data table
terminal	The route terminal associated with the event	RoutePoint
routes	A comma-separated list of DNs for the SelectRoute action	#91140,#91138,105098
css	The calling search space for the SelectRoute action, e.g. DEFAULT_SEARCH_SPACE, CALLINGADDRESS_SEARCH_SPACE, and ROUTEADDRESS_SEARCH_SPACE	ROUTEADDRESS_SEARCH_SPACE
reason	The reason for ending a route session for the EndRoute action, e.g. CAUSE_NO_ERROR, ERROR_UNKNOWN, ERROR_RESOURCE_BUSY, and ERROR_RESOURCE_OUT_OF_SERVICE	CAUSE_NO_ERROR

Route event data includes the JTAPI route events received by InformaCast and its plugins during CTI calls, as shown in the following table:

Field	Definition	Example
routeEvent	The type of route event, e.g RouteEvent, ReRouteEvent, RouteUsedEvent, and RouteEndEvent	RouteEvent
<Time-data>	The time when the action was performed	See Time Data table
terminal	The route terminal	RoutePoint
<Call-Data>	The call data for the event	See Call Data table

Terminal event data, not shown in the previous picture, includes the JTAPI terminal events received by InformaCast and its plugins during CTI calls, as shown in the following table:

Field	Definition	Example
terminalEvent	The name of the terminal event	CiscoRTPOutputStartedEv
<Time-data>	The time when the event was received	See Time Data table
terminal	The name of the terminal	CtiPort01
localAddress	The local IP address where RTP packets are received, triggered by the CiscoRTPInputStartedEv JTAPI terminal event	xxx.xx.xxx.x
localPort	The UDP port where RTP packets are received, triggered by the CiscoRTPInputStartedEv JTAPI terminal event	32068
remoteAddress	The remote IP address where RTP packets are sent, triggered by the CiscoRTPOutputStartedEv JTAPI terminal event	xxx.xx.xxx.x
remotePort	The UDP port where RTP packets are sent, triggered by the CiscoRTPOutputStartedEv JTAPI terminal event	29738

Broadcast action data includes the action taken by InformaCast and its plugins to trigger a broadcast during a CTI call, as shown in the following table:

Field	Definition	Example
broadcastAction	The broadcast action, e.g. Trigger	Trigger
<Time-data>	Time when the event was received	See Time Data table
messageID	The ID of the message sent during a broadcast for a Trigger action	899
recipientGroupIDs	List of the recipient group IDs used during a broadcast for a Trigger action	n105098,954

Info data includes the additional information added by InformaCast and its plugins to a call detail record during a CTI call, as shown in the following table:

Field	Definition	Example
info	The info identifier	callResult
<Time-data>	The time when the info was collected	See Time Data table
	Zero or more fields depending on need	result: HUNG_UP

Time data includes the time when various actions and events have occurred during a CTI call, as shown in the following table:

Field	Definition	Example
time	The formatted date-time string	2016-07-19 13:12:26,723
epochTime	The number of seconds since Jan 1, 1970 00:00:00 UTC	1468951946

Maintain InformaCast

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

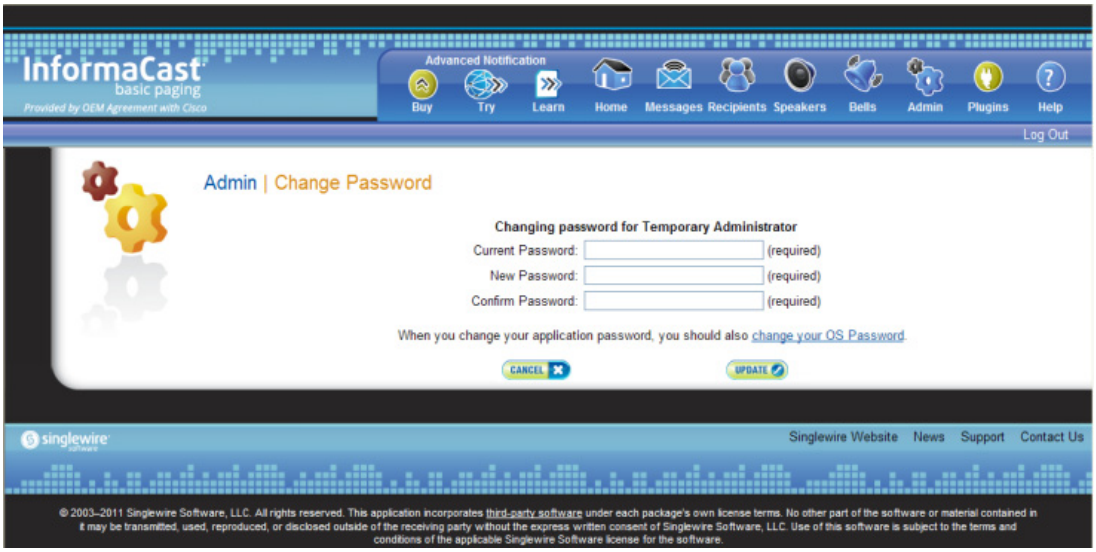
Beyond simply using InformaCast to send broadcasts, you can set up InformaCast backups and manage phone updates, SNMP monitoring, and session timeouts.

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 23 on page 2-27. 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 Virtual Appliance's Password" on page 9-11).

Manage Login Banners

Login banners allow you to display text to your users before and/or after they log into InformaCast, which includes its web interface, Webmin, the command-line interface, and the API explorer. You can use login banners to welcome users to your alert system or make them aware of acceptable use or security policies.

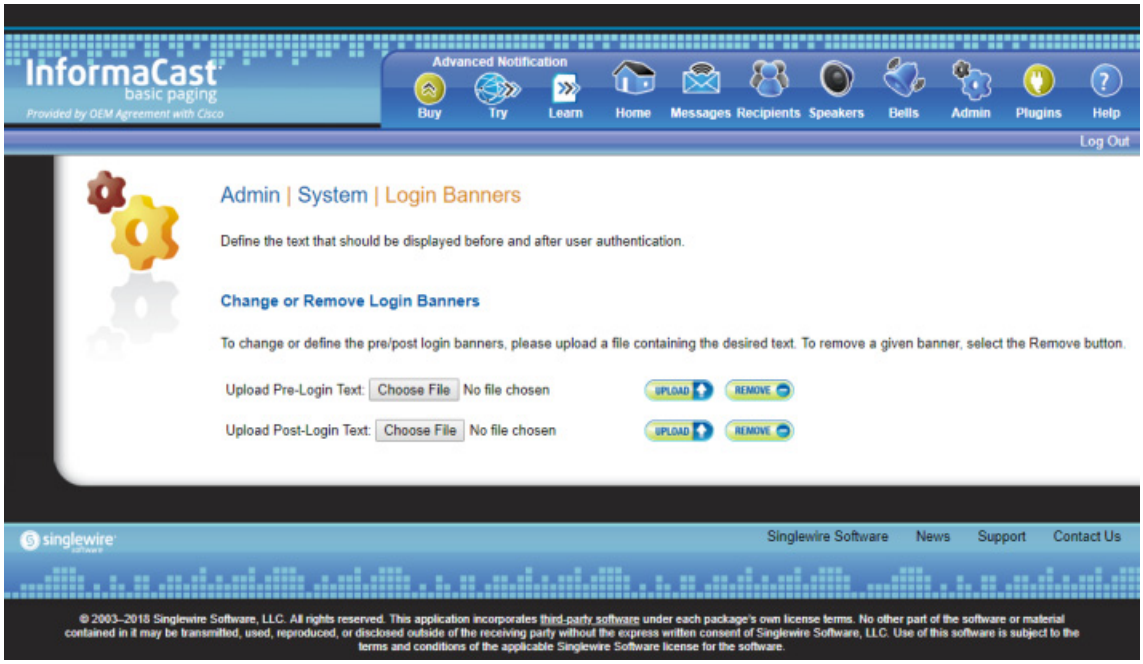
Add a Login Banner

Login banners allow you to display text to your users before and/or after they log into InformaCast.

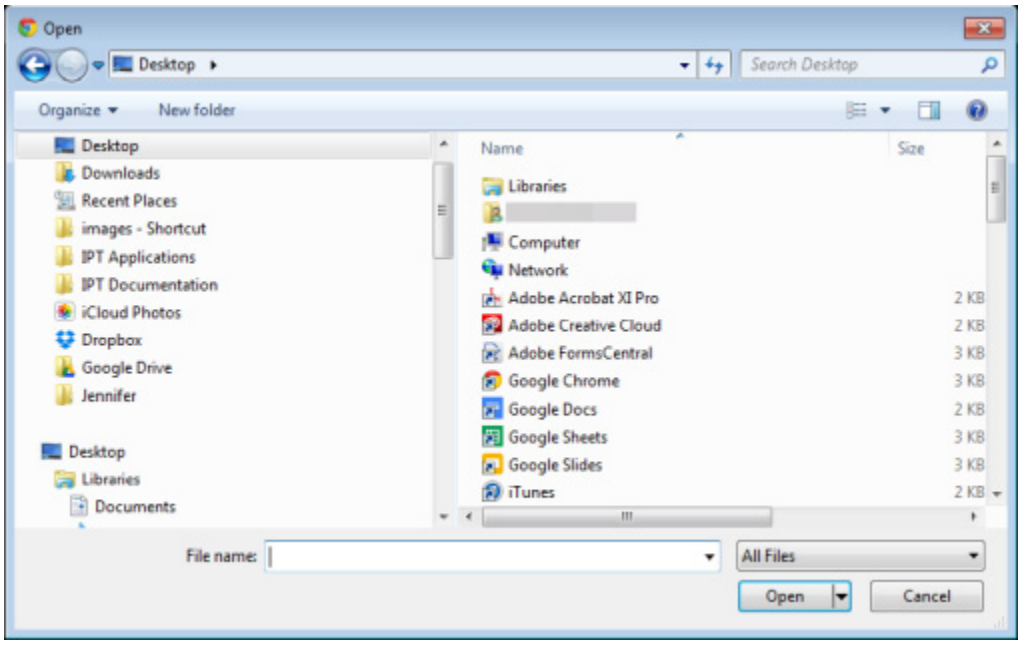
Step 1 Create a text file that contains the text you want to display to users and save it to a location accessible to your web browser.

Note Text files(.txt) must contain plain text only, i.e. no HTML or code. Also, you control the line breaks in your banner text. If your pre-login text is longer than your desired screen size, add carriage returns to your text file. They will be replicated on InformaCast's pages.

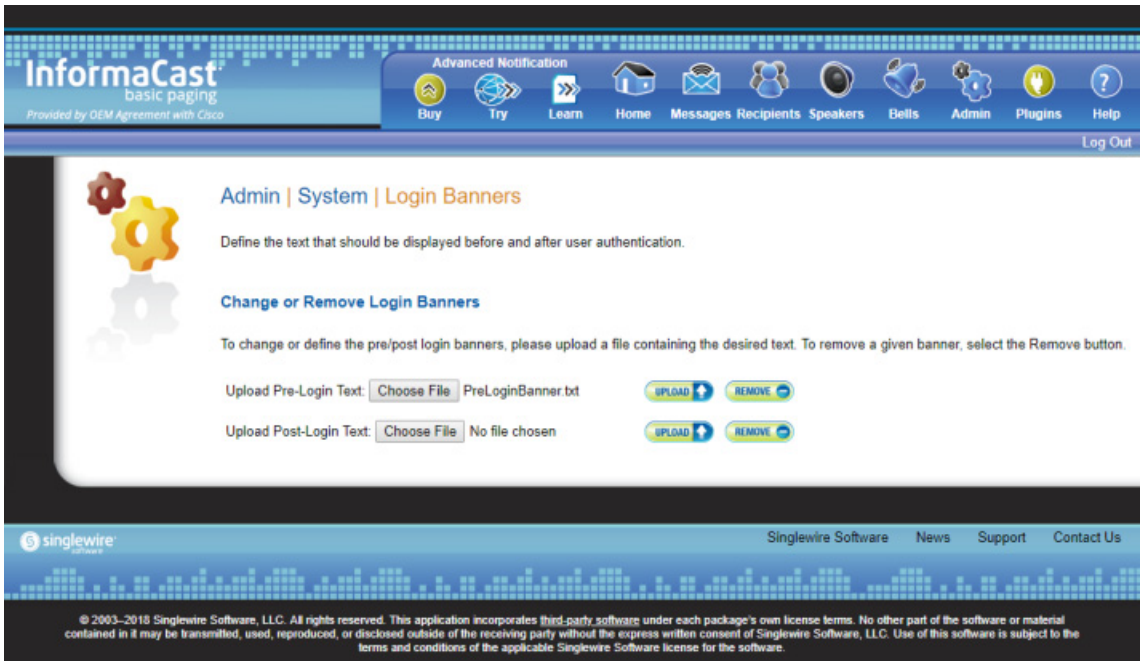
Step 2 Go to **Admin** | **System** | **Login Banners**. The Login Banners page appears.



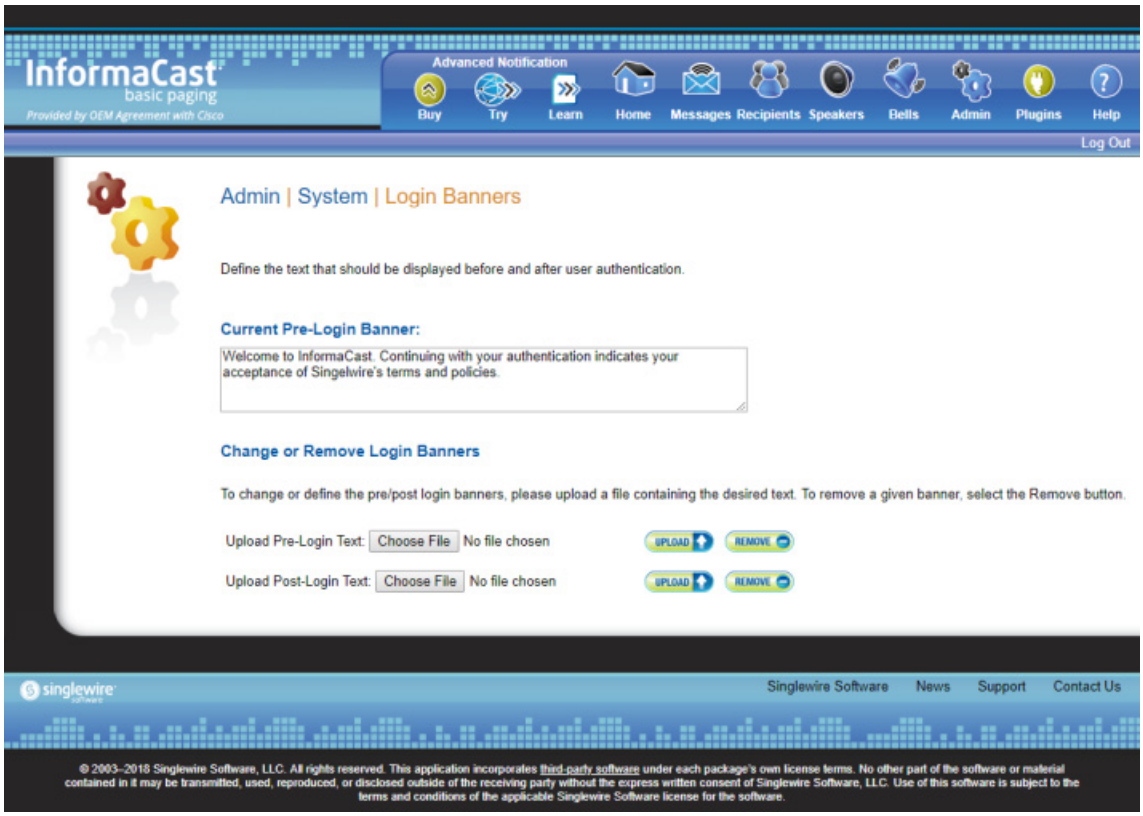
Step 3 Click one of the **Choose File** buttons to upload either pre-login or post-login text. The Open dialog box appears.



Step 4 Navigate to where you saved your text file, select it, and click the **Open** button. The Login Banners page refreshes and you can see your text file's name next to the **Choose File** button you clicked.

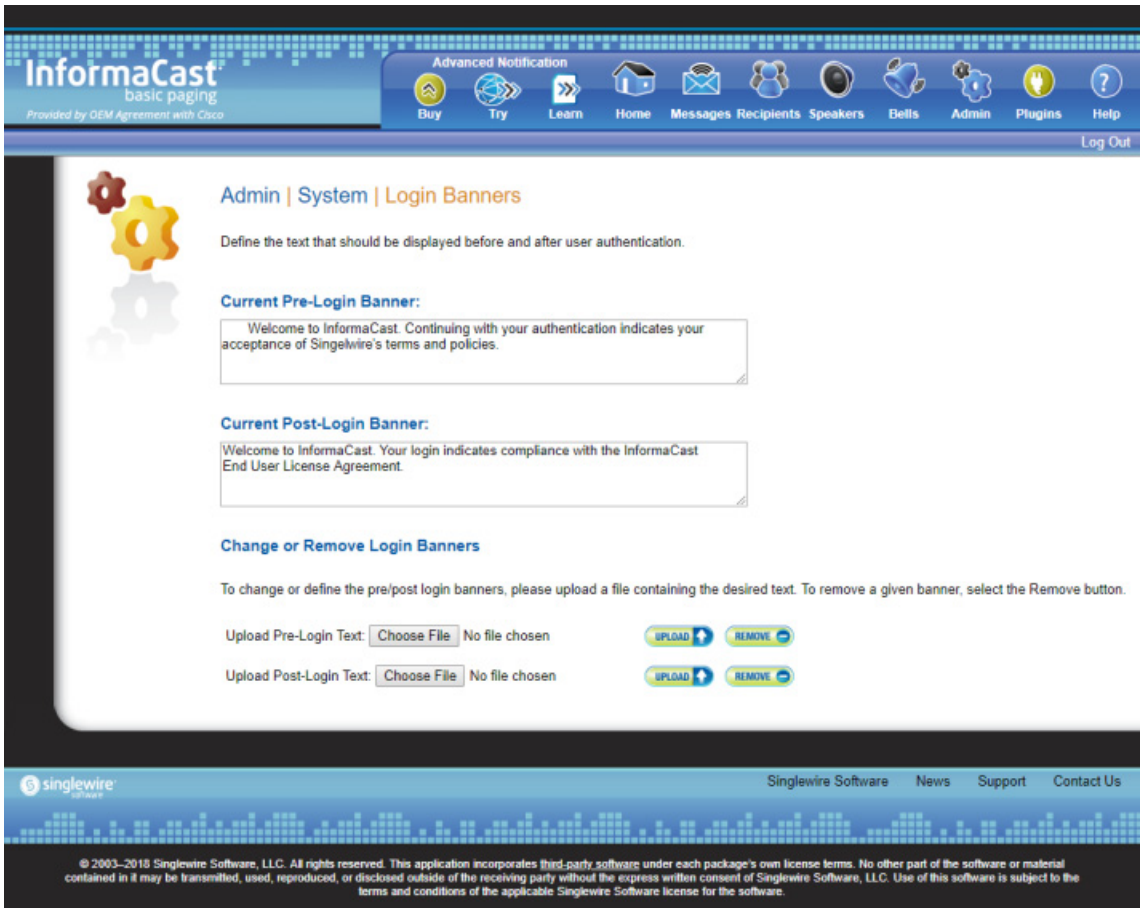


Step 5 Click the **Upload** button for the login text you added. The Login Banners page refreshes and you can see your uploaded text.



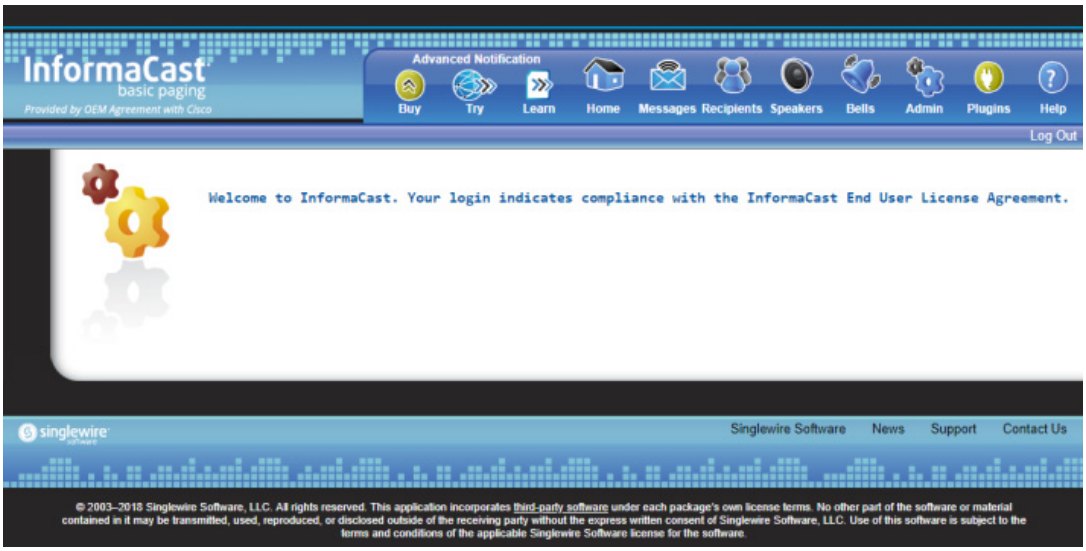
Step 6 Click the other **Choose File** button and repeat the process to upload the other login text (optional).

Step 7 Log out of InformaCast. The Login page appears and (if you uploaded pre-login text) you should see your new banner text.

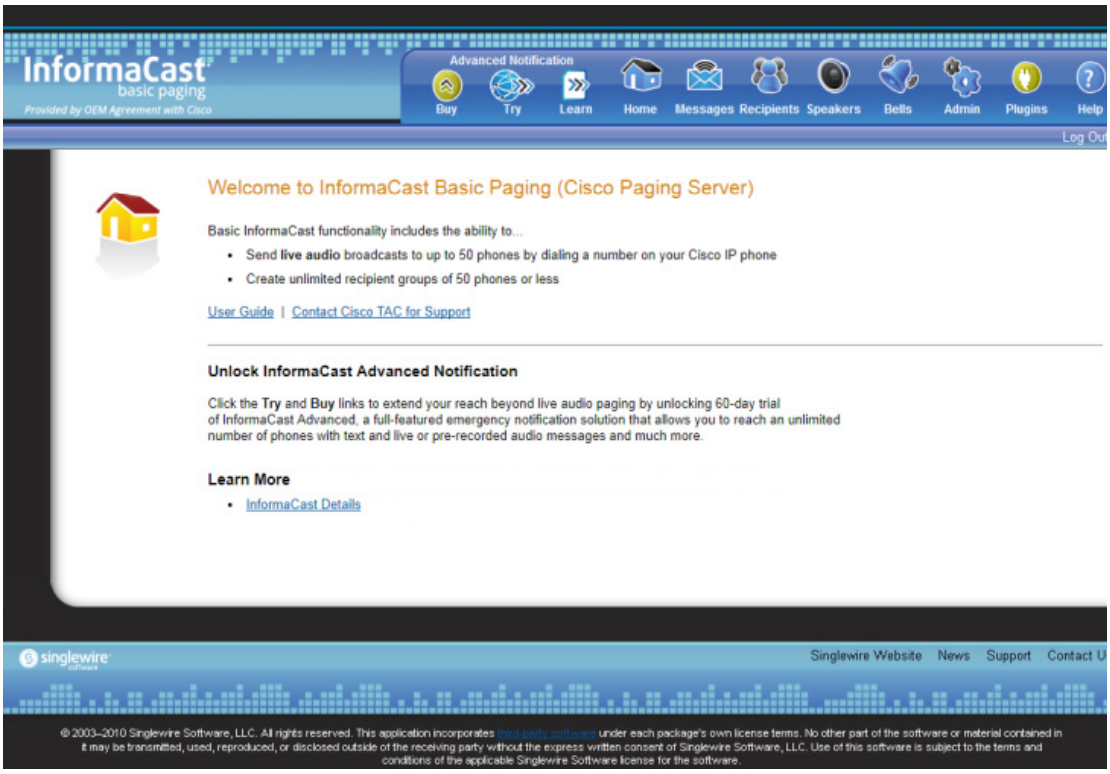


Step 8 Log into InformaCast. One of two things will happen:

- If you added post-login text, you will see that text.



- If you didn't add post-login text, you will be brought immediately to InformaCast's homepage.



Note Login banner text will only appear for Webmin, and the command-line interface after you reboot the Virtual Appliance.

Step 9 Continue by selecting your desired InformaCast menu option.

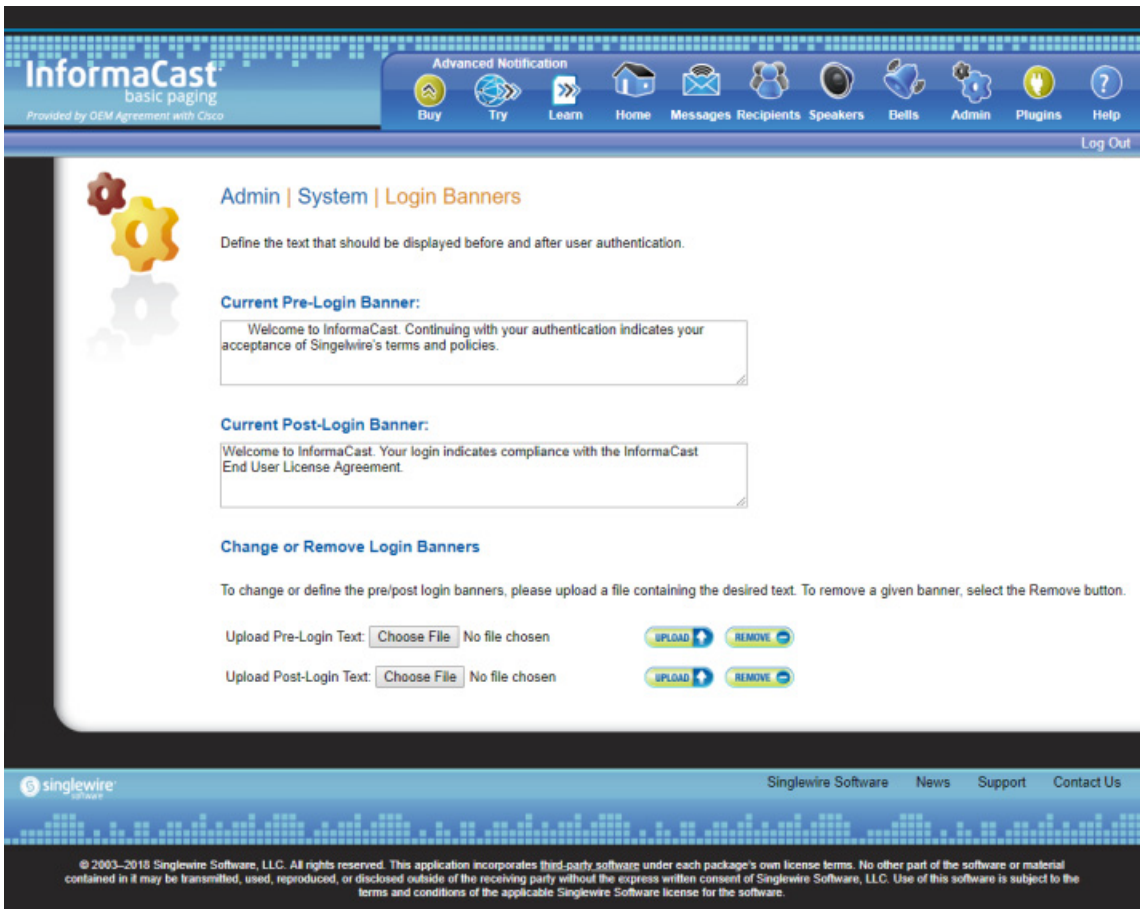
Edit a Login Banner

Once you've added login banners to InformaCast, you may need to update their information.

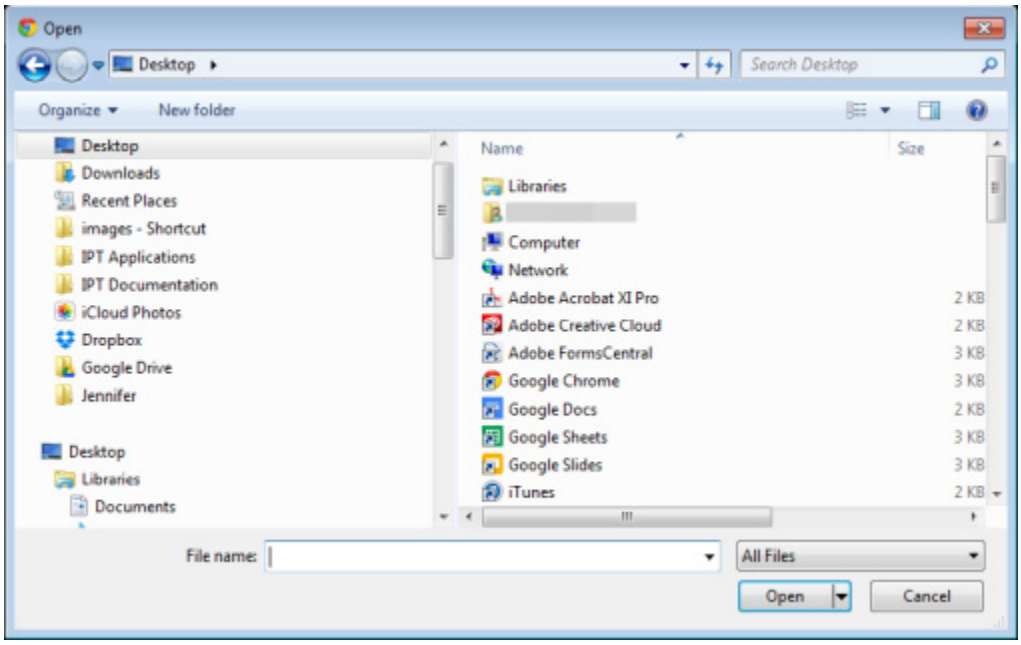
Step 1 Create a new text file that contains the updated text you want to display to users and save it to a location accessible to your web browser.

Note Text files(.txt) must contain plain text only, i.e. no HTML or code. Also, you control the line breaks in your banner text. If your pre-login text is longer than your desired screen size, add carriage returns to your text file. They will be replicated on InformaCast's pages.

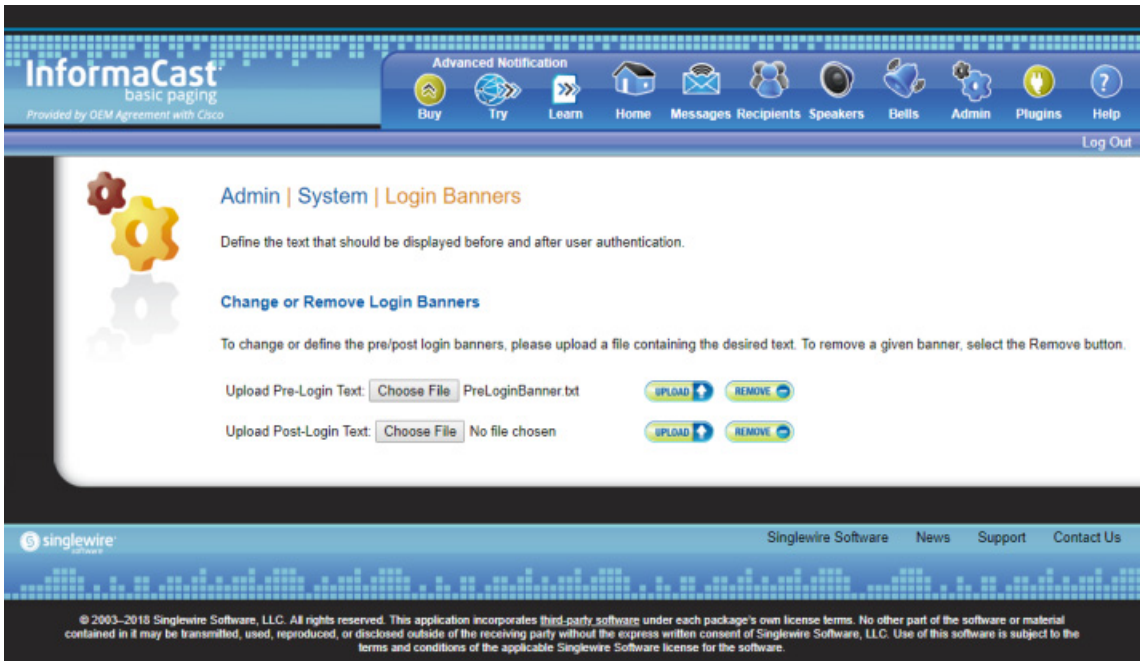
Step 2 Go to **Admin** | **System** | **Login Banners**. The Login Banners page appears.



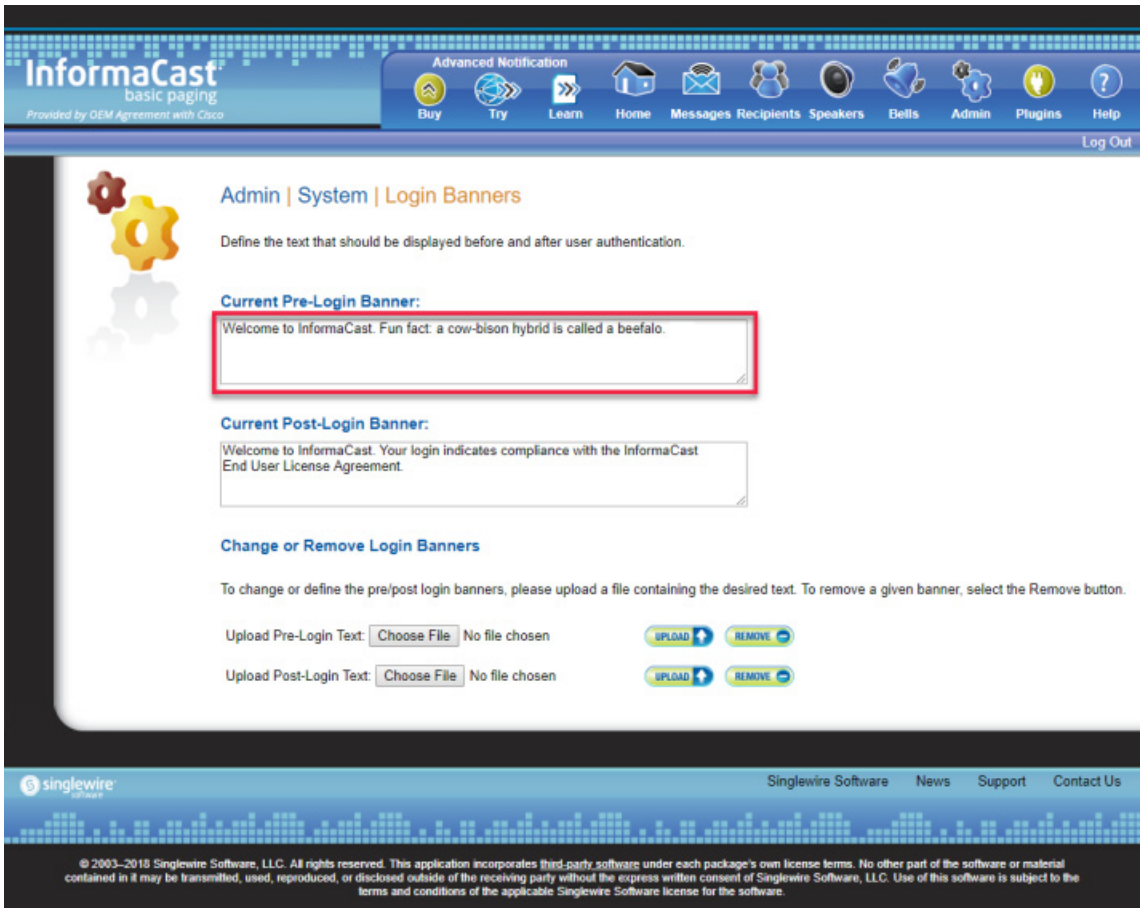
Step 3 Click one of the **Choose File** buttons to upload either pre-login or post-login text. The Open dialog box appears.



Step 4 Navigate to where you saved your text file, select it, and click the **Open** button. The Login Banners page refreshes and you can see your text file's name next to the **Choose File** button you clicked.



Step 5 Click the **Upload** button for the login text you edited. The Login Banners page refreshes and you can see your updated text.



Note Every time you click a **Choose File** button followed by its **Upload** button, the new login banner is saved over the top of the text that existed there before.

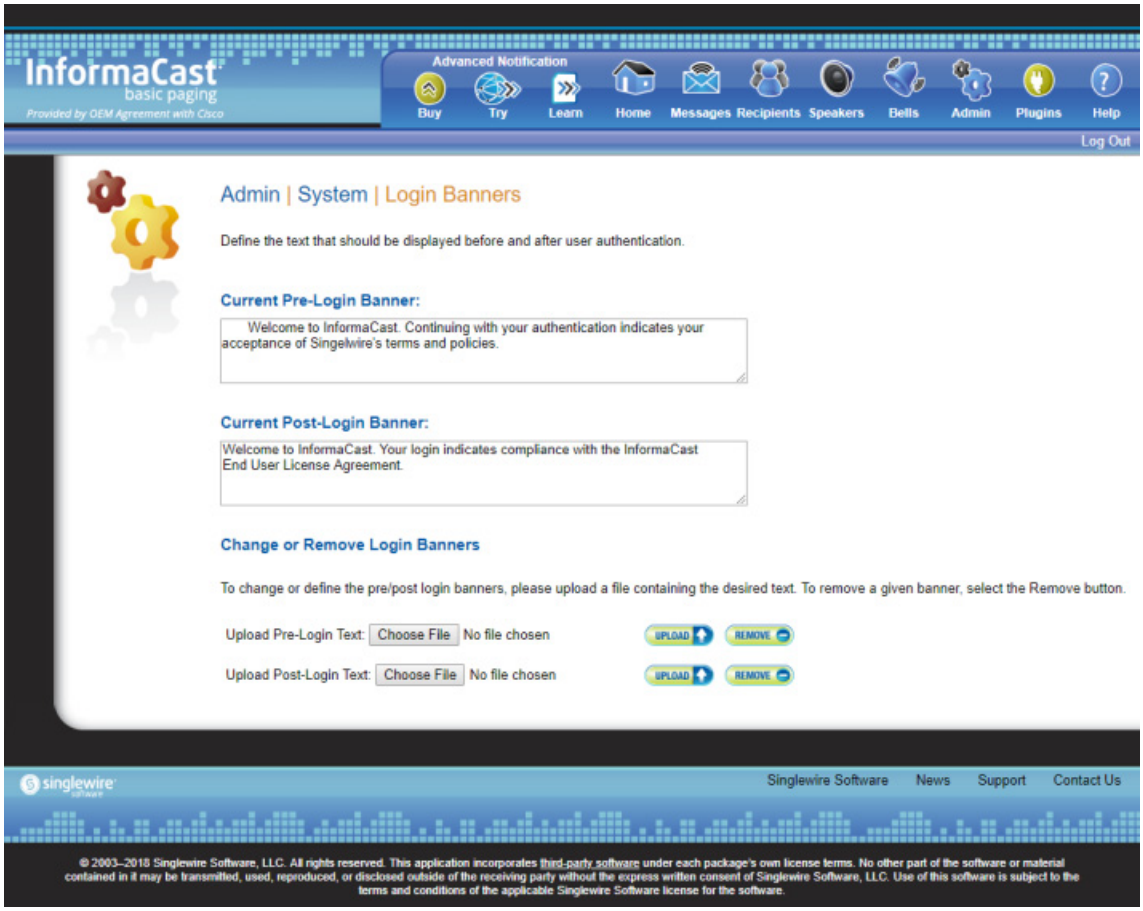
Step 6 Log out and back into InformaCast to ensure the appropriate text appears.

Note Login banner text will only appear for Webmin, and the command-line interface after you reboot the Virtual Appliance.

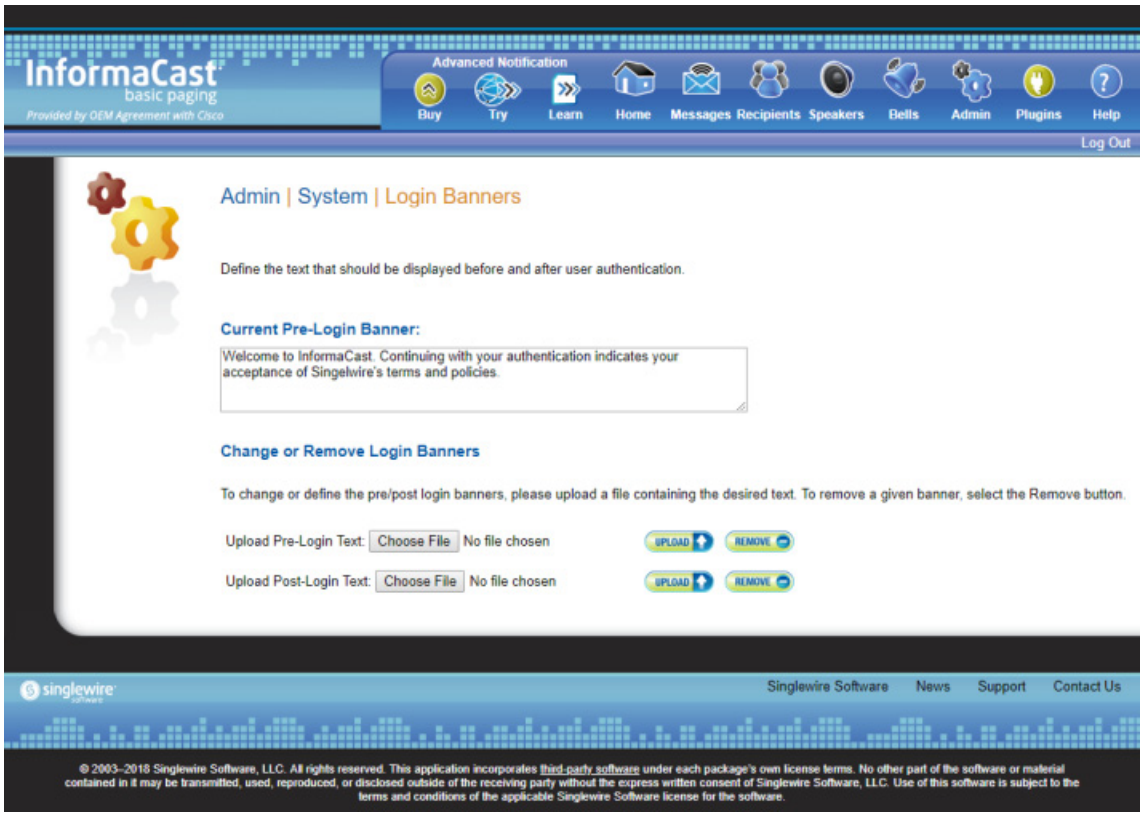
Delete a Login Banner

As your needs change, you may need to remove login banners from InformaCast.

Step 1 Go to **Admin** | **System** | **Login Banners**. The Login Banners page appears.



Step 2 Click the **Remove** button of the login banner you want to delete. The Login Banners page refreshes and your login banner (in this case, the post-login text) is removed.



Manage InformaCast Backups

InformaCast allows you to back up its configuration to an external server using Secure File Transfer Protocol (SFTP) and configure the timing of that backup through a scheduled job. The InformaCast database, configuration data, phone display assets, all certificates, and SSH server keys are preserved during this process.

If you are already backing up your virtual machine inside VMware, you can continue to do so. If you do not back up your virtual machines inside VMware, and wish to start, there are many applications that perform virtual-machine-level backups. One such application is Veeam Backup and Replication. Singlewire does not endorse any particular vendor's implementation. Consult the vendor's documentation on how to integrate your VMware environment with a backup strategy.

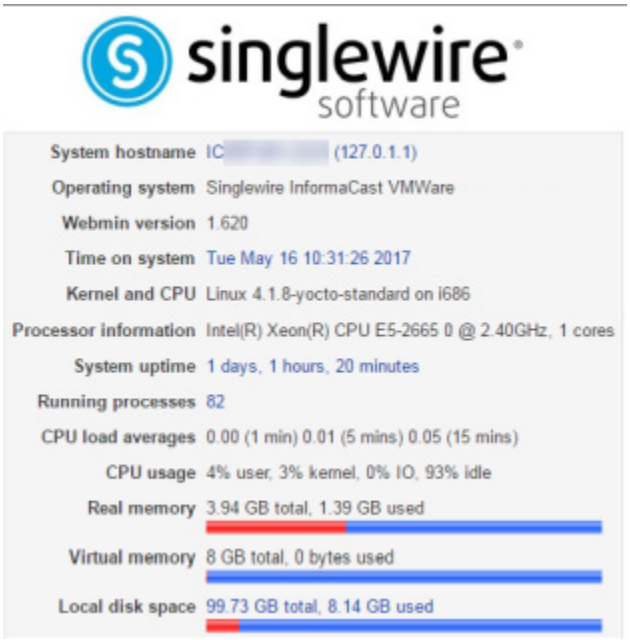
Configure InformaCast's Connection to an SFTP Server

You must configure a connection to an SFTP server in order for InformaCast to properly back up its configuration. InformaCast's backups are fully encrypted using the security passphrase you set up when you installed InformaCast (see "Deploy InformaCast" on page 2-6).

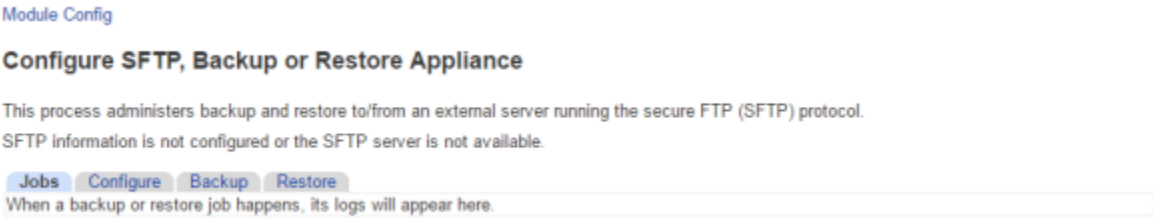
Currently, OpenSSH is the only SFTP server supported by Singlewire, although other servers may work.

Note New backups will overwrite previous backup files.

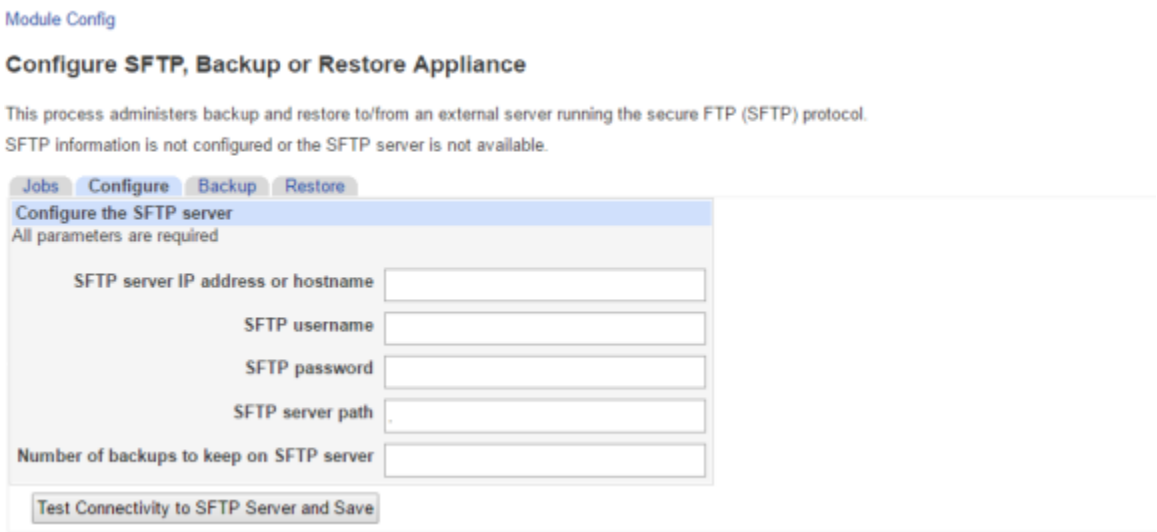
Step 1 Log into Webmin (see "Log into Webmin" on page 2-35 for specific steps). The Webmin homepage appears.



Step 2 Go to **Others** | **Backup and Restore**. The Configure SFTP, Backup or Restore Appliance page appears.



Step 3 Click the **Configure** tab. The Configure SFTP, Backup or Restore Appliance page refreshes.



Step 4 Enter the IP address or hostname of your SFTP server in the S**FTP server IP address or hostname** field.

Step 5 Enter the username for your SFTP server in the **SFTP username** field.

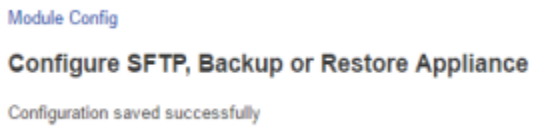
Step 6 Enter the password for your SFTP server in the **SFTP password** field.

Step 7 Enter the network path to your SFTP server in the **SFTP server path** field. Leave the . in the **SFTP server path** field to use the default directory.

Note The directory path you enter in the **SFTP server path** field is relative to the default directory on the SFTP server. It is not possible to back up to a path outside of the default directory. No other applications should write files to that directory. If you have more than one InformaCast server, ensure that each has its own directory.

Step 8 Enter a numeric value in the **Number of backups to keep on SFTP server** field, which tells InformaCast to keep that number of backups on the SFTP server.

Step 9 Click the **Test Connectivity to SFTP Server and Save** button. InformaCast will attempt to connect to your SFTP server. Once it connects, you will see a success statement.



Step 10 Continue with "Backup InformaCast's Configuration" on page 6-15.

Backup InformaCast's Configuration

You can configure the timing behind a scheduled job that backs up InformaCast's configuration or you can back up InformaCast manually in one of two ways.

Before you perform any of the steps in the following sections, you must have first performed the steps in "Configure InformaCast's Connection to an SFTP Server" on page 6-12.

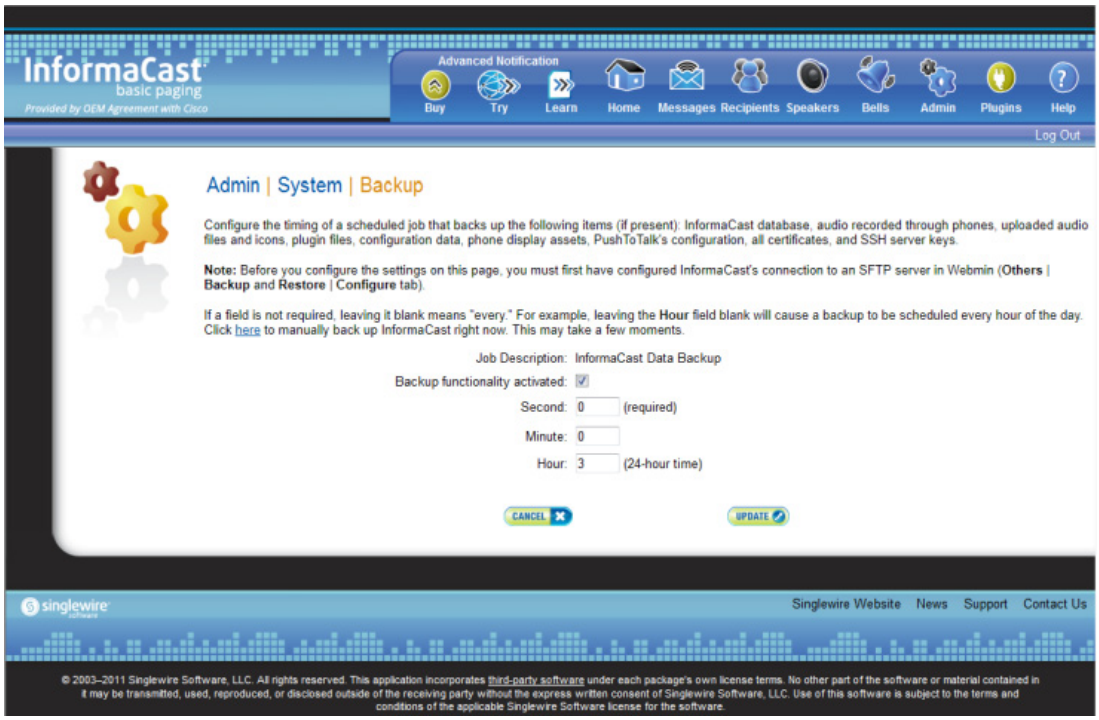
Note You can only back up InformaCast when it is running. In order to achieve a consistent backup, perform it when configuration changes are not expected to be taking place.

Configure a Scheduled Job to Back Up InformaCast

Note If you do not set a time for backups, automatic backups will not occur.

Configure the timing behind a scheduled job that backs up InformaCast's configuration.

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 Click the **Update** button to save your changes. On the Overview page, you can see your changes reflected in the *Backup* section.

Backup

Backup Activated	true
Next Scheduled Backup	2017-05-23 03:00:00

Manually Back Up InformaCast Through Its User Interface

Use the following steps to back up InformaCast manually through the InformaCast user interface.

Step 1 Go to **Admin** | **System** | **Backup**. The Backup page appears.

Step 2 Click the **here** link. InformaCast will begin backing itself up to the location you specified on your SFTP server (see "Configure InformaCast's Connection to an SFTP Server" on page 6-12 for more information). This may take a few moments.

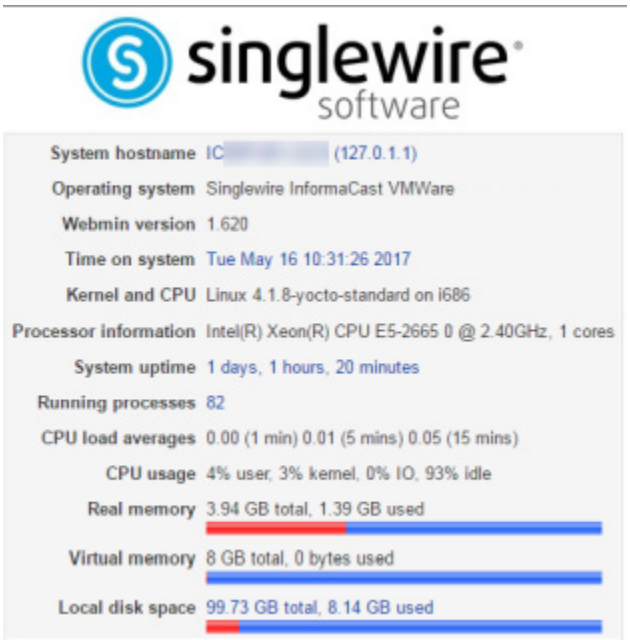
Note New backups will overwrite previous backup files once the value specified in the **Number of backups to keep on SFTP server** field is met (you set this value in "Configure InformaCast's Connection to an SFTP Server" on page 6-12)

When InformaCast is finished, you will be taken to the Overview page and "Backup process complete" will appear at the top of the page.

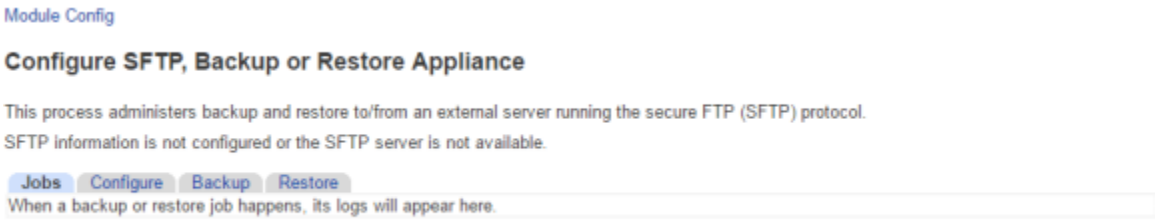
Manually Back Up InformaCast Through Webmin

Use the following steps to back up InformaCast manually through the Webmin interface.

Step 1 Log into Webmin (see "Log into Webmin" on page 2-35 for specific steps). The Webmin homepage appears.

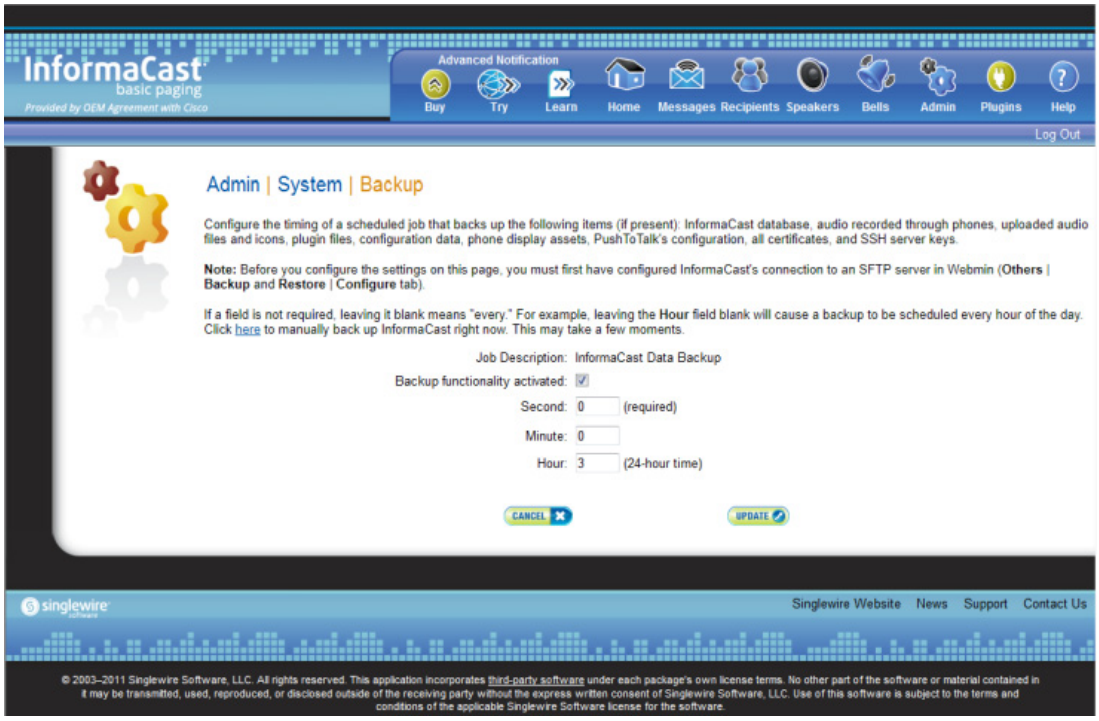


Step 2 Go to **Others** | **Backup and Restore**. The Configure SFTP, Backup or Restore Appliance page appears.



Step 3 Click the **Backup** tab. The Configure SFTP, Backup or Restore Appliance page refreshes.

Step 4 Click the **InformaCast** link. You will be redirected to InformaCast's Backup page.



Step 5 Click the **here** link. InformaCast will begin backing itself up to the location you specified on your SFTP server (see "Configure InformaCast's Connection to an SFTP Server" on page 6-12 for more information). This may take a few moments.

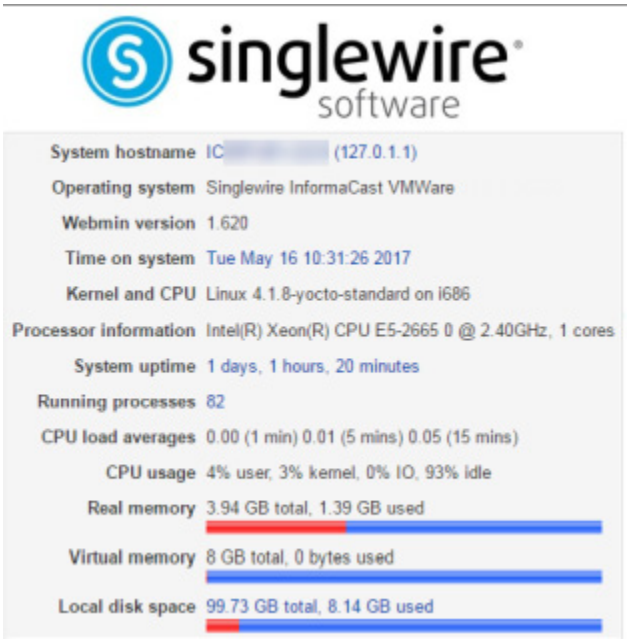
Note New backups will overwrite previous backup files once the value specified in the **Number of backups to keep on SFTP server** field is met (you set this value in "Configure InformaCast's Connection to an SFTP Server" on page 6-12)

When InformaCast is finished, you will be taken to the Overview page and "Backup process complete" will appear at the top of the page.

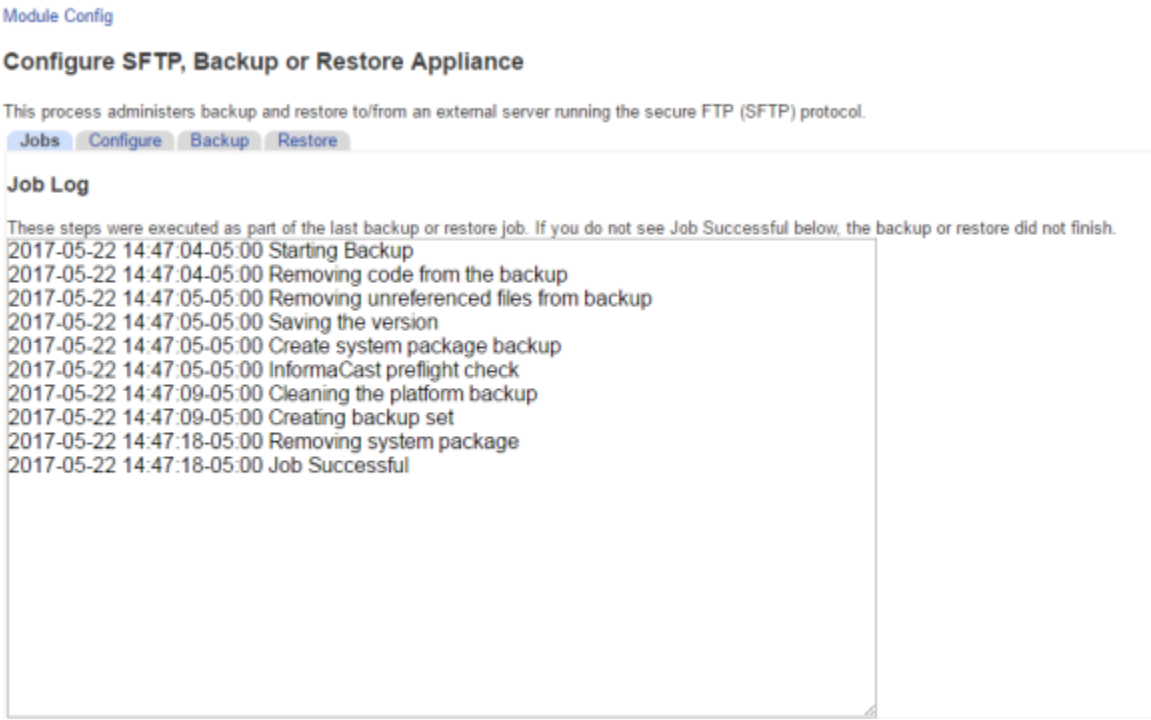
Restore InformaCast From a Backup

Once you have configured InformaCast's backups, you can restore InformaCast from a backup, if necessary.

Step 1 Log into Webmin (see "Log into Webmin" on page 2-35 for specific steps). The Webmin homepage appears.

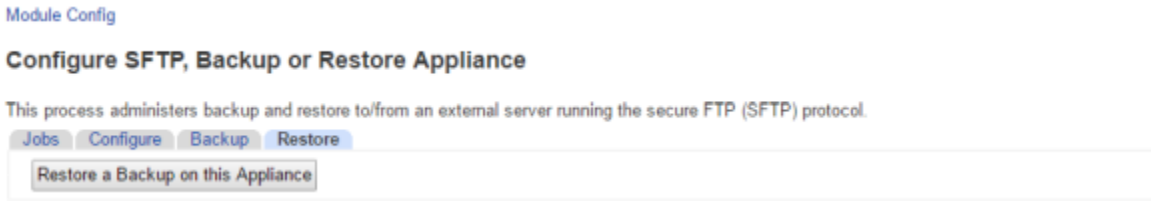


Step 2 Go to **Others** | **Backup and Restore**. The Configure SFTP, Backup or Restore Appliance page appears.

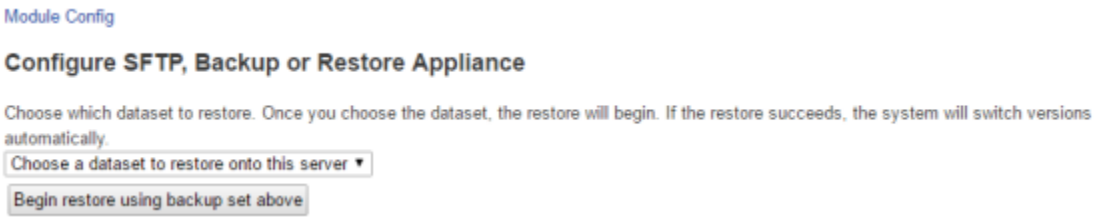


Once a backup has occurred, you can view the steps InformaCast took to back itself up in the Job Log.

Step 3 Click the **Restore** tab. The Configure SFTP, Backup or Restore Appliance page refreshes.

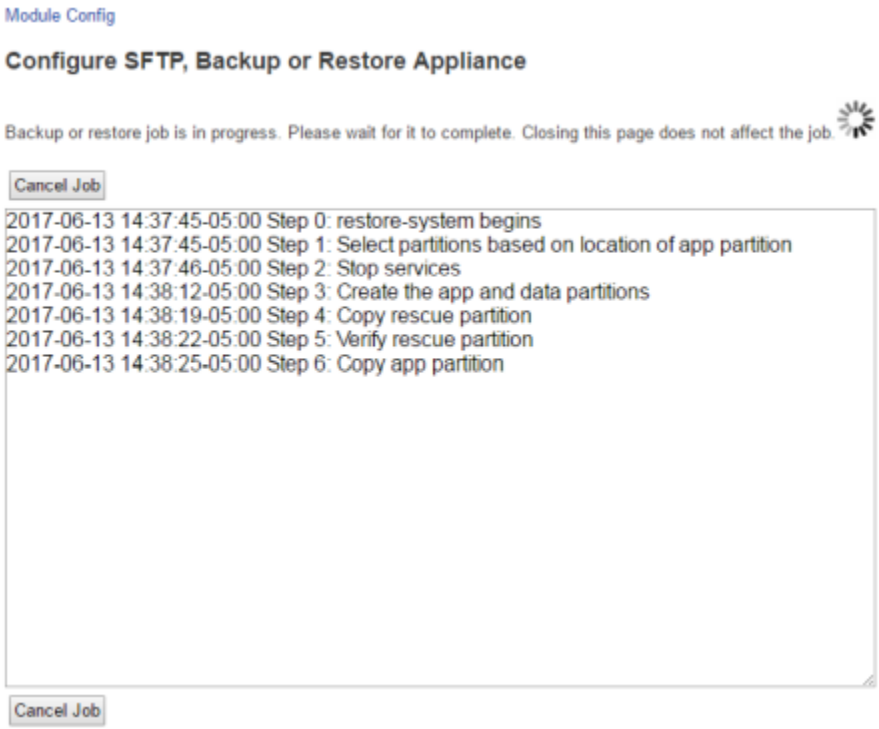


Step 4 Click the **Restore a Backup on this Appliance** button. The Configure SFTP, Backup or Restore Appliance page refreshes.



Step 5 Select a backup from the Choose a dataset to restore onto this server dropdown menu and click the Begin restore using backup set above button.

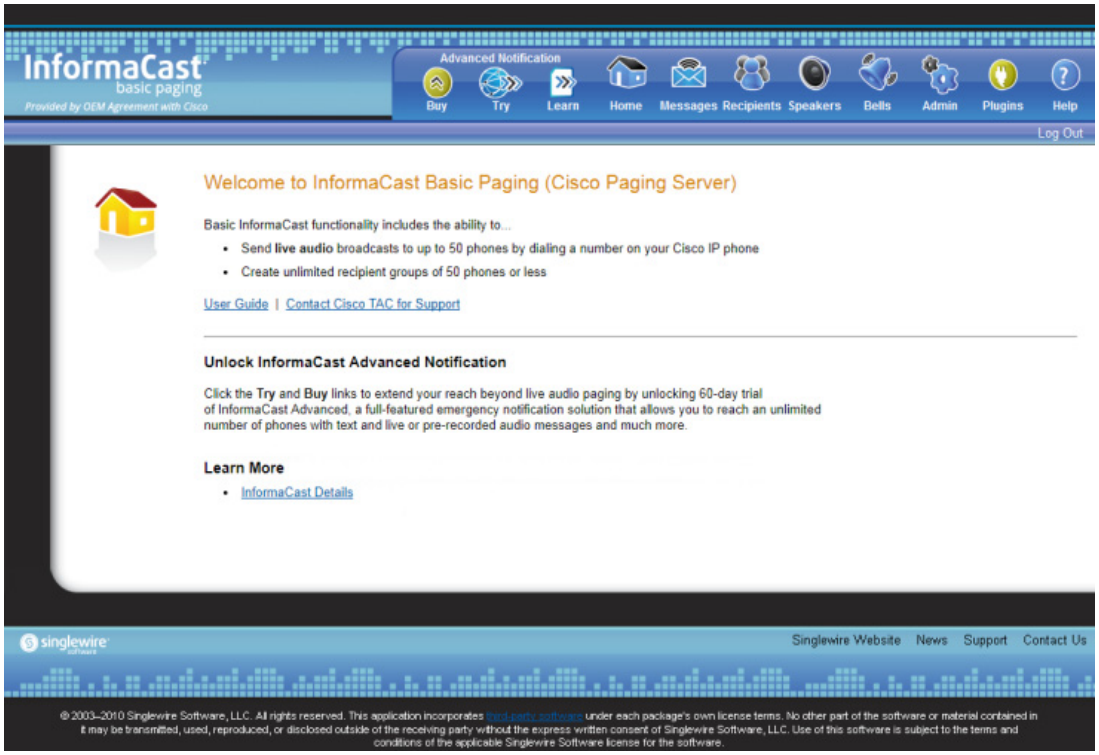
InformaCast begins restoring itself to the backup you selected.



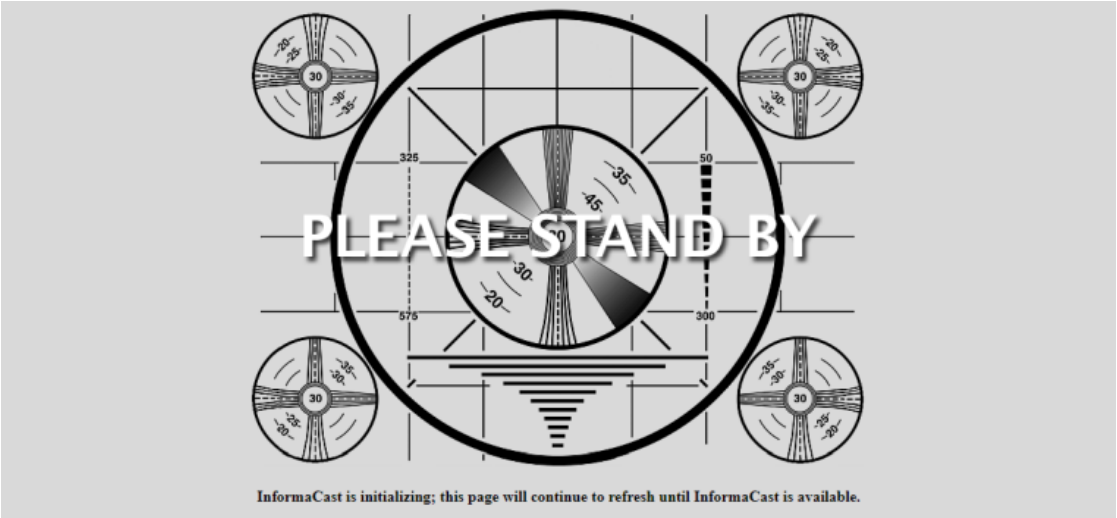
This may take a few moments, and while InformaCast is performing the restoration, it may look like the Configure SFTP, Backup or Restore Appliance page has failed. It has not.

InformaCast's disk is divided into two partitions: active and inactive. When InformaCast is running, it runs off of the active partition, where your data is stored. When you perform a restore, InformaCast performs the restore to the inactive partition. If the restore succeeds, InformaCast switches the partitions: the inactive partition becomes active and InformaCast runs from it. This means that after a restore, you can also switch versions again, which takes you back to the way the system was before the restore. You can use this as a way to test a restoration with minimal impact on your running system.

Step 6 Log into InformaCast (see "Log into InformaCast" on page 2-31). InformaCast's homepage appears.



InformaCast may still be initializing, in which case you will see the following initialization page. Once InformaCast is done initializing, you may log in.



Step 7 Test the functionality.

Manage Phone Updates

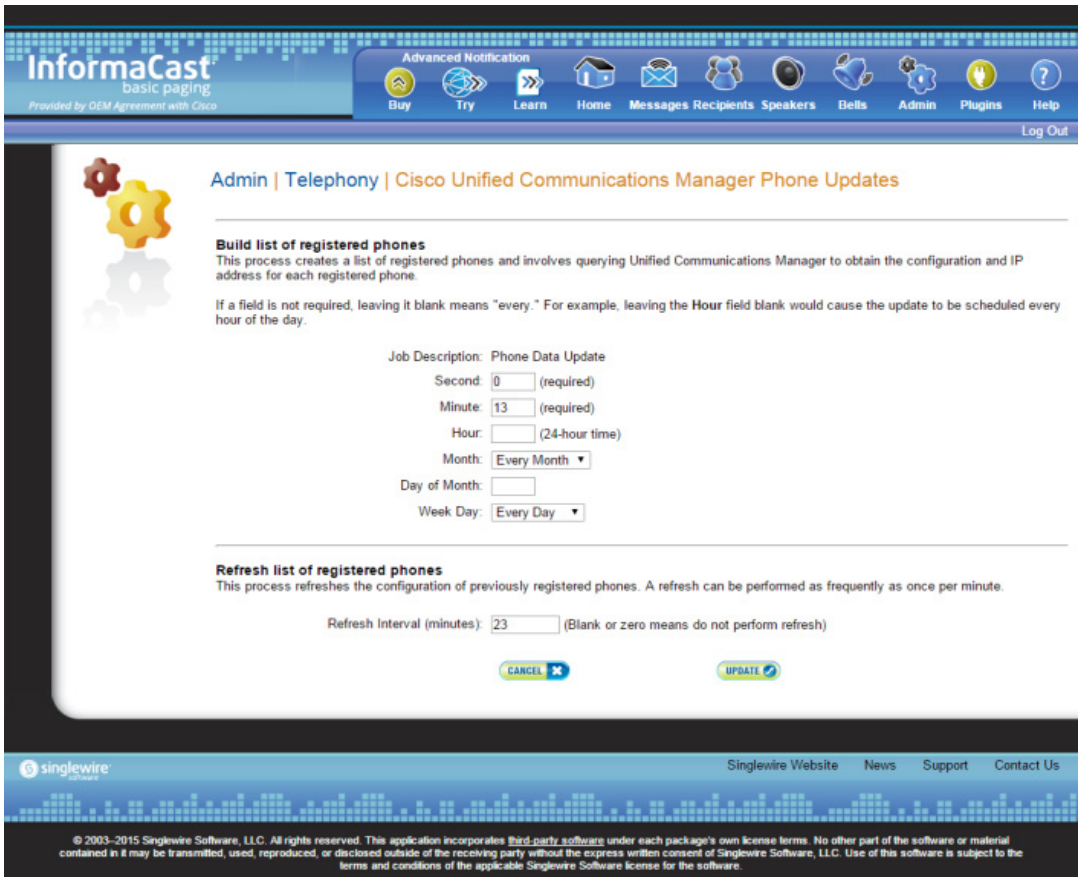
Phone updates allow you to configure the timing for two scheduled jobs of how often InformaCast will update its phone information: build a list of registered phones and refresh a list of registered phones.

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.



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.

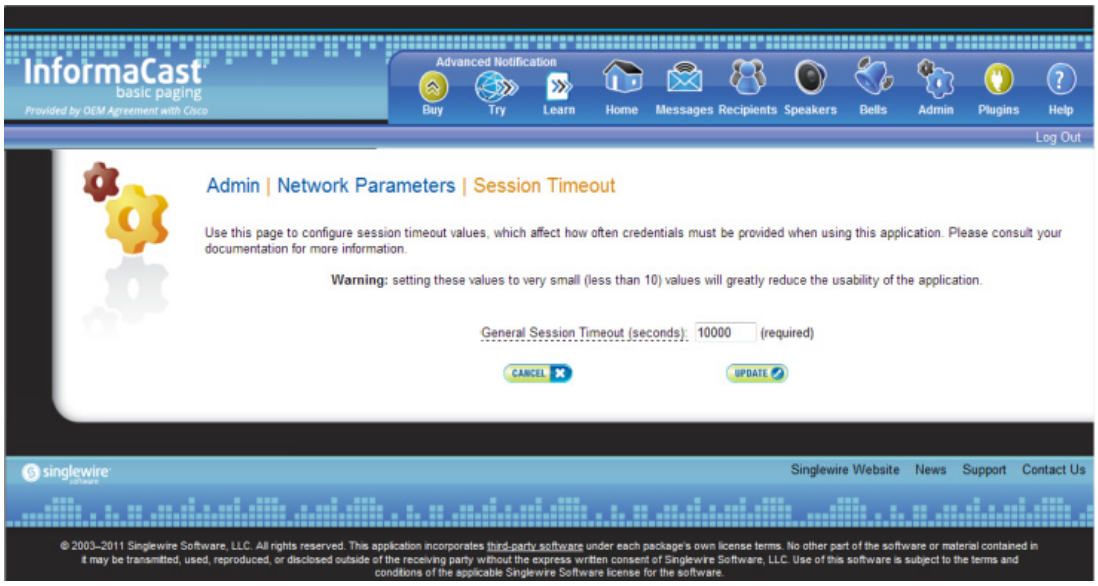
Note Refreshing a list of registered phones picks up the changes to phones that use extension mobility as well as other configuration changes. Refreshing the list only updates the phones already in InformaCast's phone cache. Newly registered phones will not be seen in the cache until the next rebuild 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 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 9-76.

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 "Deploy InformaCast" 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 2-42 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.

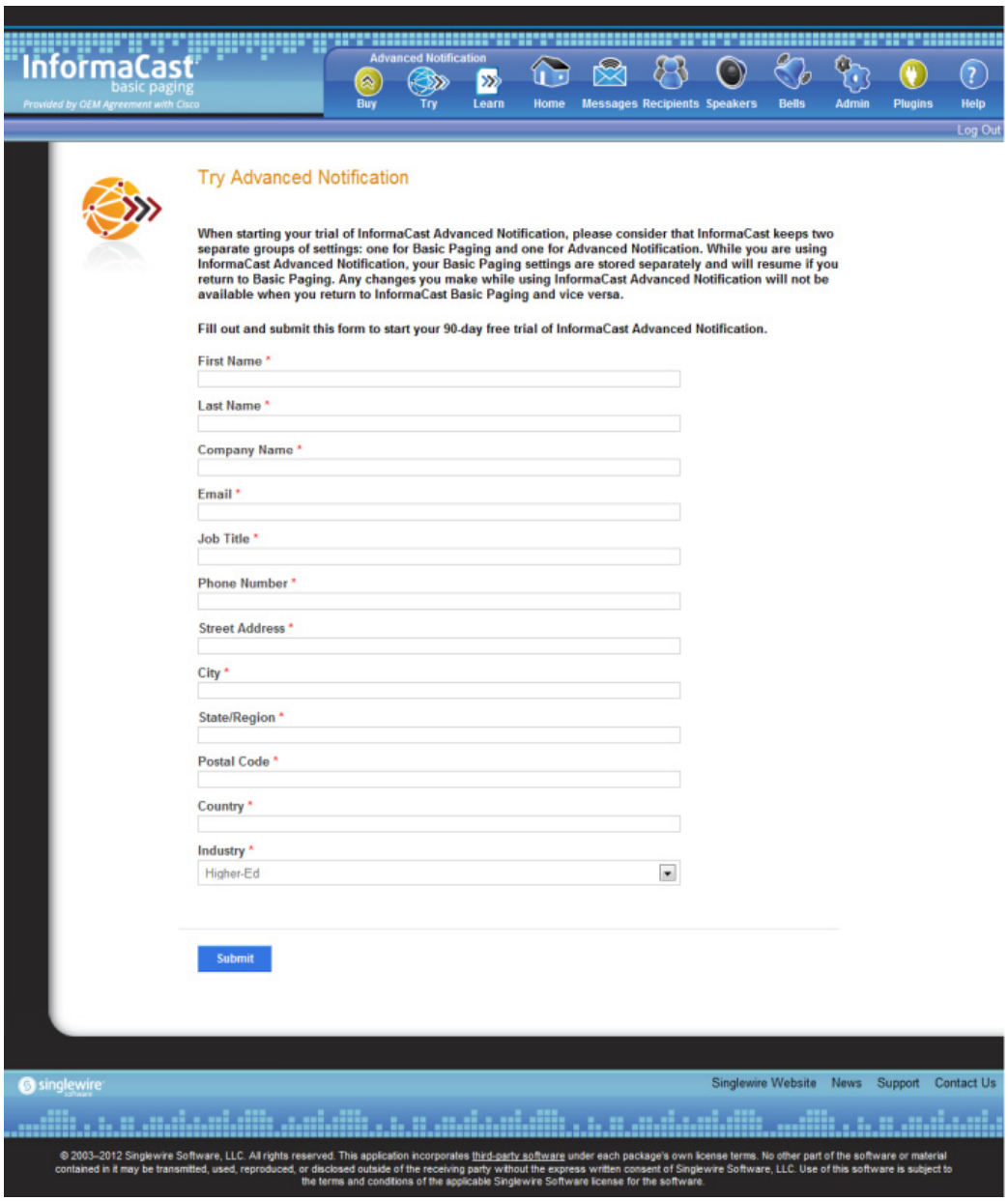
Note You will want to access the InformaCast Virtual Appliance Help System for Advanced Notification in a Cisco Unified Communications Manager Environment in order to make full use of all of InformaCast's functionality. After upgrading, it can be obtained from **Help** | **InformaCast User Guide**. If 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

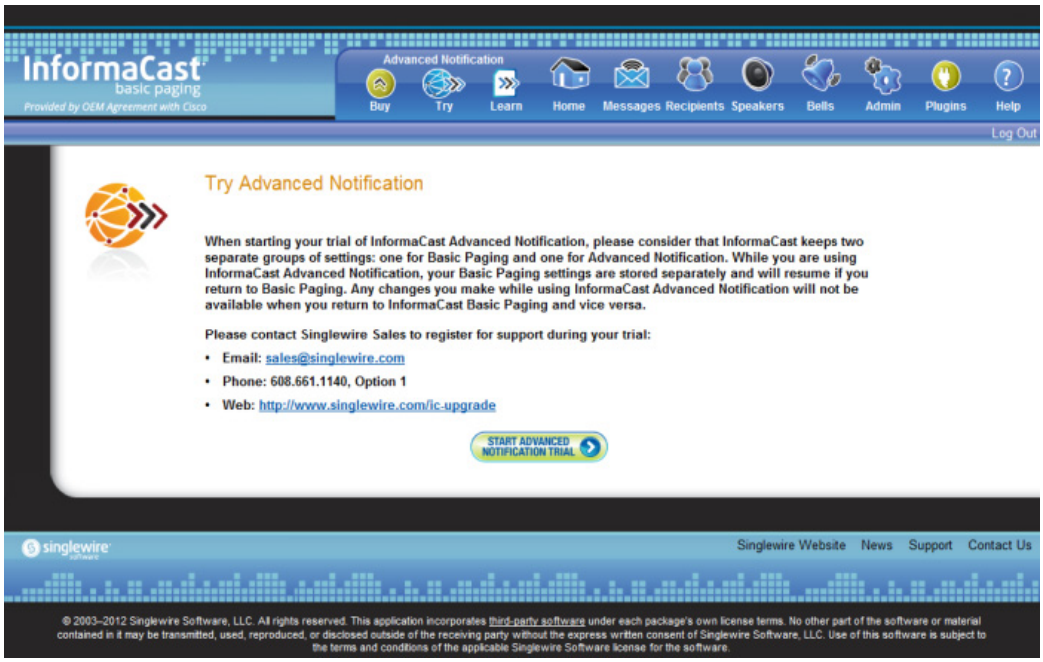
By clicking the **Try** icon (), you start your 60-day free trial of Advanced InformaCast.

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.



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.



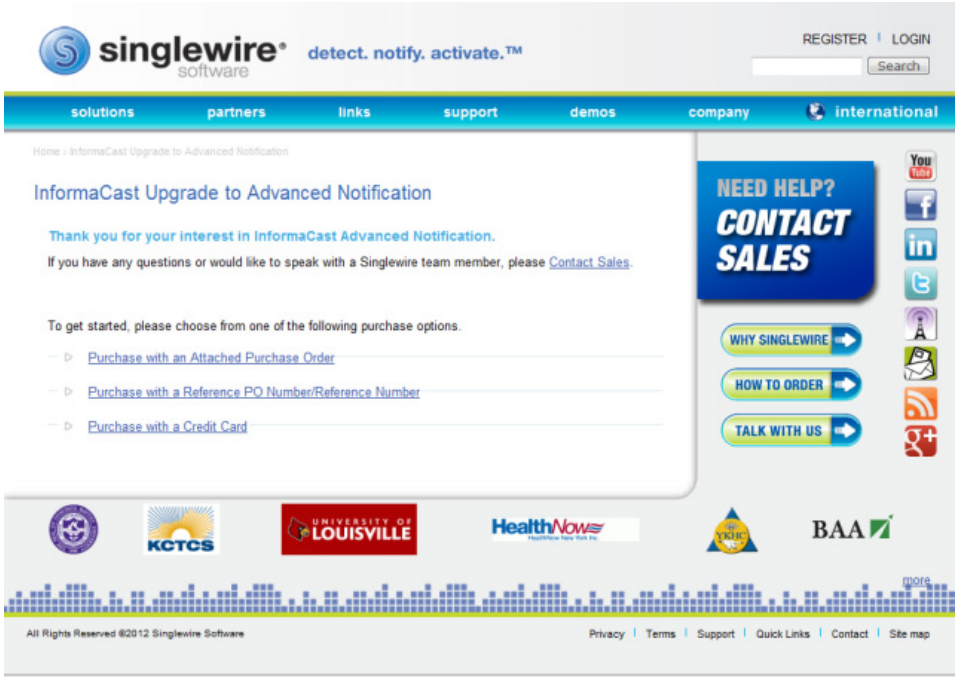
Step 2 Click the **Start Advanced Notification Trial** button. Your window refreshes with InformaCast's homepage, showing that you are in your trial of InformaCast Advanced Notification.

Buy Advanced Notification

By clicking the **Buy** icon, you start the process of obtaining InformaCast Advanced Notification through either a demonstration, subscription, or perpetual license.

Step 1 Click the **Buy** icon ( ) any time while using Basic InformaCast.

If your server is connected to the Internet, you will be redirected to a Singlewire Software website. Follow the prompts to obtain a new license.



If your server is not connected to the Internet, you will see a QR code that you can scan with your smartphone to access the Singlewire website. Once there, follow the prompts to obtain your new license.

Step 2 Continue with "Enter Your New License Key" on page 7-8.

Enter Your New License Key

Note If you are in your free trial of Advanced InformaCast, you can skip this section.

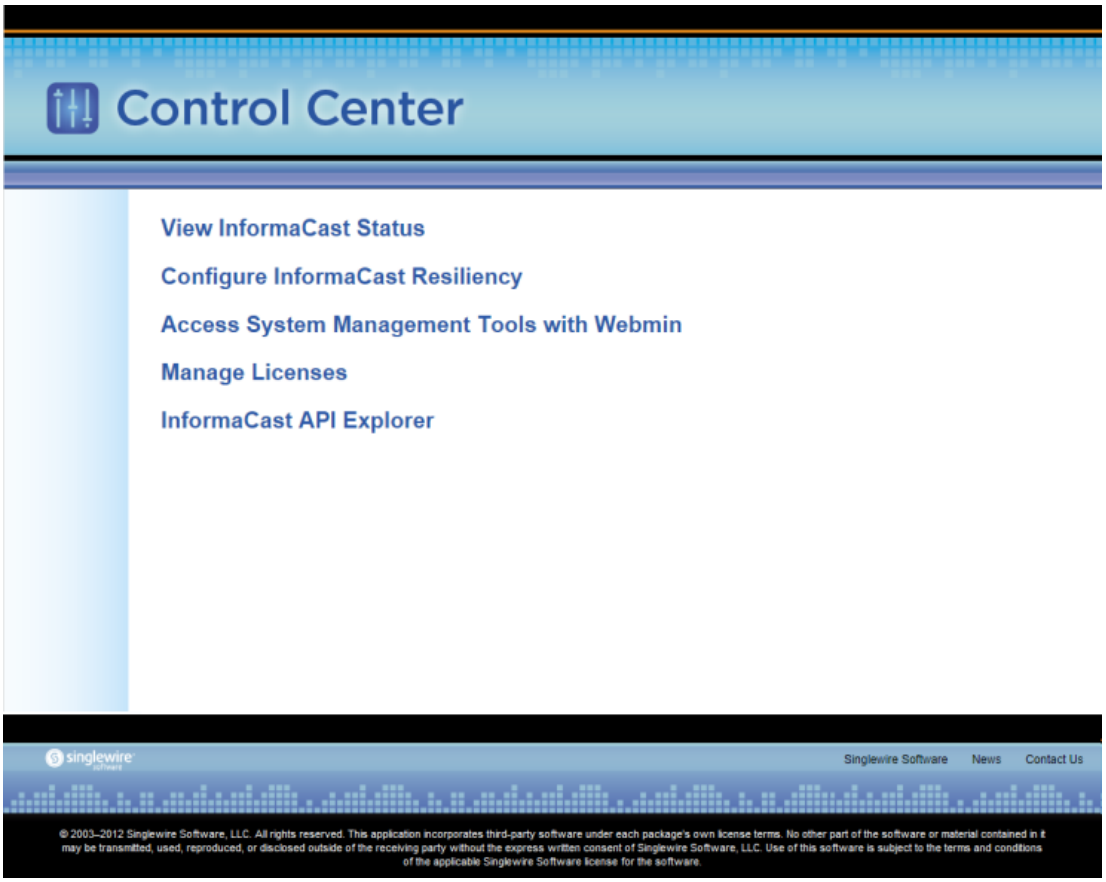
When you upgrade from Basic InformaCast to Advanced InformaCast (with the exception of your free trial of Advanced InformaCast), you will install a new license key to activate the various features of your InformaCast system. The license key will be in the form of an XML file that was sent to you by email from a Singlewire sales representative. Make sure to save this XML file to a safe location that can be accessed by the machine running your web browser.

Note If you are in participating in your free trial of Advanced InformaCast functionality, your license will already be installed for you and will be visible on InformaCast's Manage License Key page (**Admin | Manage License Key**). Your license will not appear on Singlewire's License Manager page until you upgrade to Advanced InformaCast on a demonstration, subscription, or perpetual license.

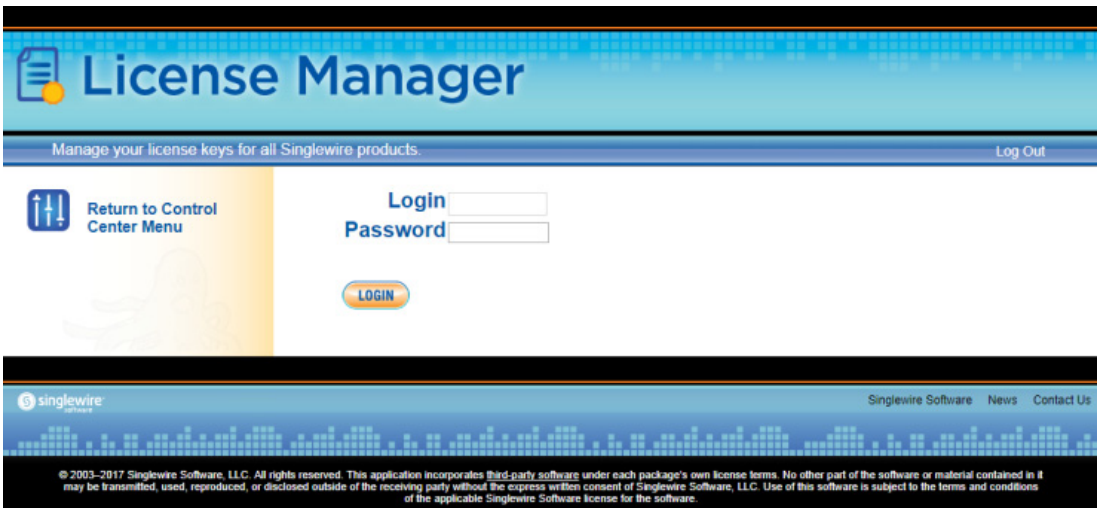
Note Bell schedules, the number of IP phones and speakers, Unified Communications Manager clustering, and message confirmation are all controlled by your license key. If you are expecting certain functionality and cannot access it, contact your Singlewire salesperson.

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.**

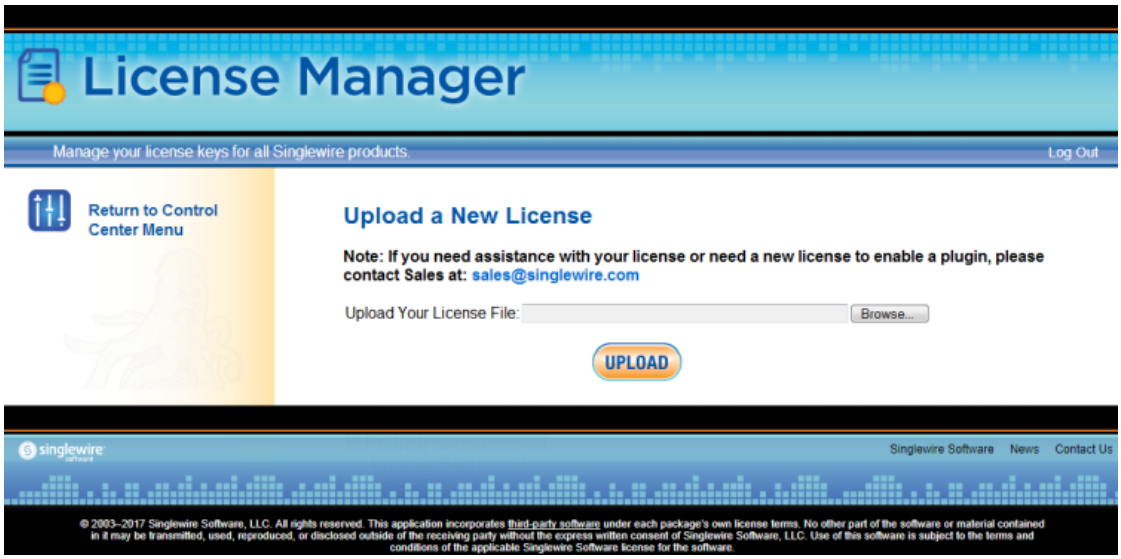
Step 1 Log into the Control Center (see "Log into the Control Center" on page 2-33 for specific steps). The Control Center menu page appears.



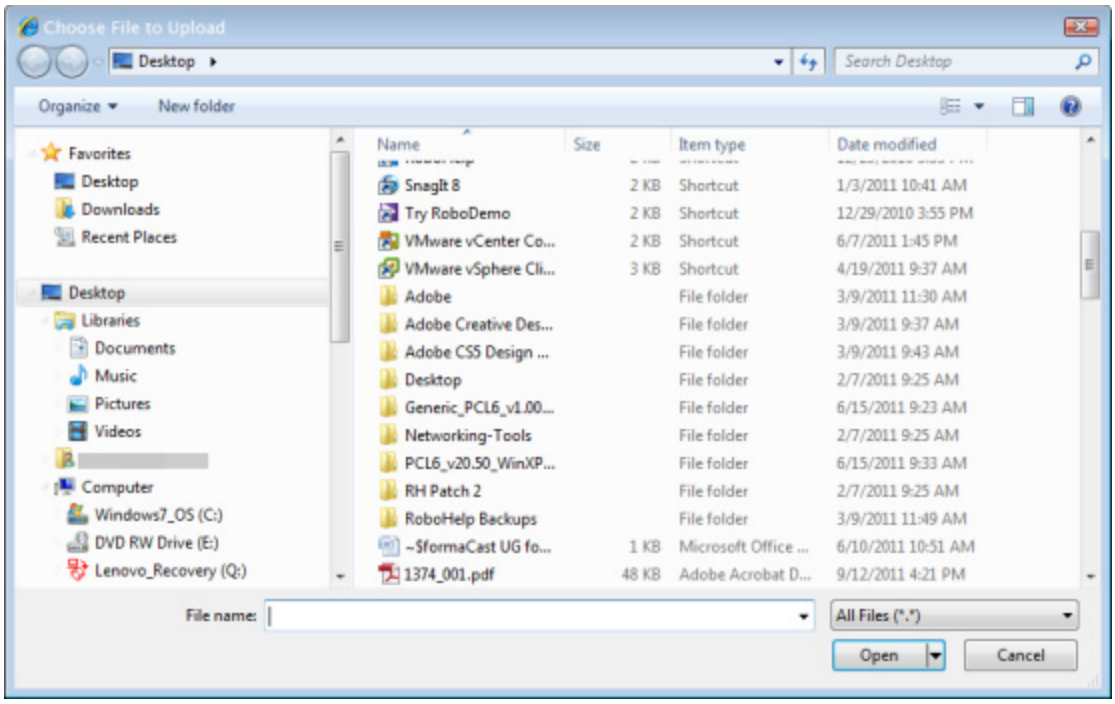
Step 2 Click the **Manage Licenses** link. The License Manager page appears.



Step 3 Enter your OS credentials in the **Login** and **Password** fields. Click the **Login** button. The Upload a New License page appears.



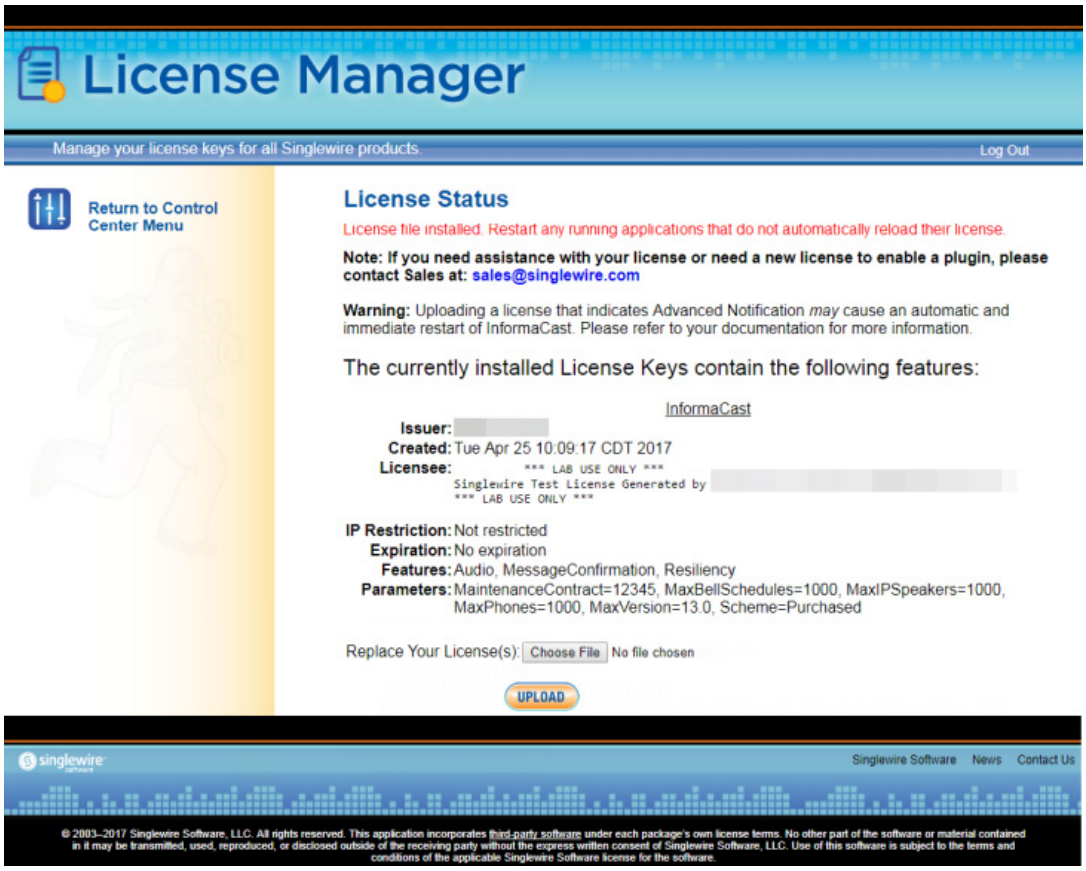
Step 4 Click the **Browse** button. The Choose File to Upload dialog box appears.



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.



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 9-39).

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 2-78.
- 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?

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.

Q. How do I capture traffic?

A. See "Verify Multicast with a Network Traffic Capture" on page 2-86.

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 4-42.

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 9-53 will walk you through the steps for changing the Virtual Appliance's IP address.

Manage InformaCast Virtual Appliance

The following sections detail how to manage InformaCast Virtual Appliance from the server side.

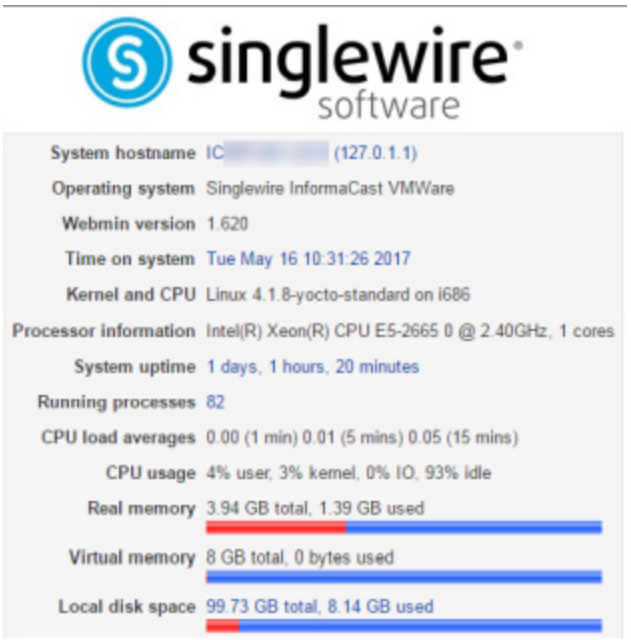
Manage Virtual Appliance Actions

Starting, stopping, and restarting applications and rebooting or shutting down the Virtual Appliance are all management actions you can perform through Webmin.

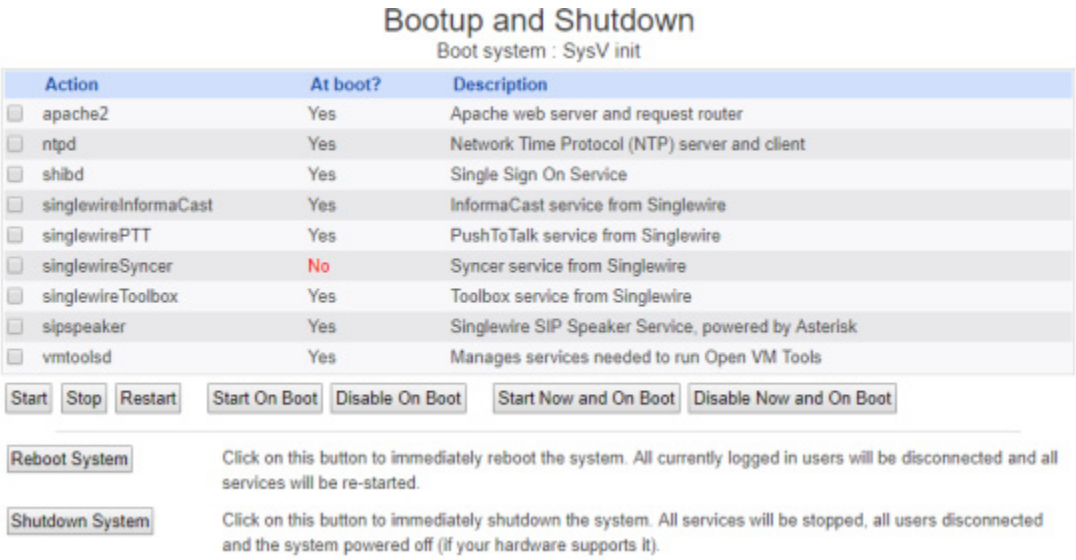
Stop an Application on InformaCast Virtual Appliance

Follow these steps to stop individual applications on InformaCast Virtual Appliance.

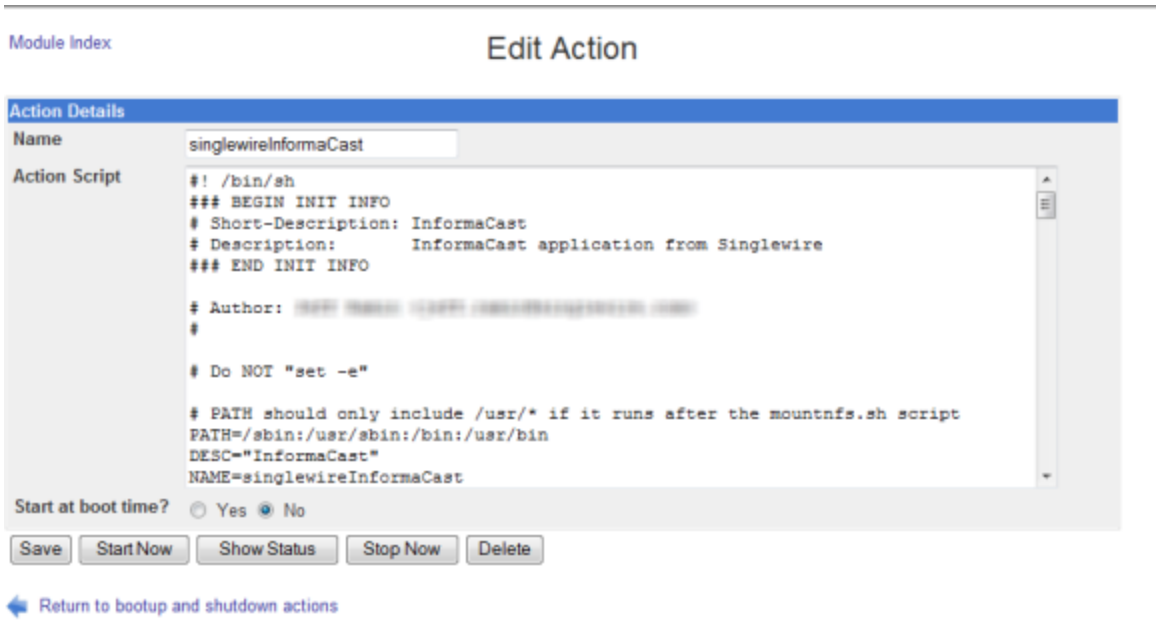
Step 1 Log into Webmin (see "Log into Webmin" on page 2-35 for specific steps). The Webmin homepage appears.



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



Step 3 Scroll down the list of actions until you come to your application's name (e.g. **singlewireInformaCast**). Click its link. The Edit Action page appears.

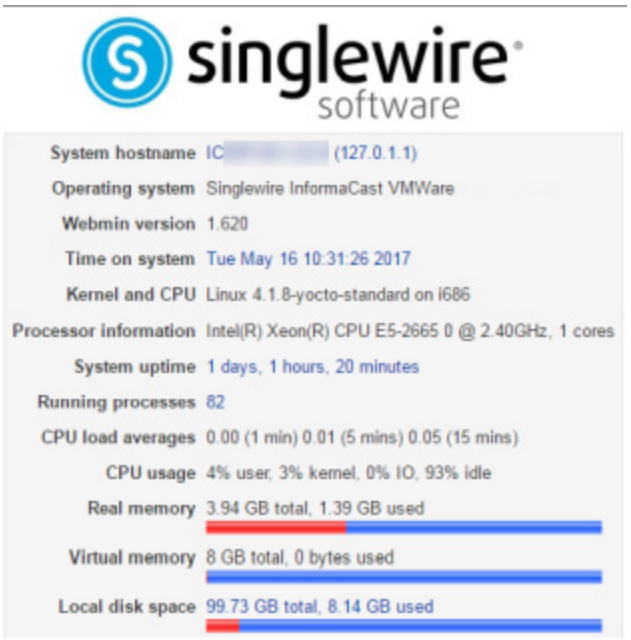


Step 4 Click the **Stop Now** button. It will take a minute or so for the application to stop.

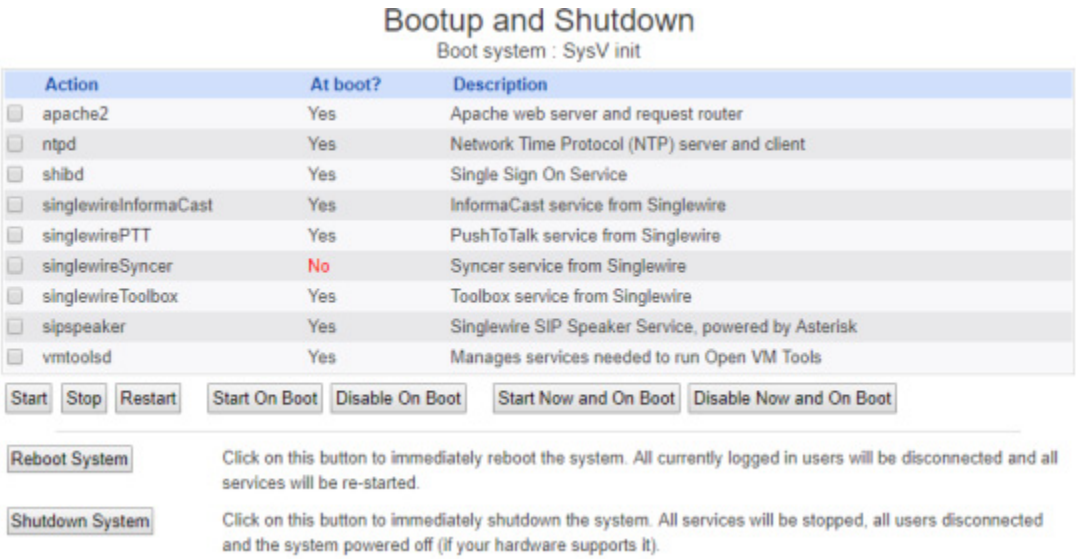
Start an Application on InformaCast Virtual Appliance

Follow these steps to start individual applications on InformaCast Virtual Appliance.

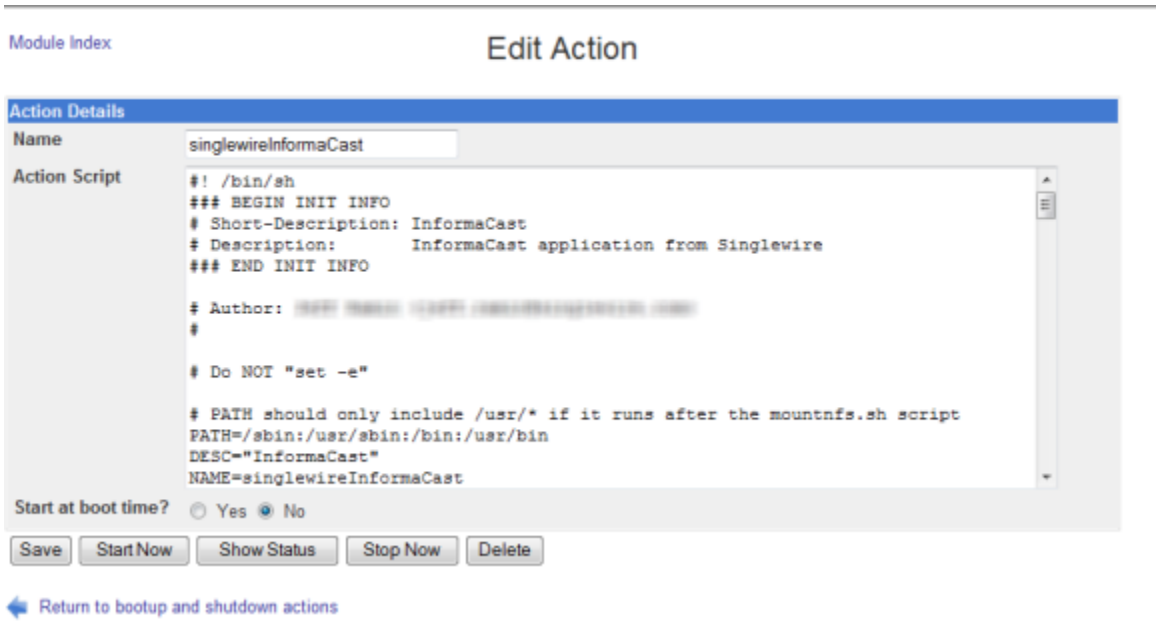
Step 1 Log into Webmin (see "Log into Webmin" on page 2-35 for specific steps). The Webmin homepage appears.



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



Step 3 Scroll down the list of actions until you come to your application's name (e.g. **singlewireInformaCast**). Click its link. The Edit Action page appears.



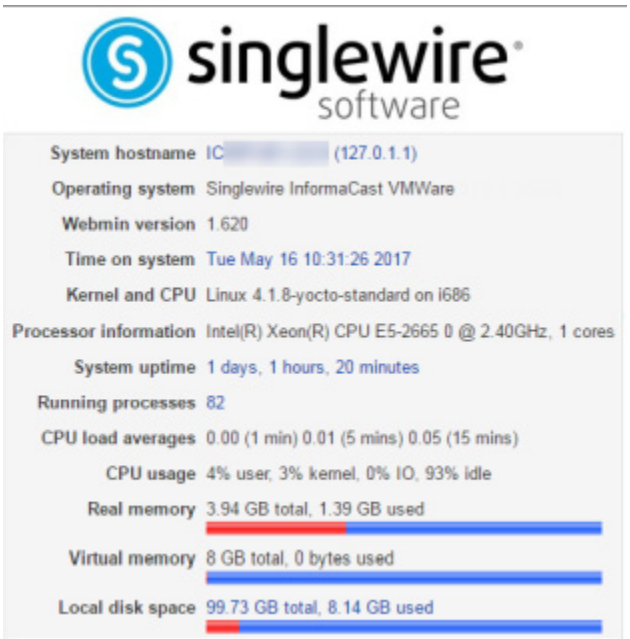
Step 4 Click the **Start Now** button. It will take a minute or so for the application to start.

Restart an Application on InformaCast Virtual Appliance

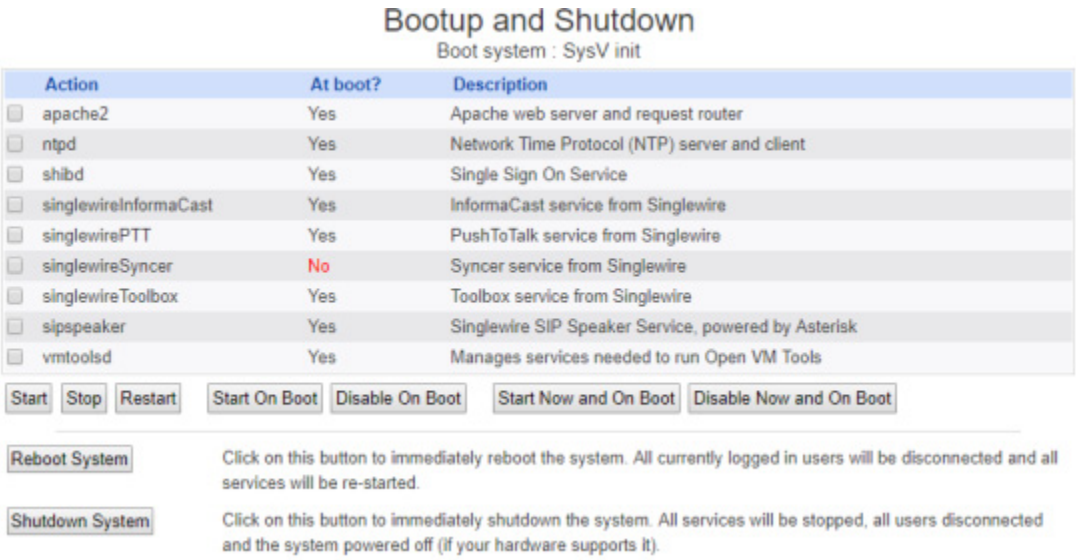
Changing the Virtual Appliance's IP address or hostname all require you to restart the singlewireInformaCast service. The singlewireInformaCast service is a Linux service that manages recipients (e.g. Cisco IP phones). Linux services are a set of processes running in the background of a server that are typically in charge of executing system tasks or running server applications, like databases.

Note JTAPI automatically updates every time the singlewireInformaCast service is restarted.

Step 1 Log into Webmin (see "Log into Webmin" on page 2-35 for specific steps). The Webmin homepage appears.



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



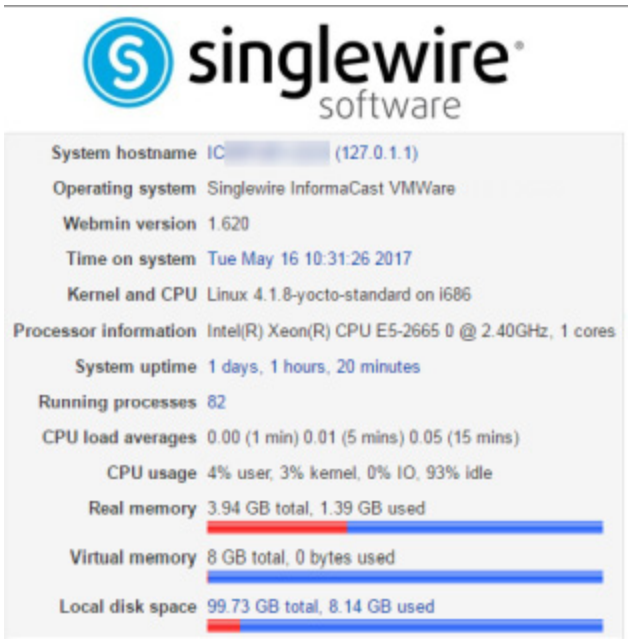
Step 3 Scroll down the list of actions until you come to your application's name (e.g. **singlewireInformaCast**). Select it by placing a checkmark in its Action column and click the **Restart** button. The Restarting Actions page appears.

It will take a minute for your application to restart.

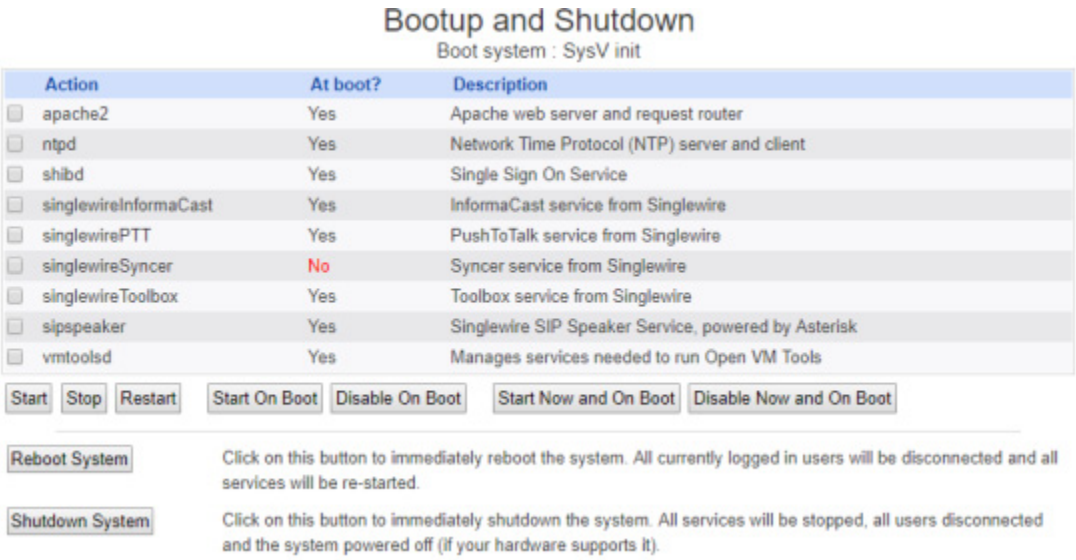
Reboot the InformaCast Virtual Appliance

Follow these steps to reboot the InformaCast Virtual Appliance.

Step 1 Log into Webmin (see "Log into Webmin" on page 2-35 for specific steps). The Webmin homepage appears.



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



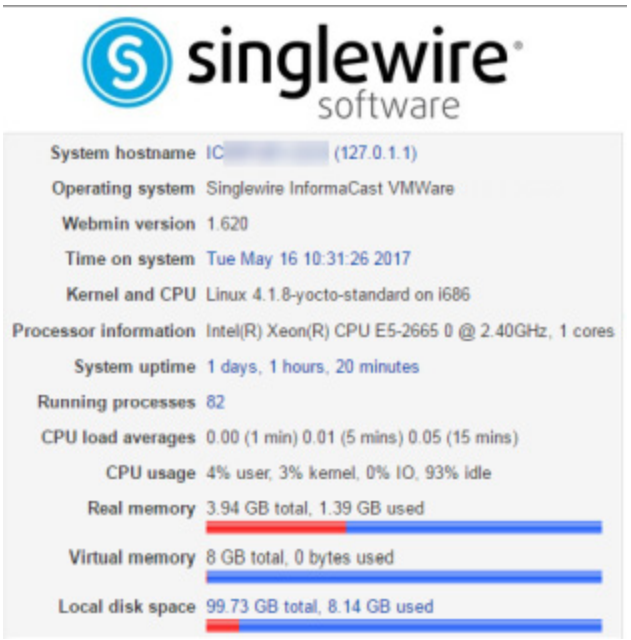
Step 3 Scroll to the bottom of the page and click the **Reboot System** button. The Reboot page appears.

Step 4 Click the **Reboot System** button. The server will shutdown, then restart.

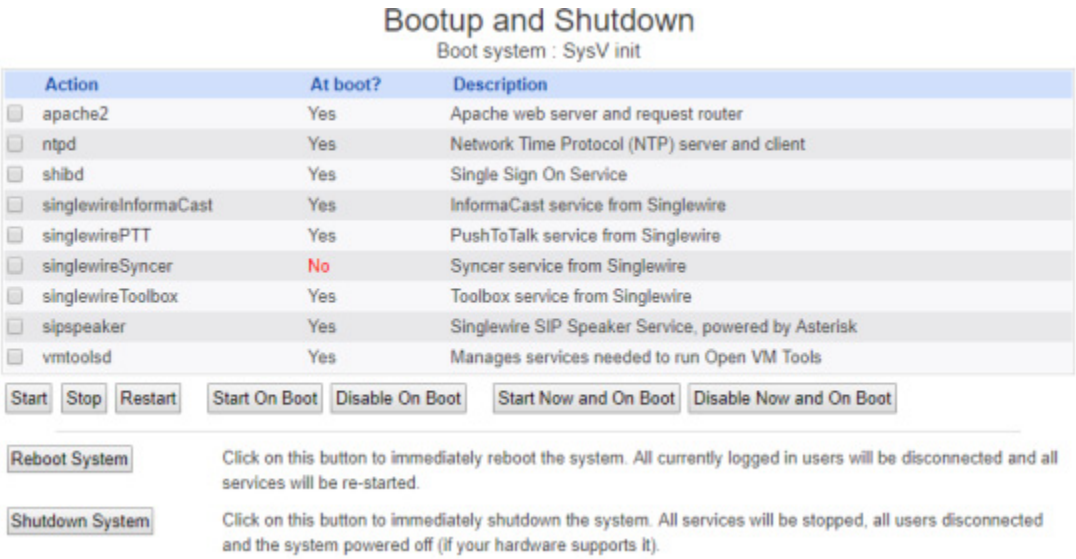
Shut Down the Virtual Appliance

Certain troubleshooting remedies may require you to shut down your Virtual Appliance.

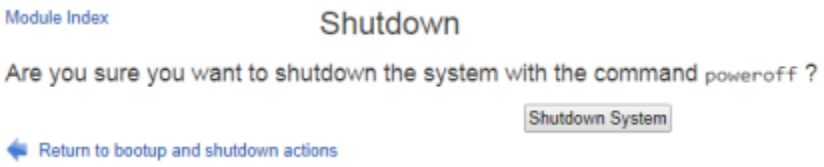
Step 1 Log into Webmin (see "Log into Webmin" on page 2-35 for specific steps). The Webmin homepage appears.



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



Step 3 Click the **Shutdown System** button. The Shutdown page appears.

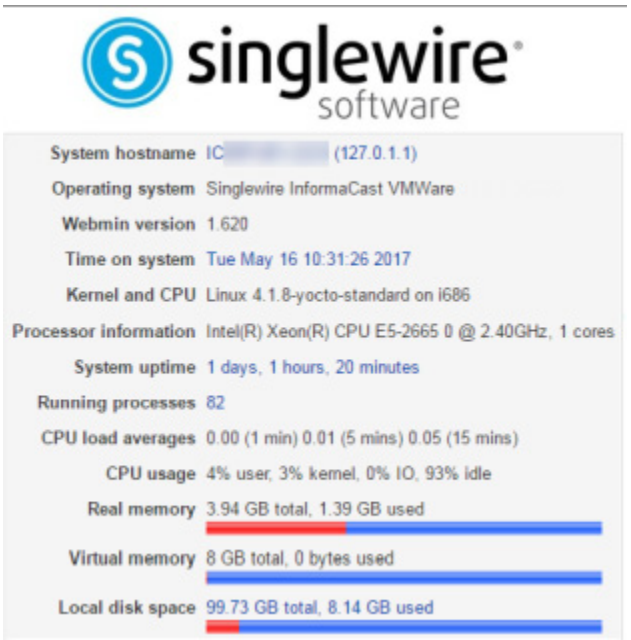


Step 4 Click the **Shutdown System** button. The Virtual Appliance will power off. This may take some time. While the Virtual Appliance is powered off, InformaCast's features may be inoperable.

Capture Virtual Appliance Network Traffic

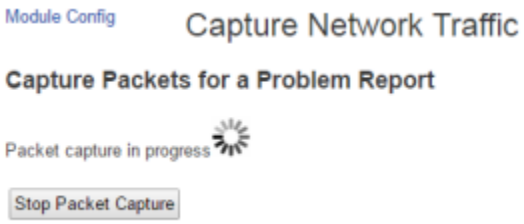
Some issues may arise that are beyond the scope of InformaCast's logs. In troubleshooting those issues, it may prove beneficial to capture network traffic to/from the Virtual Appliance server.

Step 1 Log into Webmin (see "Log into Webmin" on page 2-35 for specific steps). The Webmin homepage appears.



Step 2 Go to **System** | **Capture Network Traffic**. The Capture Network Traffic page appears.

Step 3 Click the **Start a new packet capture** button. The packet capture will begin.



Step 4 Perform the action that prompted you to run the traffic capture. For example, if you sent a broadcast to a recipient group of IP speakers and it failed, start the packet capture and then try sending the broadcast again.

Step 5 Wait for the packet capture to finish (the packet capture will stop by itself after capturing 33,000 packets) or click the **Stop Packet Capture** button.

If you need to submit your capture to Singlewire for analysis as part of your support case, follow the steps in "Collect the Virtual Appliance's Logs" on page 9-26. The collection of logs will include the packet capture you just performed as well as the Virtual Appliance's other logs.

Change the Virtual Appliance'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 21 on page 2-26. Because of its elevated status, you may find it helpful to change this password periodically. When creating your OS and application credentials, the characters in the following table are allowed.

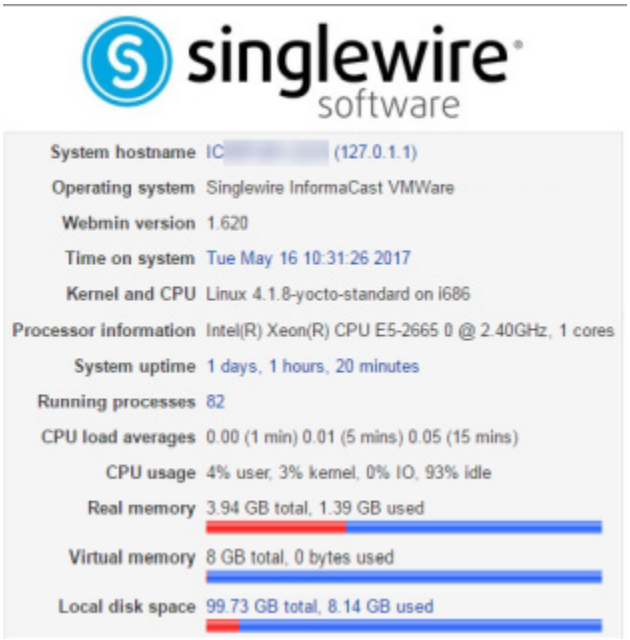
Symbol	Description
!	Exclamation mark
"	Double quotes (or speech marks)
#	Number
$	Dollar
%	Percent
&	Ampersand
'	Single quote
(	Open parenthesis (or open bracket)
)	Close parenthesis (or close bracket)
*	Asterisk
+	Plus
,	Comma
-	Hyphen
.	Period, dot or full stop
/	Slash or divide
0	Zero
1	One
2	Two
3	Three
4	Four
5	Five
6	Six
7	Seven
8	Eight
9	Nine
:	Colon
;	Semicolon
<	Less than (or open angled bracket)
=	Equals
>	Greater than (or close angled bracket)

Symbol	Description
?	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/f	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
\	Backslash
]	Closing bracket
^	Caret - circumflex
_	Underscore
`	Grave accent

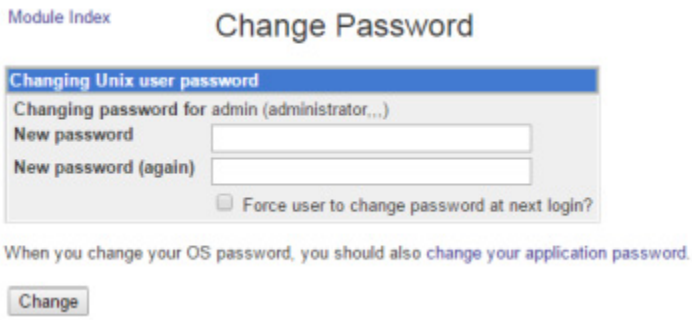
In addition, the following password restrictions apply:

- 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)

Step 1 Log into Webmin (see “Log into Webmin” on page 2-35 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).

Manage Password Recovery for the Virtual Appliance

Your Virtual Appliance allows for password recovery management:

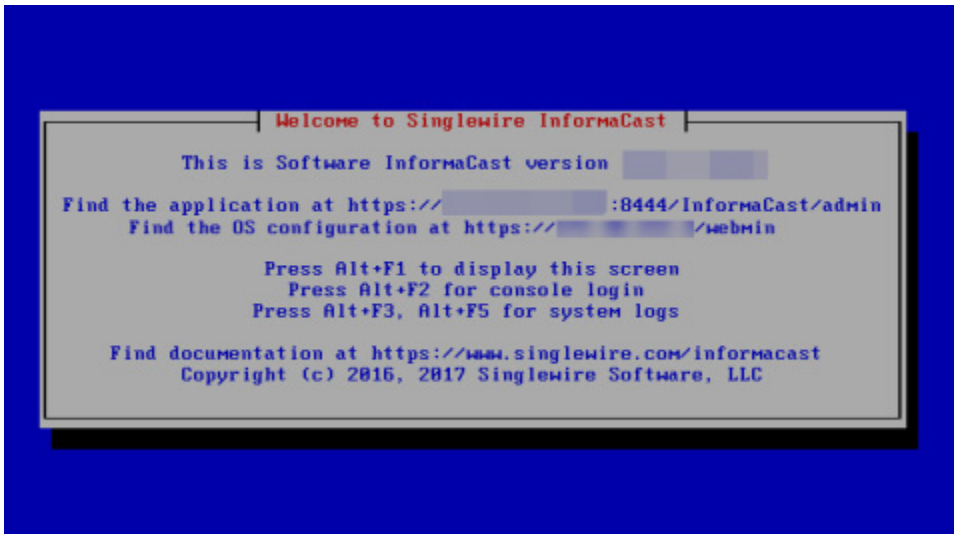
- If you lose your Virtual Appliance's password or accidentally delete admin (the default superuser account), you can contact Cisco TAC. Together, you'll use InformaCast's built-in process to recover your password.
- By default, the ability for you to reset your Virtual Appliance's password is enabled, but you may need to turn off/on this functionality depending on your environment's needs.

Recover Your OS and Application Passwords

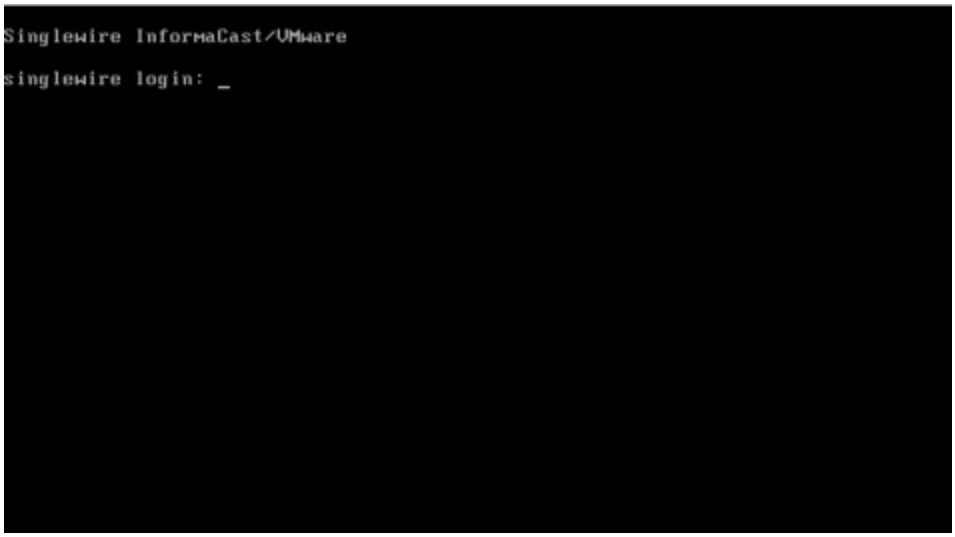
Your OS credentials are used to enter Webmin and Control Center and when using SSH to access the InformaCast Virtual Appliance. Your application credentials are used to enter InformaCast. This process will reset both sets of credentials to the same value.

Note Completing this process will cause your Virtual Appliance to reboot.

Step 1 Log into vSphere and open a console window to your Virtual Appliance. A console window to your Virtual Appliance appears.

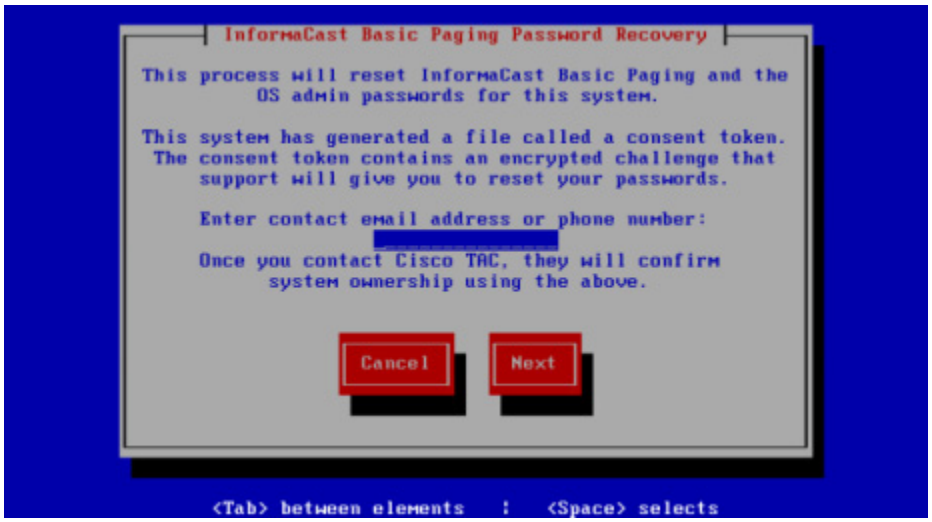


Step 2 Press the **Alt** + F2 keys to switch to the console screen where you can enter commands.

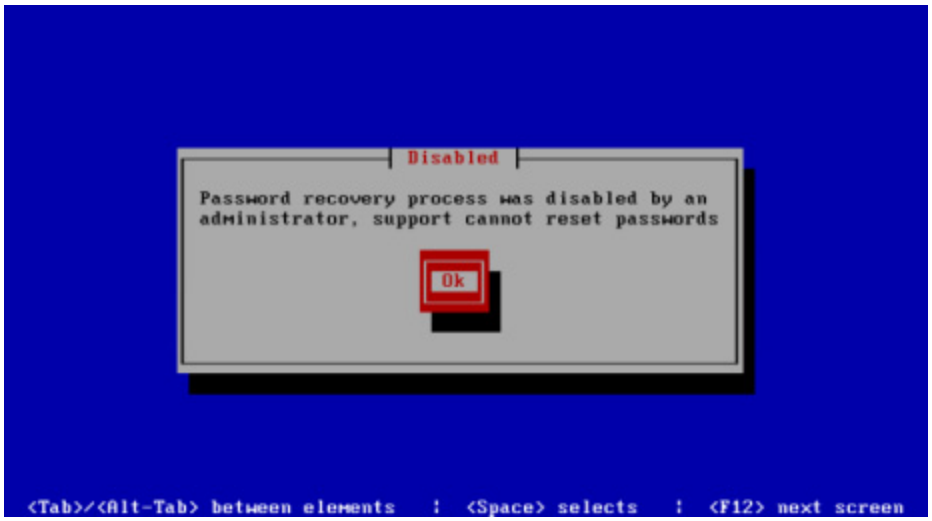


Step 3 Enter **recovery** at the prompt and press the **Enter** key.

If you have password recovery enabled, this console window appears and you can continue with these steps.

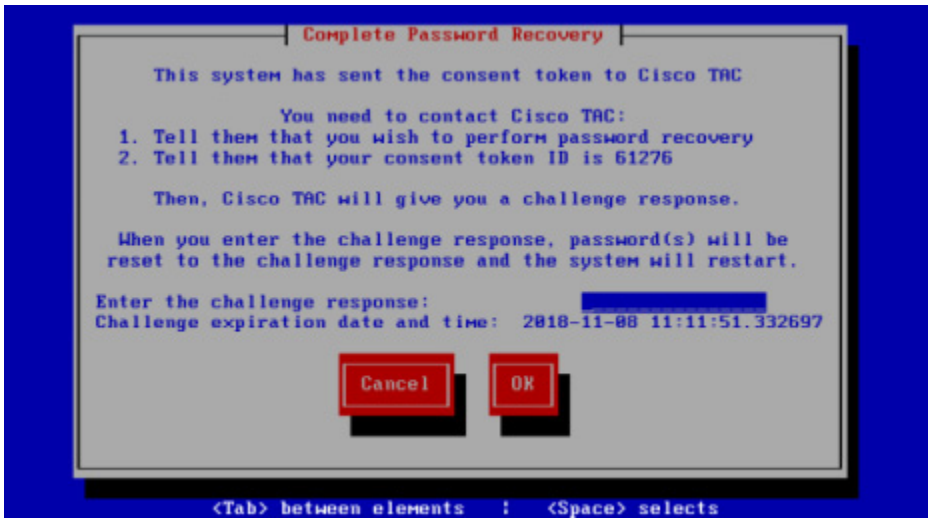


If you don't have password recovery enabled, this console window appears, and you cannot continue with these steps until you enable password recovery.

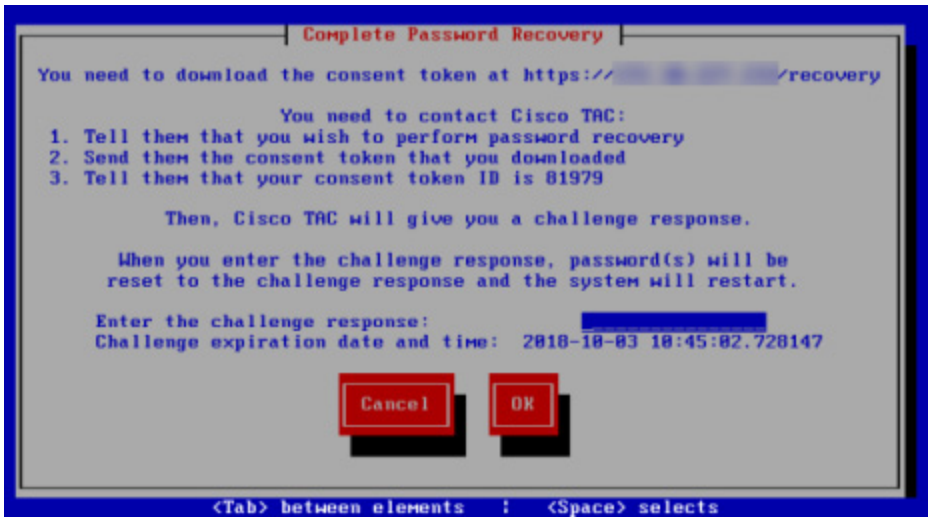


Step 4 Enter your email address or phone number, press the **Tab** or **Right Arrow** key to highlight the **Next** button, and press the **Spacebar** to select it.

If your Virtual Appliance has internet access, a consent token will be sent to Cisco TAC, this console window appears, and you should continue with the following steps, skipping Step 5.



If your Virtual Appliance doesn't have internet access, this console window appears and you should continue with the following steps.



Step 5 Go to the URL cited at the top of the console window, e.g. https://<ServerIPAddress>/recovery, where <ServerIPAddress> is the IP address of your Virtual Appliance. A token.txt file should download immediately. Save this file.

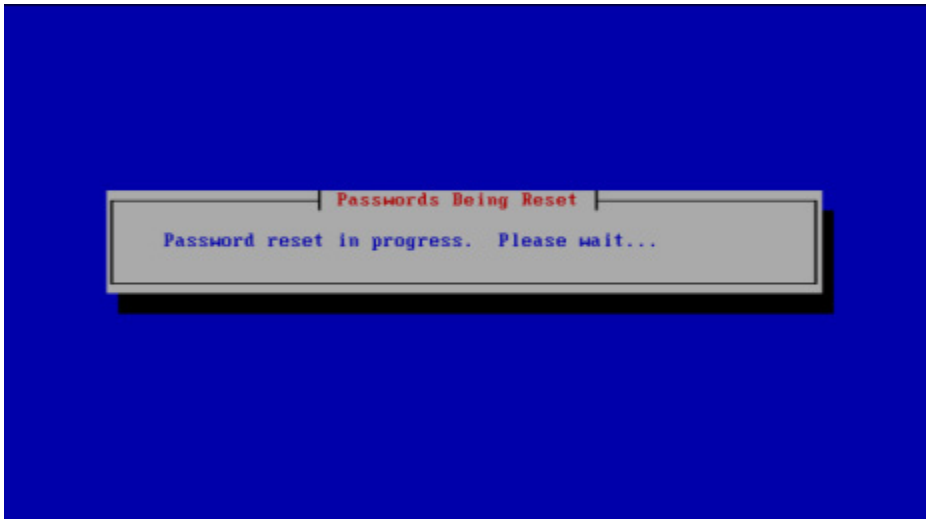
Note You now have 48 hours to complete the steps in this section. After 48 hours, your token and token ID number will expire.

Step 6 Make note of your token ID number, e.g. 01867. This ID lets Cisco TAC know you are who you say you are.

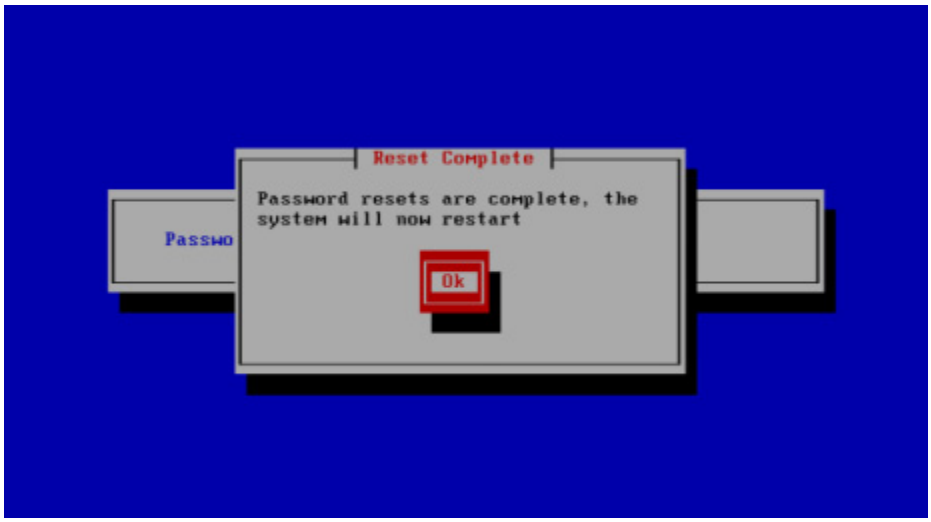
Step 7 Contact Cisco TAC and tell them you want to reset your OS and application passwords.

Step 8 Send them your token.txt file (if you have internet access, the TXT file has already been sent) and tell them your token ID number. They will provide you with a challenge response. This is your new password.

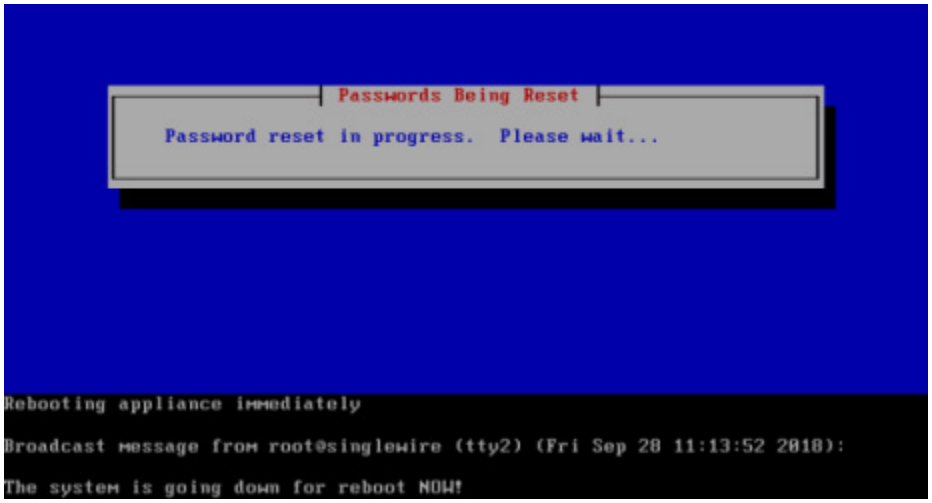
Step 9 Enter the challenge response (three sets of four alpha-numeric characters including the dashes), press the **Tab** or **Right Arrow** key to highlight the **Next** button, and press the **Spacebar** to select it. The command-line interface refreshes.



Once the resetting process is complete, your Virtual Appliance will need to reboot.



Step 10 Press the **Spacebar** to select the **Ok** button. Your Virtual Appliance will reboot.



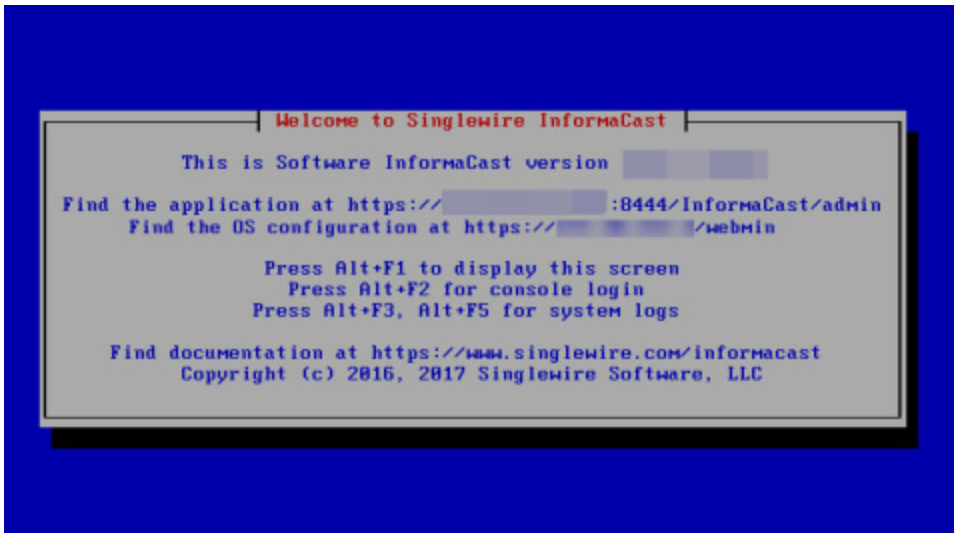
Once your Virtual Appliance reboots, log in with your new password. Depending on your policy, you may need to change it again:

- "Change the Virtual Appliance's Password" on page 9-11
- "Change the Application Administrator's Password" on page 6-2

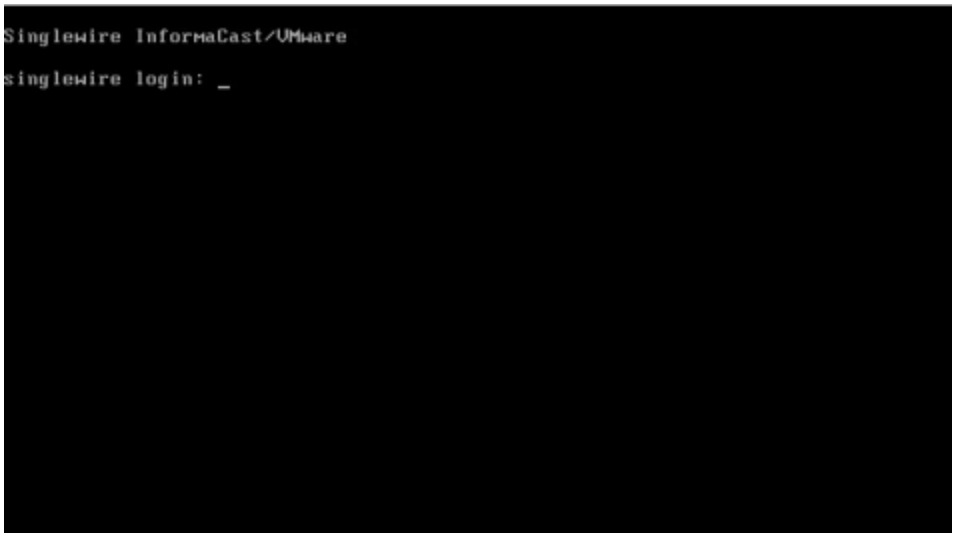
Disable/Enable Password Recovery

This process will turn off/on your ability to recover your Virtual Appliance's password. By default, password recovery is enabled. Singlewire recommends you only change this setting if your organization's security policy requires you to do so. If you disable password recovery and lock yourself out of the system, you will have to reinstall InformaCast.

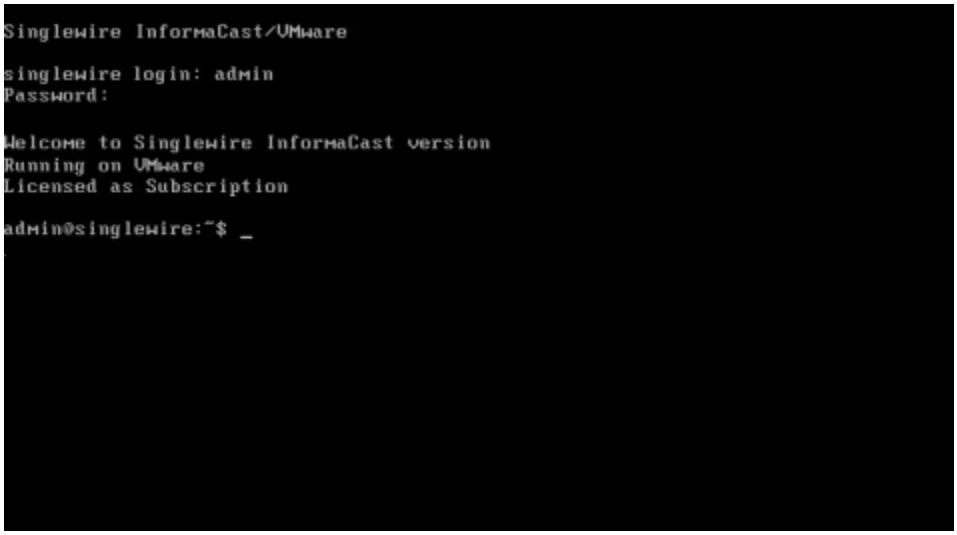
Step 1 Log into vSphere and open a console window to your Virtual Appliance. A console window to your Virtual Appliance appears.



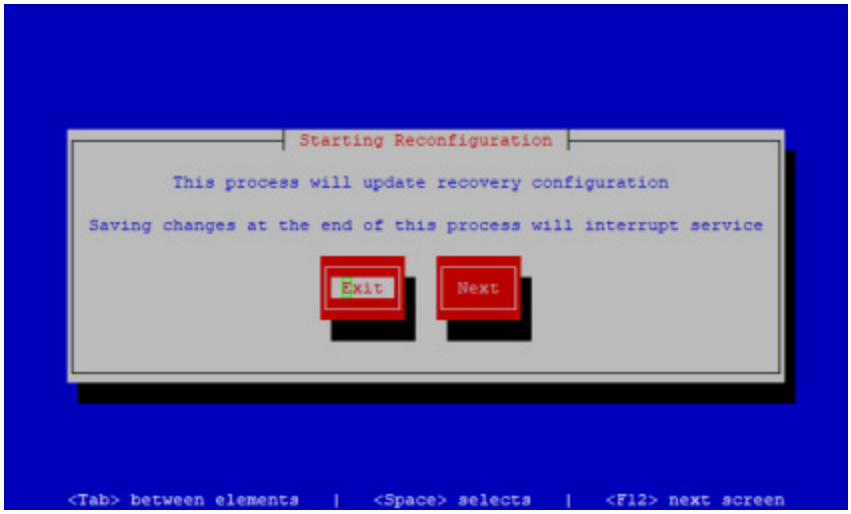
Step 2 Press the **Alt** + F2 keys to switch to the console screen where you can enter commands.



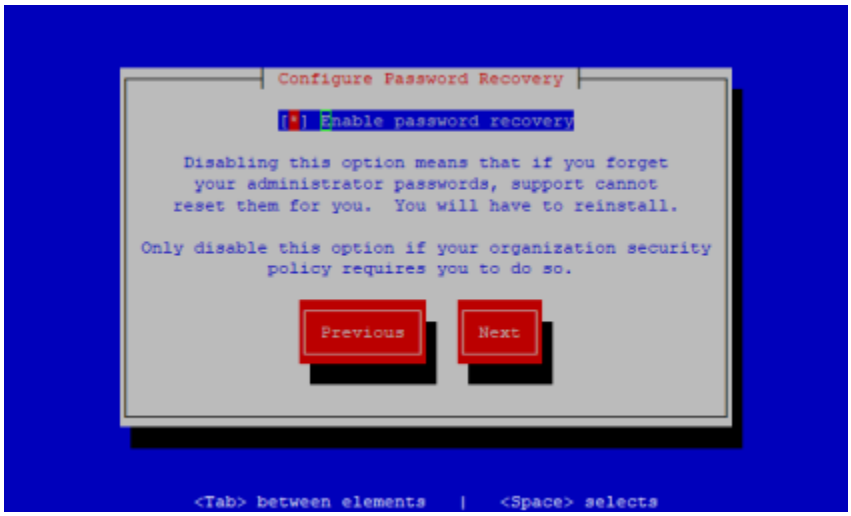
Step 3 Log in. The console window refreshes, showing you that you're logged in.



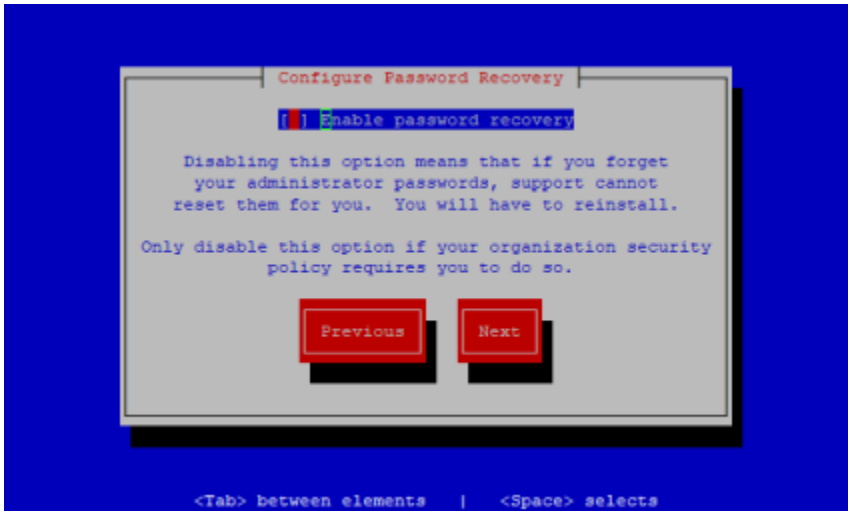
Step 4 Enter **configure-recovery** at the prompt and press the **Enter** key. The Starting Reconfiguration window appears.



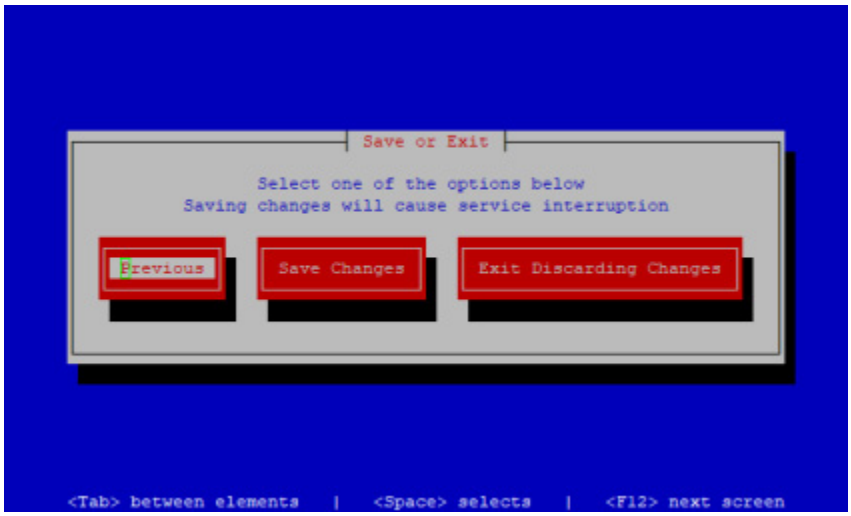
Step 5 Use the **Tab** or **Right Arrow** key to highlight the **Next** button, then press the **Spacebar** to select it. The Configure Password window appears.



Step 6 Press the **Spacebar** to disable password recovery. Notice the asterisk is now missing from the **[] Enable password recovery** statement.



Step 7 Use the **Tab** or **Right Arrow** key to highlight the **Next** button, then press the **Spacebar** to select it. The Save or Exit window appears.



Step 8 Use the **Tab** or **Right Arrow** key to highlight the **Save Changes** button, then press the **Spacebar** key to select it. The command-line interface appears.

Password recovery is now disabled. Repeat the process to enable the functionality again.

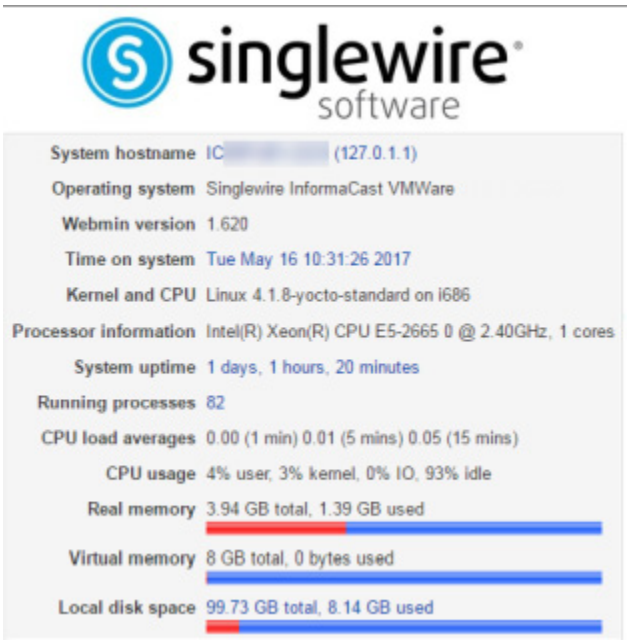
Access the Virtual Appliance's Logs

InformaCast has several system logs that may be of use to you (or required by Singlewire Support) when troubleshooting an issue:

- Various OS logs:
  - File /var/log/auth.log

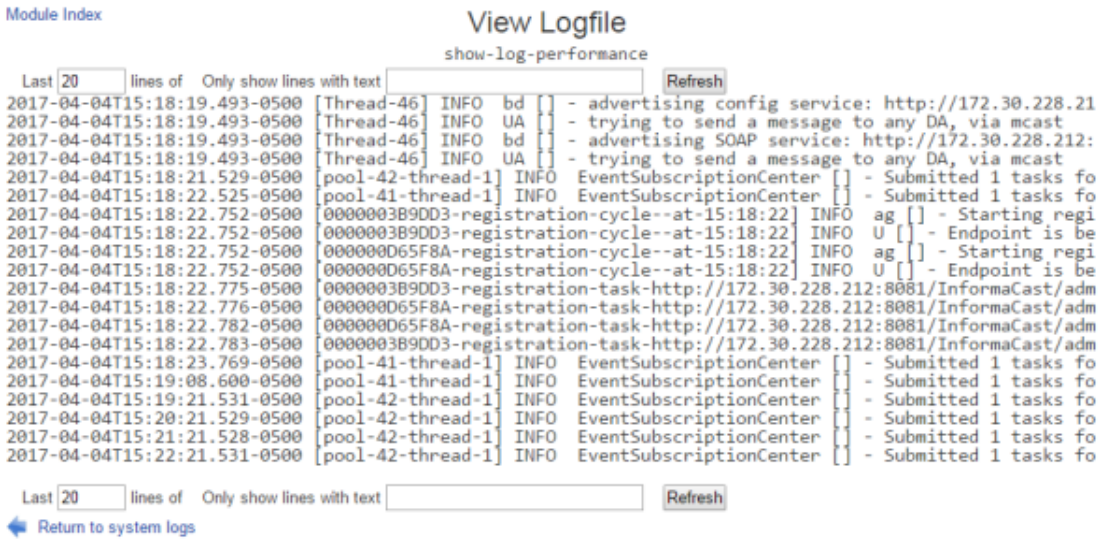
  - File /var/log/syslog
  - File /var/log/cron.log
  - File /var/log/daemon.log
  - File /var/log/kern.log
  - File /var/log/lpr.log
  - File /var/log/mail.log
  - File /var/log/user.log
  - File /var/log/mail.info
  - File /var/log/mail.warn
  - File /var/log/mail.err
  - File /var/log/news.crit
  - File /var/log/news.err
  - File /var/log/news.notice
  - File /var/log/debug
  - File /var/log/messages
  - Users :omusrmsg
  - File /var/log/boot.log
  - Unix socket file remote-host:514
  - Output from dmesg
- The InformaCast Performance log (Output from show-log-performance)
- The InformaCast Summary log (Output from show-log-summary)
- The InformaCast REST API log (Output from show-log-restapi)
- The InformaCast Audit log (Output from show-log-audit)
- The InformaCast SIP Stack log (Output from show-log-sipstack)
- The Webmin Error log (File /var/webmin/miniserv.error)

Step 1 Log into Webmin (see "Log into Webmin" on page 2-35 for specific steps). The Webmin homepage appears.



Step 2 Go to **System** | **System Logs**. The System Logs page appears.

Step 3 Click the **View** link for a particular log to view its contents. In the following example, you're viewing the contents of the InformaCast Performance log.

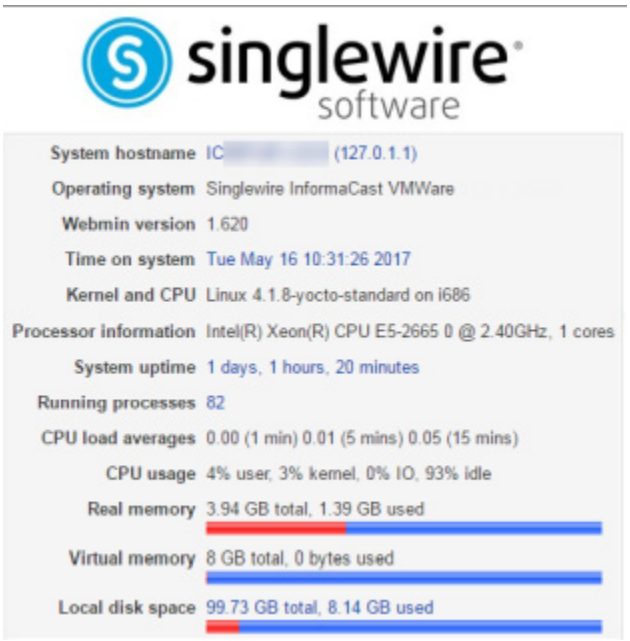


Collect the Virtual Appliance's Logs

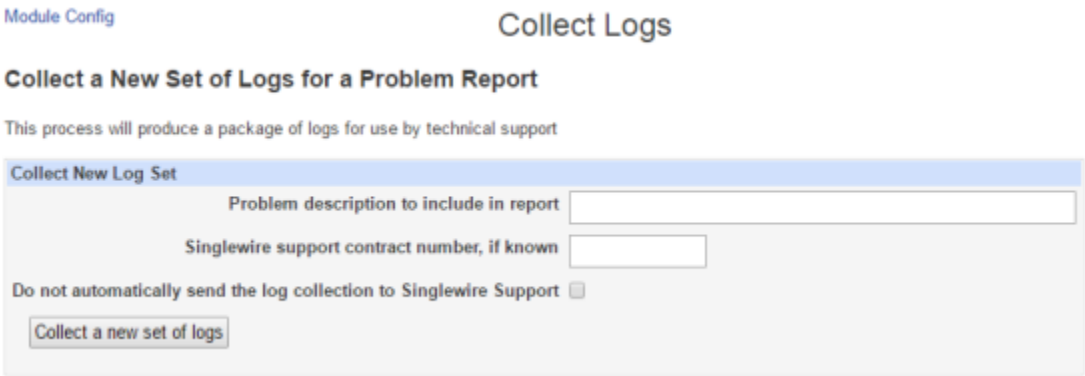
If you are having an issue with InformaCast that you cannot resolve without help, it is likely that Singlewire Support would ask for a collection of your logs in order to analyze your problem. Webmin offers a way to create an encrypted log archive that can be downloaded and emailed to Singlewire Support, or securely sent by InformaCast as long as it has Internet access without an HTTPS proxy in the way.

Note Logs are encrypted using a dynamically generated 32-byte, AES-256-bit key that is encrypted in a 2048-bit RSA public key, and only Singlewire has the private key; it is not possible for you to decrypt and view the log contents.

Step 1 Log into Webmin (see "Log into Webmin" on page 2-35 for specific steps). The Webmin homepage appears.



Step 2 Go to **System** | **Collect Logs**. The Collect Logs page appears.

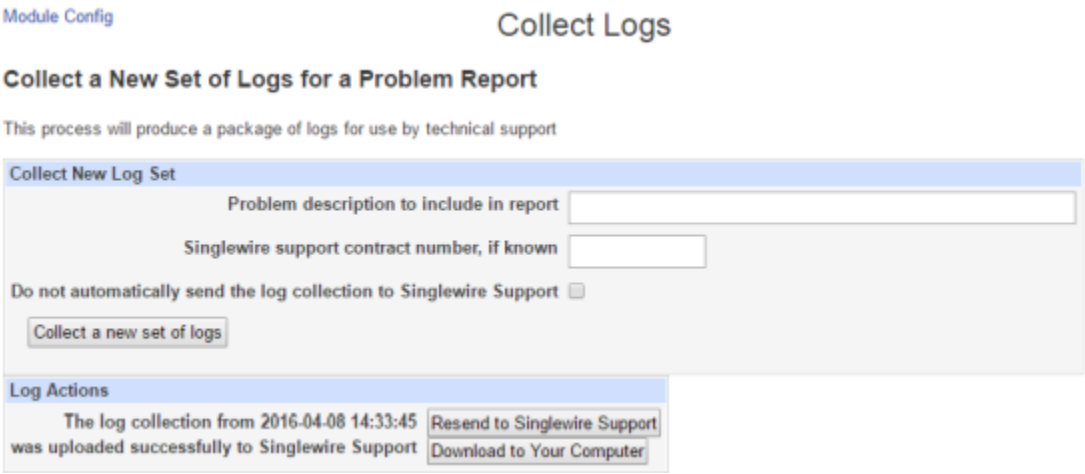


Step 3 Enter a short description of the problem you're having in the **Problem description to include in report** field.

Step 4 Enter your maintenance contract number (if you know it) in the **Singlewire support contract number** field.

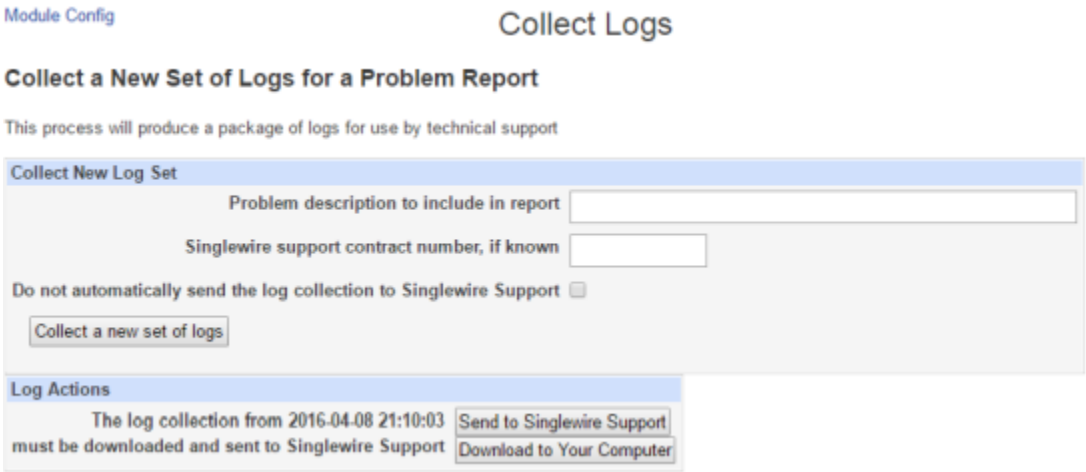
Step 5 Select the **Do not automatically send the log collection to Singlewire Support** checkbox if you don't want InformaCast to collect its logs and immediately send them to Singlewire Support.

Step 6 Click the **Collect a new set of logs** button. The Collect Logs page refreshes.



If you didn't select the **Do not automatically send the log collection to Singlewire Support** checkbox or you don't have an HTTPS proxy server prohibiting its Internet access, InformaCast will send your logs to Singlewire Support.

If you did select the **Do not automatically send the log collection to Singlewire Support** checkbox or InformaCast can't send the logs to Singlewire Support, your page will look slightly different.



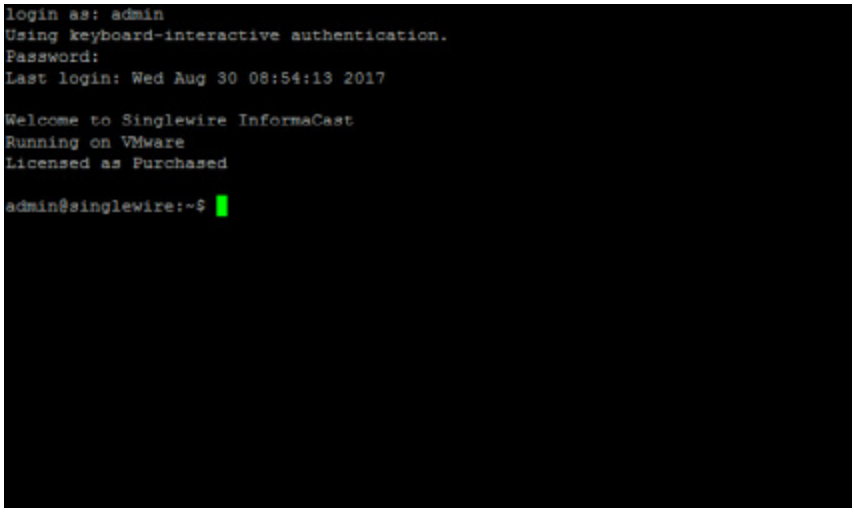
Click the **Download to Your Computer** button, email Singlewire Support, and attach the log file.

Enable the Singlewire Support Account

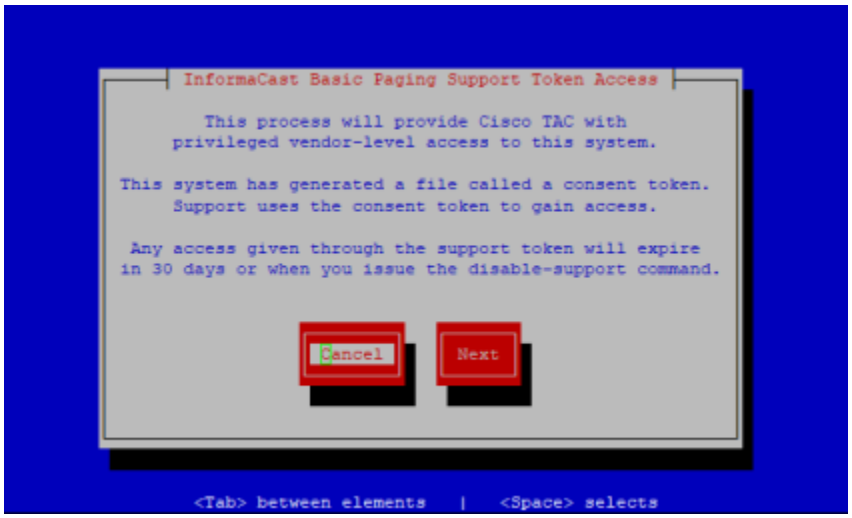
Sometimes, when troubleshooting an issue, it is helpful to "turn on" access to your Virtual Appliance for Singlewire Support personnel. **enable-support**, a command for the command-line interface, sets the Support account to accept a new password that it then generates as a hash for you to send to Singlewire. Singlewire Support personnel can use this password to access your Virtual Appliance's

Support account from the command-line interface (either through vSphere or PuTTY; these steps illustrate using PuTTY). If you don't explicitly disable the Support account (**disable-support**), it will automatically revert to a disabled state in 30 days.

Step 1 Use an SSH client to log into the command-line interface (see "Log into the Command-line Interface" on page 2-37). The command-line interface appears, showing you that you're logged in.

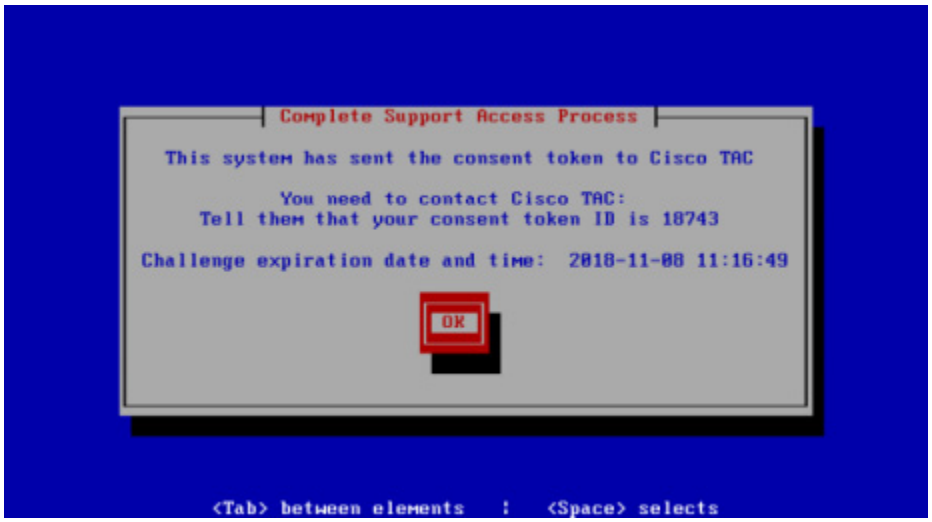


Step 2 Enter **enable-support** at the prompt and press the **Enter** key. The command-line interface refreshes.

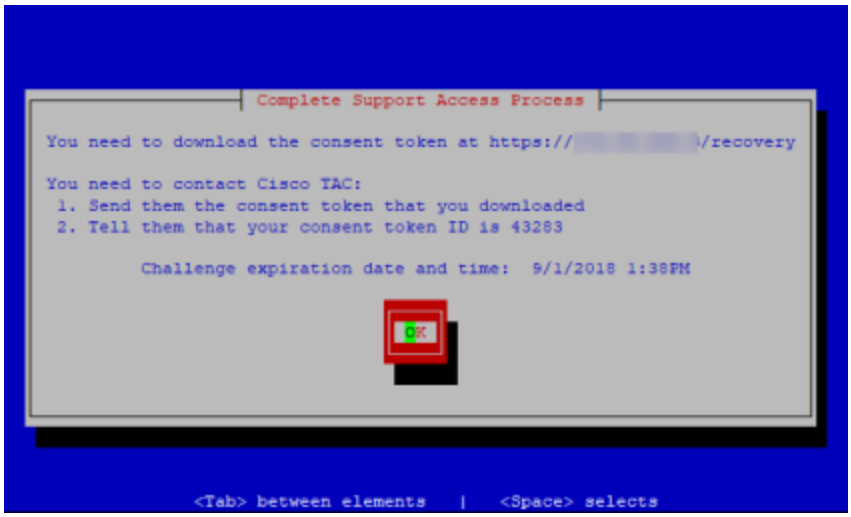


Step 3 Use the **Tab** or **Right Arrow** key to highlight the **Next** button, then press the **Spacebar** to select it.

If your Virtual Appliance has internet access, a consent token will be sent to Cisco TAC, this console window appears, and you should continue with the following steps, skipping Step 4.



If your Virtual Appliance doesn't have internet access, this console window appears and you should continue with the following steps.



Step 4 Go to the URL cited at the top of the console window, e.g. https://<ServerIPAddress>/recovery, where <ServerIPAddress> is the IP address of your Virtual Appliance. A token.txt file should download immediately. Save this file.

Step 5 Make note of your token ID number, e.g. 01867. This ID lets Cisco TAC know you are who you say you are.

Step 6 Contact Cisco TAC and tell them you want to enable the Support account.

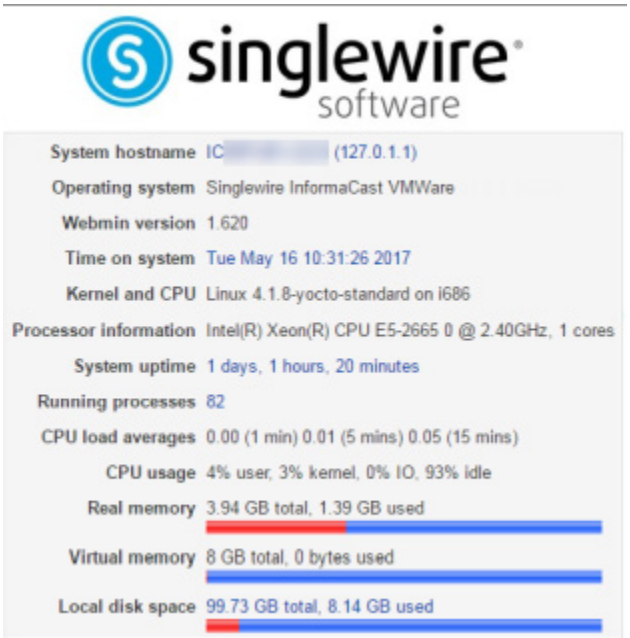
Step 7 Send them your token.txt file (if you have internet access, the TXT file has already been sent) and tell them your token ID number. They will enable the Support account.

Tip Disable the Support account by entering **disable-support** at the prompt and pressing the **Enter** key. If you don't explicitly disable the Support account, it will automatically revert to a disabled state in 30 days.

Display a List of Processes Running on the Virtual Appliance

Viewing a list of running processes allows you to verify services, such as singlewireInformaCast, are running. It can also help with troubleshooting.

Step 1 Log into Webmin (see "Log into Webmin" on page 2-35 for specific steps). The Webmin homepage appears.



Step 2 Go to **System | Running Processes**. The Running Processes page appears and you can see all of the services that InformaCast is running.

Help..
Module Config

Running Processes

Display : PID | User | Memory | CPU | Search

ID	Owner	Started	Command
1	root	Oct11	init [5]
101	root	Oct11	/sbin/udevd -d
730	root	Oct11	/usr/sbin/haveged -w 1024 -v 1
760	root	Oct11	/bin/bash
3515	ntp	10:45	/usr/sbin/ntpd -c /var/lib/ntp/ntp.conf -u ntp:ntp -p /var/run/ntpd.pid -g
3912	ptt	Oct11	/usr/local/singlewire/java/jdk/bin/java -Djava.util.logging.config.file=/usr/loc ...
4035	toolbox	Oct11	/usr/local/singlewire/java/jdk/bin/java -Djava.util.logging.config.file=/usr/loc ...
4157	root	Oct11	/usr/bin/perl /usr/libexec/webmin/miniserv.pl /etc/webmin/miniserv.conf
24159	root	12:28	[/usr/libexec/we] <defunct>
24160	root	12:28	/usr/libexec/webmin/proc/index_tree.cgi
24167	root	12:28	sh -c ps --cols 2048 -eo user:80,ruser:80,group:80,rgroup:80,pid,ppid,pgid,pcpu, ...
24168	root	12:28	ps --cols 2048 -eo user:80,ruser:80,group:80,rgroup:80,pid,ppid,pgid,pcpu,vsz,ni ...
4461	root	Oct11	/usr/sbin/sshd
25657	root	09:53	sshd: admin [priv]
25686	admin	09:53	sshd: admin@pts/0
25687	admin	09:53	-sh
4540	root	Oct11	/usr/sbin/httpd -k start
4542	root	Oct11	/usr/sbin/rotatelogs -f -c -l var/log/apache2/error_log.%Y%m%d-%H%M%S 86400
4543	root	Oct11	/usr/sbin/rotatelogs -f -c -l /var/log/apache2/error_log.%Y%m%d-%H%M%S 86400
4544	root	Oct11	/usr/sbin/rotatelogs -f -c -l var/log/apache2/access_log.%Y%m%d-%H%M%S 86400
4545	root	Oct11	/usr/sbin/rotatelogs -f -c -l /var/log/apache2/ssl_request_log.%Y%m%d-%H%M%S 864 ...
4546	root	Oct11	/usr/sbin/rotatelogs -f -c -l /var/log/apache2/ssl_request_log.%Y%m%d-%H%M%S 864 ...
4547	root	Oct11	/usr/sbin/rotatelogs -f -c -l /var/log/apache2/ssl_request_log.%Y%m%d-%H%M%S 864 ...
4548	root	Oct11	/usr/sbin/rotatelogs -f -c -l /var/log/apache2/ssl_request_log.%Y%m%d-%H%M%S 864 ...
4549	root	Oct11	/usr/sbin/rotatelogs -f -c -l /var/log/apache2/ssl_request_log.%Y%m%d-%H%M%S 864 ...
4551	apache	Oct11	/usr/sbin/httpd -k start
4552	apache	Oct11	/usr/sbin/httpd -k start
4553	apache	Oct11	/usr/sbin/httpd -k start
4934	apache	Oct11	/usr/sbin/httpd -k start
4650	root	Oct11	/usr/sbin/rsyslogd
7535	root	Oct11	/bin/bash /usr/local/singlewire/platform/bin/license-mode-changes
3400	root	10:45	/usr/bin/inotifywait -e modify /usr/local/singlewire/InformaCast/web/WEB-INF/Lic ...

Show the Virtual Appliance's Version

The **show-version** command displays the Virtual Appliance version in use. Verifying your version can aid in troubleshooting issues.

Note The Webmin homepage also displays version information.

Step 1 Log into the command-line interface (see "Log into the Command-line Interface" on page 2-37). The command-line interface appears, showing you that you're logged in.

```
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Wed Aug 30 08:54:13 2017

Welcome to Singlewire InformaCast
Running on VMware
Licensed as Purchased

admin@singlewire:~$
```

Step 2 Enter **show-version** at the prompt and press the **Enter** key. The command-line interface refreshes with application version details.

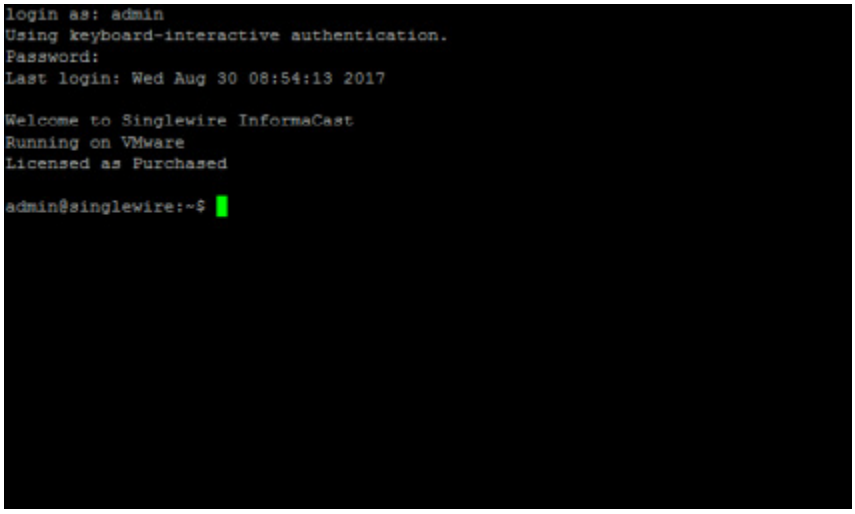
```
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Wed Aug 30 08:54:13 2017

Welcome to Singlewire InformaCast
Running on VMware
Licensed as Purchased

admin@singlewire:~$ show-version

This is Singlewire InformaCast version [redacted]
Build [redacted] is a release build from release/IC-[redacted] branch
Running on VMware
Licensed as Purchased

Copyright (c) 2017 Singlewire Software, LLC
https://www.singlewire.com

admin@singlewire:~$
```

Set Allowed SSL Protocols

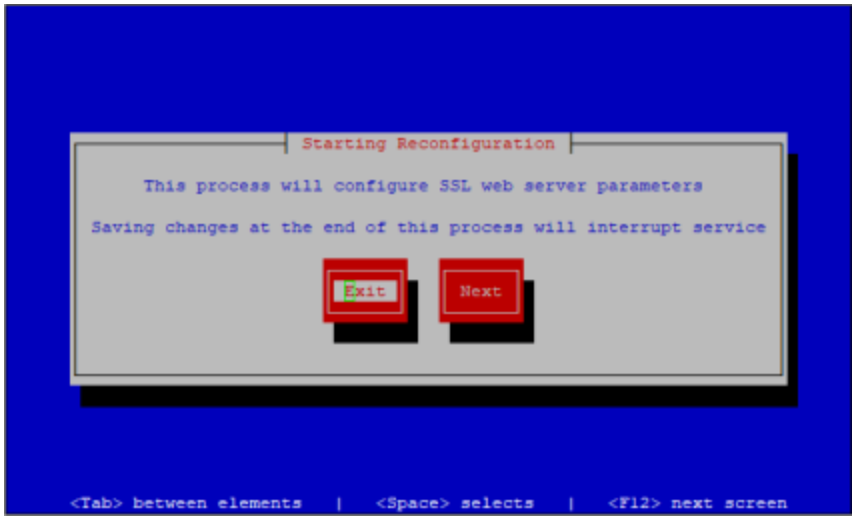
Secure Socket Layer (SSL) and Transport Layer Security (TLS) are both cryptographic protocols that provide authentication and data encryption between servers, machines, and applications operating over a network (e.g. a client connecting to a web server). For example, InformaCast uses them for communication between itself and the Control Center. In addition, web browsers use SSL and TLS to communicate with InformaCast.

InformaCast supports SSLv3, TLS 1.0, TLS 1.1, and TLS 1.2; however, SSLv3 has been deprecated by the IETF, and TLS 1.2 is preferred over TLS 1.0 and 1.1. Due to newer versions of the protocols supporting stronger, more secure cipher suites and algorithms, you may want to disable the older protocols, or your organization's security policy may dictate that only certain protocols are used.

Step 1 Log into the command-line interface (see "Log into the Command-line Interface" on page 2-37). The command-line interface appears, showing you that you're logged in.



Step 2 Enter **configure-ssl-parameters** at the prompt and press the **Enter** key. The Starting Reconfiguration window appears.



Step 3 Press the **Tab** key to highlight the **Next** button, then the **Spacebar** to select it. The Configure SSL Parameters window appears.

By default, SSLv3 is disabled and all supported versions of TLS are enabled.

Step 4 Use the **Tab** key to enter the different protocols' fields, pressing the **Spacebar** to disable the ones you don't need. Disabled protocols will have the * removed from between [ ]. Enabled protocols will have the * between [*].

Note At least one version of TLS must be enabled.

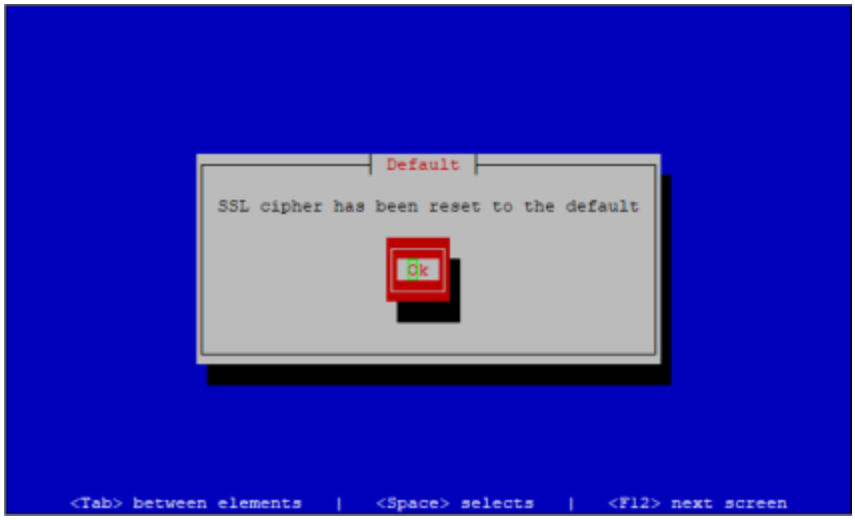
Step 5 Press the **Tab** key to enter the **Enable Landing Page HTTP Port** field and the **Spacebar** to disable HTTP when accessing the InformaCast Virtual Appliance landing page. With HTTP disabled, HTTPS will be used when accessing the InformaCast Virtual Appliance landing page.

Step 6 Press the **Tab** key to enter the **SSL Cipher String** field and either accept the cipher string provided or enter your cipher string of choice.

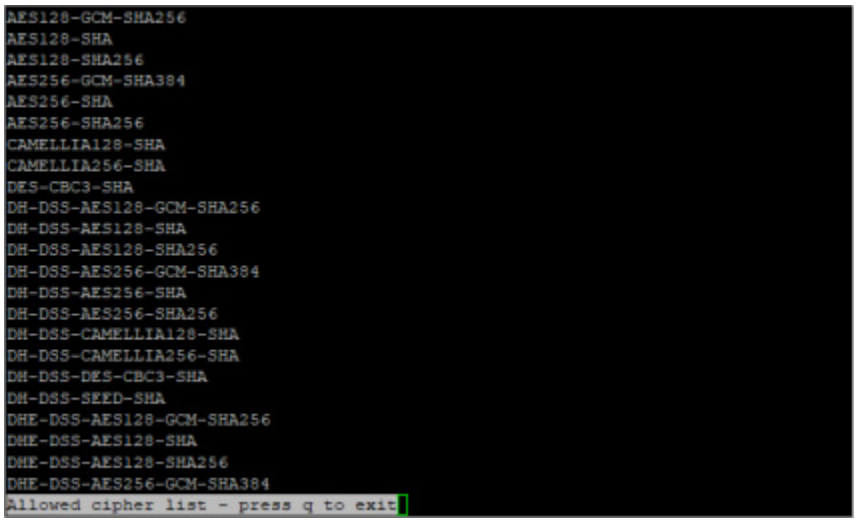
A cipher suite is a set of algorithms that help secure a network connection that uses SSL or TLS. The set of algorithms that cipher suites usually contain include: a key exchange algorithm, a bulk encryption algorithm, and a message authentication code (MAC) algorithm. There are hundreds of different cipher suites that contain different combinations of these algorithms.

If you want to change the provided cipher string, you need to understand Apache SSL Cipher configuration.

If you change your cipher string in error, press the **Tab** key to highlight **Restore Cipher String To FIPS Default**, then press the **Spacebar** to select it. The Default window appears and your cipher string is set back to its default value.



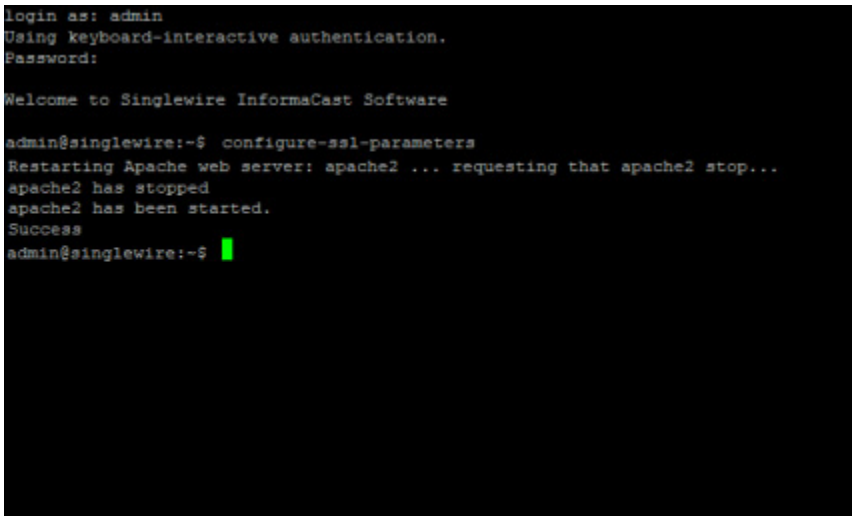
Step 7 Press the **Tab** key to highlight **Show Matching Ciphers**, then the **Spacebar** to select it. A list of ciphers that match your string appears.



Step 8 Press **Q** to exit this list.

Step 9 Press the **Tab** key to highlight the **Next** button, then the **Spacebar** to select it. The Save or Exit window appears.

Step 10 Press the **Tab** key to highlight the **Save Changes** button, then the **Spacebar** to select it. Your SSL parameters are saved. You're returned to the command-line interface and InformaCast's Apache web server is restarted to accept your SSL parameter changes.



Manage Trust Certificates

Note This topic and its related topics are optional.

The InformaCast Virtual Appliance installs with a self-signed certificate that establishes trust between its components, e.g. InformaCast, Control Center, Webmin, etc. However, whenever you access those components, 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).

When presented with a certificate, a client validates its trust in that certificate by trusting the entity who issued the certificate, i.e. the CA. Often, there is a chain of trust with multiple issuers, e.g. the root certificate and any intermediate certificates. A root certificate is automatically trusted by browsers because any certificate signed with its private key has been validated and issued by a CA. However, CAs don't issue end-user SSL certificates directly from their root certificates because any mistake involving issuing a certificate or a malicious attack would require that root certificate to be revoked along with every certificate signed using it. To protect against this mass invalidation, CAs issue an intermediate certificate. They sign the intermediate certificate with their private key and use the intermediate root's private key to sign the end-user SSL certificate. This creates the chain of trust.

In order to maintain its trust, InformaCast checks its certificates (either self-signed or signed) whenever it boots/reboots. If its certificates are invalid, e.g. through a hostname change without a reboot or certificate regeneration, a certificate's expiration, etc., InformaCast automatically regenerates new self-signed certificates; however, you will see the website certificate warning again.

When working with trust certificates, you can:

- "Create and Install a Signed Certificate" on page 9-39
- "Display Your Trusted Certificates" on page 9-45
- "Display Your Local Trust" on page 9-47
- "Remove Added Trust Certificates" on page 9-48
- "Regenerate Trust Certificates" on page 9-50

Create and Install a Signed Certificate

When you installed InformaCast, you went through the initial steps of entering the necessary information for a public key and certificate. You'll now produce a certificate-signing request and import a certificate (or a chain of certificates) signed and provided by your Certificate Authority (CA).

Step 1 Log into the command-line interface (see "Log into the Command-line Interface" on page 2-37). The command-line interface appears, showing you that you're logged in.

```
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Wed Aug 30 08:54:13 2017

Welcome to Singlewire InformaCast
Running on VMware
Licensed as Purchased

admin@singlewire:~$
```

Step 2 Enter **create-certificate-signing-request** at the prompt and press the **Enter** key. InformaCast will load its private key and generate a certificate-signing request.

```
login as: admin
Using keyboard-interactive authentication.
Password:

Welcome to Singlewire InformaCast Software

admin@InformaCastWest:~$ create-certificate-signing-request
Loading private key
Generating CSR
Certificate request:
-----BEGIN CERTIFICATE REQUEST-----
MIIC4zCCAcsCAQAweTELMAkGA1UEBhMCdXMxCzAJBgNVBAgMAndpMQowCAYDVQQH
DAFhMQowCAYDVQQKDAFhMQowCAYDVQQLDAFhMScwJQYDVQQDDB5JbmZvcmlhQ2Fz
 ...abridged...
GN3irc+2FfVMZIVBOgkrZZqF0UNzkkkAwTGo5FvJ4Uuaety2ng4j95tZU+TmAsyf
aKMmQ8jeorsO5oimC7CblxwJ9lu7Z02UIjLQprD/EQ90i6xexVc/UPsTIU0RNiBS
ucQv8JWsmlS/vYfn5D0Y7sSulBUsHIk=
-----END CERTIFICATE REQUEST-----

Done
Now, copy and paste this CSR into a request to your certificate authority to sig
n the certificate.
When the certificate authority returns the signed certificate, run the command i
mport-signed-certificate.
admin@InformaCastWest:~$
```

Step 3 Copy the certificate request, including "-----BEGIN CERTIFICATE REQUEST-----" and "-----END CERTIFICATE REQUEST-----" and paste it into a text file.

Step 4 Send this file to your certificate authority, which will sign this request and return a signed certificate to you.

Note This part of the process could take a few days.

Step 5 Download the certificate from your CA as a PEM file. PEM-formatted files start with "-----BEGIN CERTIFICATE-----", end with "-----END CERTIFICATE-----", and typically look like the following:


```
-----BEGIN CERTIFICATE-----
   MIID+zCCAuOgAwIBAgIGeuawB+wrMA0GCSqGSIb3DQEBBQUAMBsxGTAXBgNVBAoT

EFZNd2FyZSBJbnN0YWxsZXIwHhcNMTMwOTA2MDc1NTU4WhcNMjUwMzA3MDc1NTU4 ..abridged..
   kAzsSQBSKGHKeXTU92wuH0aVfg5kVC4alL4CP03dhHICafbJaLRyDOTwPnZy0+n+

rRa8XH0AtP4fVYPJn/qyOf+Qp2cgT1oroCbeCcAHY5VGEMpoM/w9WB9RuwzCwgcL
   X/I1aOhaPqiDeW44oNsO

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


Note Certificates commonly come in two file types: PEM and DER. InformaCast 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 6 Re-establish your PuTTY connection to the Virtual Appliance.

Step 7 Enter **import-signed-certificate** at the prompt and press the **Enter** key. InformaCast warns you of a service interruption and asks you if you want to upload a private key (optional).

```
login as: admin
Using keyboard-interactive authentication.
Password:

Welcome to Singlewire InformaCast Software

admin@singlewire:~$  import-signed-certificate
This operation will import a signed certificate.  This operation will
interrupt services.  Press Ctrl+C if you do not want to perform this
operation now.

Import a private key with the certificate (OPTIONAL) (y/n)?
```

Step 8 Determine if you will upload a private key:

- Yes, continue with Step 9.
- No, continue with Step 12.

Step 9 Press **Y** and the **Enter** key to upload a private key. InformaCast asks you to enter your private key's passphrase.

```
login as: admin
Using keyboard-interactive authentication.
Password:

Welcome to Singlewire InformaCast Software

admin@singlewire:~$  import-signed-certificate
This operation will import a signed certificate.  This operation will
interrupt services.  Press Ctrl+C if you do not want to perform this
operation now.

Import a private key with the certificate (OPTIONAL) (y/n)? y
Enter the passphrase for the private key (enter if none):
```

Step 10 Enter your private key's passphrase (if you have one) and press the **Enter** key. If you don't have a passphrase, press the **Enter** key. InformaCast asks you to paste in your private key.

```
login as: admin
Using keyboard-interactive authentication.
Password:

Welcome to Singlewire InformaCast Software

admin@singlewire:~$  import-signed-certificate
This operation will import a signed certificate.  This operation will
interrupt services.  Press Ctrl+C if you do not want to perform this
operation now.

Import a private key with the certificate (OPTIONAL) (y/n)? y
Enter the passphrase for the private key (enter if none): Paste in the private k
ey.  Ensure that you include the --- BEGIN PRIVATE KEY --- and --- END PRIVATE K
EY --- lines.
Press enter on a line by itself when done.
```

Step 11 Paste in your private key and press the **Enter** key. InformaCast asks you to paste in your certificate. Continue with Step 13.

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

Step 12 Press **N** and the **Enter** key. InformaCast asks you to paste in your certificate.

```
login as: admin
Using keyboard-interactive authentication.
Password:

Welcome to Singlewire InformaCast Software

admin@singlewire:~$  import-signed-certificate
This operation will import a signed certificate.  This operation will
interrupt services.  Press Ctrl+C if you do not want to perform this
operation now.

Import a private key with the certificate (OPTIONAL) (y/n)? n
Loading certificate
Paste in the certificate.  Ensure that you include the --- BEGIN CERTIFICATE ---
 and --- END CERTIFICATE --- lines.
Press enter on a line by itself when done.
```

Step 13 Paste in your certificate and press the **Enter** key. InformaCast validates that the information in your certificate matches the private key information it generated when you entered the **create-certificate-signing-request** command, and it asks you if you'd like to use the certificate you just pasted in.

```
AaOCAUkwggFFMBMGA1UdJQQMMAoGCCsGAQUFBwMBMB0GA1UdDgQWBBSGtTCvBLIT
0d6Vq3                                                  IfSkVO5UM5
MFBVQj                                                  BF67JxWe77
9dglyl                                                  NpbmdsZW13
cmUubG                                                  E4LVFBLmNy
bDA+Bg                                                  iC5O86hsWi
T4EKhK                                                  EFBQcDATAN
Bgkqhk                                                  G9O6WW1OBW
PzySpE                                                  y36qZpYVOL
I1n1T6                                                  mI9EPHh4+j
UYdpQT5484RkSLfzvQjInTR3PpMY6327WAjtdEh5Oles9SayVBu6ShOb2nM0jx6w
Mfhq40bTP+IQkGZVqTvDqzuZ4gpVekTO0JfgxOrUFU+UDb7xfI5RIqLyBK/bTyvF
X6vh2pvAgjn61KsGY6oUI6n0ghkacGBmHIPWcCIXJbodiA==
-----END CERTIFICATE-----

Certificate subject and fingerprints:
subject= /C=us/ST=wi/L=wi/O=Singlewire/OU=qa/CN=[redacted].singlewire.lan/
emailAddress=qa-internal@singlewire.com
MD5:    49:16:86:42:FA:35:[redacted]:AF
SHA1:   78:27:F5:8A:4A:E2:[redacted]:C0:1D:6F:F8:27
SHA256: 34:1F:7F:96:A8:65:[redacted]:44:C2:C8:F3:93:10:11:1D:49:
EA:BE:1A:CC:55:EC:70:33

Use this certificate as the host certificate? (y/n)?
```

Step 14 Press **Y** and the **Enter** key. InformaCast validates that your certificate is trusted.

If it is, skip to Step 16.

If it's not, you'll need to upload the root and any intermediate certificates, which you should have received from your Certificate Authority.

Continue with Step 15.

Step 15 Paste in your root and intermediate certificates separately, pressing the **Enter** key after each one. InformaCast will ask you if you want to use each certificate that you enter. Press **Y** and the **Enter** key at each prompt.

```
CLtKrhYTpkHhrM8+[redacted]QKtxaRltKmg
95I69Lapq4d+mpuC[redacted]LryNij9ikLG
W891j1LrZgWUwSsC[redacted]tEwDgYDVR0P
AQH/BAQDAgGGMA8G[redacted]f5rvMyBQwk3
+KJtWpRXoQKjMBAG[redacted]vUAA4IBAQBF
8BQXmOZ1OT6//GRt[redacted]XqoxEEfEqyx
j9Gps6orS8v0iIbe[redacted]sqXhVZZ13GF
tTgik8KQVyQzqOrI[redacted]3Lh/4m+ntz8
aQBsfWfsK7zJp8URARuyk75ZmKP8L0OBVYa1N3oyyqMRiGRZwKGfW5kQSH9uZg6v
yKZqetDSDJKE9E7JQgNLE7MH5NBvO3AVv33OzU6f+SuiY77uhn4MV5PuqG3GUabb
1GDy8VuyFaiRX5qQVRBc
-----END CERTIFICATE-----


Analyzing certificate, please wait...

Trusted certificate subject and fingerprints:
subject= /DC=lan/DC=singlewire/CN=SinglewireRootCA-2018-QA
MD5:    C9:B3:22:25:D1:10:[redacted]:84
SHA1:   16:7B:B6:23:D6:78:[redacted]:DA:BB:8C:36:05
SHA256: 9E:1E:8D:9D:D1:5B:[redacted]:2D:86:E0:7A:9B:75:2B:E2:ED:
9A:01:11:5E:4C:94:60:1B

Should the system trust this certificate? (y/n)?
```

InformaCast will validate each certificate until it is able to establish trust.

```
eDd8aoBEcMO88/MeT12NJStw44dcOR9fwnuPCHUxjUyFsJXRrO+0cr886ffRd5mL
ggxTqufxs6zmpKjleWuRbqRlBFqPNzjwLnncROIIqsQ0rVwZolSgja0Y5mE+aY5I
lOzdSrQbHlXhN821qGBTXNbelEvnVQqrt8qxln6SIz+9MlKGVscZEZH9Qw72zQ==
-----END CERTIFICATE-----


Analyzing certificate, please wait...

Trusted certificate subject and fingerprints:
subject= /DC=lan/DC=singlewire/CN=SinglewireIssuingCA-2018-QA
MD5:    FA:11:77:96:05:FA:                    4E:62
SHA1:   E7:9C:C2:DC:51:02:                    45:D4:C7:DD:C7:B0
SHA256: 9F:E8:BC:29:0A:7B:                    72:7F:DC:03:18:89:B8:FE:83:7A:
A6:FF:FE:0D:4B:13:D4:18

Should the system trust this certificate? (y/n)? y
2 trusted certs accepted
Trust is successfully established between the web server certificate and the
root and intermediate certificates.

Please confirm that you wish to commit the uploaded certificates.
If you answer yes, services will be interrupted and your system will be changed.

Commit certificates (y/n)?
```

Tip You can import root and intermediate certificates independently of the process in this topic by entering the **import-trusted-certificate** command.

Step 16 Press **Y** and the **Enter** key to commit your certificate(s). InformaCast will stop all applications running on the Virtual Appliance, apply your signed certificate, and start the Virtual Appliance's applications.

```
SHA1:   E7:9C:C2:DC:51:02:A5:29:C6:3B:1A:1C:17:36:45:D4:C7:DD:C7:B0
SHA256: 9F:E8:BC:29:0A:7B:97:1D:33:35:34:72:A0:72:72:7F:DC:03:18:89:B8:FE:83:7A:
A6:FF:FE:0D:4B:13:D4:18

Should the system trust this certificate? (y/n)? y
2 trusted certs accepted
Trust is successfully established between the web server certificate and the
root and intermediate certificates.

Please confirm that you wish to commit the uploaded certificates.
If you answer yes, services will be interrupted and your system will be changed.

Commit certificates (y/n)? y
Installing certificates, please wait
Installing trusted certificates
Applying certificates
Applying new private key and certificate
writing RSA key
writing RSA key
Done
Updating the system certificate trust store and restarting applications, please
wait...
Application restart complete.
admin@singlewire:~$
```

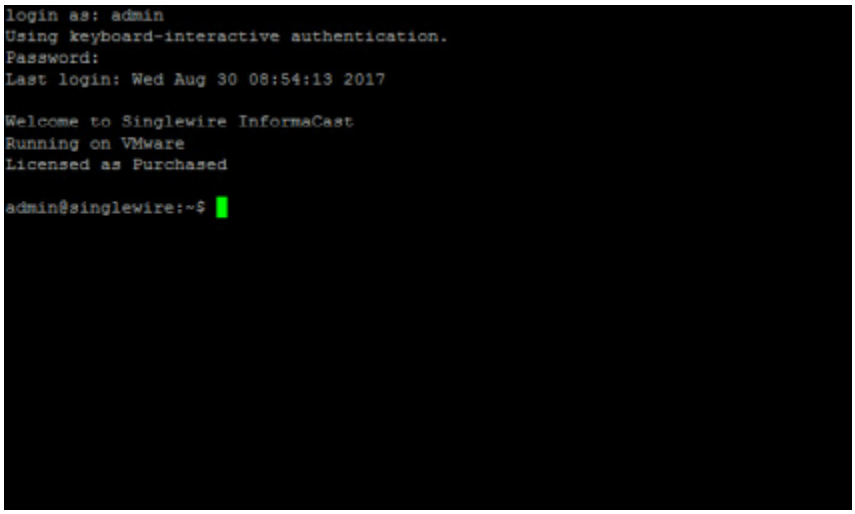
Step 17 Enter **exit** at the prompt and press the **Enter** key. You have finished installing your signed certificate.

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.

Display Your Trusted Certificates

The show-trusted-certificates command displays certificates that your Virtual Appliance server trusts, either signed or self-signed.

Step 1 Log into the command-line interface (see "Log into the Command-line Interface" on page 2-37). The command-line interface appears, showing you that you're logged in.



Step 2 Enter **show-trusted-certificates** and press the **Enter** key. The command-line interface refreshes, displaying the configuration of your currently trusted certificates.

```
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Wed Aug 30 14:14:06 2017

Welcome to Singlewire InformaCast Fusion Software

admin@singlewire:~$ show-trusted-certificates
Locally trusted certificates loaded in system store (1):

Filename: trusted-local.pem
SHA1 Fingerprint=7D:FB:EB:82:00:EF:2D:AC:B3:F3:46:D1:0F:84:B7:96:5A:99:56:44
subject= /C=us/ST=wi/L=wi/O=Singlewire/OU=qa/CN=JENIC90PUB1-2223.singlewire.lan/
emailAddress=qa-internal@singlewire.com

Locally trusted certificates loaded in openssl trust store (1):

Filename: trusted-local.pem
SHA1 Fingerprint=7D:FB:EB:82:00:EF:2D:AC:B3:F3:46:D1:0F:84:B7:96:5A:99:56:44
subject= /C=us/ST=wi/L=wi/O=Singlewire/OU=qa/CN=JENIC90PUB1-2223.singlewire.lan/
emailAddress=qa-internal@singlewire.com

Locally trusted certificates loaded in Java trust store (1):

local-local, Nov 7, 2018, trustedCertEntry,
Certificate fingerprint (SHA1): 7D:FB:EB:82:00:EF:2D:AC:B3:F3:46:D1:0F:84:B7:96:
5A:99:56:44

admin@singlewire:~$
```

Display Your Local Trust

Certificates become untrusted if any of them expire or are removed. The **show-local-trust** command displays the state of trust between InformaCast and the currently installed certificate and trusted certificates. It's run automatically as part of system boot to ensure that InformaCast can trust the certificate that it is configured to present. Independently running the **show-local-trust command** can be useful to Singlewire Support when helping you to troubleshoot issues.

Step 1 Log into the command-line interface (see "Log into the Command-line Interface" on page 2-37). The command-line interface appears, showing you that you're logged in.

```
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Wed Aug 30 08:54:13 2017

Welcome to Singlewire InformaCast
Running on VMware
Licensed as Purchased

admin@singlewire:~$
```

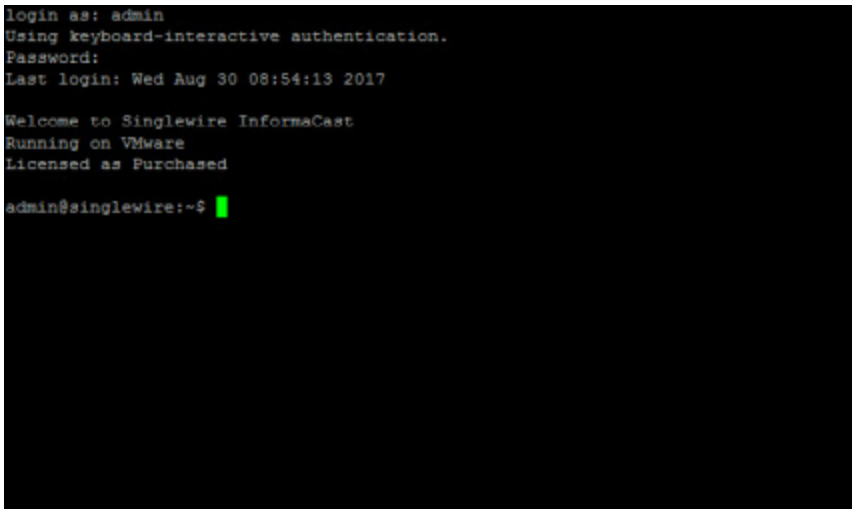
Step 2 Enter **show-local-trust** and press the **Enter** key. The command-line interface refreshes, displaying the state of trust on InformaCast.

```
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Wed Aug 30 14:14:06 2017

Welcome to Singlewire InformaCast Fusion Software

admin@singlewire:~$ show-local-trust
Local certificate is trusted

admin@singlewire:~$
```

Remove Added Trust Certificates

The **remove-all-user-added-trusted-certificates** command removes any Certificate Authority root and intermediate certificates that you've added, which causes InformaCast to no longer trust the signed certificate. Once you reboot the Virtual Appliance server, InformaCast will regenerate certificates and you'll return to a self-signed certificate.

Step 1 Log into the command-line interface (see "Log into the Command-line Interface" on page 2-37). The command-line interface appears, showing you that you're logged in.



Step 2 Enter **remove-all-user-added-trusted-certificates** and press the **Enter** key. The command-line interface refreshes, and InformaCast goes through its trust store and removes any Certificate Authority root and intermediate certificates that you've added. Your signed certificate remains installed, but InformaCast can no longer trust it without the root and intermediate certificates.

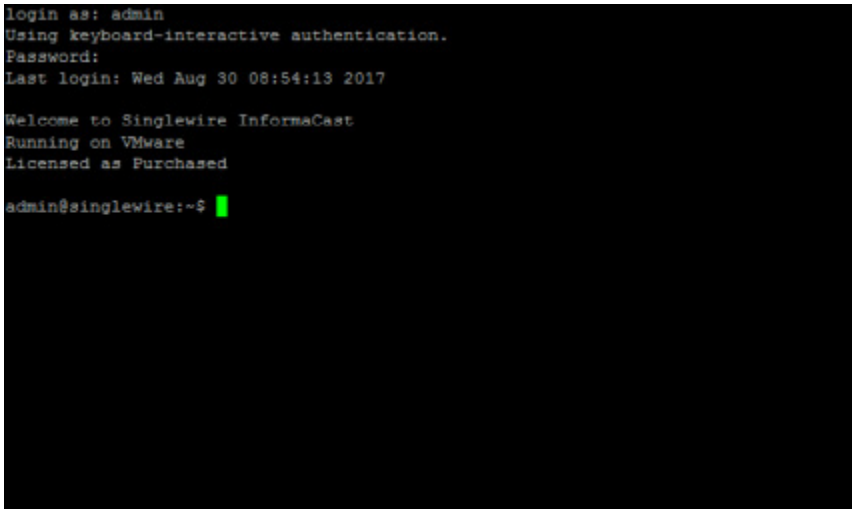
```
login as: admin
Using keyboard-interactive authentication.
Password:

Welcome to Singlewire InformaCast Software

admin@singlewire:~$  remove-all-user-added-trusted-certificates
Removing
removed '/usr/local/singlewire/.security/trusted-local.pem'
Replacing system trust store in /etc/ssl/certs with that of the JDK in /etc/ssl/
cacerts
and locally trusted certs, please wait
0
1123
863
1725
2017
1505
1959
1609
1559
1387
1445
1357
1511
Importing locally trusted certificate local-local
Certificates successfully hashed: 105
Success
admin@singlewire:~$
```

Step 3 Reboot your Virtual Appliance server (see "Reboot the InformaCast Virtual Appliance" on page 9-6). InformaCast checks to see if it can trust the signed certificate, and since it can't, returns you to a self-signed certificate.

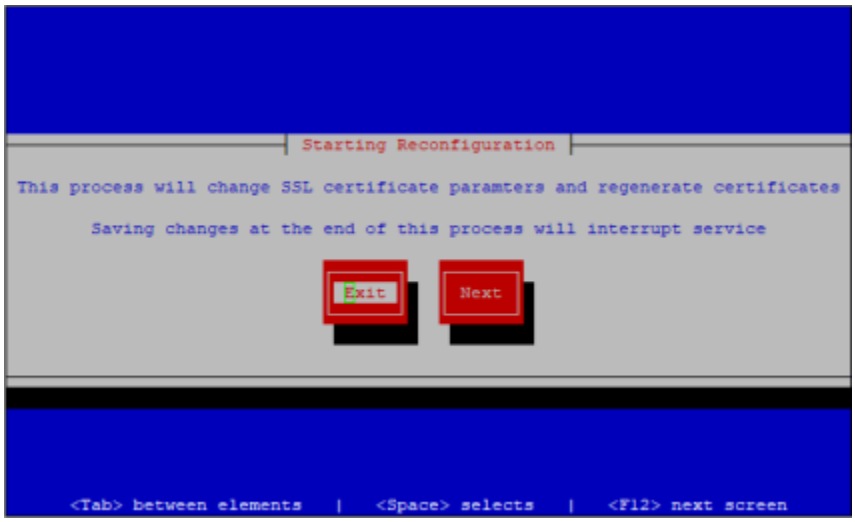
Regenerate Trust Certificates

Once you've imported a signed certificate, the **regenerate-ssl-certificates** command reverts you to a self-signed certificate, removes your previous signed certificate, and keeps the Certificate Authority root and intermediate certificates.

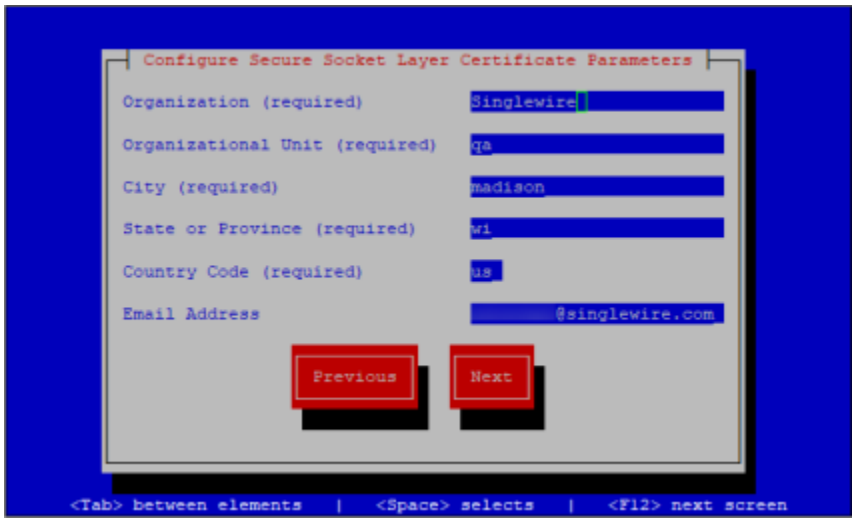
Step 1 Log into the command-line interface (see "Log into the Command-line Interface" on page 2-37). The command-line interface appears, showing you that you're logged in.



Step 2 Enter **regenerate-ssl-certificates** and press the **Enter** key. The Starting Reconfiguration window appears.

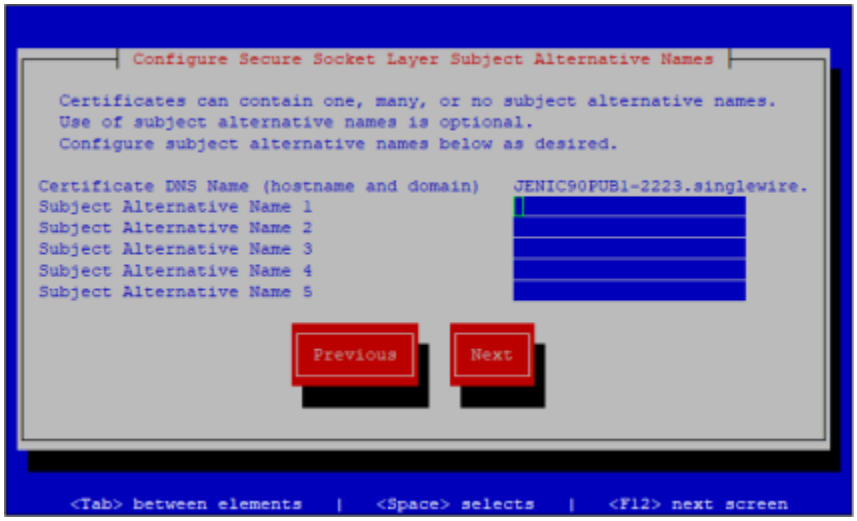


Step 3 Press the **Tab** key to highlight the **Next** button, then the **Spacebar** to select it. The Configure Secure Socket Layer Certificate Parameters window appears.



Step 4 Review the information in the Configure Secure Socket Layer Certificate Parameters window and make any corrections.

Step 5 Press the **Tab** key to highlight the **Next** button, then the **Spacebar** to select it. The Configure Secure Socket Layer Subject Alternative Names window appears.

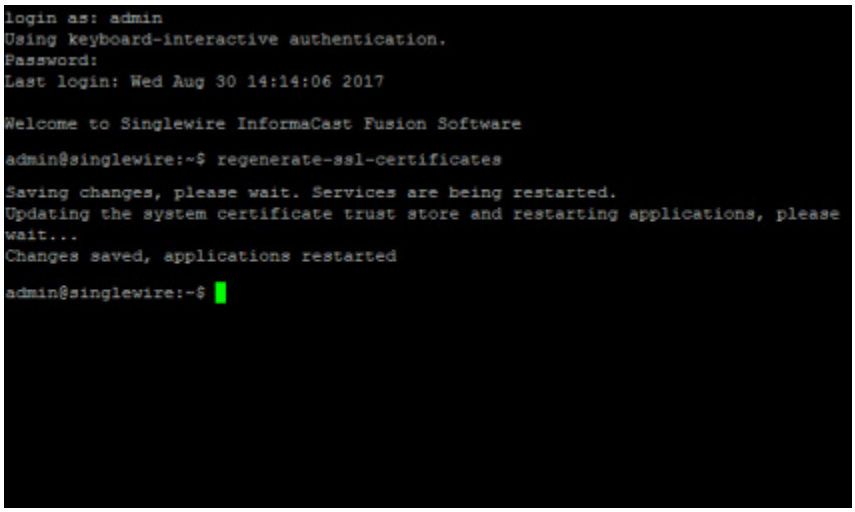


Step 6 Review the information in the Configure Secure Socket Layer Subject Alternative Names window and make any corrections.

Step 7 Press the **Tab** key to highlight the **Next** button, then the **Spacebar** to select it. The Save or Exit window appears.

Your certificate changes aren't saved until you select the **Save Changes** button.

Step 8 Press the **Tab** key to highlight the **Save Changes** button, then the **Spacebar** to select it. Your certificate changes are saved. You're returned to the command-line interface, and InformaCast's trust store is updated to accept your certificate changes.



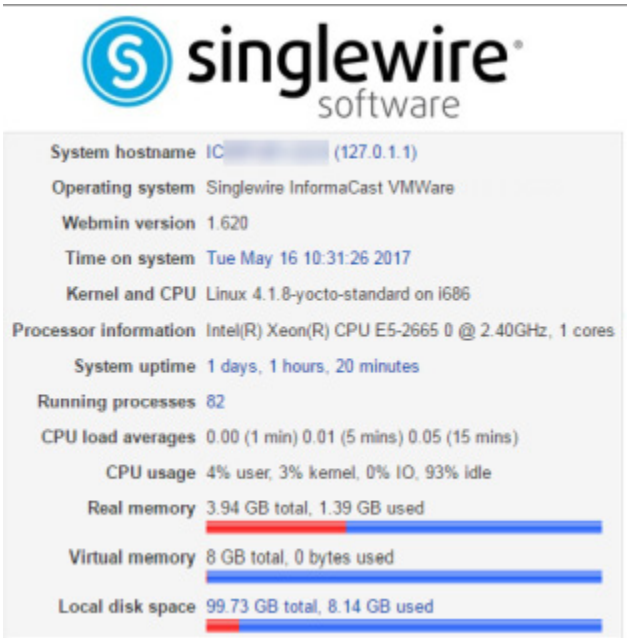
Change InformaCast Virtual Appliance's IP Address

You set the static IP address for your Virtual Appliance when you installed InformaCast (see "Deploy InformaCast" on page 2-6), but you may need to change it.

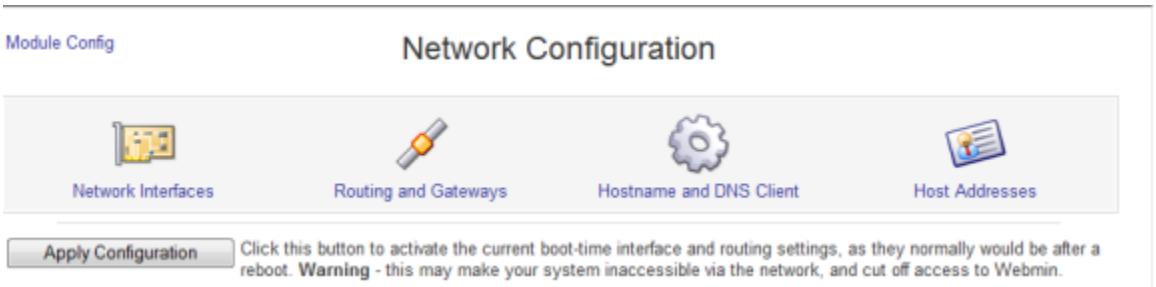
Note Complete the steps in this topic before making any changes to your network, e.g.changing the virtual network assigned to the VMware virtual NIC or the upstream network configuration for the assigned virtual network.

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 "Deploy InformaCast" on page 2-6).**

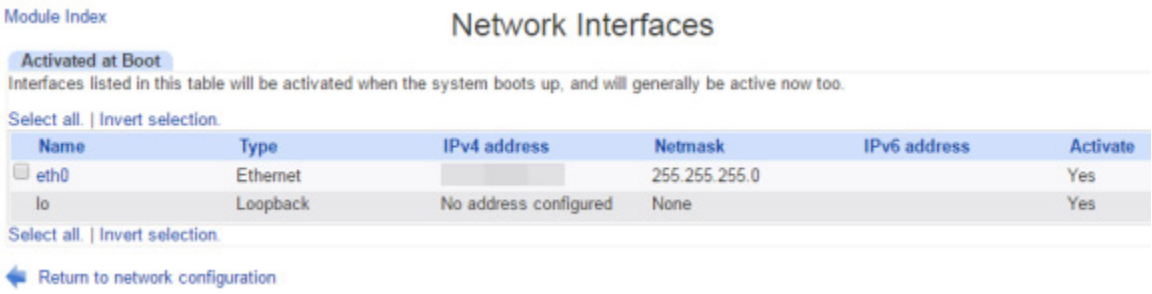
Step 1 Log into Webmin (see "Log into Webmin" on page 2-35 for specific steps). The Webmin homepage appears.



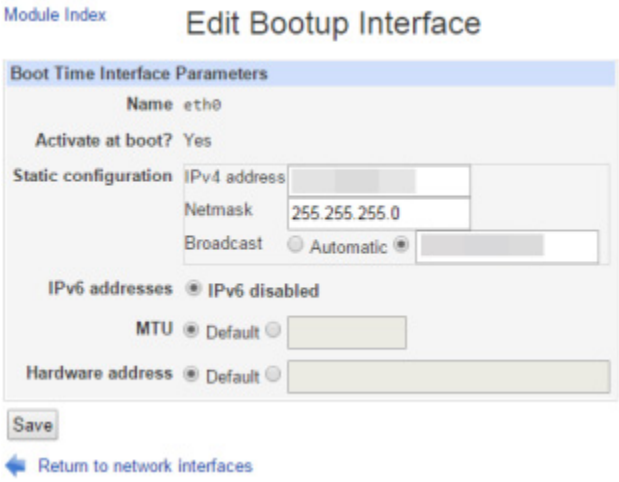
Step 2 Go to **Networking** | **Network Configuration**. The Network Configuration page appears.



Step 3 Click the **Network Interfaces** icon. The Network Interfaces page refreshes.



Step 4 Click the **eth0** link. The Edit Bootup Interface page appears.



Step 5 Enter your new IP address and netmask in the **IP Address** and **Netmask** fields, respectively.

Step 6 Enter an IP address in the **Broadcast** field if your current one is not what would be expected for the given **IP Address** and **Netmask** fields.

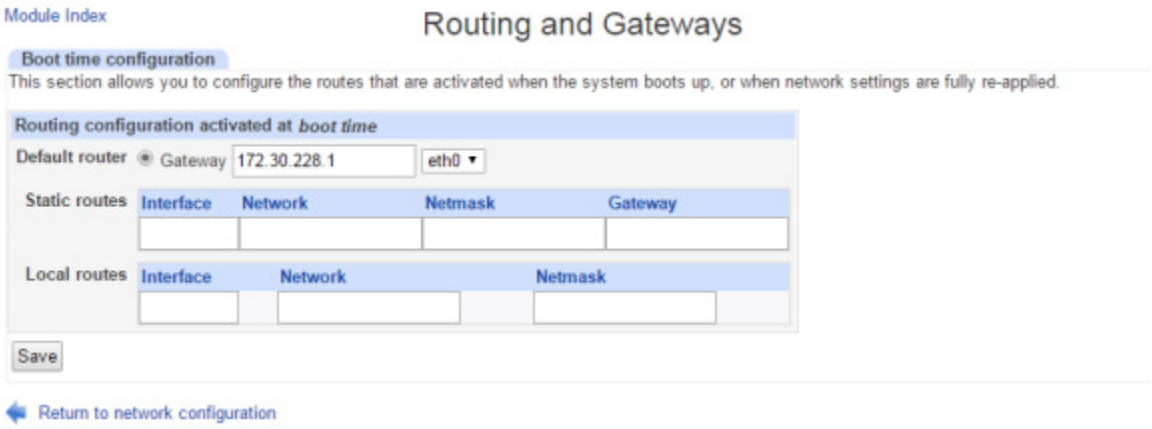
Note Contact your network administrator if you have questions about what to enter in the **IP Address**, **Netmask**, and/or **Broadcast** fields.

Step 7 Click the **Save** button.

Step 8 Click the **Return to network interfaces** link on the Edit Bootup Interfaces page.

Step 9 Click the **Return to network configuration** link on the Network Interfaces page.

Step 10 Click the **Routing and Gateways** icon on the Network Configuration page. The Routing and Gateways page appears.



Step 11 Enter the IP address of the gateway in the **Gateway** field.

Note Optionally, additional routes can be specified on this page, but should not be necessary in most situations.

Step 12 Click the **Save** button. Your changes are saved, but not yet applied.

Step 13 Reboot the Virtual Appliance (see "Reboot the InformaCast Virtual Appliance" on page 9-6).

Step 14 Log into Unified Communications Manager, go to **System | Enterprise Parameters**, and change the **URL Authentication** and **Secured Authentication URL** fields.

Also, go to **Device | Device Settings | Phone Services**, and change the IP address for any InformaCast service URLs you have created.

You need to use the **Update Subscriptions** button whenever you change service information, so that any subscribed phones are properly updated.

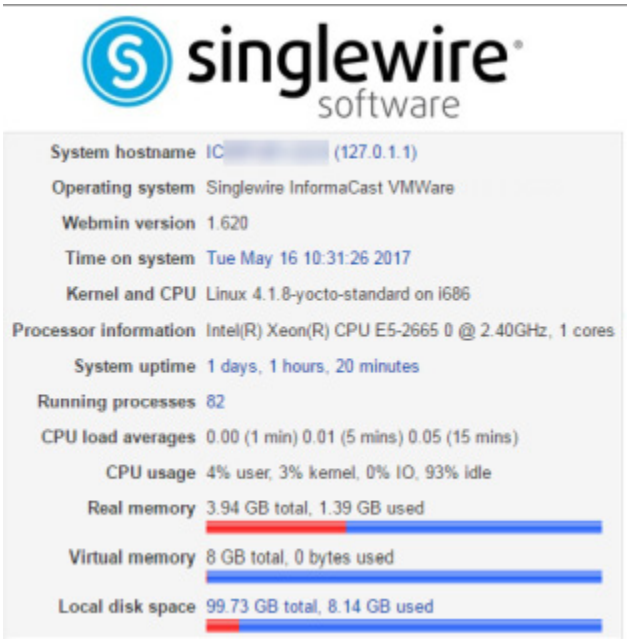
InformaCast SIP certificates are regenerated whenever InformaCast is installed or its IP address is changed, so if you are using TLS protocol with SIP, you will need to install the InformaCast SIP certificate on all Unified Communications Managers in your InformaCast environment (see "Install the InformaCast SIP Certificate on Unified Communications Manager" on page 5-15).

Step 15 Reset all of your phones.

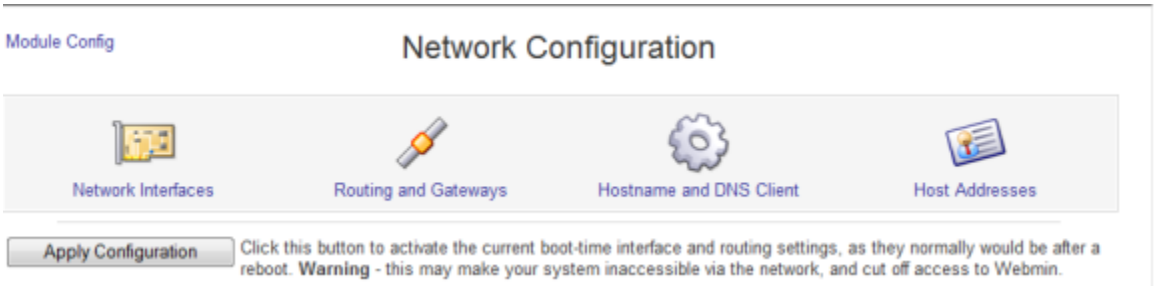
Change the Virtual Appliance's Hostname

You set your Virtual Appliance's hostname when you installed InformaCast (see "Deploy InformaCast" on page 2-6), but you may need to change it.

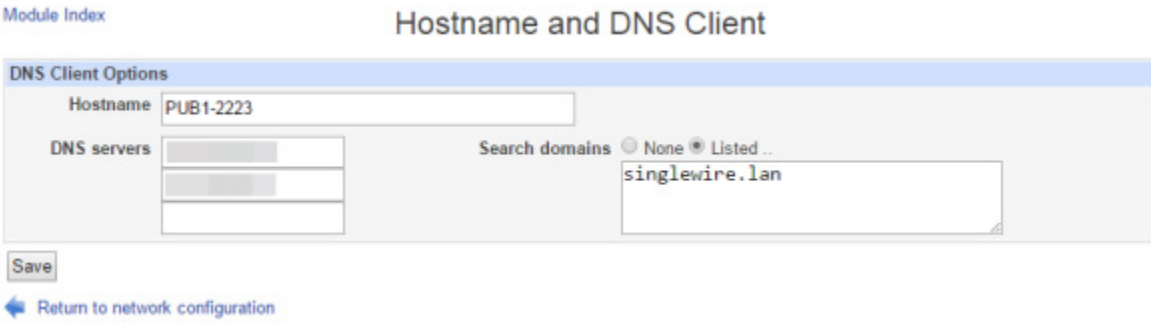
Step 1 Log into Webmin (see "Log into Webmin" on page 2-35 for specific steps). The Webmin homepage appears.



Step 2 Go to **Networking** | **Network Configuration**. The Network Configuration page appears.

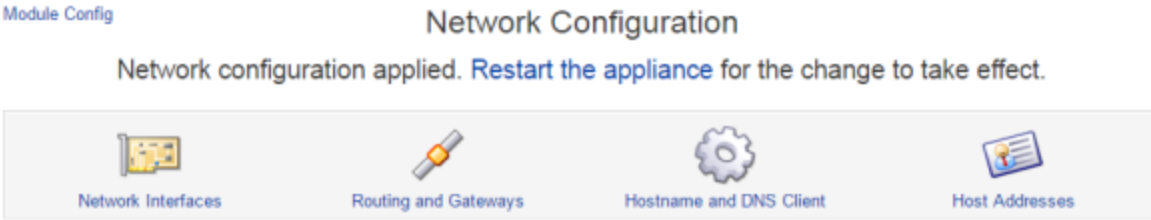


Step 3 Click the **Hostname and DNS Client** icon. The Hostname and DNS Client page appears.



Step 4 Enter your new name in the **Hostname** field, e.g. WestHeadquarters.

Step 5 Click the **Save** button. Your changes are applied and you are redirected to the Network Configuration page.



Note You must reboot the Virtual Appliance for your changes to take effect.

Step 6 Click the **Restart the appliance** link. The Reboot page appears.

Step 7 Click the **Reboot System** button. The Virtual Appliance will restart. This may take some time. Until the restart has completed, some of InformaCast's features may be inoperable.

Set the System Time

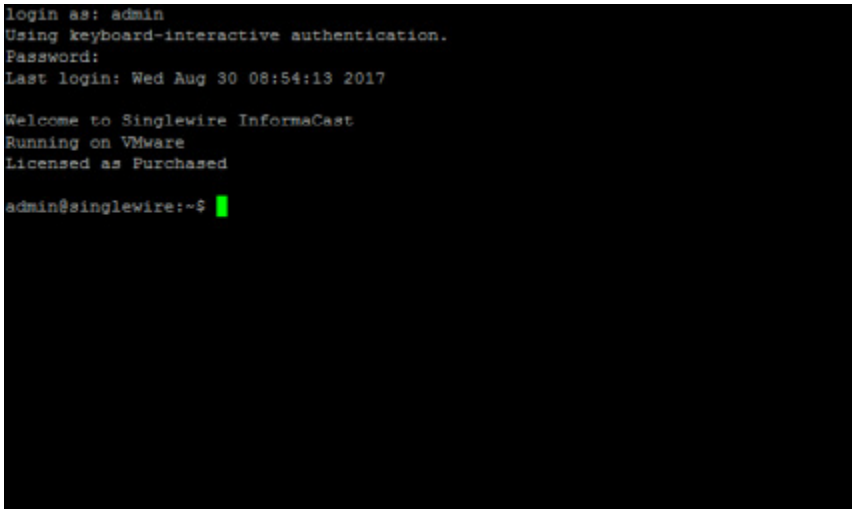
You already set the system time when you entered your NTP server(s) addresses during InformaCast's initial configuration (see "Set the Initial Configuration" on page 2-20). However, you may need to change them, or determine the state of NTP and/or InformaCast's sync status with it.

InformaCast uses the Network Time Protocol daemon (ntpd) for time synchronization. ntpd is a server process that maintains InformaCast's system time in synchronization with time servers using the Network Time Protocol (NTP).

List Current NTP Servers

The **show-time-configuration** command lists your currently configured NTP server(s)

Step 1 Log into the command-line interface (see "Log into the Command-line Interface" on page 2-37). The command-line interface appears, showing you that you're logged in.



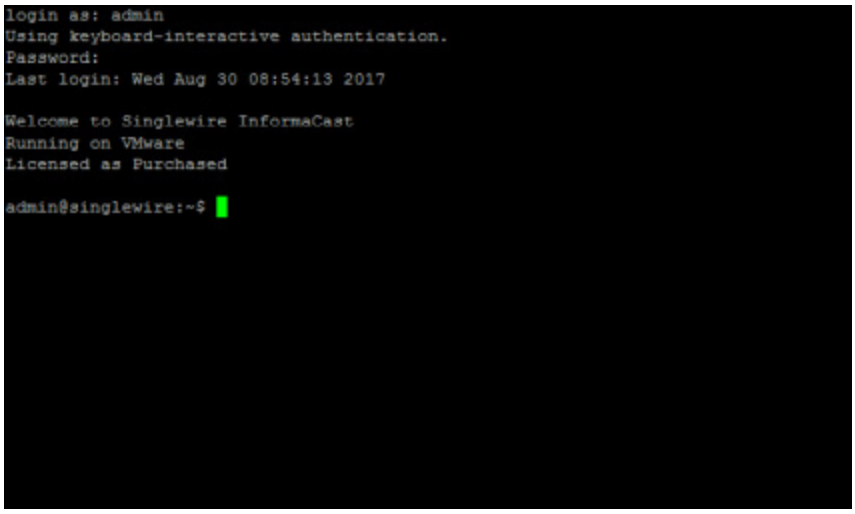
Step 2 Enter **show-time-configuration** at the prompt and press the **Enter** key. The command-line interface refreshes with your current NTP information, e.g. whether ntpd is enabled and running, your time zone, your current NTP servers' fully qualified domain names, and their authentication method.

```
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Wed Aug 30 08:54:13 2017

Welcome to Singlewire InformaCast
Running on VMware
Licensed as Purchased

admin@singlewire:~$ show-time-configuration
NTP Service Status
------------------
ntpd is enabled
ntpd (pid  4434) is running...

Time Configuration
------------------
Time zone: America/Chicago

NTP Server 1 address:               ntp1.singlewire.lan
NTP Server 1 authentication method: NO_AUTH
NTP Server 1 SHA1 shared key:       <not displayed>

NTP Server 2 address:
NTP Server 2 authentication method: NO_AUTH
NTP Server 2 SHA1 shared key:       <not displayed>

NTP Server 3 address:
NTP Server 3 authentication method: NO_AUTH
NTP Server 3 SHA1 shared key:       <not displayed>

admin@singlewire:
```

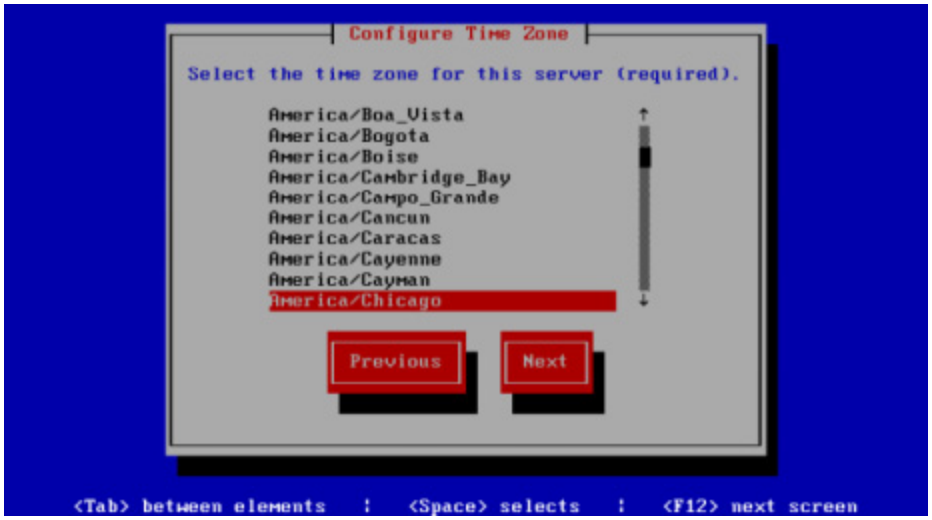
Change NTP Servers

The **configure-time** command allows you to change your NTP server(s).

Step 1 Log into the command-line interface (see "Log into the Command-line Interface" on page 2-37). The command-line interface appears, showing you that you're logged in.

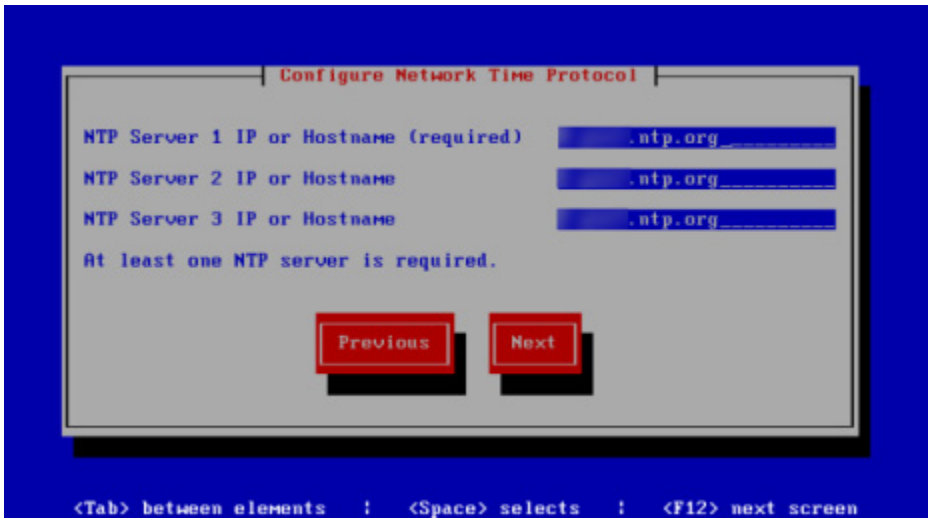


Step 2 Enter **configure-time** at the prompt and press the **Enter** key. The command-line interface refreshes.



Step 3 Use the arrow keys to select a time zone for your InformaCast Virtual Appliance server.

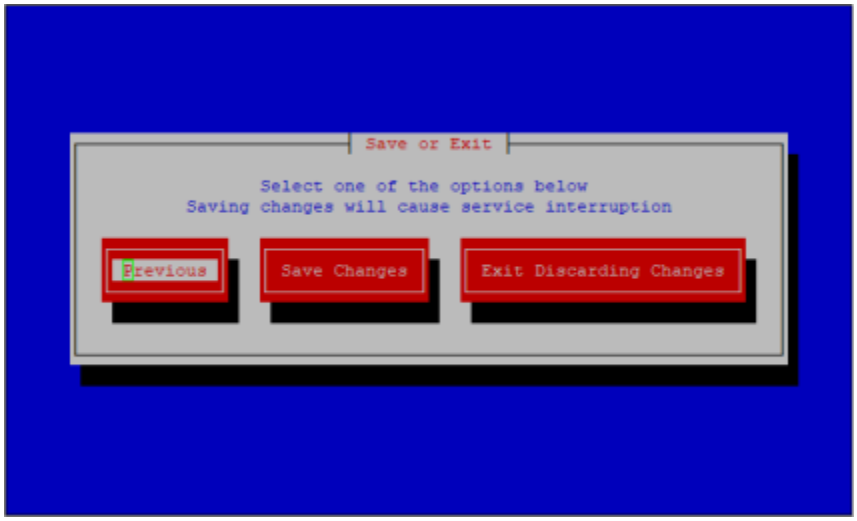
Step 4 Press the **Tab** key to highlight the **Next** button, then the **Spacebar** to select it. The command-line interface refreshes, and the InformaCast Virtual Appliance lists the currently configured NTP servers.



Step 5 Accept the suggested NTP server IP address or provide a valid one of your own in the **NTP Server 1 IP or Hostname** field.

Step 6 Press the **Tab** key and enter up to two more NTP servers (optional).

Step 7 Press the **Tab** key to highlight the **Next** button, then the **Spacebar** to select it. The InformaCast Virtual Appliance validates your NTP configuration, and the command-line interface refreshes.



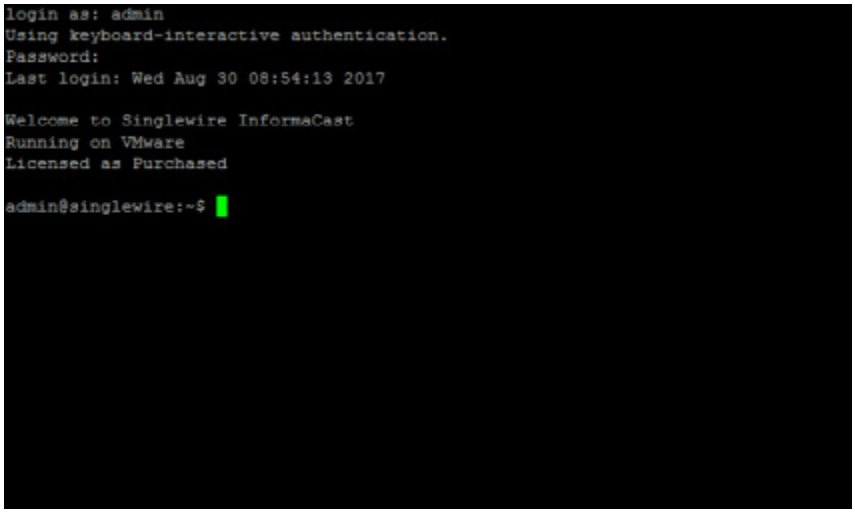
Step 8 Press the **Tab** key to highlight the **Save Changes** button, then the **Spacebar** to select it. The command-line interface refreshes, and InformaCast stops and starts the ntpd service to pick up your changes.

Tip You can also manually stop and start the ntpd service through Webmin's Bootup and Shutdown page or by entering **ntp-service disable** or **ntp-service enable** in the command-line interface.

Display ntpd State and InformaCast's Sync Status

The **show-time-status** command displays the current state of the NTP daemon and whether InformaCast is in sync with it.

Step 1 Log into the command-line interface (see "Log into the Command-line Interface" on page 2-37). The command-line interface appears, showing you that you're logged in.



Step 2 Enter **show-time-status** at the prompt and press the **Enter** key. The command-line interface refreshes with your current NTP information, e.g. whether ntpd is enabled and running, the NTP firewall status, and performance statistics, etc.

```
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Wed Aug 30 08:54:13 2017

Welcome to Singlewire InformaCast
Running on VMware
Licensed as Purchased

admin@singlewire:~$ show-time-status
Current Date/Time
--------------------------------
Fri Oct 12 11:29:01 CDT 2018

NTP Service Status
--------------------------------
ntpd is enabled
ntpd (pid  3515) is running...

NTP Firewall Status
--------------------------------
    0     0 ACCEPT     udp  --  *      *       0.0.0.0/0           0.0.0.0/0
         udp dpt:123 /* NTP server, allow incoming NTP */

NTP Associations and Performance
--------------------------------
     remote       refid   assid  st t when poll reach   delay   offset  jitter
==============================================================================
 ntp1.singlewire.lan
                 .POOL.   46666  16 p    -   64    0    0.000    0.000   0.000
*fit-swl-vlan205.singlewire.lan
                 26e54701 46667   3 u   77  128  377    2.412    0.290   9.059

ind assid status  conf reach auth condition  last_event cnt
===========================================================
  1 46666  8811   yes  none  none    reject    mobilize  1
  2 46667  163a    no   yes  none  sys.peer    sys_peer  3

admin@singlewire:
```

Upgrade Your Open VM Tools

InformaCast uses Open VM Tools, "a set of services and modules that enable several features in VMware products for better management of, and seamless user interactions with, guests."[1] Open VM Tools offers the same services as the previously used VMware Tools, and simplifies your management because you no longer have to manage these tools' upgrades separately in vSphere: Open VM Tools upgrades are nearly transparent to you, occurring only during InformaCast upgrades.

Manage SNMP Monitoring

Listening on port 1161, InformaCast's embedded SNMP agent can be paired with your own Network Management Software (NMS) in order to monitor certain aspects of InformaCast e.g. the last time a phone rebuild succeeded, the count of registered IP speakers, InformaCast's version, etc.

1. https://github.com/vmware/open-vm-tools

Several OIDs, both native and InformaCast-specific are available for your use as well as both native and InformaCast-specific MIBs. While SNMP monitoring is able to handle many of your needs, there are some configuration caveats you should take into consideration before configuring SNMP monitoring.

Note If you would like SNMP monitoring to include functionality that it currently doesn't have, open a Singlewire Support case.

Available OIDs

The following capabilities are natively possible through SNMP:

- System description (SNMPv2-MIB::sysDescr.0)
- System name (SNMPv2-MIB::sysName.0)
- Uptime (DISMAN-EVENT-MIB::sysUpTimeInstance)
- Contact (SNMPv2-MIB::sysContact.0)
- Location (SNMPv2-MIB::sysLocation.0)
- Ethernet network adapter description, type, packet count, error count
- Netstat TCP connection table, including listening sockets and established connections
- UDP bound ports
- SNMP total packet counts
- System clock
- Partition list, and for each partition: mount point, size, and whether it's used
- CPU model and type
- SCSI disk list
- Process list, including process name, path, parameters, state (e.g. runnable), CPU utilized, memory used
- Network interface, including name, multicast packet count, and broadcast packet count
- Memory /proc/meminfo information
- Load average in one-minute, five-minute, 15-minute intervals

The following table displays the capabilities that are specific to InformaCast:

OID	Data	Example
1.3.6.1.4.1.3137.1.1.1.1.3.0	InformaCast version	12.2.5
1.3.6.1.4.1.3137.1.1.1.1.4.0	JTAPI version	Cisco Jtapi version 8.6(2.24091)-1 Release
1.3.6.1.4.1.3137.1.1.1.3.5.2.0	Multicast TTL	16
1.3.6.1.4.1.3137.1.1.1.3.5.3.0	Multicast traffic class	160
1.3.6.1.4.1.3137.1.1.1.2.4.1.0	Last time phone rebuild started	20180805071459, yyyy-mm-dd hh:mm:ss
1.3.6.1.4.1.3137.1.1.1.2.4.2.0	Last time phone rebuild succeeded	19691231180000, yyyy-mm-dd hh:mm:ss

OID	Data	Example
1.3.6.1.4.1.3137.1.1.1.2.4.3.0	Next time phone update scheduled	20180805081000, yyyy-mm-dd hh:mm:ss
1.3.6.1.4.1.3137.1.1.1.2.4.4.0	Phone count in cache	241
1.3.6.1.4.1.3137.1.1.1.2.4.5.0	Time cache update started	19691231180000, yyyy-mm-dd hh:mm:ss
1.3.6.1.4.1.3137.1.1.1.2.4.6.0	Time cache update succeeded	19691231180000, yyyy-mm-dd hh:mm:ss
1.3.6.1.4.1.3137.1.1.1.2.5.1.0	Defined IP speaker count	55
1.3.6.1.4.1.3137.1.1.1.2.5.2.0	Registered IP speaker count	54
1.3.6.1.4.1.3137.1.1.1.2.5.3.0	Unregistered IP speaker count	1
1.3.6.1.4.1.3137.1.1.1.3.2.1.0	Backup activated?	false
1.3.6.1.4.1.3137.1.1.1.3.2.2.0	Time of next backup	20180806030000, yyyy-mm-dd hh:mm:ss
1.3.6.1.4.1.3137.1.1.1.3.2.3.0	Backup location	/usr/local/singlewire/InformaCast/backup
1.3.6.1.4.1.3137.1.1.1.3.3.1.0	SLP Advertise CFS?	false
1.3.6.1.4.1.3137.1.1.1.3.3.2.0	SLP Advertise SOAP?	true
1.3.6.1.4.1.3137.1.1.1.3.3.3.0	SLP Advertise HTTP	deprecated
1.3.6.1.4.1.3137.1.1.1.3.4.1.0	Is LDAP auth enabled?	false
1.3.6.1.4.1.3137.1.1.1.3.4.2.0	Is LDAP grouping enabled?	false
1.3.6.1.4.1.3137.1.1.1.3.4.3.0	Time of next LDAP update	20180805074000, yyyy-mm-dd hh:mm:ss

MIBs

A management information base (MIB) is a database used for managing the SNMP OIDs common to all Unix hosts and those provided specifically through InformaCast.

SNMP native MIBs, e.g. those common to all Unix hosts, can be found in /usr/share/snmp/mibs on the Virtual Appliance.

InformaCast MIBs can be found in three locations:

- /usr/local/singlewire/InformaCast/web/resources/mib/ on the Virtual Appliance
- As a downloadable ZIP on Singlewire's website
- Through a link to the Virtual Appliance:
  - 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

Supported Configurations

The following SNMP configurations are supported:

- SNMPv2c
- SNMPv3 for a single user for authentication and/or privacy, e.g. Secure Hash Algorithm (SHA) and/or Advanced Encryption Standard (AES)
- SNMP polling over UDP
- Host filtering
- Scanning, e.g. snmpnext and snmpwalk
- The generic UNIX MIBs supported by net-snmp out of the box
- SNMP polling of UNIX MIBs and the InformaCast MIB

Unsupported Configurations

The following SNMP configurations are not supported:

- Subnet filtering
- Read/write permissions; clients must be read-only
- Installing a MIB on the Virtual Appliance
- SNMP over DTLS; if you want encryption, use SNMPv3 with privacy
- SNMP over SSH; if you want encryption, use SNMPv3 with privacy
- SNMPv3 with MD5 authentication
- SNMPv3 with DES privacy
- SNMP traps
- Multiple SNMP community strings
- Multiple SNMP users
- Different SNMPv2 and SNMPv3 IP address filters; you can have one filter for inbound SNMP packets: it will apply to both SNMPv2 and SNMPv3 packets

Now that you're familiar with your SNMP capabilities, you can proceed with:

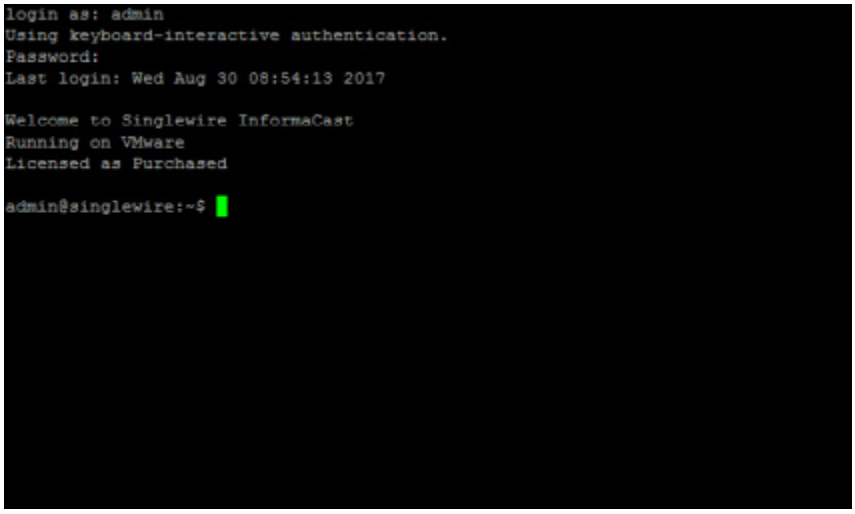
- “Configure SNMP Monitoring” on page 9-66
- “Display Current SNMP Monitoring Configuration” on page 9-72
- “Restart SNMP Monitoring Service” on page 9-74
- “Remove Current SNMP Monitoring Configuration” on page 9-75

Configure SNMP Monitoring

InformaCast's embedded SNMP agent can be paired with your own Network Management Software (NMS) in order to monitor certain aspects of InformaCast (i.e. the last time a phone rebuild succeeded, the count of registered IP speakers, InformaCast's version, etc.).

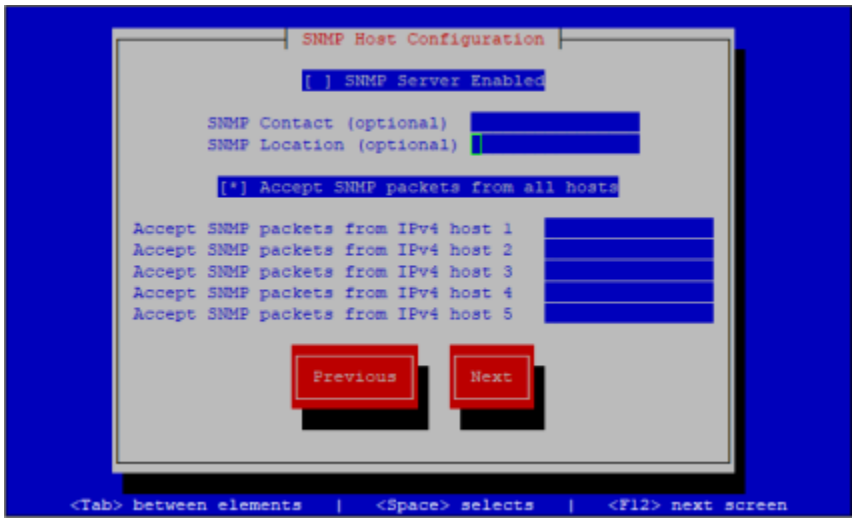
During your configuration, you can choose to configure SNMPv2, SNMPv3, or both. SNMPv2 is unencrypted and not recommended due to security concerns. SNMPv3, when used with a password and/or secret key, is the more secure option. Pairing authentication and encryption with SNMPv3 makes it much stronger against vulnerabilities.

Step 1 Log into the command-line interface (see "Log into the Command-line Interface" on page 2-37). The command-line interface appears, showing you that you're logged in.



Step 2 Enter **configure-snmp** at the prompt and press the **Enter** key. The Starting Reconfiguration window appears.

Step 3 Press the **Tab** key to highlight the **Next** button, then the **Spacebar** to select it. The SNMP Host Configuration window appears.



You will first enable SNMP (it's disabled by default) and enter your SNMP contact and host information.

Step 4 Press the **Spacebar** while in the **SNMP Server Enabled** field to enable SNMP.

Note Once you've enabled SNMP monitoring, you can disable it again by pressing the **Spacebar** while in the **SNMP Server Enabled** field, removing the * from between [ ]. You can also run the remove-snmp-configuration command to reset your SNMP monitoring configuration to its default values, e.g. disabled with no additional settings.

Step 5 Press the **Tab** key to enter the **SNMP Contact** field and enter your SNMP contact's information, e.g. John Lennon, SNMP Admin (optional).

Step 6 Press the **Tab** key to enter the **SNMP Location** field and enter your SNMP contact's location, e.g. Madison (optional).

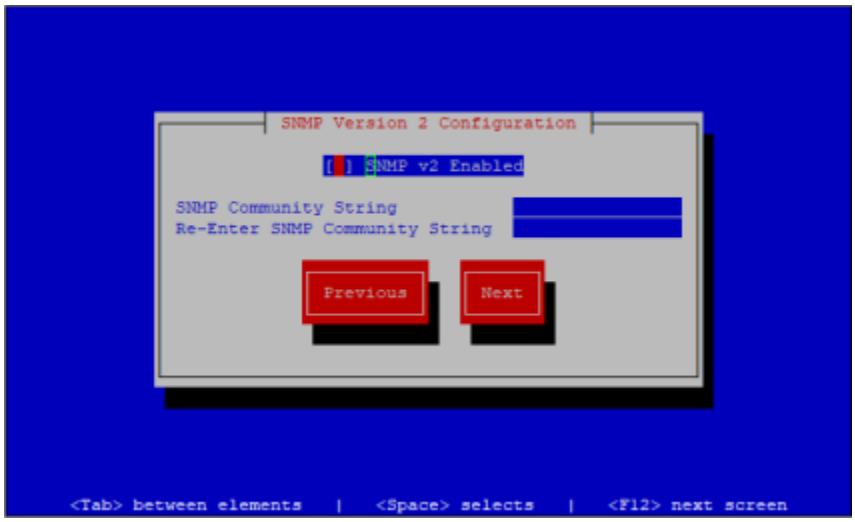
Step 7 Press the **Tab** key to enter the **Accept SNMP packets from all hosts** field and either leave it as accepting SNMP packets from all hosts (not recommended due to attack vulnerabilities) or press the **Spacebar** to disable SNMP packets from all hosts.

Note If you choose to enable the **Accept SNMP packets from all hosts** field, skip to Step 10.

Step 8 Press the **Tab** key to enter the **Accept SNMP packets from IPv4 host 1** field and enter the IP address of your SNMP host, e.g. your NMS's IP address.

Step 9 Continue entering SNMP host IP addresses (up to five) in the **Accept SNMP packets from IPv4 host** fields, pressing the **Tab** key to advance between fields (optional).

Step 10 Press the **Tab** key to highlight the **Next** button, then the **Spacebar** to select it. The SNMP Version 2 Configuration window appears.



You will now configure SNMPv2 (optional). If you don't want to configure SNMPv2, press the **Tab** key to highlight the **Next** button, then the **Spacebar** to select stand skip to Step 15. Otherwise, continue with Step 11.

Step 11 Press the **Spacebar** while in the **SNMPv2 Enabled** field to enable SNMPv2.

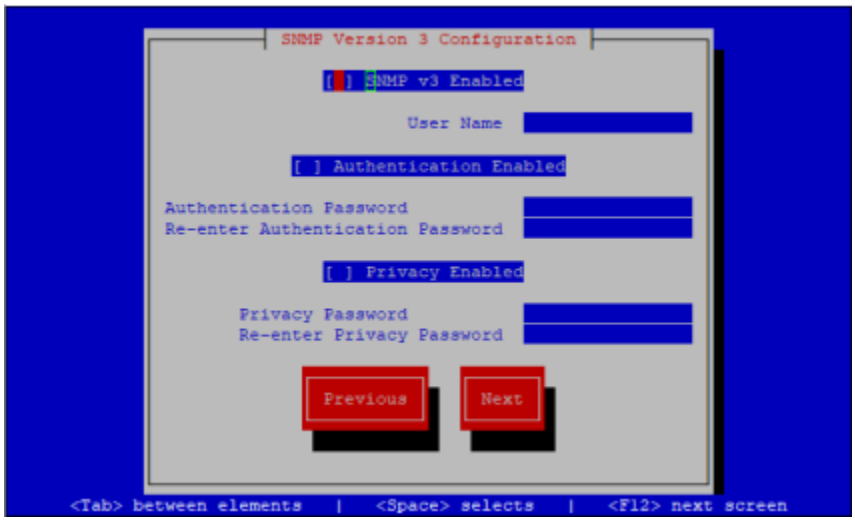
Step 12 Press the **Tab** key to enter the **SNMP Community String** field and enter the SNMP community string used by your SNMP host.

Note While you are allowed to add up to five SNMP hosts, if you are using SNMPv2, they must all use the same community string.

Step 13 Press the **Tab** key to enter the **Re-Enter SNMP Community String** field and enter that community string again.

Note If you enter community string information without enabling SNMPv2, your configuration cannot be saved.

Step 14 Press the **Tab** key to highlight the **Next** button, then the **Spacebar** to select it. The SNMP Version 3 Configuration window appears.



You will now configure SNMPv3 (optional). If you don't want to configure SNMPv3, press the **Tab** key to highlight the **Next** button, then the **Spacebar** to select it and skip to Step 24. Otherwise, continue with Step 15.

Step 15 Press the **Spacebar** while in the **SNMPv3 Enabled** field to enable SNMPv3.

Step 16 Press the **Tab** key to enter the **User Name** field and enter the username used by your SNMP host.

With just a username, SNMPv3 is only as secure as SNMPv2; however, you can choose to pair your username with a password and/or a password and secret key (optional).

Step 17 Press the **Tab** key to enter the **Authentication Enabled** field, then the **Spacebar** to enable it (optional). InformaCast uses SHA authentication.

Step 18 Press the **Tab** key to enter the **Authentication Password** field and enter your user's password.

Step 19 Press the **Tab** key to enter the **Re-enter Authentication Password** field and enter your user's password again.

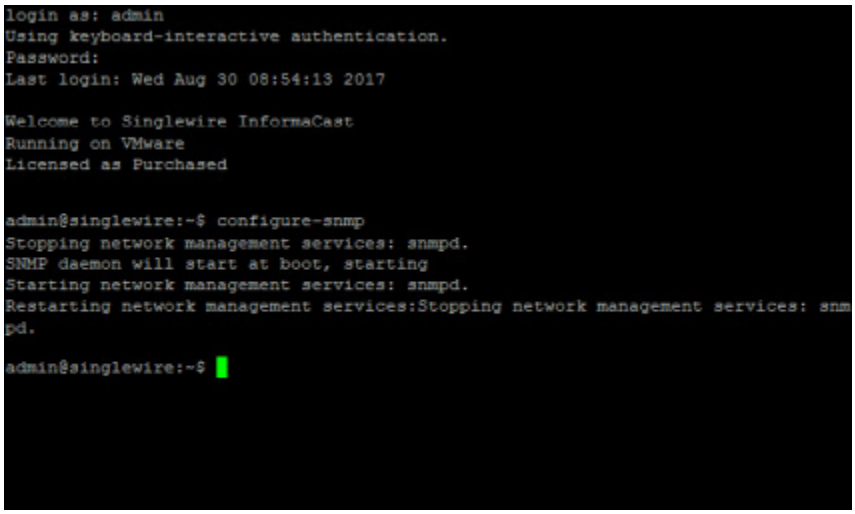
Step 20 Press the **Tab** key to enter the **Privacy Enabled** field, then the **Spacebar** to enable it (optional). InformaCast uses AES encryption.

Step 21 Press the **Tab** key to enter the **Privacy Password** field and enter your privacy password.

Step 22 Press the **Tab** key to enter the **Re-enter Privacy Password** field and enter your privacy password again.

Step 23 Press the **Tab** key to highlight the **Next** button, then the **Spacebar** to select it. The Save or Exit window appears.

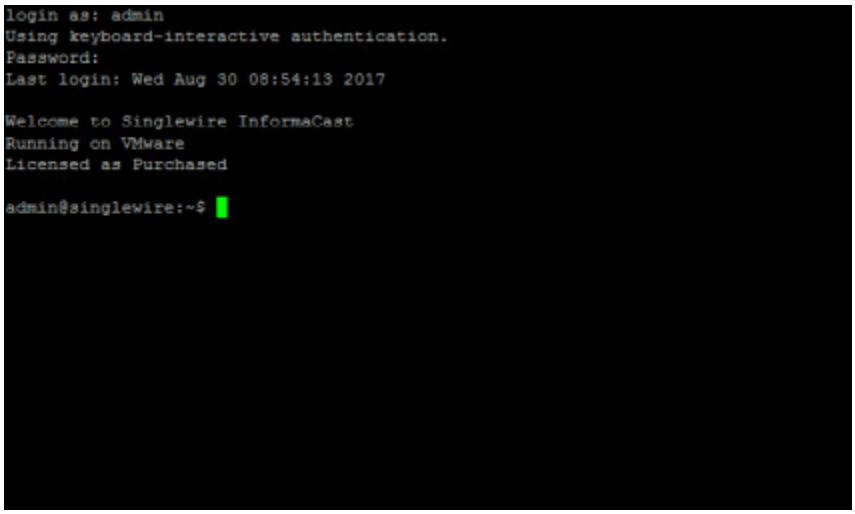
Step 24 Press the **Tab** key to highlight the **Save Changes** button, then the **Spacebar** to select it. Your SNMP configuration is saved. You're returned to the command-line interface and InformaCast's SNMP monitoring service is restarted to accept your SNMP changes.



Display Current SNMP Monitoring Configuration

Once you've configured SNMP monitoring, the **show-snmp-configuration** command will display your current SNMP configuration, omitting any password or community string values.

Step 1 Log into the command-line interface (see "Log into the Command-line Interface" on page 2-37). The command-line interface appears, showing you that you're logged in.



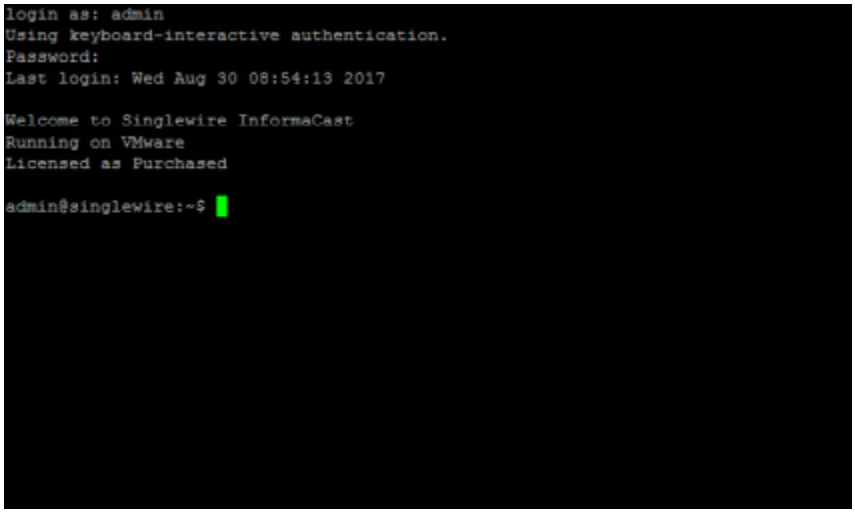
Step 2 Enter **show-snmp-configuration** at the prompt and press the **Enter** key. The command-line interface refreshes, displaying your current SNMP configuration, e.g. whether it's enabled and running, the SNMP hosts you've added, your SNMP contact information, whether you're using SNMPv2 or SNMPv3, etc.

```
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Wed Aug 30 14:14:06 2017

Welcome to Singlewire InformaCast Fusion Software

admin@singlewire:~$ show-snmp-configuration

SNMP Service Status:
SNMP daemon is enabled
Status of snmptrapd: stopped
Status of snmpd: running

SNMP Firewall Status:
    0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0
         state ESTABLISHED /* M2M plugin SNMP responses */
    0     0 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0
         udp dpt:1162 /* M2M plugin SNMP traps */
    0     0 ACCEPT     udp  --  *      *       [redacted].4         0.0.0.0/0
         udp dpt:161 /* SNMP traffic from 172.30.222.4 */
    0     0 ACCEPT     udp  --  *      *       [redacted].103       0.0.0.0/0
         udp dpt:161 /* SNMP traffic from 172.30.228.103 */
    0     0 REJECT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0
         udp dpt:161 /* SNMP traffic */ reject-with icmp-port-unreachable
    0     0 REDIRECT   udp  --  *      *       0.0.0.0/0            0.0.0.0/0
         udp dpt:162 /* Inbound SNMP traps arrive on UDP 1162 */ redir ports 116
2

SNMP Feature Configuration:
SNMP enabled:                   True
SNMP contact:                   John Lennon, SNMP Admin
SNMP location:                  Madison
Accept SNMP from all hosts:     False
Accept SNMP host address 1:     [redacted].4
Accept SNMP host address 2:     [redacted].103
Accept SNMP host address 3:
Accept SNMP host address 4:
Accept SNMP host address 5:
SNMPv2 enabled:                 True
SNMPv2 community string:        True
SNMPv3 enabled:                 True
SNMPv3 user name:               True
SNMPv3 authentication required: True
SNMPv3 privacy required:        True

admin@singlewire:~$
```

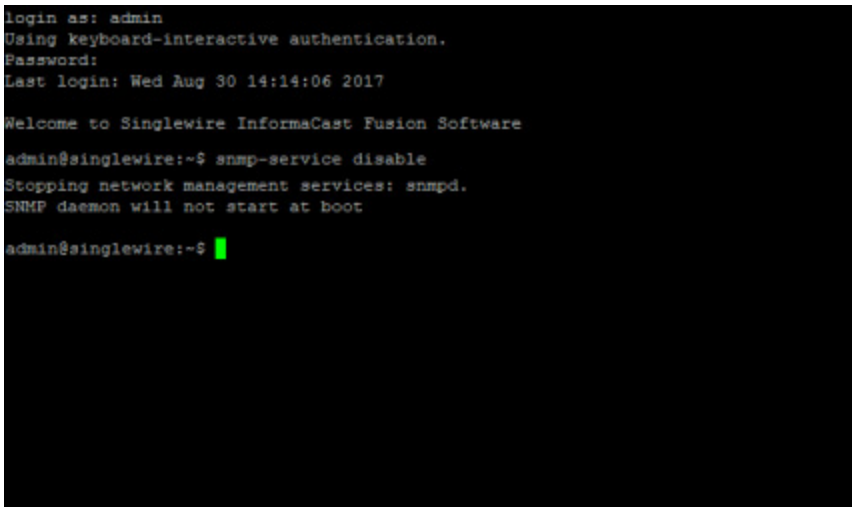
Restart SNMP Monitoring Service

Once you've configured SNMP monitoring, the snmp-service disable and snmp-service enable commands will restart InformaCast's SNMP monitoring service independent of any SNMP monitoring changes. Restarting the SNMP monitoring service can be helpful when troubleshooting issues.

Step 1 Log into the command-line interface (see "Log into the Command-line Interface" on page 2-37). The command-line interface appears, showing you that you're logged in.



Step 2 Enter **snmp-service disable** at the prompt and press the **Enter** key. The command-line interface refreshes, and the SNMP monitoring service is disabled.



Step 3 Enter **snmp-service enable** at the prompt and press the **Enter** key. The command-line interface refreshes, and the SNMP monitoring service is started.

```
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Wed Aug 30 14:14:06 2017

Welcome to Singlewire InformaCast Fusion Software

admin@singlewire:~$ snmp-service enable

SNMP daemon will start at boot, starting
Starting network management services: snmpd.

admin@singlewire:~$
```

Remove Current SNMP Monitoring Configuration

Once you've configured SNMP monitoring, the remove-snmp-configuration command will reset your SNMP monitoring configuration to its default values, e.g. disabled with no additional settings.

Step 1 Log into the command-line interface (see "Log into the Command-line Interface" on page 2-37). The command-line interface appears, showing you that you're logged in.

```
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Wed Aug 30 08:54:13 2017

Welcome to Singlewire InformaCast
Running on VMware
Licensed as Purchased

admin@singlewire:~$
```

Step 2 Enter **remove-snmp-configuration** at the prompt and press the **Enter** key. The command-line interface refreshes, and any SNMP configuration settings you had are removed.

```
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Wed Aug 30 14:14:06 2017

Welcome to Singlewire InformaCast Fusion Software

admin@singlewire:~$ remove-snmp-configuration
Resetting SNMP configuration to default, stopping SNMP service
Stopping network management services: snmpd.
SNMP daemon will not start at boot

admin@singlewire:~$
```

Upgrade InformaCast Virtual Appliance

Stay current with the latest InformaCast features by upgrading the Virtual Appliance, which includes the InformaCast application and the platform on which InformaCast runs. Curious about your new features? Review "Release Notes" on page 10-1 for a list of everything that has improved with your new version.

Note the Differences

If you are upgrading from an earlier version of InformaCast Virtual Appliance, please review "Release Notes" on page 10-1 for a list of new features.

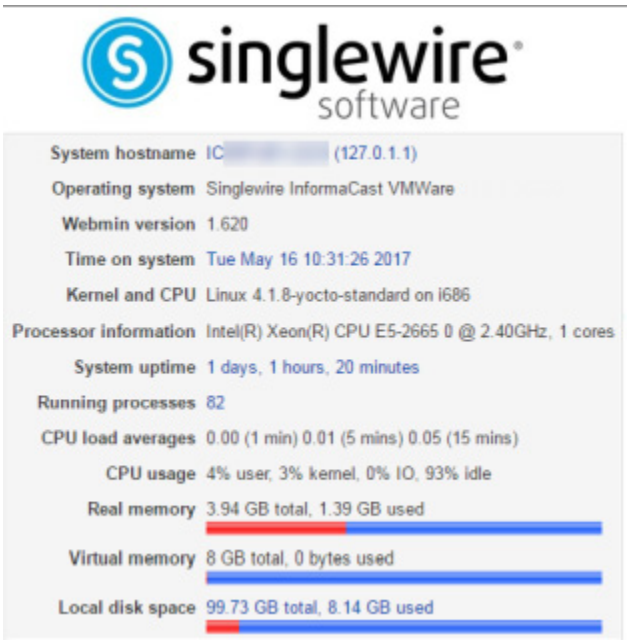
Determine Your Current Version

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 2-31 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 "Upgrade InformaCast Pre-12.0.1" on page 9-77. 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 2-35 for specific steps). The Webmin homepage appears.



Step 4 Look at the top line of the Webmin homepage, e.g. Virtual Appliance version or Operating system. That is your current version of InformaCast.

Step 5 Make note of your version number and continue with "Upgrade InformaCast Pre-12.0.1" on page 9-77 or "Upgrade InformaCast 12.0.1 and Later" on page 9-104.

Upgrade InformaCast Pre-12.0.1

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 and one ISO file that must be uploaded/attached in the following order:
  - CiscoPagingServer_8.5.1.deb
  - CiscoPagingServer_9.1.1.deb
  - CiscoPagingServer_11.5.2.deb
  - CiscoPagingServer_UpgradeFrom115To-12.5.1.iso
- **8.5.1, 9.0.1, or 9.0.2 Virtual Appliance to Current Version.** Your download will include two package files and one ISO file that must be uploaded/attached in the following order:
  - CiscoPagingServer_9.1.1.deb
  - CiscoPagingServer_11.5.2.deb

  - CiscoPagingServer_UpgradeFrom115To-12.5.1.iso
- 9**.1.1, 11.0.1, 11.0.2, 11.0.5 Virtual Appliance to Current Version.** Your download will include one package file and one ISO file that must be uploaded/attached in the following order:
- CiscoPagingServer_11.5.2.deb
- CiscoPagingServer_UpgradeFrom115To-12.5.1.iso
- **11.5.1 or 11.5.2 Virtual Appliance to Current Version.** Your download will include one ISO file: CiscoPagingServer_UpgradeFrom115To-12.5.1.iso.

Once you've obtained your package file(s) and ISO file, you can install them and update your version of InformaCast Virtual Appliance. Depending on your starting version of InformaCast, you will follow different steps:

- If your starting version of InformaCast is 8.3, 8.4, 8.5.1, 9.0.1, 9.0.2, 9.1.1, 11.0.1, 11.0.2, or 11.0.5, go to "Upgrade from 8.3 through 11.0.5" on page 9-78 first and finish with "Upgrade from 11.5.1 or 11.5.2" on page 9-83
- If your starting version of InformaCast is 11.5.1 or 11.5.2, go directly to "Upgrade from 11.5.1 or 11.5.2" on page 9-83

Upgrade from 8.3 through 11.0.5

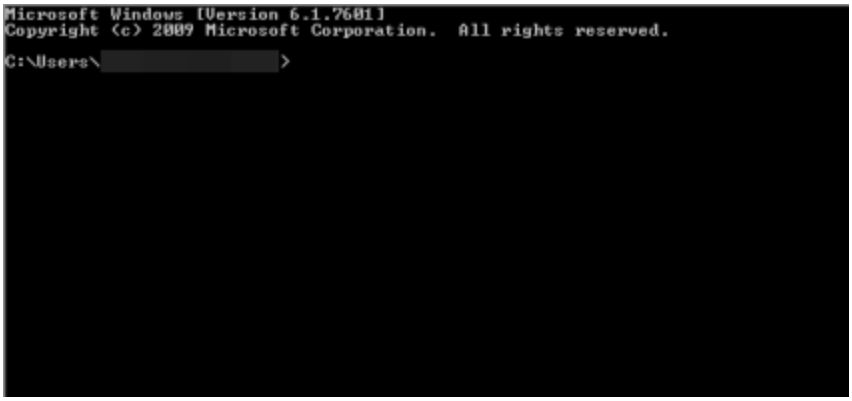
If your starting version of InformaCast is 8.3, 8.4, 8.5.1, 9.0.1, 9.0.2, 9.1.1, 11.0.1, 11.0.2, or 11.0.5, please follow these steps carefully to ensure a successful InformaCast Virtual Appliance upgrade. Once you finish these steps, continue with "Upgrade from 11.5.1 or 11.5.2" on page 9-83.

Step 1 Declare an outage window and ensure that it falls outside of regular business hours.

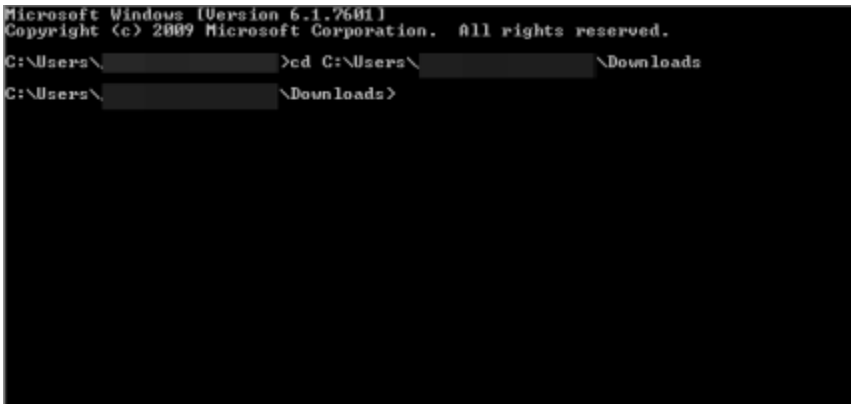
Step 2 Create a clone of your current InformaCast Virtual Appliance installation, which allows for a return to the previous version of InformaCast if there are problems with the upgrade. Snapshots are not sufficient.

Step 3 Use PuTTY's PSCP functionality to transfer your .deb file(s) to your Virtual Appliance. PuTTY is available as a free download and it should be installed on the machine from which you'll transfer files to the Virtual Appliance.

a. Open a command window on the machine on which you've saved your .deb file(s). A command window appears.

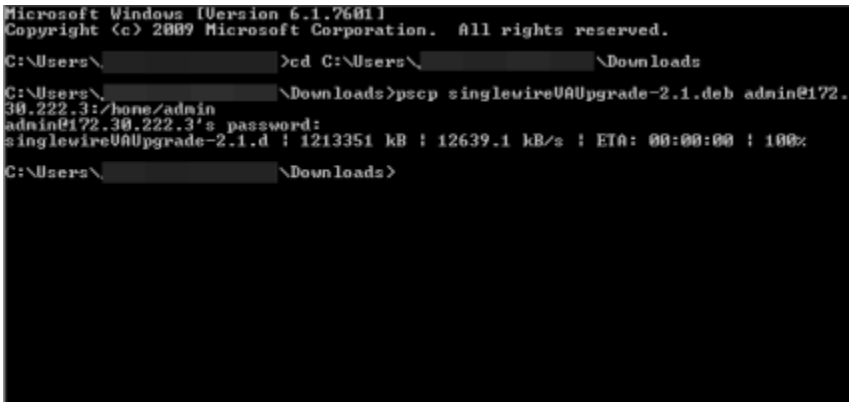


b. Enter **cd <directory>** and press the **Enter** key, where <directory> is the location of your .deb file(s). The command window refreshes to the location of your directory.



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 InformaCast_9.1.1.deb CiscoPagingServer_9.1.1.deb admin@111.22.333.4:/home/admin.

d. Enter your Virtual Appliance password at the prompt and press the **Enter** key. The file will be transferred.

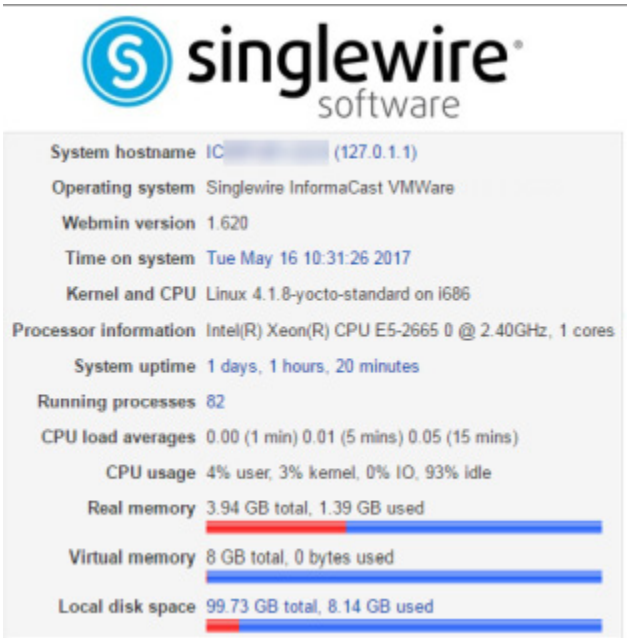


e. Repeat Steps a through d until you've copied all of your .deb files to the Virtual Appliance.

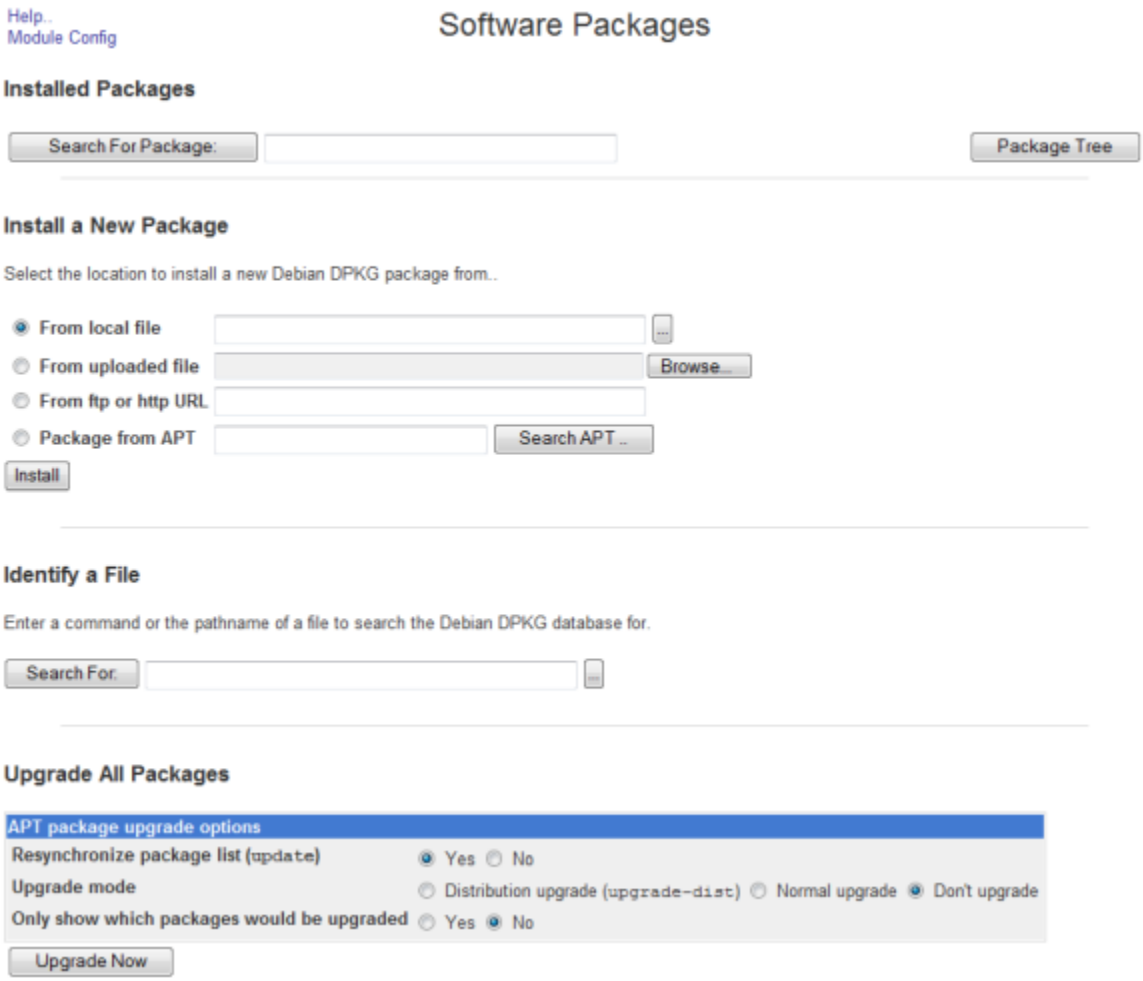
Step 4 Log into Webmin (see "Log into Webmin" on page 2-35 for specific steps).

Note For versions of InformaCast Virtual Appliance prior to 8.4, you will need to go to https://<InformaCast Virtual Appliance IP Address>/webmin, where <InformaCast Virtual Appliance IP Address> is InformaCast Virtual Appliance's statically configured IP address.

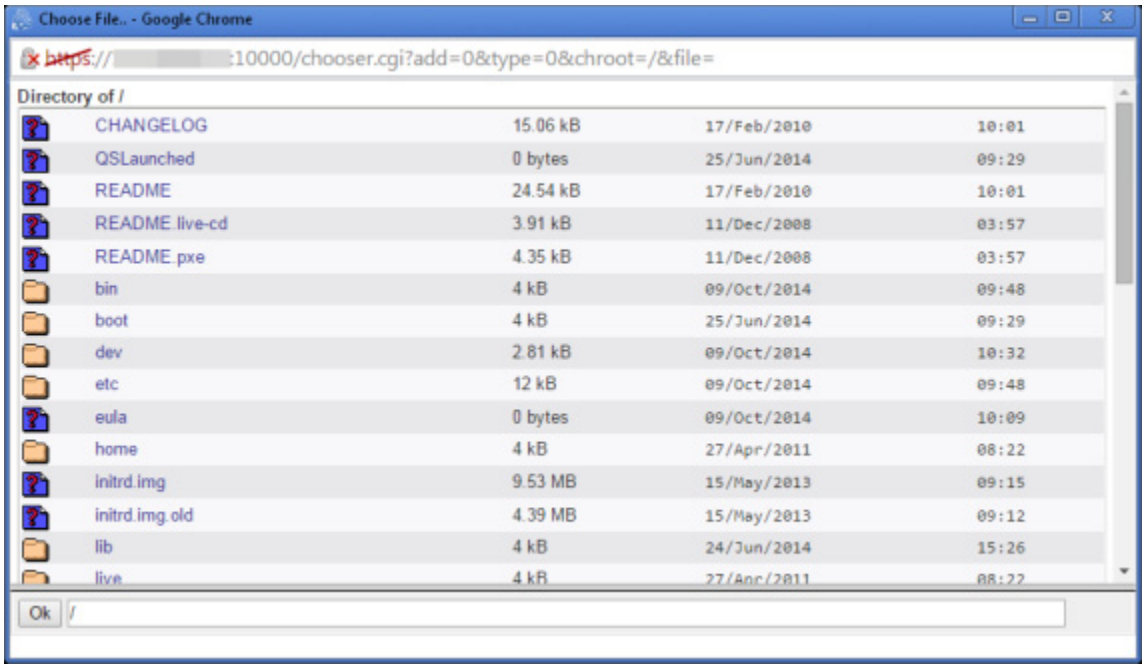
The Webmin homepage appears.



Step 5 Go to **System** | **Software Packages**. The Software Packages page appears.



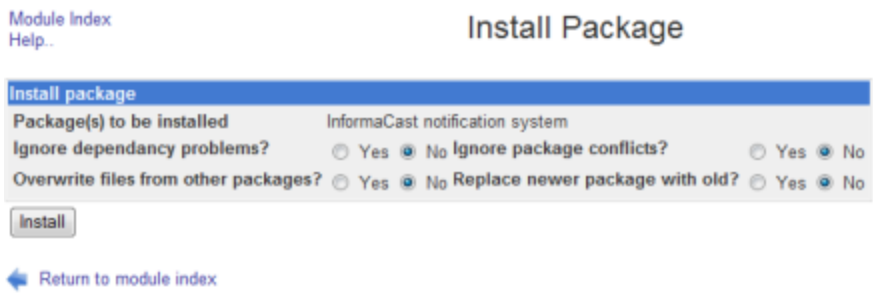
Step 6 Select the **From local file** radio button in the *Install a New Package* area and click its **Browse** button. The Choose File window appears.



Step 7 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 version 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, or 11.0.5 version of InformaCast Virtual Appliance: CiscoPagingServer_11.5.2.deb

Step 8 Click the **Install** button in the *Install a New Package* area. The Install Package page appears.



Step 9 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 a red error message with no listing of files, your upgrade has failed.

Step 10 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 9-6)
  - Go to **System** | **Software Packages** and follow Steps 6 through 9, selecting the CiscoPagingServer_9.1.1.deb file
  - Reboot the Virtual Appliance (see "Reboot the InformaCast Virtual Appliance" on page 9-6)
  - Go to **System** | **Software Packages** and follow Steps 6 through 9, selecting the CiscoPagingServer_11.5.2.deb file
  - Continue with "Upgrade from 11.5.1 or 11.5.2" on page 9-83
- If you are upgrading from the 8.5.1, 9.0.1, or 9.0.2 version of InformaCast Virtual Appliance: 9.1.1, 11.0.1, 11.0.2, or 11.0.5
  - Reboot the Virtual Appliance (see "Reboot the InformaCast Virtual Appliance" on page 9-6)
  - Go to **System** | **Software Packages** and follow Steps 6 through 9 one more time, selecting the CiscoPagingServer_11.5.2.deb file
  - Continue with "Upgrade from 11.5.1 or 11.5.2" on page 9-83
- If you are upgrading from the 9.1.1, 11.0.1, 11.0.2, or 11.0.5 version of InformaCast Virtual Appliance, continue with "Upgrade from 11.5.1 or 11.5.2" on page 9-83.

Upgrade from 11.5.1 or 11.5.2

If your starting version of InformaCast is 11.5.1 or 11.5.2, please follow these steps carefully to ensure a successful InformaCast Virtual Appliance upgrade.

Note If you're coming here from "Upgrade from 8.3 through 11.0.5" on page 9-78, you can skip Steps 1 and 2.

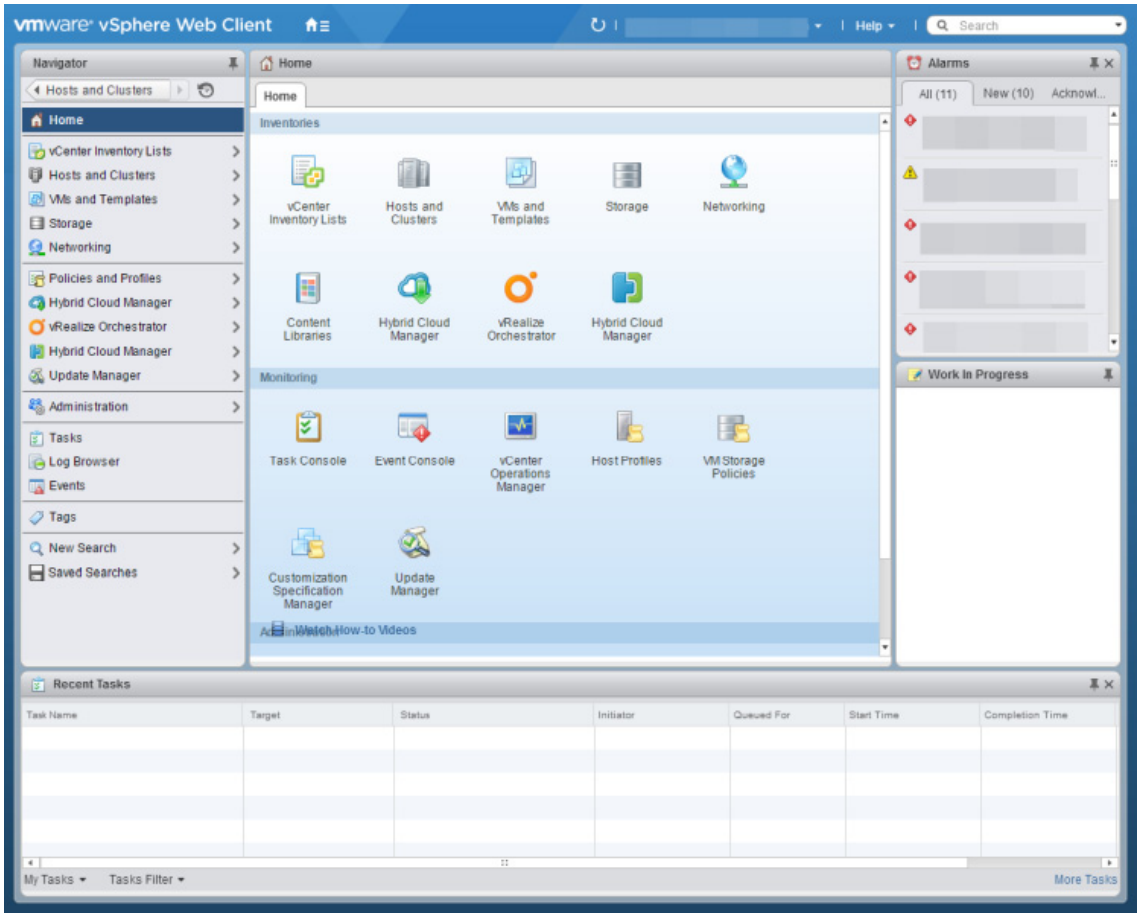
Step 1 Declare an outage window and ensure that it falls outside of regular business hours.

Step 2 Create a clone of your current InformaCast Virtual Appliance installation, which allows for a return to the previous version of InformaCast if there are problems with the upgrade. Snapshots are not sufficient.

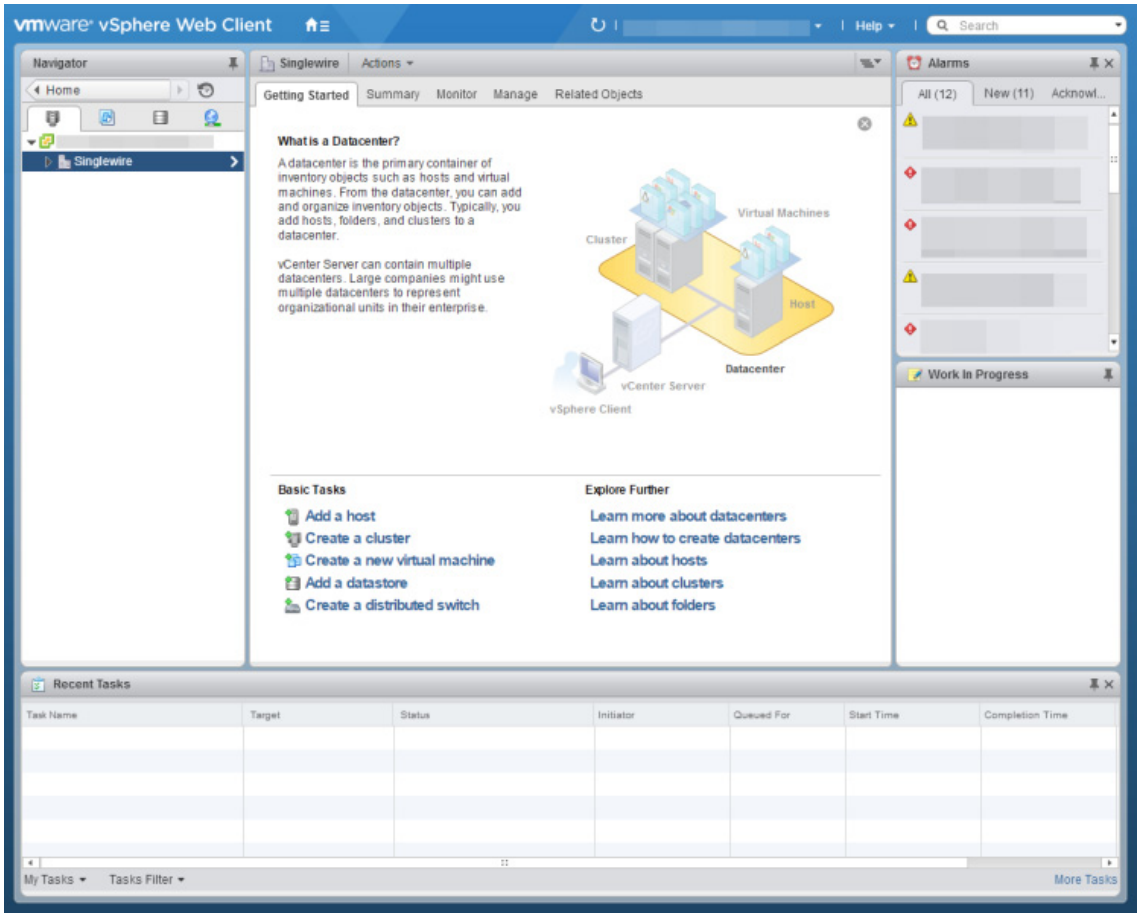
Step 3 Shut down the Virtual Appliance (see "Shut Down the Virtual Appliance" on page 9-8).

Step 4 Connect the CiscoPagingServer_UpgradeFrom115To-12.5.1.iso file to the Virtual Appliance. There are two ways to do this: uploading the ISO through vSphere or serving the ISO from a workstation. This section will document uploading the ISO through vSphere. If you'd like to serve the ISO from a workstation, VMware Remote Console may assist you. You can download it here and documentation is available here.

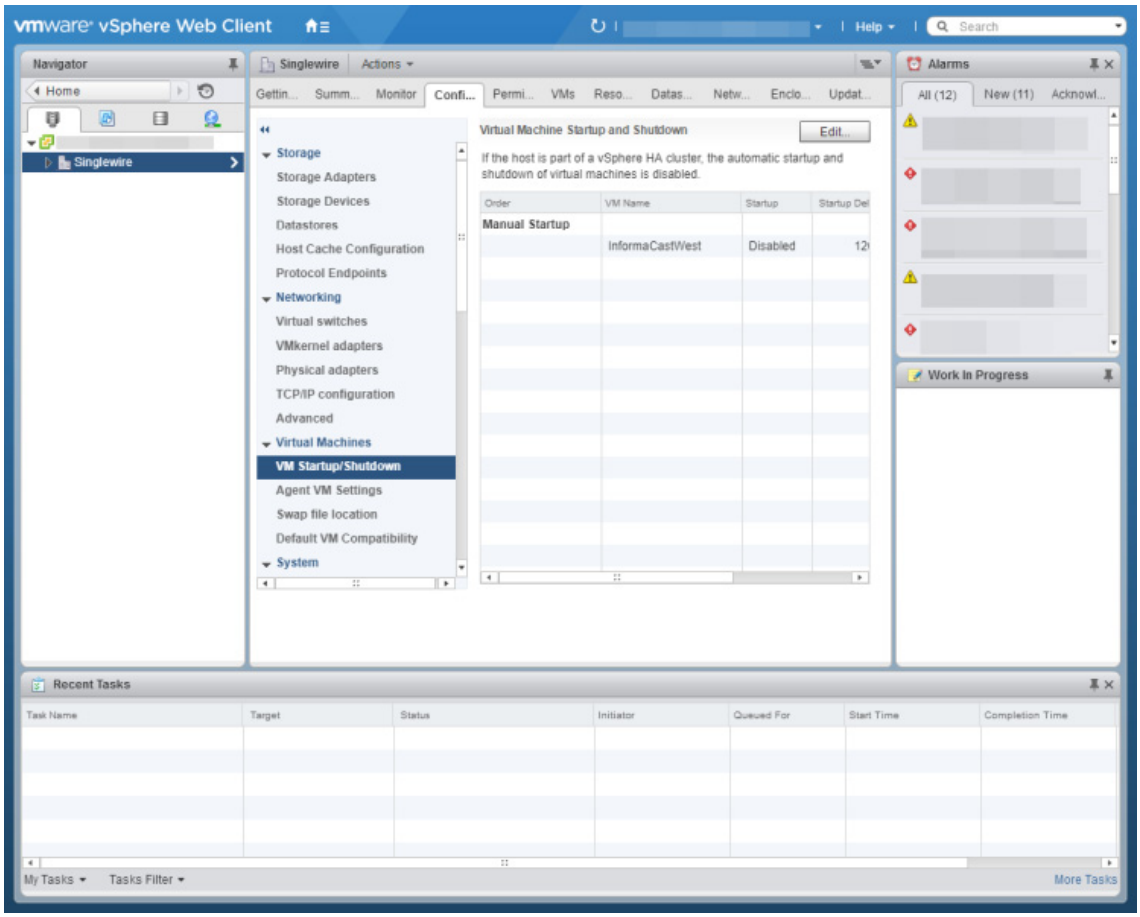
Step 5 Open a web browser and log into your vSphere web client. The vSphere Web Client page appears.



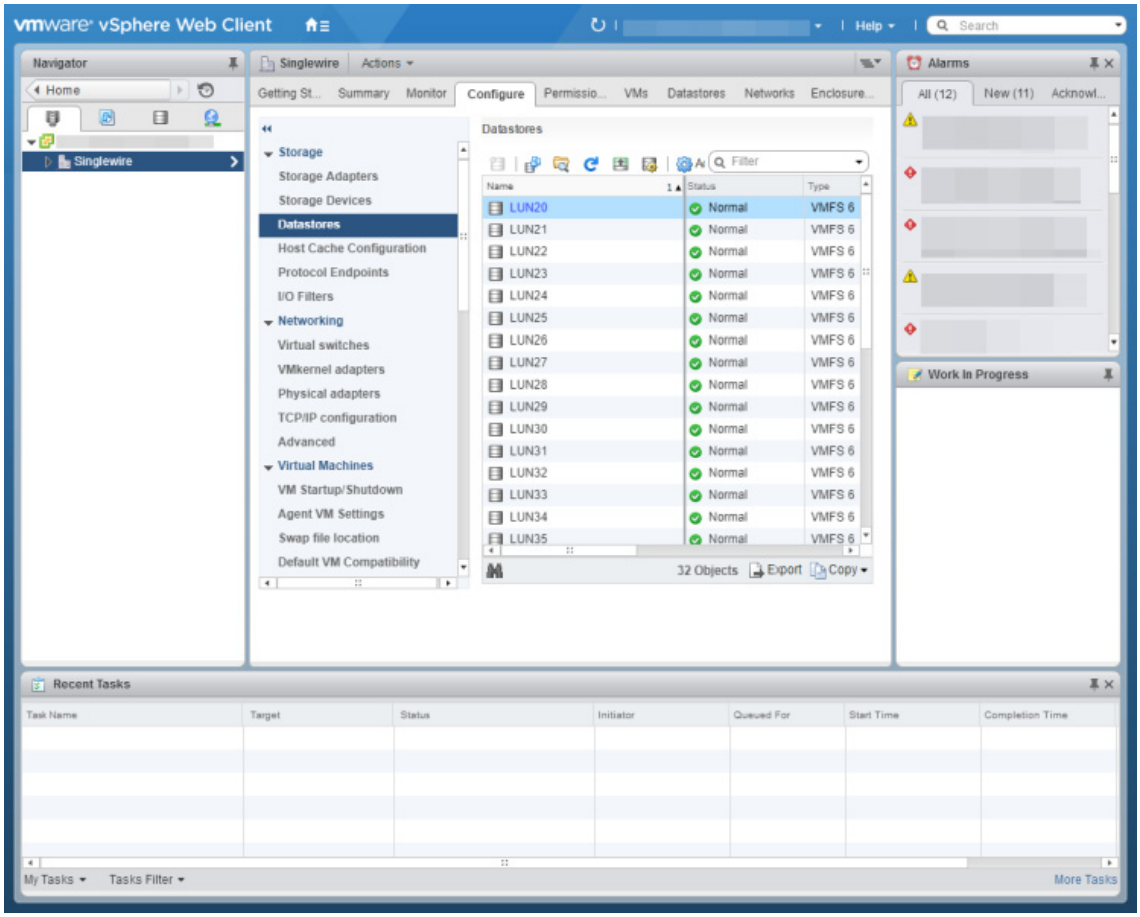
Step 6 Click the **Hosts and Clusters** icon. The vSphere Web Client page refreshes.



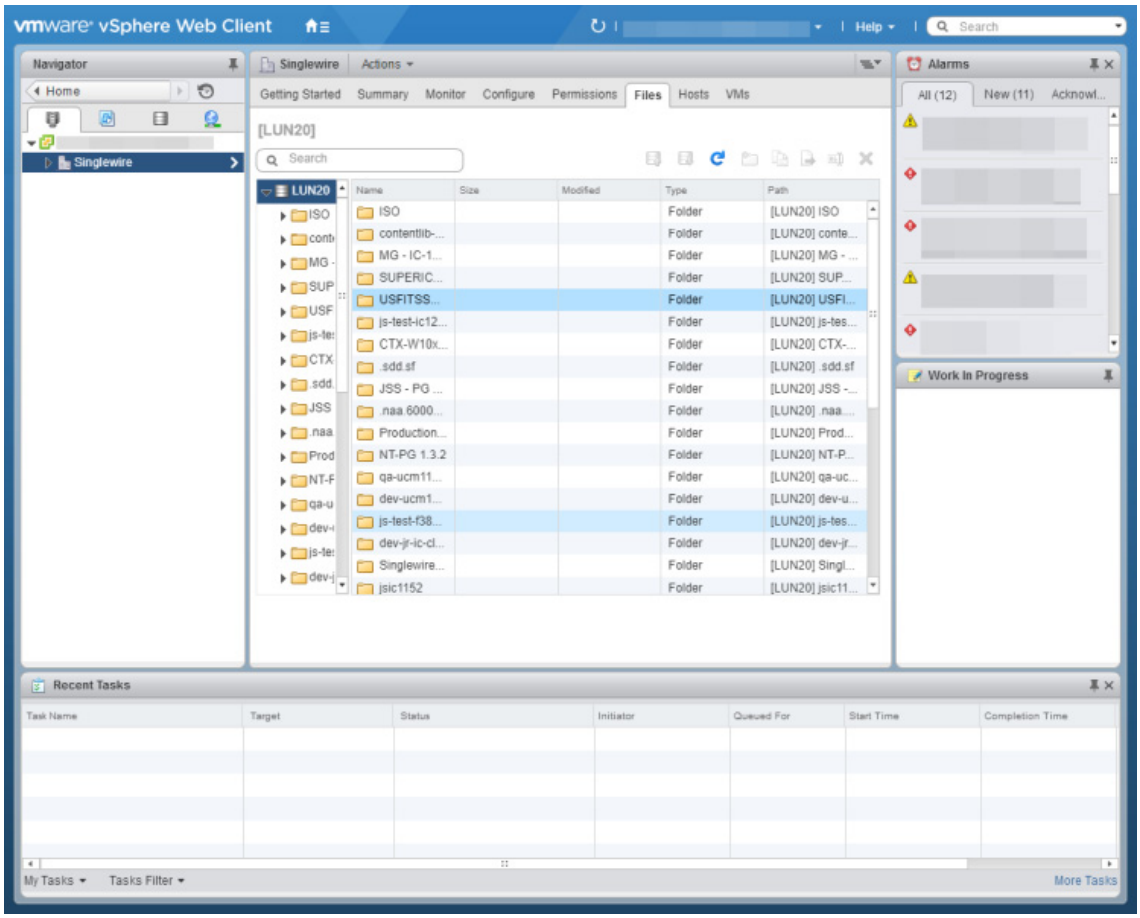
Step 7 Select the host server on which the InformaCast Virtual Appliance is located and select its **Configure** tab. The vSphere Web Client window's right pane refreshes.



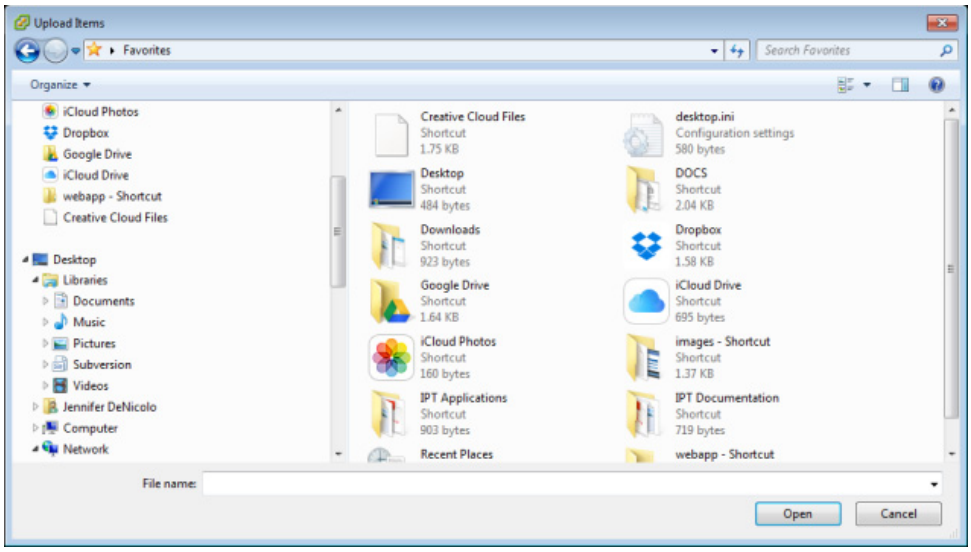
Step 8 Click the **Datastores** link under **Storage**. The vSphere Web Client window right pane refreshes.



Step 9 Right click the datastore to which you want to upload the CiscoPagingServer_UpgradeFrom115To-12.5.1.iso file and select **Browse Files**. The vSphere Web Client window right pane refreshes and you're taken to the **Files** tab.

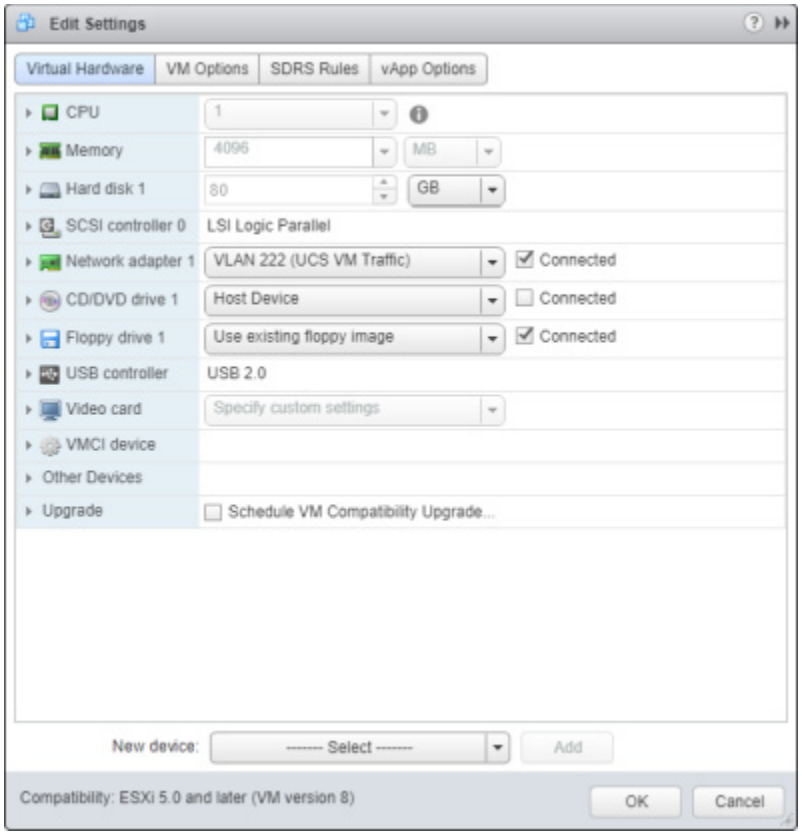


Step 10 Click the **Upload a file to this datastore** icon and select **Upload File.** The Upload Items dialog box appears.



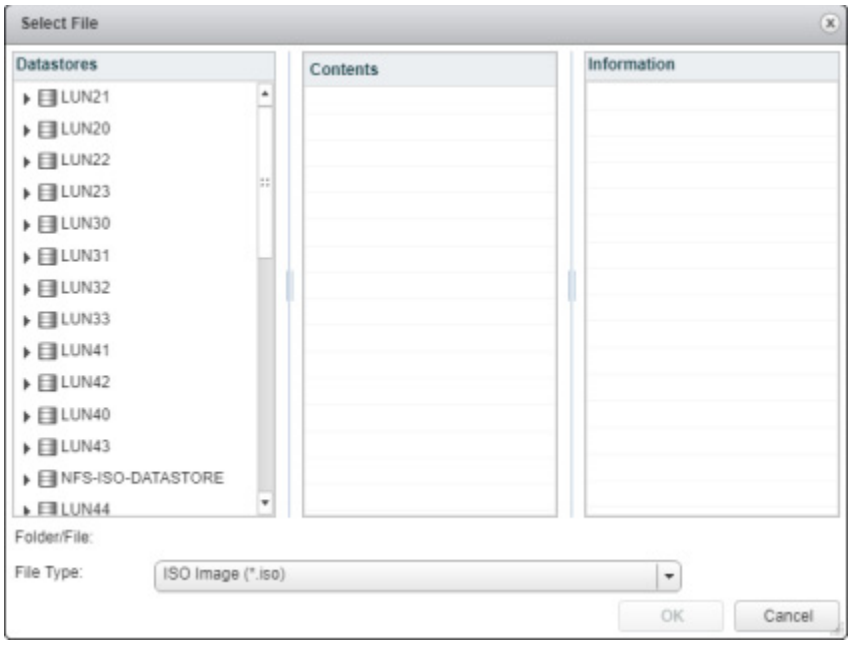
Step 11 Navigate to the location of the CiscoPagingServer_UpgradeFrom115To-12.5.1.iso file, select it, and click the **Open** button. vSphere will upload the ISO file to your host server.

Step 12 Right click your virtual machine and select **Edit Settings**. The Edit Settings pop-up window appears.



Step 13 Select the **CD/DVD drive 1** link. The Edit Settings pop-up window refreshes.

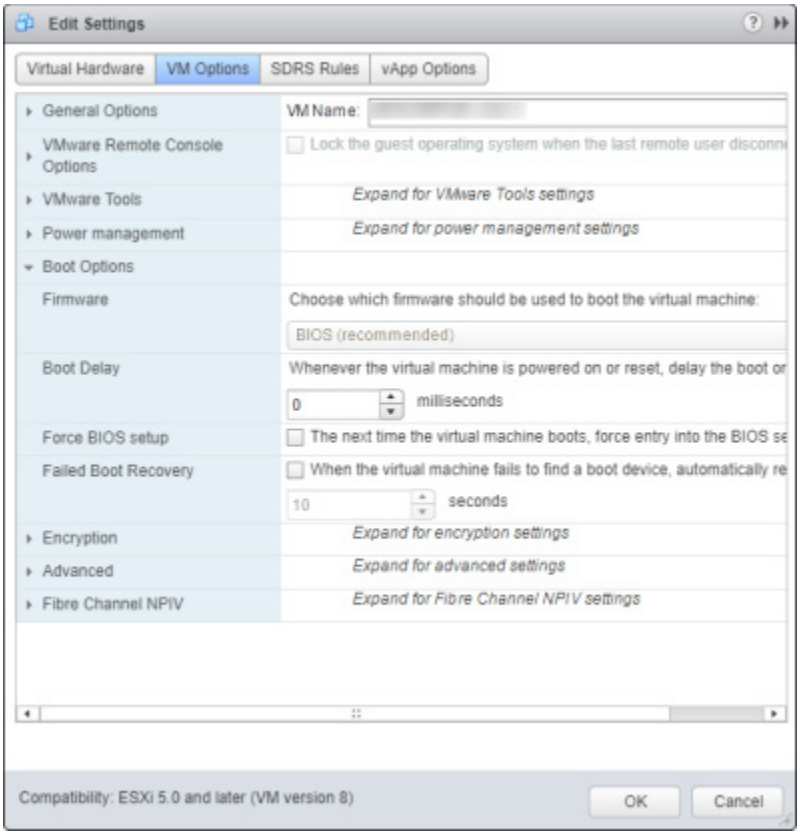
Step 14 Select **Datastore ISO File** from the second dropdown menu. The Select File pop-up window appears.



Step 15 Navigate to the location of the CiscoPagingServer_UpgradeFrom115To-12.5.1.iso file, select it, and click the **OK** button.

Step 16 Select the **Connect at Power On** checkbox.

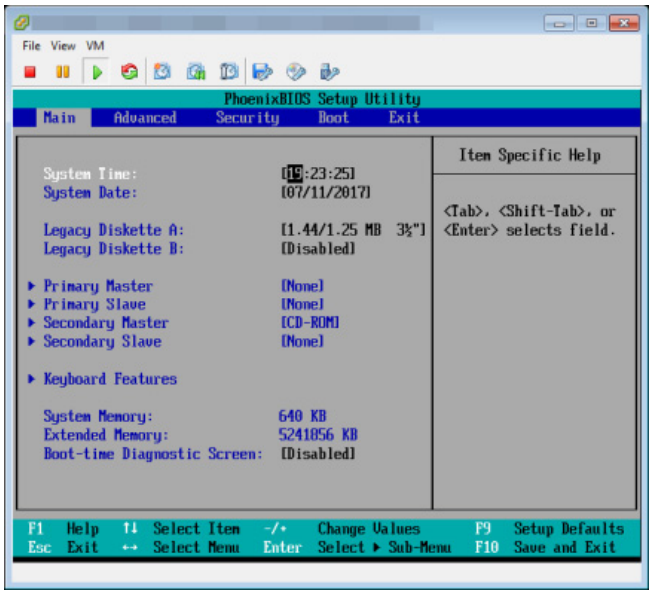
Step 17 Select the **VM Options** tab and expand **Boot Options**. The Edit Settings pop-up window refreshes.



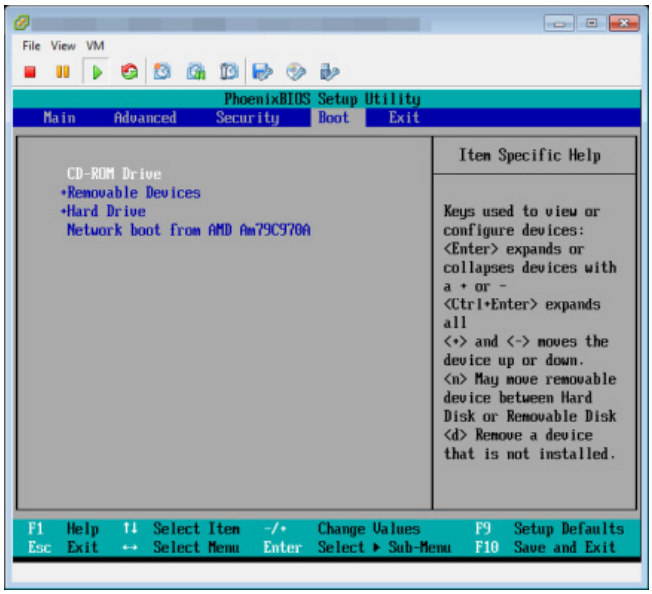
Step 18 Select the **Force BIOS setup** checkbox and click the **OK** button. The Edit Settings pop-up window closes.

Step 19 Right click your virtual machine in the vSphere Web Client window and select **Power | Power On**.

Step 20 Right click your virtual machine and select and select **Open Console**. The Singlewire InformaCast VM console window appears.

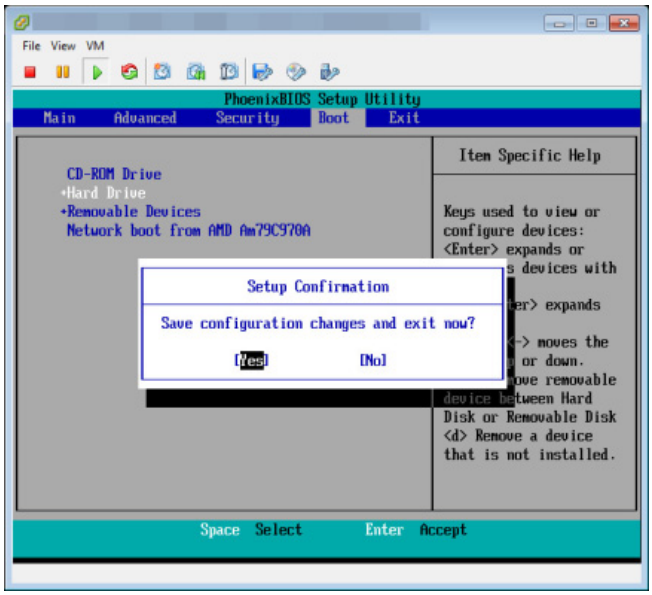


Step 21 Click inside the Singlewire InformaCast VM console window and press your right arrow key three times to move to the **Boot** tab. The Singlewire InformaCast VM console window refreshes.

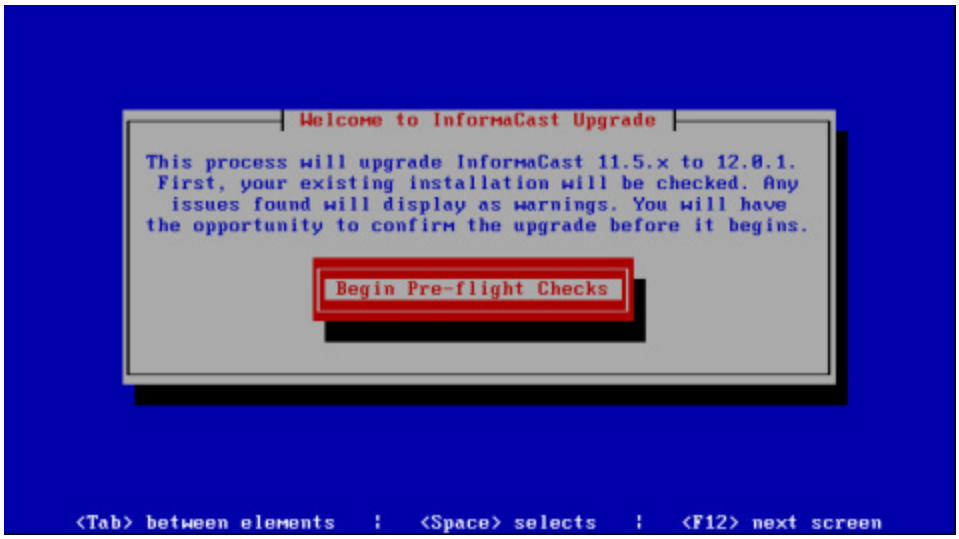


Step 22 Ensure that **CD-ROM Drive** is the first item in the boot list. If it's not, use your down arrow key to highlight **CD-ROM Drive**. Once highlighted, press the **Shift** and **+** keys to move **CD-ROM Drive** to the top of the boot list.

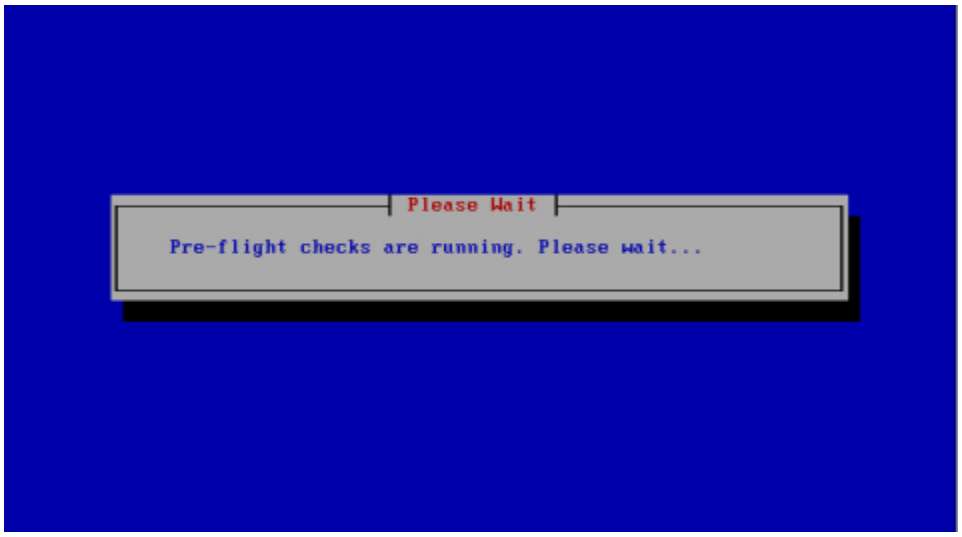
Step 23 Press the **F10** key. The Singlewire InformaCast VM console window refreshes.



Step 24 Press the **Enter** key to save your changes. The Virtual Appliance begins booting. This may take a few moments. When the Virtual Appliance is finished booting, the Singlewire InformaCast VM console window refreshes.

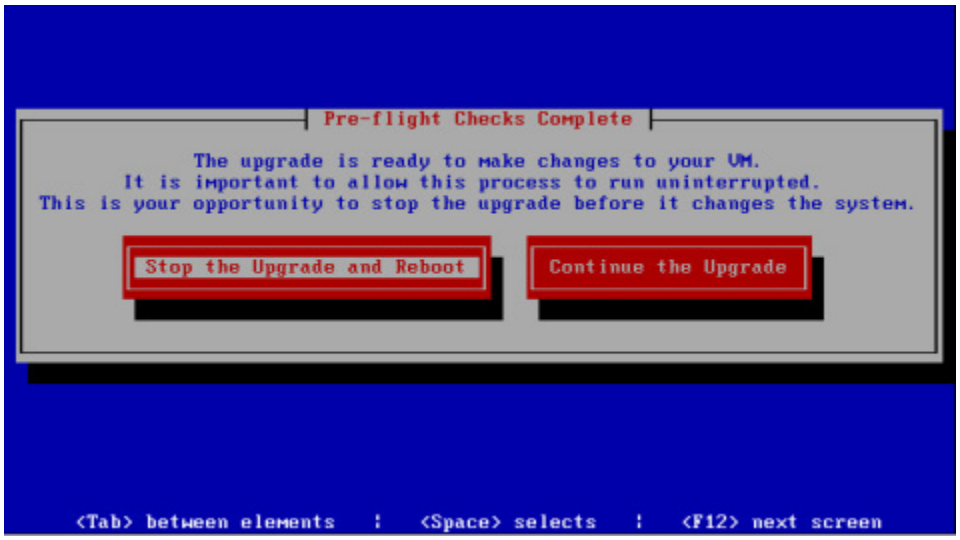


Step 25 Press the **Enter** key to begin pre-flight checks. The Singlewire InformaCast VM console window refreshes.



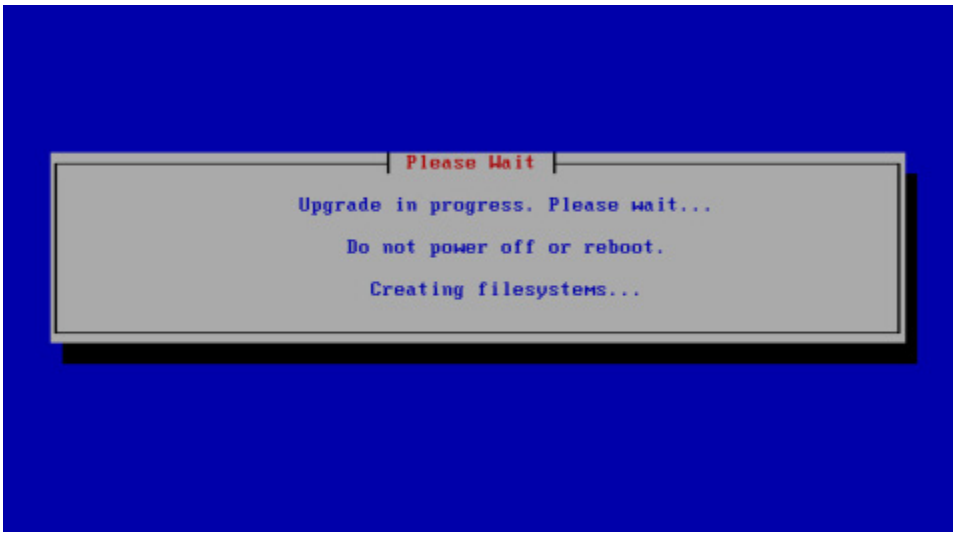
Pre-flight checks do not make any changes to the Virtual Appliance. They merely check that everything is in order for your upgrade and give you a way to back out if anything is not in order. If the pre-flight checks do find anything amiss, you may be prompted to address the issues before continuing with your upgrade.

When pre-flight checks are finished, the Singlewire InformaCast VM console window refreshes.

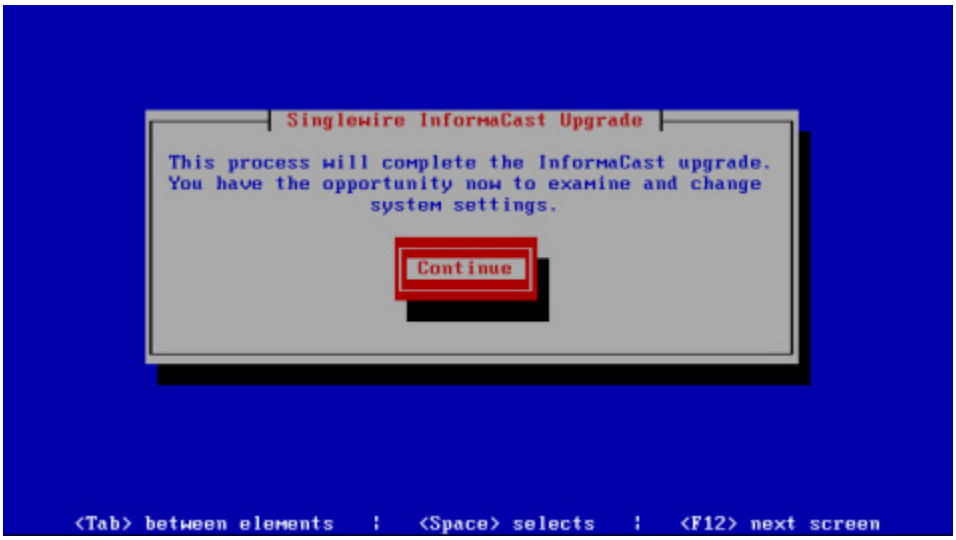


Note Continuing with the following steps will make changes to the Virtual Appliance. Once started, you must finish the process to ensure a successful upgrade.

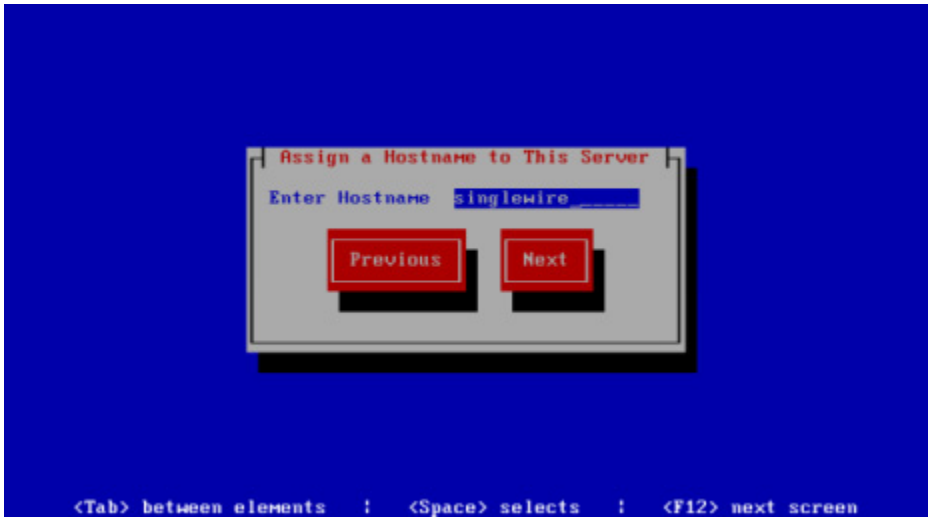
Step 26 Select the **Continue the Upgrade** button. The Singlewire InformaCast VM console window refreshes and your upgrade begins. This may take a few moments.



When your upgrade is finished, the Singlewire InformaCast VM console window refreshes.

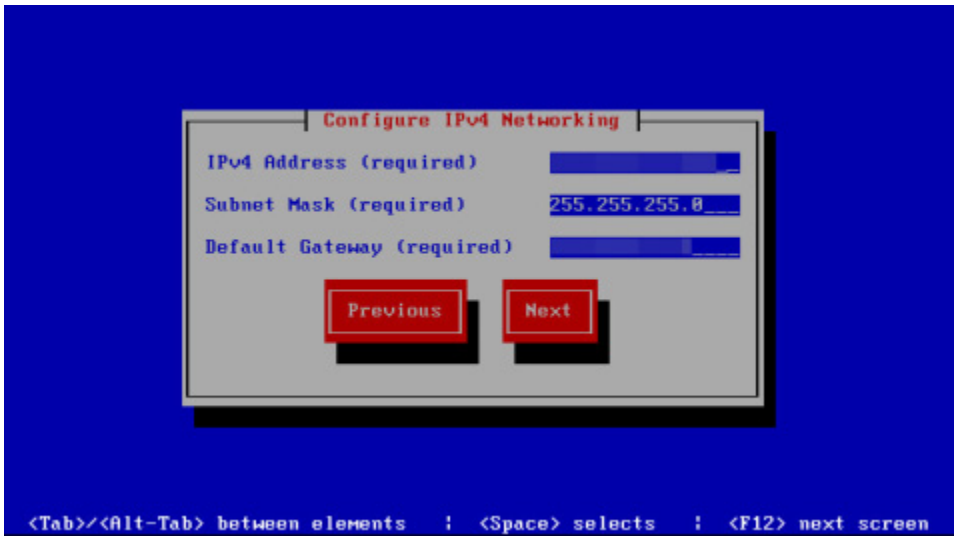


Step 27 Select the **Continue** button. The Singlewire InformaCast VM console window refreshes.

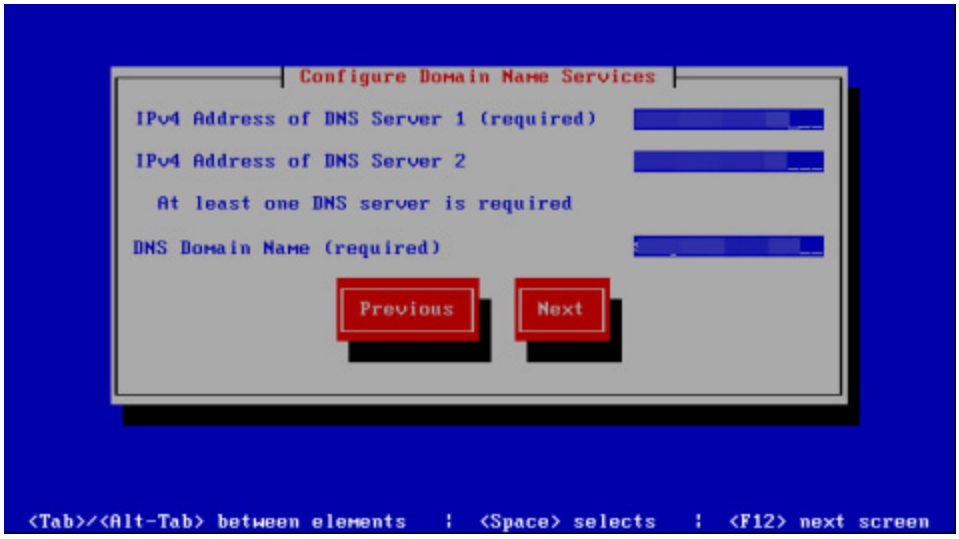


Step 28 Enter a hostname for your InformaCast Virtual Appliance server in the **Enter Hostname** field, e.g. InformaCastWest. This hostname will appear in Webmin's user interface.

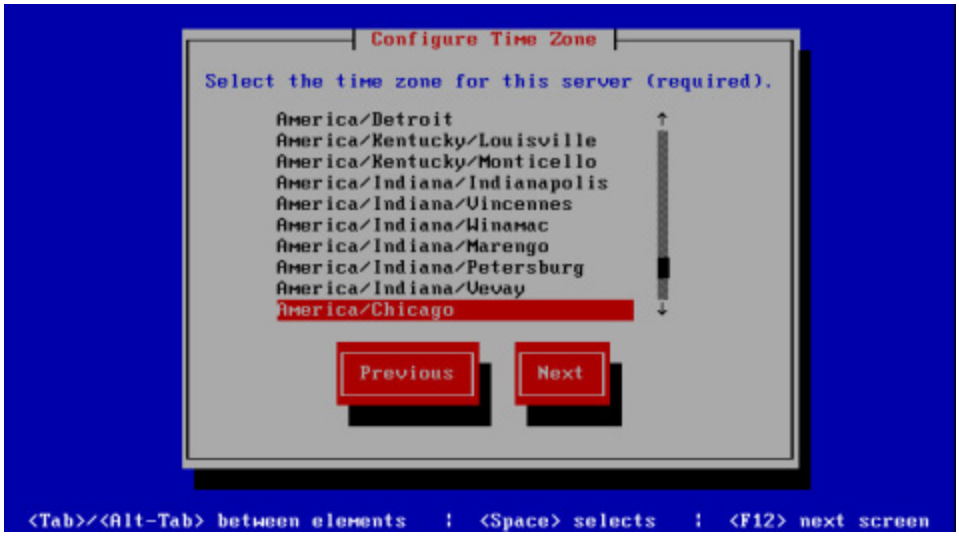
Step 29 Select the **Next** button. The InformaCast Virtual Appliance then attempts to use DHCP to find suitable IP addresses on your network. The Singlewire InformaCast VM console window refreshes.



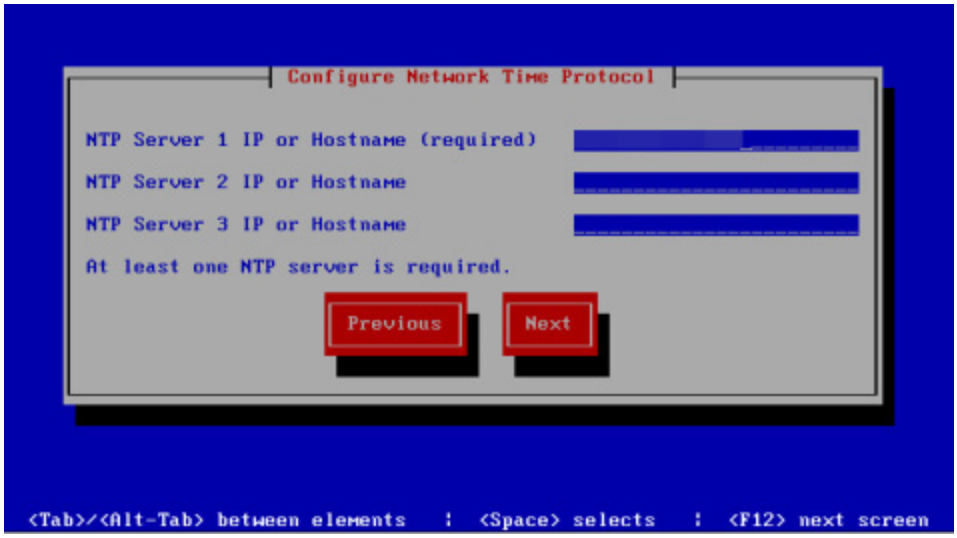
Step 30 Accept these IP addresses or provide valid ones of your own in the **IPv4 Address**, **Subnet Mask**, and **Default Gateway** fields and select the **Next** button. The Singlewire InformaCast VM console window refreshes.



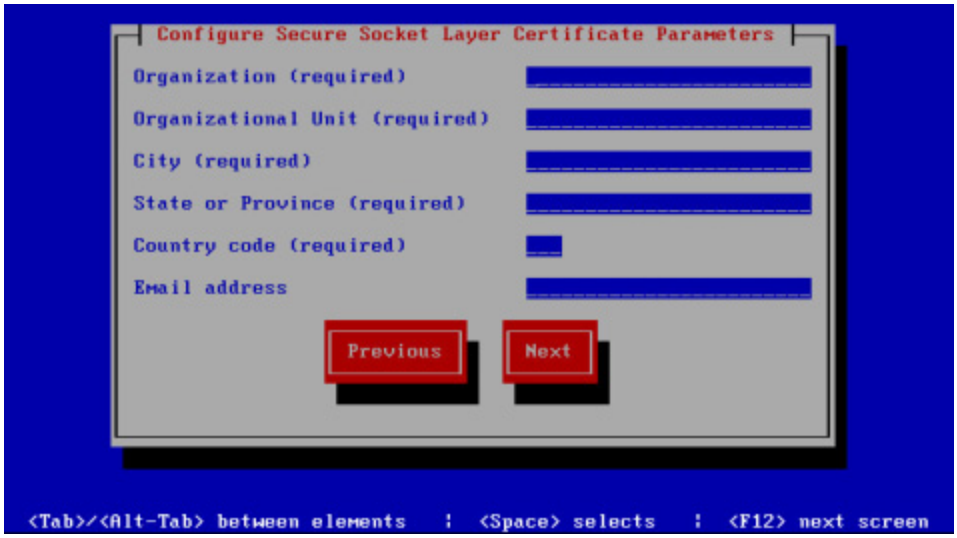
Step 31 Enter at least one DNS server IP address in the field provided or accept the one provided to you and enter a DNS domain name. Select the **Next** button. The Singlewire InformaCast VM console window refreshes.



Step 32 Select a time zone for your InformaCast Virtual Appliance and select the **Next** button. The InformaCast Virtual Appliance then attempts to find an NTP server on your network. The Singlewire InformaCast VM console window refreshes.



Step 33 Accept the suggested NTP server IP address or provide a valid one of your own in the **NTP Server 1 IP or Hostname** field and select the **Next** button. The Singlewire InformaCast VM console window refreshes.



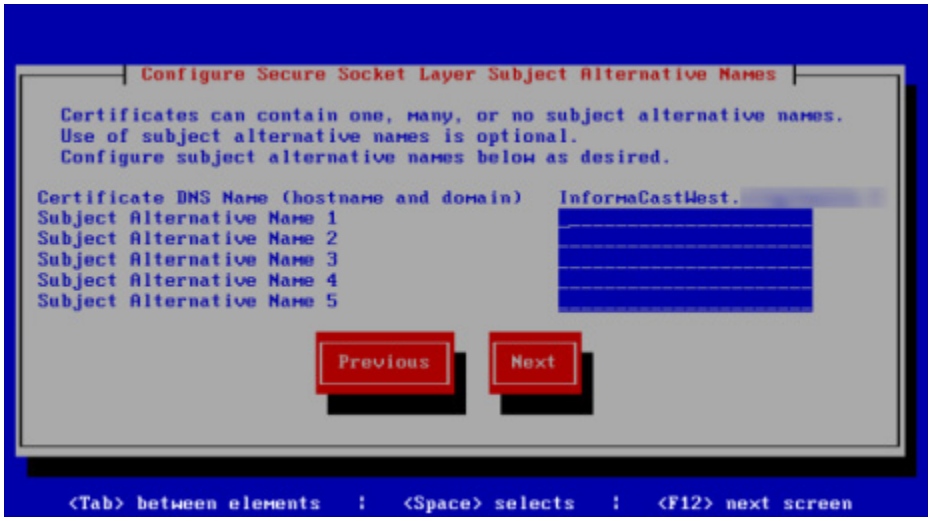
Step 34 Enter the information necessary for a signed certificate (while the information is required, signing the certificate is not). A signed certificate, which can protect against Man-in-the-Middle (MITM) attacks, is an electronic document that proves ownership of a public key; it includes information about the key, its owner's identity, and the digital signature of a certificate authority (CA).

You must enter the information dictated by your certificate authority in its required form:

- Your organization's name, e.g. Acme Company
- Your organizational unit, e.g. Security

- Your city, e.g. Madison
- Your state or province, e.g. WI
- The alphabetic abbreviation for your country, e.g. US for United States
- An email address (optional)

Step 35 Select the **Next** button. The Singlewire InformaCast VM console window refreshes.



Step 36 Enter the common name of your server, e.g. InformaCastWest.singlewire.lan in the **Certificate DNS Name (hostname and domain)** field, then continue entering information for your signed certificate by entering any Subject Alternative Names (SANs) in the fields provided. 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.

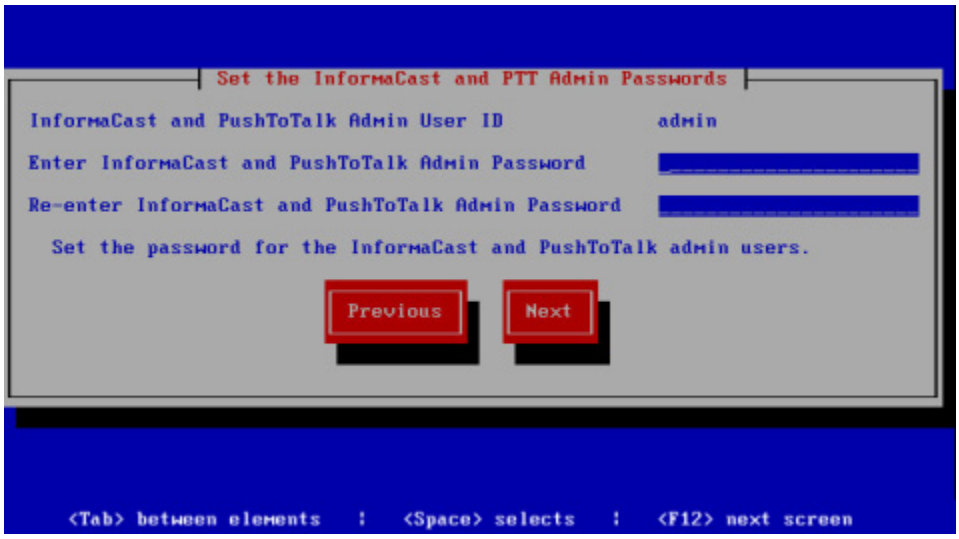
Step 37 Select the **Next** button. Depending on the security of your OS credentials from your previous version of the Virtual Appliance, you may either keep your previous OS credentials or be forced to enter new ones. The Singlewire InformaCast VM console window refreshes.

Note If you've never changed your password from the default of "changeMe," you will be forced to change your password.

Step 38 Enter a password in the **Enter OS Admin Password** field, press the **Tab** key, and enter the password again in the **Re-enter OS Admin Password** field. Your OS credentials are used to enter Webmin and Control Center and when using SSH to access the InformaCast Virtual Appliance.

Note Your password must be at least six characters in length, and contain at least one lowercase letter, one number, and one of the following characters: !\"#$%"() *+,-./ :;<=>?@[]^_`. Also, when setting your password, you cannot use "changeMe."

Step 39 Select the **Next** button. Depending on the security of your application credentials from your previous version of the Virtual Appliance, you may either keep your previous application credentials or be forced to enter new ones. The Singlewire InformaCast VM console window refreshes.



Note If you've never changed your password from the default of "changeMe," you will be forced to change your password.

Step 40 Enter a password in the **Enter InformaCast and PTT 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 Your password must be at least six characters in length, and contain at least one lowercase letter, one number, and one of the following characters: !\"#$%"() *+,-./ :;<=>?@[\\]^_`. Also, when setting your password, you cannot use "changeMe."

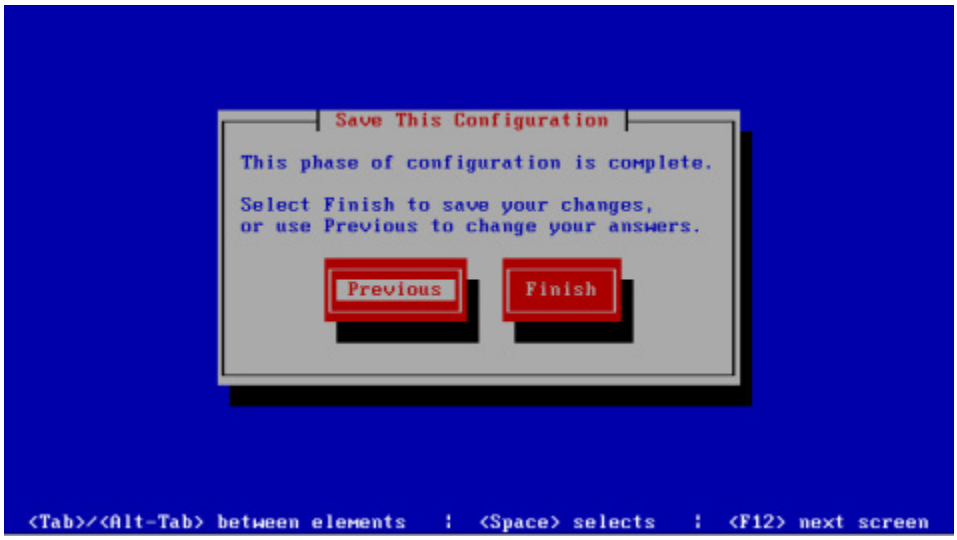
Note PushToTalk is only available to Advanced InformaCast users.

Step 41 Select the **Next** button. The Singlewire InformaCast VM console window refreshes.

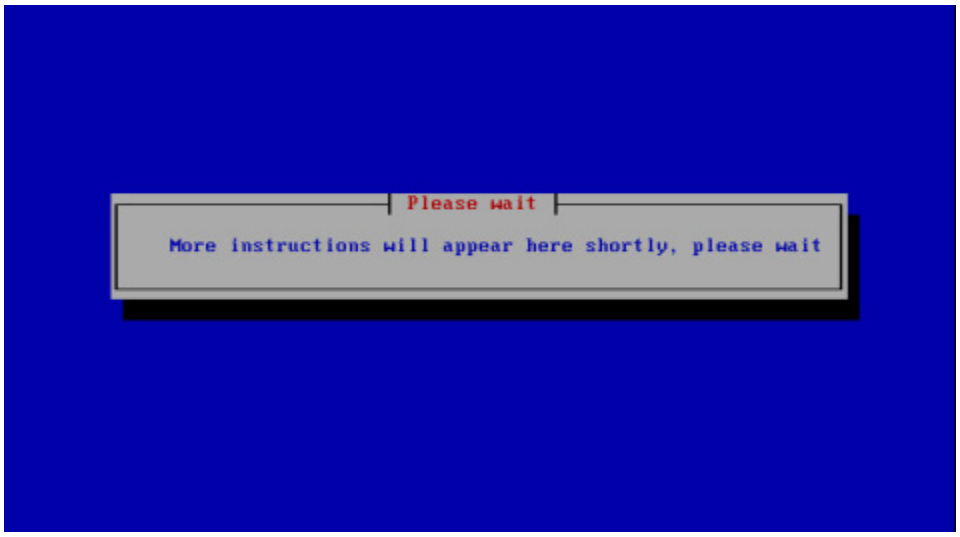
Step 42 Enter a security passphrase in the **Enter Security Passphrase** and **Re-enter Security Passphrase** fields. This passphrase is used to secure your backups of the InformaCast Virtual Appliance. You must remember this passphrase. Singlewire Support personnel cannot recover it for you if it's lost.

Note Your passphrase must follow the same character requirements as your OS admin password.

Step 43 Select the **Next** button. The Singlewire InformaCast VM console window refreshes.

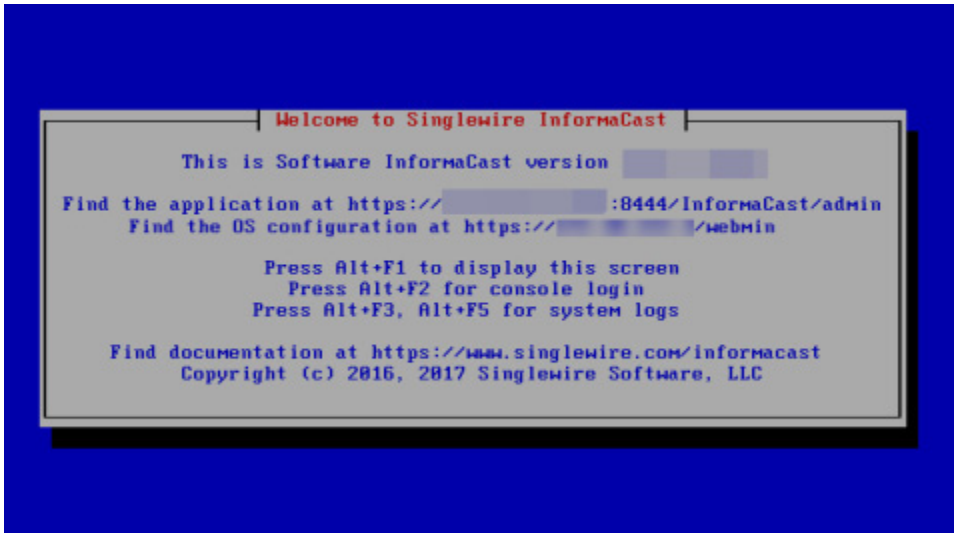


Step 44 Select the **Finish** button to save your changes. The Singlewire InformaCast VM console window refreshes.



Note There may be a short wait while your changes are written to disk.

Once your changes have been saved, the Singlewire InformaCast VM console window refreshes.



Step 45 Make a note of the displayed IP address. This is the IP address of the InformaCast Virtual Appliance's landing page, which you will use to access the InformaCast Virtual Appliance, Control Center, and Webmin web user interfaces.

Step 46 Close your open console window.

Step 47 Create a new snapshot of your Virtual Appliance.

Step 48 Clear your web browser's cache.

Note If your starting version of InformaCast was 11.0.5 and earlier and 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 5-38).

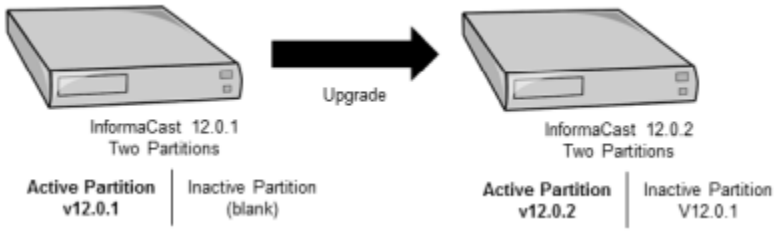
Step 49 Proceed with "Upload a New License" on page 9-109 if you're going between major versions of InformaCast, e.g. whole number versions.

Upgrade InformaCast 12.0.1 and Later

Note The upgrade steps in this topic only apply to version of InformaCast 12.0.1 and later. If you are using a pre-12.0.1 version of InformaCast, you must follow the steps in "Upgrade InformaCast Pre-12.0.1" on page 9-77.

Due to InformaCast's dually-partitioned platform (comprised of one active partition and one inactive partition), you can move between versions of easily and preserve the previous version of in case of conflict.

When upgrading 12.0.1 and later, you load the new version to your inactive partition, and then switch your inactive partition to be active. During an upgrade, all of your configuration information is carried over to your new active partition.



If this is your first upgrade, your inactive partition would initially be blank. If you've upgraded before, your inactive partition would contain a past version of InformaCast.

In case of conflict, you can switch back to your previous version and continue using InformaCast as before, although any changes you made while in your new version will not be carried over to your old version.

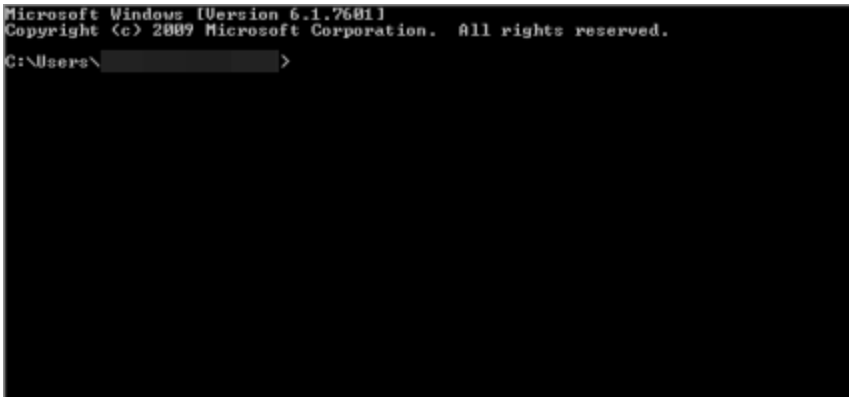
Step 1 Declare an outage window and ensure that it falls outside of regular business hours.

Step 2 Back up InformaCast (see "Backup InformaCast's Configuration" on page 6-15). Optionally, take a VMware snapshot.

Step 3 Download the upgrade file from cisco.com.

Step 4 Use PuTTY's PSCP functionality to transfer your .upg file to your Virtual Appliance. PuTTY is available as a free download and it should be installed on the machine from which you'll transfer files to the Virtual Appliance.

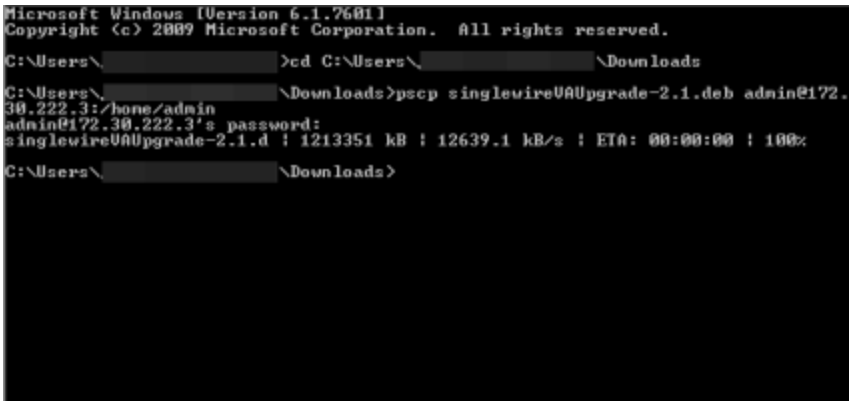
a. Open a command window on the machine on which you've saved your .upg file. A command window appears.



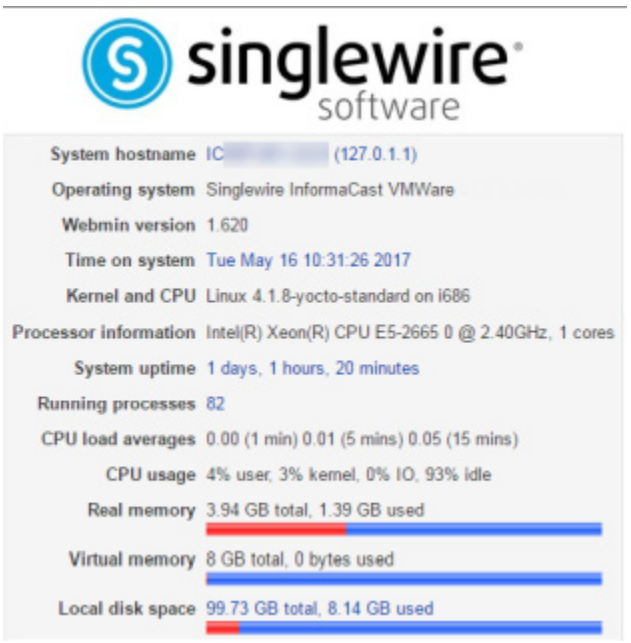
b. Enter **cd <directory>** and press the **Enter** key, where <directory> is the location of your .upg file. The command window refreshes to the location of your directory.

c. Enter **pscp <file name> admin@<InformaCast Virtual Appliance IP Address>:/upgrade** at the prompt and press the **Enter** key, where <file name> is the name of your .upg file and <InformaCast Virtual Appliance IP Address> is your actual Virtual Appliance's IP address, e.g. pscp CiscoPagingServer-UpgradeTo12.5.1_XXXX.upg admin@111.22.333.4:/upgrade.

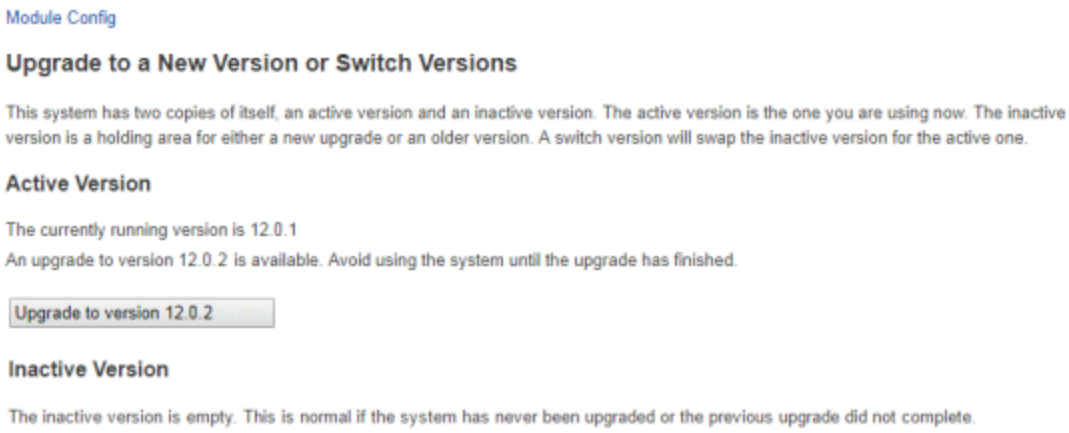
d. Enter your Virtual Appliance password at the prompt and press the **Enter** key. The file will be transferred.



Step 5 Log into Webmin (see "Log into Webmin" on page 2-35). The Webmin homepage appears.



Step 6 Go to **System | Upgrade or Switch Versions**. The Upgrade to a New Version or Switch Versions page appears.

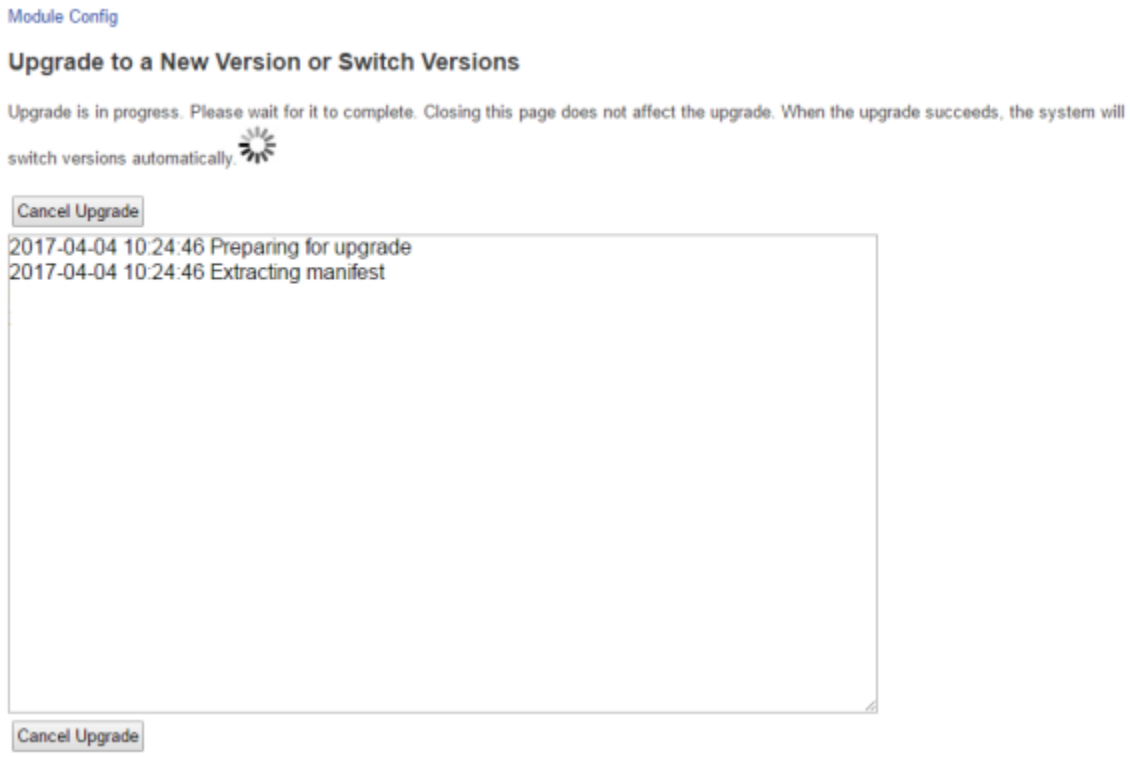


On the Upgrade to a New Version or Switch Versions page, you can see the version of InformaCast you are currently running in the *Active Version* area. InformaCast can also "see" that a new version is available.

Because this is the first time InformaCast has been upgraded, the *Inactive Version* area is empty.

Step 7 Click the **Upgrade to version** button in the *Active Version* area. The Upgrade to a New Version or Switch Versions page refreshes.

Step 8 Click the **Confirm upgrade to version** button. The Upgrade to a New Version or Switch Versions page refreshes and your upgrade begins.



During the upgrade, InformaCast will go through a number of processes and your Webmin window will eventually look like it has errored. This happens when the Virtual Appliance server reboots.

Step 9 Refresh the page and log into Webmin again. Note that the version of InformaCast (visible in the Operating system line) has been upgraded.

Step 10 Go to **System | Upgrade or Switch Versions**. The Upgrade to a New Version or Switch Versions page appears.

In the *Active Version* area, you can see your upgraded InformaCast is running, and it has all of the old version's configuration information in it. The *Inactive Version* area now holds your previous version of InformaCast. If you click the **Switch version** button in the *Inactive Version* area, you can revert back to your old InformaCast version; however, any changes you made to your new version will not be reflected if you revert.

Step 11 Proceed with "Upload a New License" on page 9-109 if you're going between major versions of InformaCast, e.g. whole number versions.

Upload a New License

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.

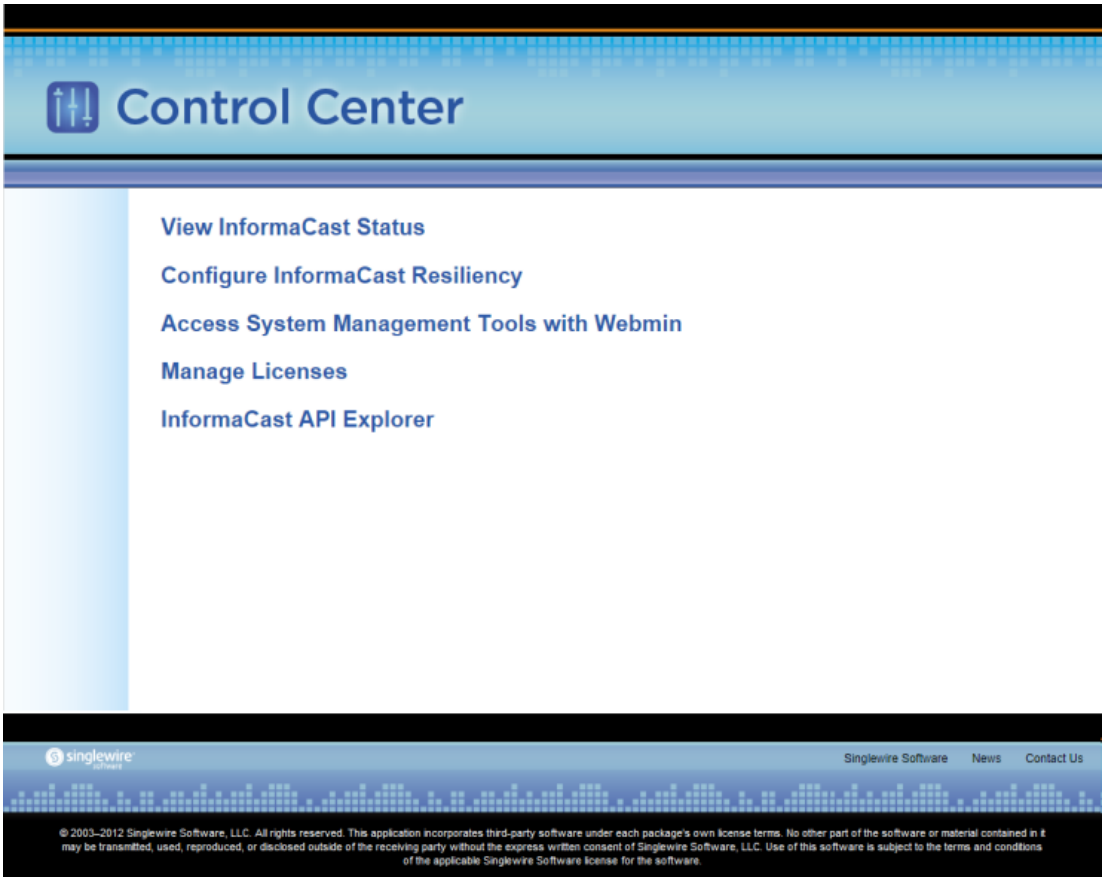
Before you can perform these steps, you must have an InformaCast Virtual Appliance license, which will be in the form of an XML file that was sent to you by email from a Singlewire sales representative. If your salesperson has not already provided one to you, contact Singlewire and request that a license 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 2-33 for specific steps).

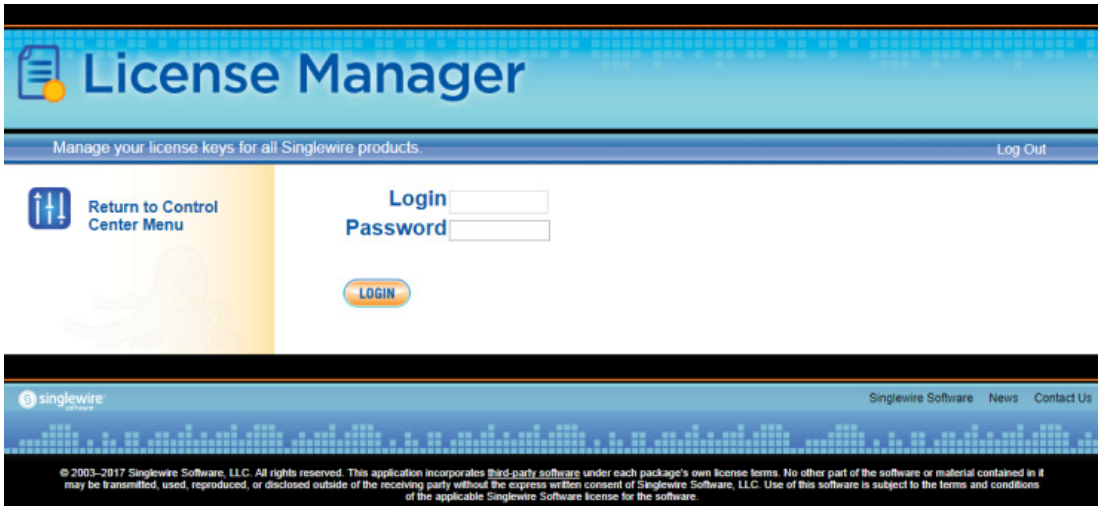
Note For versions of InformaCast Virtual Appliance prior to 8.4, you will need to go to https://<InformaCast Virtual Appliance IP Address>:8463/LicenseManager, where <InformaCast Virtual Appliance IP Address> is InformaCast Virtual Appliance's statically configured IP address. Skip to Step 3 on page 9-111.

A separate tab/window opens to the Control Center page.



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

Step 2 Click the **Manage Licenses** link. The License Manager page appears.

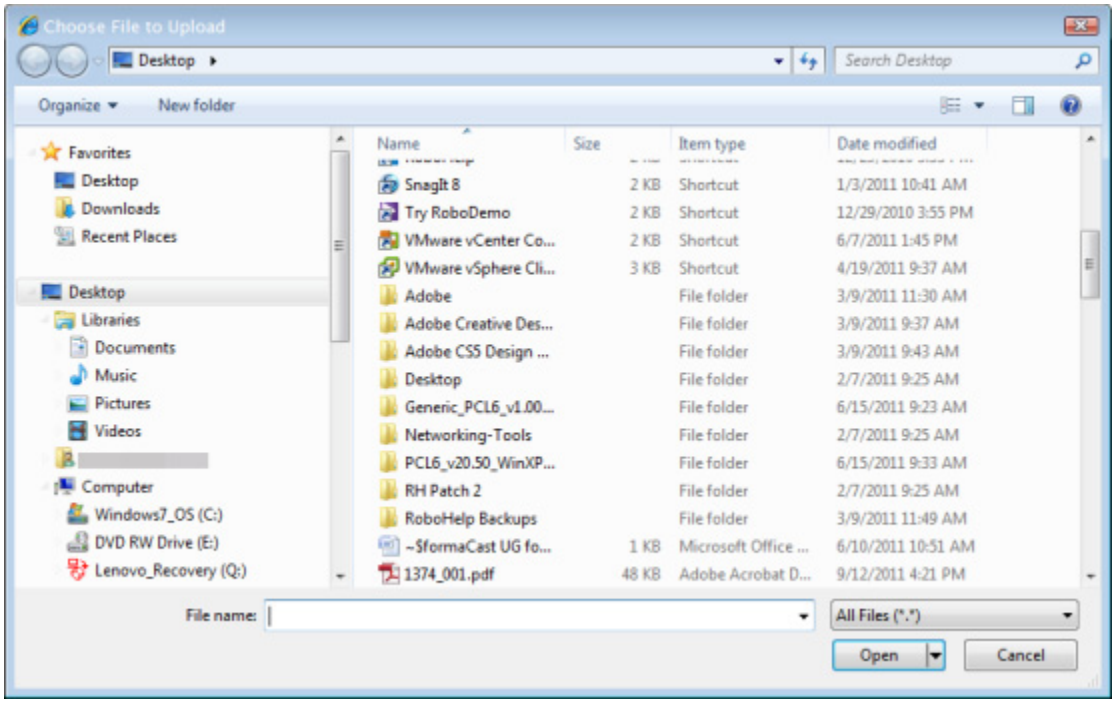


Step 3 Enter your OS credentials in the **Login** and **Password** fields.

Step 4 Click the **Login** button. The Upload a New License page appears.

The License Manager holds all of your Singlewire licenses. Depending on the software applications you are using, you will see different licenses housed on this page.

Step 5 Click the **Browse** button. The Choose File to Upload window appears.



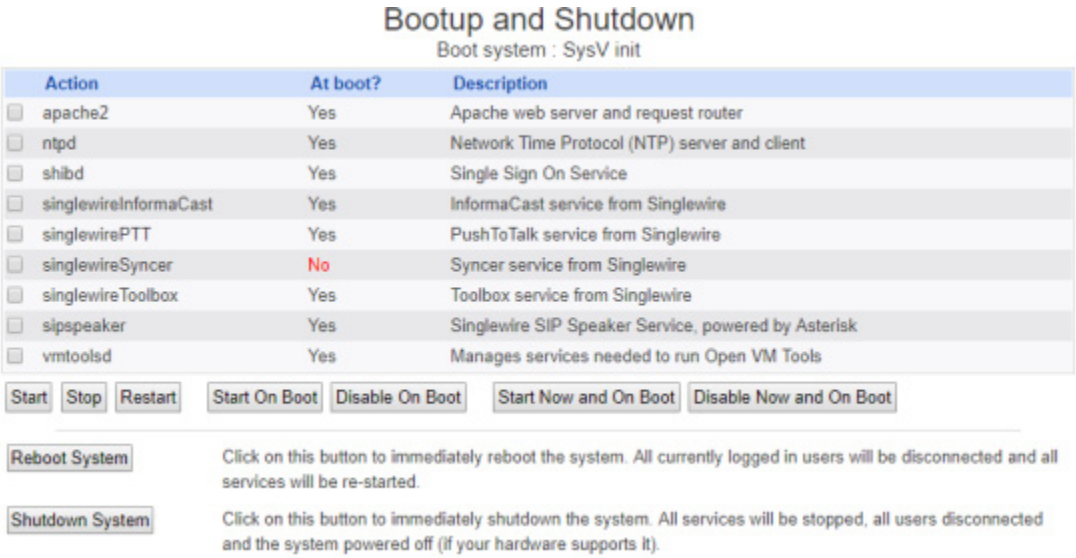
Step 6 Navigate to where you saved your new license file, select it, and click the **Open** button.

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.

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.



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.

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 12.5.1

The following information pertains to InformaCast 12.5.1.

Compatibility

InformaCast is compatible with the following versions of Cisco Unified Communications Manager server (including Business Edition 6000): 10.0.1, 10.5.2, 11.0.1, 11.5.1, 12.0.1, and 12.5.1.

New Features

- **New Login Banners.** Login banners allow you to display text to your users before and/or after they log into InformaCast. You could use login banners to welcome users to your alert system, make them aware of acceptable use policies, or let them know the data they enter is owned and governed by your company.
- **New OS and Application Credentials Password Recovery Management.** If you lose your Virtual Appliance's password or accidentally delete admin, your default superuser account, you can contact Cisco TAC. Together, you'll use InformaCast's built-in process to recover your password. You also gain the ability to turn off/on this functionality.
- **New SNMP Monitoring.** Listening on port 1161, InformaCast's embedded SNMP agent can be paired with your own Network Management Software (NMS) in order to monitor certain aspects of InformaCast, e.g. the last time a phone rebuild succeeded, InformaCast's version, etc. Several OIDs, both native and InformaCast-specific are available for your use as well as both native and InformaCast-specific MIBs. In addition to this new polling functionality, several new commands allow you to display your current configuration, restart the SNMP monitoring service, or remove your SNMP configuration entirely.
- **New Controls for SSL Parameters.** InformaCast now allows you to enable/disable the various SSL and TLS versions it supports as well as limit the protocols available for accessing the InformaCast Virtual Appliance landing page.
- **New Signed Certificates Process.** The process for importing signed certificates into InformaCast has improved to allow for a chain of trust certificates, e.g. a root certificate and any intermediate certificates. InformaCast has also become more rigorous in its validating of trust: whenever it reboots, InformaCast will check that its trust certificates are still valid. This extra validation improves your security against MITM attacks. As a result of these improvements, if you are upgrading from a pre-12.0.1 version of InformaCast, you'll need to enter SSL information in

order for InformaCast to generate its self-signed certificate. If you're upgrading from a post-12.0.1 version of InformaCast and you had previously imported a signed certificate, you'll need to import it again.

- **New NTP Controls within the Virtual Appliance.** InformaCast now uses the Network Time Protocol daemon (ntpd) for time synchronization. Several new commands are available to you, allowing for more granular control of your NTP configuration:
  - show-time-configuration lists your currently configured NTP server(s)
  - configure-time allows you to change your NTP server(s)
  - show-time-status displays the current state of the NTP daemon and whether InformaCast is in sync with it
- **Newly Supported vNIC Type.** InformaCast again supports vmxnet3 Ethernet VMware virtual Network Interface Cards (previous versions of InformaCast supported either the pcnet32/vlance or e1000 vNIC type). Depending on your originating version of InformaCast, you will have different vNIC types:
  - When you install InformaCast for the first time, your vNIC will be automatically set to the vmxnet3 type.
  - When you upgrade from an 11.5.x version, you will continue to use the pcnet32/vlance type.
  - When you upgrade from a 12.x version of InformaCast, you will continue to use the e1000 vNIC.

  For both pcnet32/vlance and e1000, there is no immediate need to change vNIC types: both are supported by InformaCast 12.5.1 on vSphere 6.5.
- **New Enable the Support Account Workflow.** The process for enabling the Support account has changed to improve its usability and fall more in line with other server platform changes. **enable-support**, a command for the command-line interface, lets CiscoTAC access your Virtual Appliance to aid in troubleshooting issues.
- **Security Enhancements Necessitate Button Removal.** If you're using the Inbound CAP Message Service (ICMS) to push CAP alerts to InformaCast, you can no longer stop and restart the service from the Inbound CAP plugin's Configuration page. Singlewire is working hard to improve the security of InformaCast. Sometimes, this necessitates the removal of trivial functionality to improve overall security.
- **Change to Webmin's URL.** Singlewire is moving away from custom ports due to the additional firewall configuration and security controls involved with them. As part of this move, Webmin's URL has changed to https://<InformaCast Virtual Appliance IP Address>/webmin. For now, the previous Webmin URL will redirect to the new one.
- **New Upgrade File for pre-12.0.1 Versions of InformaCast.** A new file (CiscoPagingServer_UpgradeFrom115To-12.5.1.iso) has been added to the upgrade process. Depending on the version of InformaCast Virtual Appliance from which you are starting, you will install different files:
  - For 8.3 or 8.4 versions to the current version, you will install three package files and attach one ISO file (CiscoPagingServer_8.5.1.deb, CiscoPagingServer_9.1.1.deb, CiscoPagingServer_11.5.2.deb, and CiscoPagingServer_UpgradeFrom115To-12.5.1.iso)

- For 8.5.1, 9.0.1, or 9.0.2 to the current version, you will install two package files and attach one ISO file (CiscoPagingServer_9.1.1.deb, CiscoPagingServer_11.5.2.deb, CiscoPagingServer_UpgradeFrom115To-12.5.1.iso)
- For 9.1.1, 11.0.1, 11.0.2, or 11.0.5 to the current version, you will install one package file and attach one ISO file (CiscoPagingServer_11.5.2.deb and CiscoPagingServer_UpgradeFrom115To-12.5.1.iso)
- For 11.5.1 or 11.5.2 to the current version, you will attach one ISO file (CiscoPagingServer_UpgradeFrom115To-12.5.1.iso)

InformaCast Virtual Appliance 8.5.1, 9.1.1, and 11.5.1/2 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, upgrade to 11.5.2, and then continue to upgrade to 12.5.1. 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, upgrade to 11.5.2, and then continue to upgrade to 12.5.1. For 9.1.1, 11.0.1, 11.0.2, and 11.0.5 versions of the Virtual Appliance, you must upgrade to 11.5.2 and then continue to upgrade to 12.5.1. For 11.5.1 and 11.5.2 versions of the Virtual Appliance, you can upgrade directly to 12.5.1.

If you're already using InformaCast 12.0.1 or later, ignore this note; your upgrade process involves fewer steps and files.

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 12.1.1

The following information pertains to InformaCast 12.1.1.

Compatibility

InformaCast is compatible with the following versions of Cisco Unified Communications Manager server (including Business Edition 6000): 10.0.1, 10.5.2, 11.0.1, 11.5.1, and 12.0.1.

New Features

- **New SIP Profile Requirement.** Previously only required for SIP with SRTP, adding a SIP profile to your SIP trunk is now required for SIP functionality. This is a configuration precaution: SIP profiles are required for full-duplex intercom calling; however, InformaCast doesn't know whether you plan to use intercom calling now or in the future (or upgrade from InformaCast Basic Paging to Advanced Notification). To avoid this important configuration step being missed, SIP profiles are now required regardless of a SIP trunk's security.
- **SIP Access Exceptions Can Include Subnets.** You can now include or exclude entire subnets of hosts when configuring your SIP access for InformaCast. If you have a lot of devices to add, specifying a subnet instead of adding an exception for each device can save you time.
- **Send Silent RTP Packets with the DialCast IVR.** A new checkbox on the Broadcast Parameters page, **Send Silence with DialCast IVR**, allows the DialCast Interactive Voice Response (IVR) to send RTP packets that contain silence to the caller after the IVR has finished interacting with it. A

DialCast call consists of one audio stream that contains the audio sent by the calling party to InformaCast, and another that contains the audio sent by the DialCast IVR. Sending silent RTP packets is necessary when the party making a DialCast call needs to receive audio during the entire call in order to prevent it from terminating the call due to perceived inactivity.

- **Enhance Security with One-time Passwords.** One-time passwords enhance the security of the HTTP communication between InformaCast and Unified Communications Manager by pairing your device's name with an ever-changing password instead of static application user credentials.
- **Improved Phones' Displays.** Many models of Cisco IP phones received updates to their display capabilities, improving the legibility of broadcasts. These updates included automatic text resizing, an enlarged display, and improved bit depth.
- **Newly Supported Phones.** InformaCast now supports the following Cisco IP phone models: 7832, and 8832.
- **New Upgrade File for pre-12.0.1 Versions of InformaCast.** A new file (CiscoPagingServer_UpgradeFrom115To-12.1.1.iso) has been added to the upgrade process. Depending on the version of InformaCast Virtual Appliance from which you are starting, you will install different files:
  - For 8.3 or 8.4 versions to the current version, you will install three package files and attach one ISO file (CiscoPagingServer_8.5.1.deb, CiscoPagingServer_9.1.1.deb, CiscoPagingServer_11.5.2.deb, and CiscoPagingServer_UpgradeFrom115To-12.1.1.iso)
  - For 8.5.1, 9.0.1, or 9.0.2 to the current version, you will install two package files and attach one ISO file (CiscoPagingServer_9.1.1.deb, CiscoPagingServer_11.5.2.deb, CiscoPagingServer_UpgradeFrom115To-12.1.1.iso)
  - For 9.1.1, 11.0.1, 11.0.2, or 11.0.5 to the current version, you will install one package file and attach one ISO file (CiscoPagingServer_11.5.2.deb and CiscoPagingServer_UpgradeFrom115To-12.1.1.iso)
  - For 11.5.1 or 11.5.2 to the current version, you will attach one ISO file (CiscoPagingServer_UpgradeFrom115To-12.1.1.iso)

  InformaCast Virtual Appliance 8.5.1, 9.1.1, and 11.5.1/2 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, upgrade to 11.5.2, and then continue to upgrade to 12.1.1. 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, upgrade to 11.5.2, and then continue to upgrade to 12.1.1. For 9.1.1, 11.0.1, 11.0.2, and 11.0.5 versions of the Virtual Appliance, you must upgrade to 11.5.2 and then continue to upgrade to 12.1.1. For 11.5.1 and 11.5.2 versions of the Virtual Appliance, you can upgrade directly to 12.1.1.

  If you're already using InformaCast 12.0.1 or later, ignore this note; your upgrade process involves fewer steps and files.

Resolved Issues

- **Updated Certificates Command.** The **regenerate-certificates** command was not updating all of InformaCast's system certificates in previous versions. This has been corrected.
- **Fixed Webmin Communication.** If you changed InformaCast's host name through Webmin, the DNS domain name would not be properly updated. This has been corrected.

- **Performed Various Security Updates.** InformaCast's security was improved in the following ways:
  - OpenSSL was upgraded to correct several security advisories: CVE-2018-0739, CVE-2018-0733, and CVE-2017-3738.
  - Nessus was improved to correct two vulnerabilities: non-FIPS cipher CAMELLIA and/or issue 83875 (weak DH cipher).

Announcement

Streamlined Support for Unified Communications Manager. InformaCast no longer supports Unified Communications Manager 9.x due to its "end of software maintenance" status with Cisco (see https://www.cisco.com/c/en/us/products/unified-communications/unified-communications-manager-callmanager/eos-eol-notice-listing.html).

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 12.0.2

The following information pertains to InformaCast 12.0.2.

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, 11.5.1, and 12.0.1.

New Features

- **New Upgrade Process for InformaCast 12.0.2.** When upgrading from InformaCast 12.0.1 to 12.0.2, you will follow an easier process that involves fewer steps and files. Due to InformaCast's two-partition platform (comprised of one active partition and one inactive partition), you can move between versions of InformaCast easily and preserve the previous version of InformaCast in case of conflict.
- **New Upgrade File for pre-12.0.1 Versions of InformaCast.** A new file (CiscoPagingServer_UpgradeFrom115To-12.0.2.iso) has been added to the upgrade process. Depending on the version of InformaCast Virtual Appliance from which you are starting, you will install different files:
  - For 8.3 or 8.4 versions to the current version, you will install three package files and attach one ISO file (CiscoPagingServer_8.5.1.deb, CiscoPagingServer_9.1.1.deb, CiscoPagingServer_11.5.2.deb, and CiscoPagingServer_UpgradeFrom115To-12.0.2.iso)
  - For 8.5.1, 9.0.1, or 9.0.2 to the current version, you will install two package files and attach one ISO file (CiscoPagingServer_9.1.1.deb, CiscoPagingServer_11.5.2.deb, CiscoPagingServer_UpgradeFrom115To-12.0.2.iso)
  - For 9.1.1, 11.0.1, 11.0.2, or 11.0.5 to the current version, you will install one package file and attach one ISO file (CiscoPagingServer_11.5.2.deb and CiscoPagingServer_UpgradeFrom115To-12.0.2.iso)

- For 11.5.1 or 11.5.2 to the current version, you will attach one ISO file (CiscoPagingServer_UpgradeFrom115To-12.0.2.iso)

InformaCast Virtual Appliance 8.5.1, 9.1.1, and 11.5.1/2 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, upgrade to 11.5.2, and then continue to upgrade to 12.0.2. 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, upgrade to 11.5.2, and then continue to upgrade to 12.0.2. For 9.1.1, 11.0.1, 11.0.2, and 11.0.5 versions of the Virtual Appliance, you must upgrade to 11.5.2 and then continue to upgrade to 12.0.2. For 11.5.1 and 11.5.2 versions of the Virtual Appliance, you can upgrade directly to 12.0.2.

Resolved Issues

- **Signed Certificate Error During Upgrades.** When upgrading from pre-12.0.1 versions of InformaCast to InformaCast 12.0.1, customers with signed certificates that contained certain characters, (e.g. spaces or asterisks) encountered an error and couldn't finish their upgrades. This error has been resolved. Upgrades using 12.0.2 will not encounter this issue.
- **IP Address Length Stopped InformaCast from Starting.** If an InformaCast server's IP address was less than nine characters long (e.g. 10.1.2.3), InformaCast would not start. This issue has been resolved.
- **Large Databases Caused Upgrades to Fail.** When upgrading from pre-12.0.1 versions of InformaCast to InformaCast 12.0.1, customers with more than 2,147,482,647 records in their database experienced upgrade failures. This issue has been resolved.
- **Corrupted Certificate File Broke Communication Between InformaCast and Unified Communications Manager.** InformaCast stores Unified Communications Manager certificates in the CUCM.bcf file. Occasionally, that file was being written to by two or more different InformaCast components simultaneously, which was causing the file to become corrupted and breaking the communication between InformaCast and Unified Communications Manager's AXL service. A change was made to ensure that the certificate file is accessed by only one InformaCast component at a time, resolving the issue.
- **Missing Font Set Resulted in Poor IP Phone Text Quality.** A font that InformaCast uses to render text messages on IP phones was inadvertently removed from InformaCast 12.0.1. InformaCast fell back on a different font set, which resulted in poor text quality. The original font set is included once again and the quality of the IP phone text messages is the same as that of InformaCast 11.5.1.

Announcement

Streamlined Support for Unified Communications Manager. Releases of InformaCast subsequent to 12.0.2 will not support Unified Communications Manager 9.x due to its end of software maintenance status with Cisco.

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 12.0.1

The following information pertains to InformaCast 12.0.1.

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, 11.5.1, and 12.0.1.

New Features

- **New Wizard Aids in InformaCast Setup on Unified Communications Manager.** On the 11.5.1 su3 and 12.0.1 versions of Unified Communications Manager, you now have access to the Emergency Notifications Paging wizard, which enables IP paging and emergency alerting through the Cisco Unified Communications Manager deployment. Once complete, you will have a 90-day trial of InformaCast Advanced Notification including a panic button added to phones to protect your employees and emergency call alerting to immediately notify your safety team whenever an emergency number is dialed.
- **Trustworthy Release Process.** Previous to this release, Singlewire prohibited, but did not prevent, installation of third-party software on the InformaCast Virtual Appliance. As of this release, all future releases of the InformaCast Virtual Appliance are cryptographically signed; the Virtual Appliance will verify that new software originated authentically from Singlewire before loading or starting it. In combination with the use of strong administrator passwords, this feature increases the security and reliability of the Virtual Appliance. The firewall settings for the Virtual Appliance were not affected by this change.
- **Expanded and Improved Backup Process.** The Virtual Appliance's backup process now includes the following items (if present): the InformaCast database, audio recorded through phones, uploaded audio files and icons, plugin files, configuration data, phone display assets, PushToTalk's configuration, all certificates, and SSH server keys. Backups are pushed from InformaCast onto an SFTP server of your choice (currently, only OpenSSH servers are supported by Singlewire, although other servers may work), and all communication between InformaCast and your SFTP server is encrypted and secured with your security passphrase. In addition, backup images are smaller than previous versions of InformaCast due to increased efficiency.
- **New Rules for Encrypted Handling of Data in Motion.** InformaCast's encryption rule changes include the addition of Federal Information Processing Standard (FIPS) 140-validated cryptographic modules. These modules provide a new set of rules for how InformaCast makes and receives connections over TLS and SSL. InformaCast always uses these approved cryptographic modules, there is no ability to turn them (or FIPS mode) off, or replace these modules with others. These rule changes also allow you to define cryptographic trust with other systems with which InformaCast communicates by configuring a setting for SSL certificates to be automatically or manually imported into InformaCast's trust store for each TLS or SSL connection.
- **Newly Supported VMware Version.** InformaCast 12.0.1 now supports VMware 6.5.
- **New VMware Management Tools.** InformaCast now uses Open VM Tools, "a set of services and modules that enable several features in VMware products for better management of, and seamless user interactions with, guests."[2] Open VM Tools offers the same services as the previously

2. https://github.com/vmware/open-vm-tools

used VMware Tools, and simplifies your management because you no longer have to manage these tools' upgrades separately in vSphere: Open VM Tools upgrades are nearly transparent to you, occurring only during InformaCast upgrades.

- **New CTI Call Detail Records.** InformaCast now generates CTI call detail records. Previous versions of InformaCast only collected call detail records for SIP calls. InformaCast now collects CTI call data, such as route actions and broadcast trigger information, as it interacts with a CTI call. 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 Support Community.** Singlewire has a new Support Community where everything is at your fingertips—software downloads, contract information, user guides, knowledge articles, forums, and more. Most relevant to this help system is that all troubleshooting has been relocated to the Support Community. Take a moment and look around, and if you're having trouble finding what you need, let us know. Our team is always happy to help!
- **New Upgrade File.** A new file (CiscoPagingServer_UpgradeFrom115To-12.0.1.iso) has been added to the upgrade process. Depending on the version of InformaCast Virtual Appliance from which you are starting, you will install different files:
  - For 8.3 or 8.4 versions to the current version, you will install three package files and attach one ISO file (CiscoPagingServer_8.5.1.deb, CiscoPagingServer_9.1.1.deb, CiscoPagingServer_11.5.2.deb, and CiscoPagingServer_UpgradeFrom115To-12.0.1.iso)
  - For 8.5.1, 9.0.1, or 9.0.2 to the current version, you will install two package files and attach one ISO file (CiscoPagingServer_9.1.1.deb, CiscoPagingServer_11.5.2.deb, CiscoPagingServer_UpgradeFrom115To-12.0.1.iso)
  - For 9.1.1, 11.0.1, 11.0.2, or 11.0.5 to the current version, you will install one package file and attach one ISO file (CiscoPagingServer_11.5.2.deb and CiscoPagingServer_UpgradeFrom115To-12.0.1.iso)
  - For 11.5.1 or 11.5.2 to the current version, you will attach one ISO file (CiscoPagingServer_UpgradeFrom115To-12.0.1.iso)

  InformaCast Virtual Appliance 8.5.1, 9.1.1, and 11.5.1/2 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, upgrade to 11.5.2, and then continue to upgrade to 12.0.1. 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, upgrade to 11.5.2, and then continue to upgrade to 12.0.1. For 9.1.1, 11.0.1, 11.0.2, and 11.0.5 versions of the Virtual Appliance, you must upgrade to 11.5.2 and then continue to upgrade to 12.0.1. For 11.5.1 and 11.5.2 versions of the Virtual Appliance, you can upgrade directly to 12.0.1.

Known Issues

- **Can't Initiate or Receive TLS or SSL Sessions with a Peer that Supports Only 3DES Key Exchange.** The InformaCast FIPS 140-2 verified modules will only negotiate an SSL session with a peer that supports AES cipher suites. Negotiation with peers that support only 3DES will fail. All shipping versions of Cisco Unified Communications Manager support AES cipher suites. Windows servers released subsequent to Windows 2003 R2 support AES cipher suites. If you encounter this issue, remove TLS from the connection or delay upgrading to 12.0.1. This issue will be addressed in a future release of InformaCast.

- **Further Specification When Entering Credentials.** When using the Emergency Notifications Paging wizard, you are prompted for InformaCast's IP address in Step 3. You must enter an IP address. If you enter a fully qualified domain name or hostname instead, the wizard will fail (refer to issue CSCvf58052). For more information on recovering from a wizard failure, refer to this article. For further assistance, contact Cisco TAC.

Announcements

Streamlined Support for Unified Communications Manager. Releases of InformaCast subsequent to 12.0.1 will not support Unified Communications Manager 9.x due to its "end of life" status with Cisco.

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 11.5.2

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 it 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 C**all 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 https://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 https://www.cisco.com/c/en/us/products/unified-communications/unified-communications-manager-callmanager/eos-eol-notice-listing.html)
- **New Standardized Name.** Coming soon: Cisco Unified Communications Manager will no longer be abbreviated as CUCM and will instead appear as Unified Communications Manager after its first mention as Cisco Unified Communications Manager. This will affect all documentation as well as InformaCast's user interface. Stay tuned.

Resolved Caveats

CDETs ID	Title
CSCuu82554	June 2015 SSL Vulnerabilities

InformaCast 11.0.1.a

Compatibility

InformaCast is compatible with the following versions of Cisco Unified Communications Manager server (including Business Edition 6000): 8.5.1, 8.6.2, 9.0.1, 9.1.2, 10.0.1, 10.5.2, or 11.0.1.

Updated Information

9.0.1 and 9.0.2 Upgrade Information. References to upgrading from 9.0.1 or 9.0.2 to the current version had been inadvertently omitted. Follow the same steps as noted for upgrading from 8.5.1, installing two package files (CiscoPagingServer_9.1.1.deb and CiscoPagingServer_11.0.1.deb).

For 9.0.1 or 9.0.2 versions of the Virtual Appliance, you must upgrade to 9.1.1, reboot the Virtual Appliance, and then continue to upgrade to 11.0.1.

InformaCast 11.0.1

Compatibility

InformaCast is compatible with the following versions of Cisco Unified Communications Manager server (including Business Edition 6000): 8.5.1, 8.6.2, 9.0.1, 9.1.2, 10.0.1, 10.5.2, or 11.0.1.

New Features

- **Newly Supported Phones.** InformaCast now supports the 7811, 8845, and 8865 Cisco IP phone models.
- **Added UTF-8 Support.** The following pages in InformaCast 11.0.1 now support UTF-8 character encoding: Edit Recipient Groups and Delete Recipient Group. The View Recipients dialog box (accessible through the **View** button on the Edit Recipient Group page) also offers UTF-8 support.
- **New Upgrade File.** A new file (CiscoPagingServer_11.0.1.deb) has been added to the upgrade process. Depending on the version of InformaCast Virtual Appliance from which you are starting, you will install different package files:

- For 8.3 or 8.4 versions to the current version, you will install three package files (CiscoPagingServer_8.5.1.deb, CiscoPagingServer_9.1.1.deb, and CiscoPagingServer_11.0.1.deb)
- For 8.5.1, 9.0.1, or 9.0.2 to the current version, you will install two package files (CiscoPagingServer_9.1.1.deb and CiscoPagingServer_11.0.1.deb)
- For 9.1.1 to the current version, you will install one package file (CiscoPagingServer_11.0.1.deb)

InformaCast Virtual Appliance 8.5.1 and 9.1.1 are waypoints in the upgrade process. For 8.3 through 8.4 versions of the Virtual Appliance, you must upgrade to 8.5.1, reboot the Virtual Appliance, upgrade to 9.1.1, reboot the Virtual Appliance, and then continue to upgrade to 11.0.1. For 8.5.1, 9.0.1, or 9.0.2 versions of the Virtual Appliance, you must upgrade to 9.1.1, reboot the Virtual Appliance, and then continue to upgrade to 11.0.1.

Resolved Issues

DSA Private Keys and the Upgrade Process. Some versions of Chrome, Firefox, and Internet Explorer reject connections to websites with DSA private keys, and some older versions of InformaCast defaulted to using DSA keys for self-signed certificates. If you are using an older version of InformaCast with DSA private keys and you upgrade the 11.0.1, the upgrade process will automatically regenerate your DSA private key as an RSA key; it will not automatically regenerate DSA keys with signed certificates. You must regenerate them manually.

Announcement

- **Streamlined Support for CUCM.** Releases of InformaCast subsequent to 11.0.1 will not support CUCM 8.5 or 8.6 due to its "end of maintenance" status with Cisco (see https://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 the 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, and should be handled by your network administrator.

Resolved Issues

- **Fixed DN Retrieval from AXL (Mantis ID #4154).** Under certain circumstances (e.g. with CUCM 6.1.3, if there were more than 26,300 DNs, or if there were multiple DNs per phone), InformaCast was not always retrieving all the necessary DNs from AXL when building the phone cache. This issue has been resolved.
- **Fixed Broadcast Jitter (Mantis ID #4300).** Previously, sending as-available messages to a large number of devices could result in degraded audio quality (jitter). This issue has been resolved.
- **Fixed Webmin Access through Internet Explorer (Mantis ID #4066).** Previously, accessing Webmin through Internet Explorer was prevented due to an out-of-date SSL certificate. This issue has been resolved.
- **Fixed Release Notes; Changed Version Number.** The release notes have been separated into Basic and Advanced categories, which necessitated a version number change from 8.4 to 8.4.a.
- **Fixed Spelling Inconsistencies, Hover Text, and Display Issues.** Many pages received new hover text, standardized hover text, and standardized word spellings to improve overall user experience.

Resolved Caveats

CDETs ID	Title
CSCuh28590	Voice prompt changed for Basic Paging
CSCuh28557	Standardize all tooltips
CSCuh28540	Missing the “please complete...” hover text on the Basic sign-in form
CSCuh28521	Phone license limit warning text incorrectly refers to Adv mode license
CSCuh22651	Webmin - Unable to get beyond the security cert error page with IE

New Caveats

CDETs ID	Title
CSCuh28628	Provide a more user-friendly interface/functions on the Start Page
CSCuh28601	IP endpoints labeled as required but isn’t on Basic sign-in form
CSCuh28499	Learn More about InformaCast links don't hold focus
CSCuh30592	change-ip-address script for backed up databases
CSCuh30601	Phone caches persists after transitioning back to Basic mode

InformaCast 8.3.a

Compatibility

InformaCast Basic Paging is compatible with the following versions of Cisco Unified Communications Manager server (including Business Edition 6000): 8.5, 8.6, 9.0, and 9.1

Known Issues

- **Updated Graphics.** Black and white graphics in the documentation were changed to color on request.
- **Incorrect Error Message.** In Basic Paging, when you exceed the limit of the number of phones to which you can broadcast in a recipient group, the error message you receive is wrong (i.e. “There are more phones associated with your CUCM server than your InformaCast license key supports. Broadcast messages will be limited to 50 total phones. The number of phones in the list that will participate in a broadcast depends on how many other phones have been broadcast participants. For example, if 50 other phones have been broadcast participants, then no phones in the list can participate. Otherwise, either all or some of the phones can participate. Please contact Singlewire at www.singlewire.com for support or to upgrade your key.”). In actuality, each recipient group is limited to 50 phones, and you can send to another separate recipient group of 50 phones. This differs from Advanced Notification where if you exceed your license limit of recipients in one recipient group, you will be unable to send to another separate group of additional phones.

InformaCast 8.3

Compatibility

InformaCast Basic Paging is compatible with the following versions of Cisco Unified Communications Manager server (including Business Edition 6000): 8.5, 8.6, 9.0, and 9.1

New Features

- **New Functionality.** InformaCast 8.3 now comes in two new versions: Basic and Advanced. Basic functionality includes live paging only. Advanced functionality contains the full-featured version of InformaCast: the ability to send a number of different types of broadcasts (e.g. live audio, pre-recorded audio, pre-recorded audio and text, etc.) using your Cisco IP phone's interface and/or InformaCast's web interface, interact with InformaCast's plugins (e.g. conduct conference calls, trigger contact closures, post to Facebook and Twitter, send broadcasts to email addresses, etc.), customize scripts that can be attached to broadcasts, and receive confirmation when broadcasts are sent, among other features. Basic functionality comes automatically installed on the Cisco Unified Communications Manager Business Edition 6000, and you have the option to upgrade to Advanced functionality.
- **New InformaCast Licensing.** Advanced InformaCast can be obtained through a limited, free trial, purchased as a subscription service, or purchased outright (perpetual) with a maintenance contract (which is how InformaCast has traditionally been purchased). The InformaCast trial and subscription licenses allow you to try InformaCast's full functionality without committing to a long-term contract (subscription) or without a contract at all (free, limited-time trial).
- **New Backup Location.** The default backup location setting in previous versions of InformaCast could produce unusable backups. As such, a new backup location was created: /usr/local/singlewire/InformaCast/backup. You should examine the InformaCast backup location that you are currently using and consider changing it to the new recommended location.
- **New License Parameter.** The MaxVersion parameter, a new license parameter, must be present in all 8.3 and later releases of InformaCast and its number must match or be greater than your version of InformaCast in order for you to access any of InformaCast's functionality.
- **Disk Performance Increase.** VMware and storage vendors recommend that virtual machines align on 64Kb boundaries to minimize disk reads, and InformaCast's partitions are now in line with this recommendation. Fewer reads with the same result means better performance, and if you are running VA/EX on SAN disks, you may notice lower IOPS (I/O operations per second) as a result of this change.

Known Issues

- **Unable to Access Webmin with Internet Explorer 9 After Installing Microsoft Security Update KB2661254.** If you've installed Microsoft Security Update KB2661254 and use Internet Explorer 9 to access Webmin (https://<InformaCast Server IP Address:10000), the site will fail. To avoid this issue, use Google, Chrome, or Firefox to access Webmin or use the solutions described by Microsoft at http://support.microsoft.com/?kbid=2661254.
- **InformaCast Not Functioning Correctly After Changing its IP Address in Advanced Notification and Switching Back to Basic Paging.** Changing InformaCast's IP address while using Advanced Notification and switching back to Basic Paging can make broadcasts unavailable to phones. There is currently a warning that occurs when executing the script that changes InformaCast's IP address; users can elect to abort or continue.

- **Phone Cache Becomes Unavailable with a License Change.** Whenever you change InformaCast's license or add/update/delete a cluster, "Default configuration Not Connected" appears for the **Communications Manager Versions** field on the Overview page. If either the license or clusters change, the phone cache must be rebuilt to reflect those changes. The phone cache is automatically rebuilt every hour, but if you want it completed sooner than that, you can click the **Update** button on the Edit Recipient Groups page to discover current IP phone info from CUCM. Once this is done, the CUCM information appears correctly on the Overview page.

Glossary

In order to fully understand your InformaCast environment, you should familiarize yourself with the terms in this section.

API

Application Programming Interface. A language and message format used by an application program to communicate with the operating system or some other control program such as a database management system (DBMS) or communications protocol.

Application 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 11-8.

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 11-5.

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 11-5.
- 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 "Subnet Mask" on page 11-9.

IP Phone

See "Cisco IP Phone" on page 11-2.

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 11-10.

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 11-3.

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 Landing Page

The Singlewire landing 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 11-6. 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 11-7.

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>/webmin.

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

W