



## InformaCast Appliance Basic Paging<sup>®</sup>

Version 14.4.2

Installation and User Guide for a Cisco<sup>®</sup> Unified Communications Manager  
Environment

January 19, 2022

**Cisco Systems, Inc.**

[www.cisco.com](http://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](http://www.cisco.com/go/offices).

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

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

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

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

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

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

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

© 2022 Cisco Systems, Inc. All rights reserved.

© 2022 Singlewire. All rights reserved.

InformaCast is a trademark of Singlewire Software.

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

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

Last Updated: January 19, 2022



- InformaCast Basic Paging Overview ..... 1-1
  - InformaCast Basic Paging ..... 1-1
  - PushToTalk ..... 1-1
  - The Appliance ..... 1-1
  - The Environment ..... 1-2
  - Intended Audience ..... 1-2
  - User Guide Standards ..... 1-2
  - Prerequisites ..... 1-3
  - Hardware Requirements ..... 1-4
  - Port Configuration ..... 1-5
  - DSCP Quality of Service Policies ..... 1-6
  - Licensing Information ..... 1-7
  - InformaCast Appliance Interface Orientation ..... 1-8
  - Interface Permissions ..... 1-14
  - Technical Support ..... 1-15
- Installation ..... 2-1
  - Prepare Your Multicast Environment ..... 2-1
  - Deploy InformaCast ..... 2-17
  - Set the Initial Configuration ..... 2-31
- Interface Access ..... 3-1
  - Access the InformaCast Appliance Landing Page ..... 3-1
  - Log into InformaCast for the First Time ..... 3-3
  - Log into InformaCast ..... 3-9
  - Log into PushToTalk ..... 3-11
  - Log into the Control Center ..... 3-12
  - Log into Webmin ..... 3-14
  - Log into the Command-line Interface ..... 3-16
- License Key Management ..... 4-1
  - View Your License Key ..... 4-2
  - Upload a New License ..... 4-2
- InformaCast Summary and Diagnostics ..... 5-1
- Log Directory ..... 6-1
- Broadcast Parameters Management ..... 7-1
- Configuration Pathways ..... 8-1

Broadcast to Cisco IP Phones for Unified CM .....	8-1
Secure CTI Communication .....	8-2
Validate Certificates for Secure, Outbound Communication .....	8-2
Send a Preconfigured Broadcast .....	8-3
Integrate Cisco Unified CM .....	8-3
Configure Host Trust .....	8-48
Manage CTI Security .....	8-49
Manage SIP Functionality .....	8-56
Recipient Management .....	9-1
Manage IP Phones .....	9-1
Manage Recipient Groups .....	9-17
Manage Recipient Administration .....	9-47
Broadcast Management .....	10-1
Manage Messages .....	10-1
Manage DialCasts .....	10-1
Manage Call Detail Records .....	10-7
Administration .....	11-1
Change the Application Administrator's Password .....	11-1
Configure Session Timeouts .....	11-3
Manage Login Banners .....	11-4
Manage InformaCast Backups .....	11-11
Advanced InformaCast Access .....	12-1
Note the Differences .....	12-1
Upgrade InformaCast .....	12-3
System Management .....	13-1
Manage the InformaCast Appliance's Actions .....	13-6
Test the InformaCast Appliance's Connectivity .....	13-21
Show Multicast Statistics .....	13-22
Manage SNMP Monitoring .....	13-23
Show the InformaCast Appliance's Network Configuration .....	13-36
Change the InformaCast Appliance's IP Address .....	13-37
Change the InformaCast Appliance's Hostname .....	13-41
Restart the Network .....	13-43
Set the System Time .....	13-43
Set the IGMP Version .....	13-49
Display the Current State of Your Firewall .....	13-51
Capture InformaCast Appliance Network Traffic .....	13-53
Display System Health Information .....	13-54
Access the InformaCast Appliance's Logs .....	13-62



Collect the InformaCast Appliance's Logs .....	13-67
Redact IP Addresses in Logs .....	13-72
Display InformaCast's Phone Cache .....	13-74
Send Logs to a Local Server .....	13-75
Display InformaCast's Logging Configuration .....	13-80
Show Technical Support Information .....	13-82
Enable the Singlewire Support Account .....	13-84
Display Your Consent Token .....	13-88
Display a List of Processes Running on the InformaCast Appliance ..	13-90
Show Monit Status .....	13-92
Show the InformaCast Appliance's Version .....	13-94
Show the Appliance Type .....	13-95
Show the BIOS Version .....	13-96
Change the InformaCast Appliance's Password .....	13-98
Manage Password Recovery for the InformaCast Appliance .....	13-101
Change the Security Passphrase .....	13-114
Set Allowed SSL Protocols .....	13-117
Display Remote SSL Certificates .....	13-121
Import a Signed SSL Certificate to InformaCast's SIP Certificate Store	13-122
Manage Trust Certificates .....	13-124
Upgrade InformaCast Appliance .....	13-139
Switch Virtual Appliance Versions .....	13-179
Return the InformaCast Appliance to its Original System State .....	13-180
Release Notes .....	14-1
InformaCast 14.4.2 .....	14-1
InformaCast 14.4.1 .....	14-2
InformaCast 14.2.1 .....	14-4
InformaCast 14.0.1 .....	14-5
InformaCast 12.22.2 .....	14-7
InformaCast 12.20.1 .....	14-8
InformaCast 12.19.2 .....	14-9
InformaCast 12.19.1 .....	14-10
InformaCast 12.17.1 .....	14-12
InformaCast 12.15.1 .....	14-14
InformaCast 12.13.1 .....	14-15
InformaCast 12.11.1 .....	14-16
InformaCast 12.5.1 .....	14-18
InformaCast 12.1.1 .....	14-20
InformaCast 12.0.2 .....	14-22
InformaCast 12.0.1 .....	14-23

InformaCast 11.5.2	14-26
InformaCast 11.5.1	14-26
InformaCast 11.0.5	14-28
InformaCast 11.0.2	14-30
InformaCast 11.0.1.a	14-31
InformaCast 11.0.1	14-31
InformaCast 9.1.1	14-33
InformaCast 9.0.2	14-34
InformaCast 9.0.1	14-35
InformaCast 8.5.1	14-37
InformaCast 8.4.a	14-37
InformaCast 8.3.a	14-39
InformaCast 8.3	14-40
Glossary	15-1
Index	16-1



# InformaCast Basic Paging Overview

InformaCast Basic Paging is Singlewire’s bundled package that contains the InformaCast application, the PushToTalk application, and a server.

## InformaCast Basic Paging

InformaCast Basic Paging is Singlewire Software’s bundled package for virtualized environments. It contains a virtual server and InformaCast Basic Paging (InformaCast or Basic InformaCast), which is an IP telephony broadcast application that allows you to send a live audio stream to Cisco IP phones for Unified CM. When these audio streams are sent through InformaCast, they are called broadcasts. In order to receive a broadcast, Cisco IP phones for Unified CM must be included in recipient groups.

InformaCast comes in two versions:

- InformaCast Basic Paging
- InformaCast Advanced Notification

Within this help system, 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.

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/v14.4.2/index.html> for more information.

## PushToTalk

Create groups of Cisco IP phones for Unified CM comprised of accessible directory numbers or InformaCast recipient groups and initiate talk/listen or intercom functionality with the press of a button.



**Note**

---

PushToTalk is only applicable to installations of Advanced InformaCast integrated with Cisco Unified Communications Manager.

---

## The Appliance

Manage server-specific actions for the InformaCast Appliance through Webmin or the command-line interface (CLI), e.g. change the InformaCast Appliance’s hostname, access logs, etc.

By packaging an operating system and these features together, Singlewire removes your burden of maintaining multiple licenses and ensures compatibility between versions by allowing for easy system administration and cross-application configuration.

## The Environment

Before using InformaCast Appliance, you should familiarize yourself with its prerequisites and environment:

- “Intended Audience” on page 1-2
- “User Guide Standards” on page 1-2
- “Prerequisites” on page 1-3
- “Hardware Requirements” on page 1-4
- “Port Configuration” on page 1-5
- “DSCP Quality of Service Policies” on page 1-6
- “Licensing Information” on page 1-7
- “InformaCast Appliance Interface Orientation” on page 1-8
- “Interface Permissions” on page 1-14
- “Technical Support” on page 1-15

## Intended Audience

This user guide is intended for the users and administrators of the InformaCast Appliance and will walk you through the installation, configuration, and administration of the InformaCast application and the InformaCast Appliance on which it runs.

There are two versions of this user guide, depending on your installation environment:

- Basic Paging installations
- Advanced Notification installations

Please make sure you have the right version by looking at the environment type on the cover page as well as at the bottom of every page. The two 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, icon, 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.

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:

- Use of one of the following supported browsers: Firefox 93, Chrome 94, and MS Edge 93
- Compliance with the hardware requirements as defined in this user guide (see “Hardware Requirements” on page 1-4)
- In installations of InformaCast integrated with Cisco Unified Communications Manager, use of one of the following Cisco Unified CM versions (including Business Edition 6000); the following versions are supported: 11.5.1, 12.0.1, 12.5.1, and 14.0.1
- Use of [supported Cisco IP phones for Unified CM](#)
- SNMP enabled on all servers in a Cisco Unified CM cluster
- The AXL service running on at least one server in the Cisco Unified CM 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.
- If you want calls to and from InformaCast to use encrypted media, you must configure SRTP support (see “Enable SIP Call Security” on page 8-88)

You’ll also need to ensure your Cisco Unified CM is running in mixed mode and optionally configure CTI security (see “Manage CTI Security” on page 8-49).

- A static IP address configured on the InformaCast Appliance
- Multicast routing enabled and configured for all network segments between InformaCast and its Cisco IP phones for Unified CM.

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 when viewing the InformaCast application.

## Hardware Requirements

You should deploy InformaCast 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](http://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 [Singlewire's Server Platforms Compatibility Matrix](#).

InformaCast Virtual Appliance requires:

- 4GB of memory
- A dedicated virtual CPU (vCPU); the InformaCast operating system and application are 64-bit, and may only run on 64-bit CPUs.
- 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 Cisco IP phone for Unified CM 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

As of InformaCast 12.19.1, new installations of InformaCast require at least VMware 6.0. If you're upgrading from previous versions of InformaCast, it's recommended that in addition to using VMware 6.0, you also make the following settings changes:

- Change your guest OS type from 32 bit to 64 bit. Within vSphere, navigate to your virtual machine and select **Actions** | **Edit Settings**. Select the **VM Options** tab and expand **General Options**. Select **Other Linux (64-bit)** from the **Guest OS Version** dropdown menu.
- Change the compatibility on your virtual machine to ESXi 6.0 or later. Within vSphere, navigate to your virtual machine and select **Actions** | **Power** | **Power Off**. Then select **Actions** | **Compatibility** | **Upgrade VM Compatibility**. Confirm your upgrade and then select **ESXi 6.0 or later** from the **Compatible with** dropdown menu. Click the **OK** button and power on your virtual machine.

## Port Configuration

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



**Note** This list of ports applies only to the InformaCast 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	<a href="#">RFC 4253</a>	Restrict access to management subnets
80	TCP	Redirect to the secure web interface of the InformaCast Appliance's landing page	<a href="#">RFC 2616</a>	Restrict access to management subnets
123	UDP	Network Time Protocol (NTP)	<a href="#">RFC 9505</a>	Restrict access to time servers
443	TCP	The secure web interface of the InformaCast Appliance's landing page SOAP traffic, regardless of SOAP's security status InformaCast's REST API	<a href="#">RFC 2616</a>	Restrict access to management subnets
1161	UDP	InformaCast SNMP	<a href="#">RFC 1157</a>	Restrict access to management subnets
8081	TCP	InformaCast's non-secure web interface Cisco IP phone for Unified CM authentication and registration traffic SOAP traffic, if insecure SOAP is enabled	<a href="#">RFC 2616</a>	Restrict to IP phone subnets
8444	TCP	Redirect to InformaCast's web interface on <a href="https://&lt;InformaCast Appliance IP Address&gt;/InformaCast">https://&lt;InformaCast Appliance IP Address&gt;/InformaCast</a>	<a href="#">RFC 2616</a>	Restrict access to management subnets and API clients
8463	TCP	Redirect to Control Center's web interface on <a href="https://&lt;InformaCast Appliance IP Address&gt;/ControlCenter">https://&lt;InformaCast Appliance IP Address&gt;/ControlCenter</a>	<a href="#">RFC 2616</a>	Restrict access to management subnets
10000	TCP	Redirect to webmin interface on <a href="https://&lt;InformaCast Appliance IP Address&gt;/webmin">https://&lt;InformaCast Appliance IP Address&gt;/webmin</a>	<a href="#">RFC 2616</a>	Restrict access to management subnets
32068-32468	UDP	InformaCast's inbound RTP streams (inbound calls to CTI ports and inbound SIP)	<a href="#">RFC 3550</a>	Unrestricted access
5060-1	TCP and UDP	InformaCast's SIP	<a href="#">RFC 3261</a>	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 Cisco IP phones for Unified CM	<a href="#">RFC 2616</a>
161	UDP	Cisco Unified Communications Manager SNMP phone data	<a href="#">RFC 1157</a>
427	UDP and TCP	InformaCast SLP	<a href="#">RFC 2608</a>
443	TCP	Secure web interface for Cisco Unified Communications Manager AXL web services	<a href="#">RFC 2616</a>
514	UDP	InformaCast Appliance system health logging	<a href="#">RFC 5424</a>
2748	TCP	Cisco Unified Communications Manager CTI ports/route points	N/A
20480-21080	UDP	Default multicast ports to which InformaCast sends audio	<a href="#">RFC 3550</a>
32068-32468	UDP	InformaCast's outbound RTP streams (outbound calls to CTI ports and outbound SIP)	<a href="#">RFC 3550</a>

## 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

The InformaCast Appliance'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. *InformaCast Basic Paging* functionality includes the ability to send live audio broadcasts to up to 50 Cisco IP phones for Unified CM 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 for Unified CM's interface and/or InformaCast's web interface
- Send broadcasts to a wide variety of recipients, e.g. Cisco IP phones for Unified CM, IP speakers, InformaCast Desktop Notifier instances, email addresses, Twitter and WordPress references, 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 **Buy InformaCast Advanced** or **Try InformaCast Advanced** buttons in InformaCast's left navigational menu 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 **End Advanced Notification Trial** button in InformaCast's left navigational menu. 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. 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 forfeit the rest of your trial period. 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 demonstration license past its expiration date.

**Note**

If you are operating InformaCast on a Communications Manager Business Edition 6000 with an IP address within the range of 172.27.199.1/254 and you decide to buy InformaCast, you will need to either change the IP address used by InformaCast or be prepared to accept a succession of one-year subscription licenses. Contact Singlewire to request an IP address change.

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 have access to Singlewire's Support team and free software upgrades, although perpetual-license customers must purchase an annual maintenance contract to gain this access.

**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—broadcast 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.**

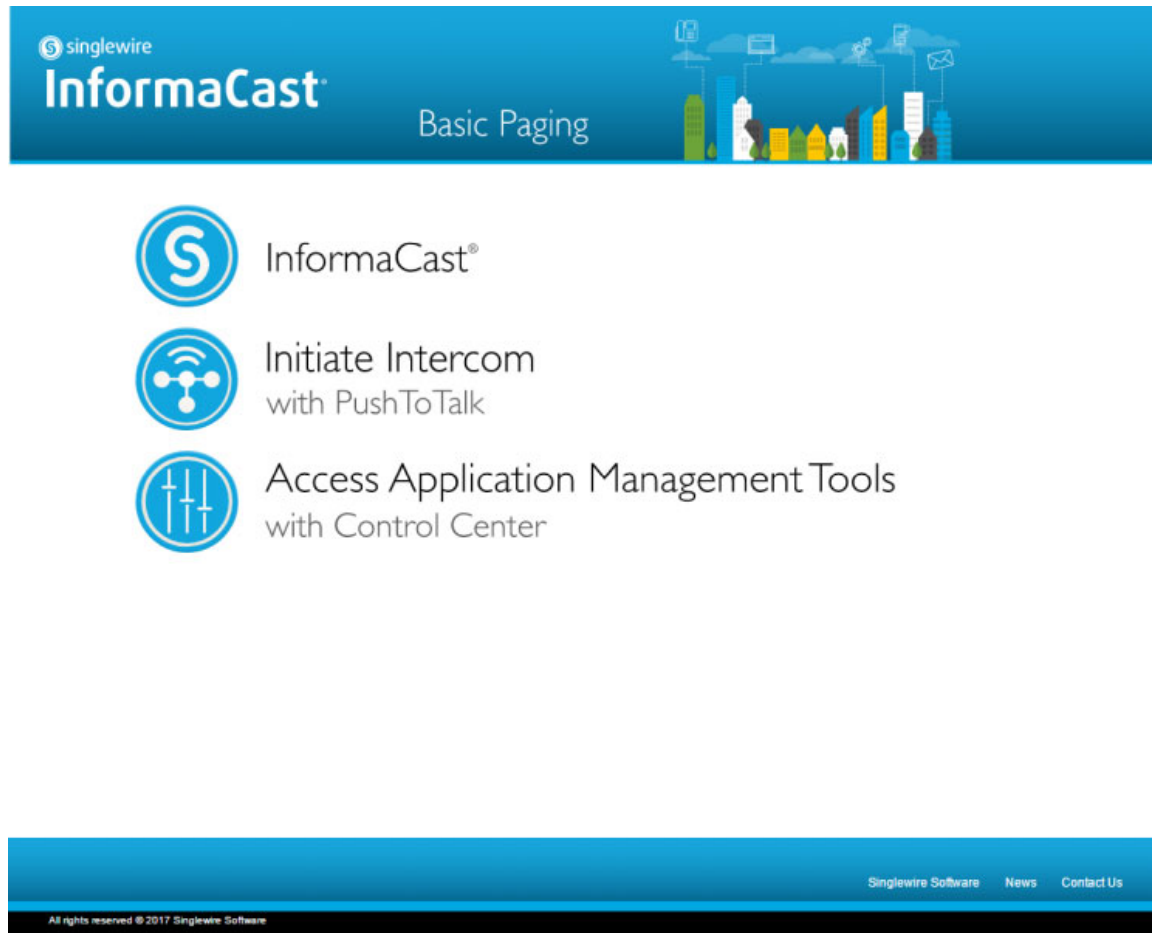
---

## InformaCast Appliance Interface Orientation

The InformaCast Appliance has multiple user interfaces that allow you to control different facets of its administration.

## InformaCast Appliance Landing Page

Accessible through a web browser addressed with the IP address of your InformaCast Appliance, the InformaCast Appliance landing page contains links to InformaCast and the Control Center.



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

## InformaCast's Web Interface

Accessible by clicking **InformaCast** on the InformaCast Appliance landing page, InformaCast's user interface is comprised of a left navigational menu and an administration pane whose contents change with what you're doing. InformaCast allows you to send a live audio stream to Cisco IP phones for Unified CM.

**Dashboard**

**Welcome to InformaCast Basic Paging (Cisco Paging Server)**

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
- Create unlimited recipient groups of 50 phones or less

[Technical Support](#)

[User Guide](#)

**Reach More People and Devices**

Upgrade to InformaCast Advanced and enjoy a full-featured emergency notification solution that allows you to reach an unlimited number of phones as well as a variety of other endpoints, send text and live or pre-recorded audio as messages, add broadcast confirmations, and much more.

Click the Buy button to begin the process of obtaining an InformaCast Advanced license. You can also click the Try button to start your free 60-day InformaCast Advanced trial. If you would like more information, click the Demo button to request a demo.

**InformaCast Advanced**

[BUY](#) [TRY](#) [DEMO](#)

**Features Include:**

- Live audio paging between Cisco IP Phones, with no limit on the number of phones per group
- Integration to existing overhead paging systems
- Text and audio (live or pre-recorded) to Cisco IP Phones and other endpoints
- Audio broadcasts to IP Speakers
- 911/emergency call monitoring/alerting/recording
- Automated weather notifications
- Dynamically-triggered emergency conference calls
- Pre-recorded/scheduled broadcasts(school bells/shift changes)
- Notification to computer desktops (Windows and MacOS) via [InformaCast Desktop Notifier](#)
- Integrate with digital signage solutions and 3rd-party mass notification providers
- Notification and confirmation to mobile devices (Apple, Android, and SMS) with [InformaCast Fusion](#)
- Trigger notification to/from other systems (panic/duress buttons, door locks, lights, etc.)
- And More

**Learn More**

- [InformaCast Details](#)

Three additional buttons, **Try**, **Buy**, and **Demo**, 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.

## PushToTalk's Web Interface

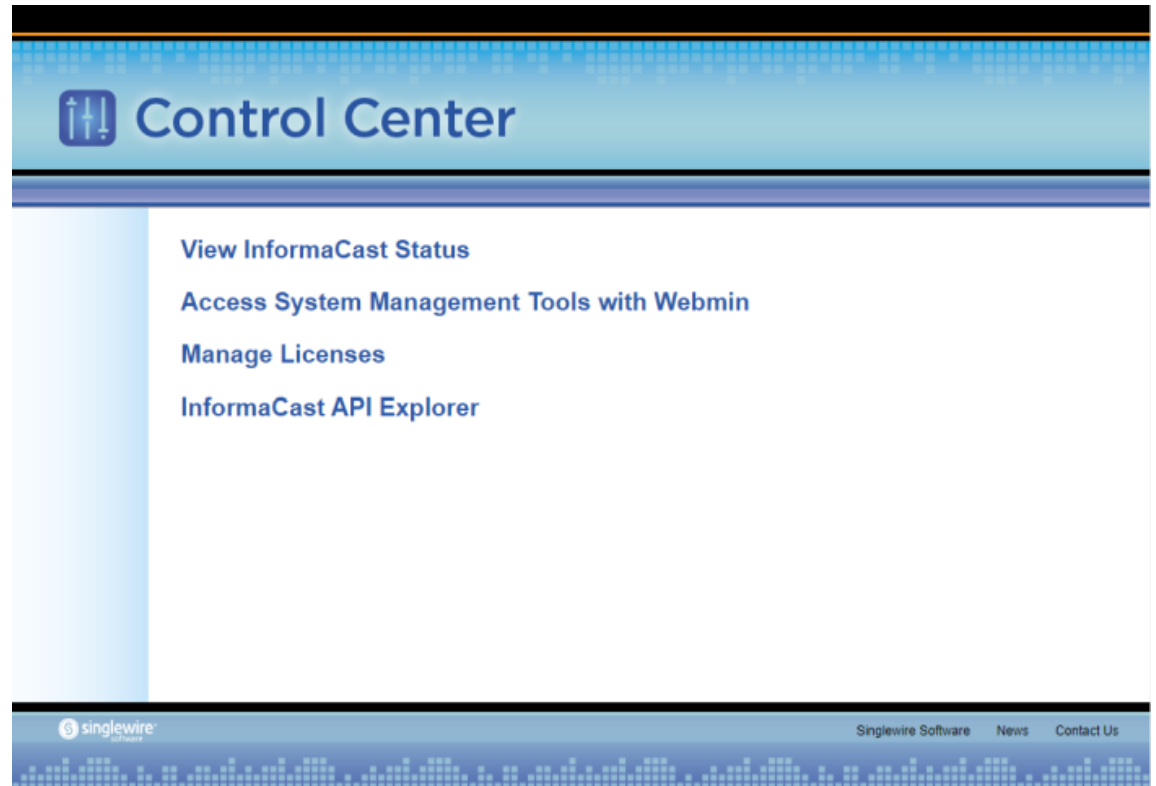
Accessible by clicking **Initiate Intercom with PushToTalk** on the InformaCast Appliance landing page, PushToTalk's user interface is comprised of a left navigational menu and an administration pane whose contents change with what you're doing. PushToTalk is designed to facilitate communication between multiple parties (or on a one-to-one basis) through talk/listen or intercom functionality on supported Cisco IP phones for Unified CM.

**Note**

While visible on the InformaCast Appliance landing page, PushToTalk is not supported by InformaCast Basic Paging. Please [contact Singlewire](#) for an upgrade to Advanced Notification.

## Control Center

Accessible by clicking **Access Application Management Tools** on the InformaCast Appliance landing page, Control Center is designed to be an inclusive destination for application- and system-level accessories.



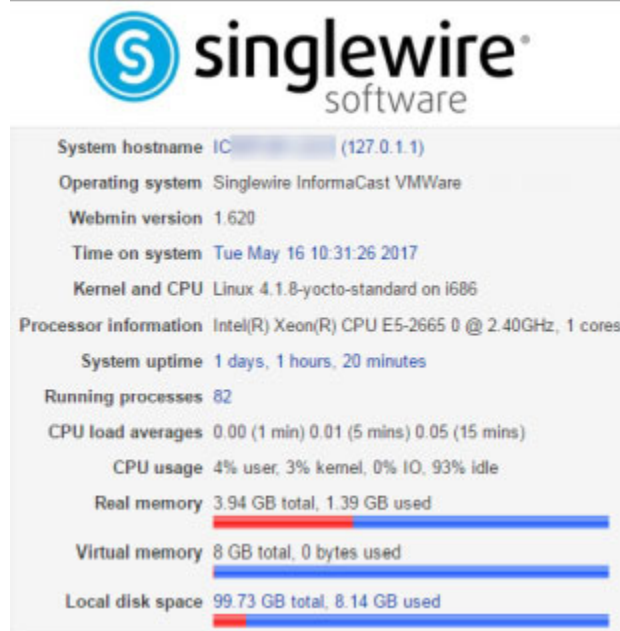
Here, you can access the License Manager to update your Basic license with an Advanced version or access Webmin, the administrative web interface of the underlying operating system of the InformaCast Appliance.

Lastly, if you're interested in InformaCast's API, the InformaCast API Explorer is your window to the operations and resources that the InformaCast API has to offer. In the Explorer, you can craft API requests and review the information the API will provide based on your requests. See [InformaCast's API documentation for more information](#).



## Webmin

Accessible by clicking the **Access System Management Tools with Webmin** link on Control Center's Menu page, Webmin 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.



“System Management” on page 13-1 contains more information on managing the InformaCast Appliance from its Webmin and command-line interfaces.

## Command Line Interface

Accessible through a virtual machine console window, such as vSphere (for virtual InformaCast Appliances only), or over the network through the use of an SSH (Secure Shell) client like [PuTTY](#), 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 InformaCast Appliance's password, restarting the server, assigning a static IP address, and collecting/viewing logs, among others.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun 2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$
```

**Note**

Rudimentary knowledge of bash is required to use the command line interface. If files are to be edited on the InformaCast Appliance 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 InformaCast. 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.

“System Management” on page 13-1 contains more information on managing the InformaCast Appliance from its Webmin and command-line interfaces.

## Keyboard and Monitor

Accessible through a monitor and keyboard, an InformaCast Appliance running as a physical machine has an interface that you can use to perform various administrative actions, such as initially setting InformaCast's configuration, changing the server's password, restarting the InformaCast Appliance or its services, assigning a static IP address, and collecting/viewing logs, among others.

**Note**

The InformaCast Physical Appliance is not available with InformaCast Basic Paging.

## Interface Permissions

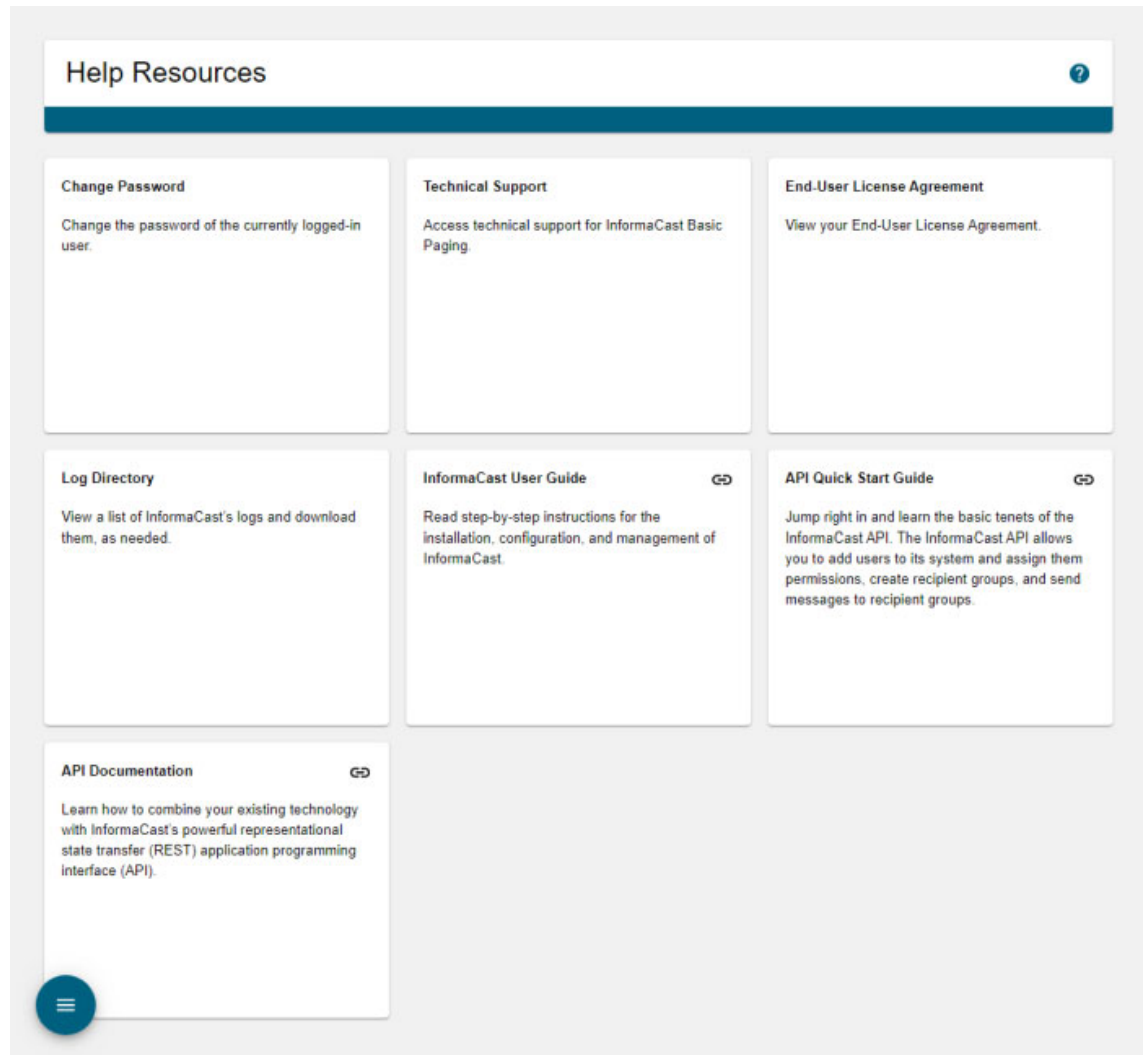
Basic InformaCast is only allowed one user with the highest level of permissions assigned to it. In order to take advantage of multiple users who can be assigned differing levels of permissions, you need Advanced InformaCast, which has a dynamic user interface that changes with your level of permissions.

**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.

## Technical Support

Your first line of support with InformaCast is the Help Resources page, which is accessible by selecting **Help** from the **User** dropdown in the left navigational menu.



On the Help Resources page, you can:

- Change your password
- Access links to Cisco's technical support
- View the End-user License Agreement
- View and download logs of InformaCast's activity

- Access this online help system
- Access an [API quick start guide](#)
- Access the [API's documentation](#)

**Note**

---

If you do not have an active network connection to the internet, not all of the content on InformaCast's Help Resources page will be available.

---

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, or [contact Cisco TAC](#).



# Installation

Installing the InformaCast Appliance involves enabling multicast across your network, installing the appliance as a virtual machine, and setting its initial configuration, e.g. establishing its communication with your network, creating your OS and Application credentials, etc.

The general steps to install InformaCast are:

- “Prepare Your Multicast Environment” on page 2-1
- “Deploy InformaCast” on page 2-17
- “Set the Initial Configuration” on page 2-31

## 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 Cisco IP phones for Unified CM 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
<a href="#">Quick Start Guide</a>	Cisco IP Multicast Quick Start Configuration that provides concise configuration examples
<a href="#">Design Guides</a>	Cisco Design Zone for IP Multicast for access to the AVVID SRND for Multicast Design
<a href="#">Multicast Troubleshooting</a>	Cisco IP Multicast Troubleshooting Guide
<a href="#">IGMP Snooping</a>	Cisco CGMP and IGMP Snooping documentation
<a href="#">GRE Tunnels</a>	Cisco Multicast over a GRE Tunnel (for when a WAN carrier will not route multicast)
<a href="#">Multicast Testing Tool</a>	Singlewire tool to send and receive multicast traffic, which can be used to verify and troubleshoot multicast routing
<a href="#">Protocol Analyzer</a>	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
<a href="#">Support Home</a>	Cisco Troubleshooting Homepage
<a href="#">Cisco Worldwide Contacts</a>	Cisco TAC Telephone Numbers and Additional Resources
<a href="#">Partner Locator</a>	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



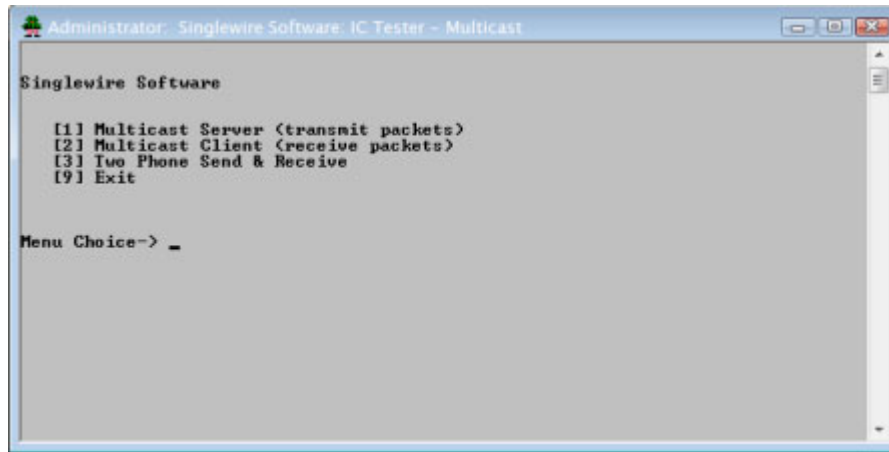
**Note** Typically, you will want to run Options 1 and 2 in tandem: Option 1 on a Windows machine on the same subnet as InformaCast and Option 2 on the location of your recipients, i.e. a PC on the same VLAN as your recipients.

- Option 3 allows the tool to “hijack” two Cisco IP phones for Unified CM: one to receive packets and the other to transmit them

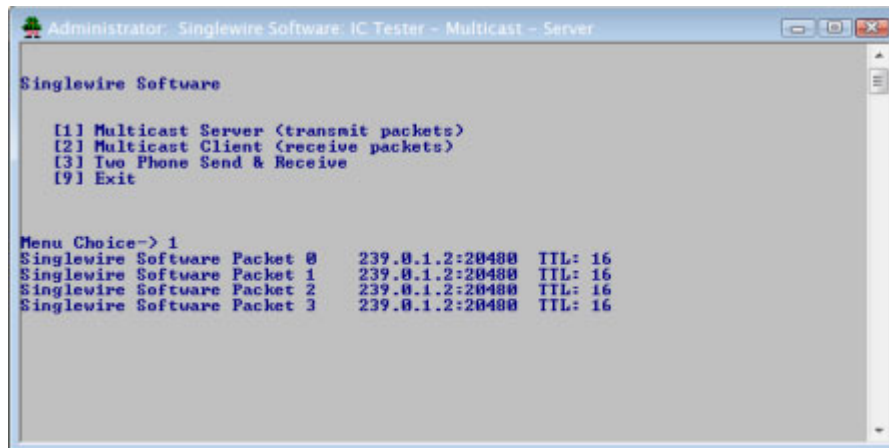
*Use Options 1 and 2*

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 InformaCast Appliance. The IC Tester - Multicast window appears.

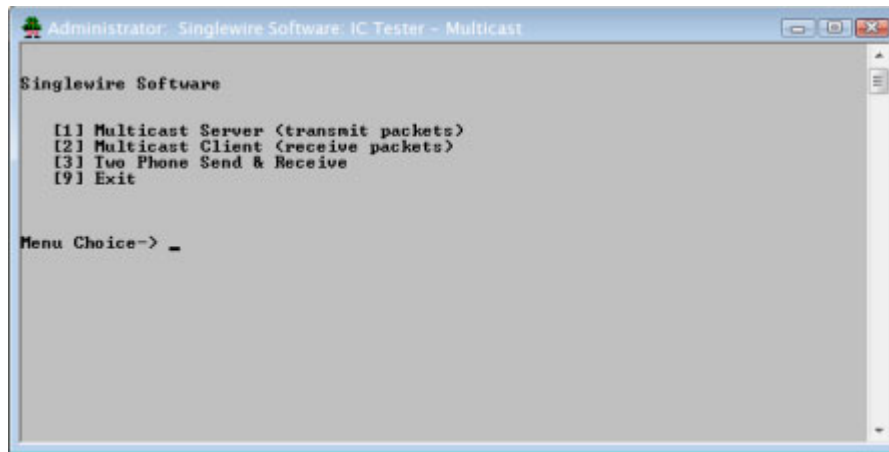


- Step 2** Enter **1** at the **Menu Choice** prompt and press the **Enter** key. The IC Tester - Multicast window refreshes, showing multicast packets being sent across your network.





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



```

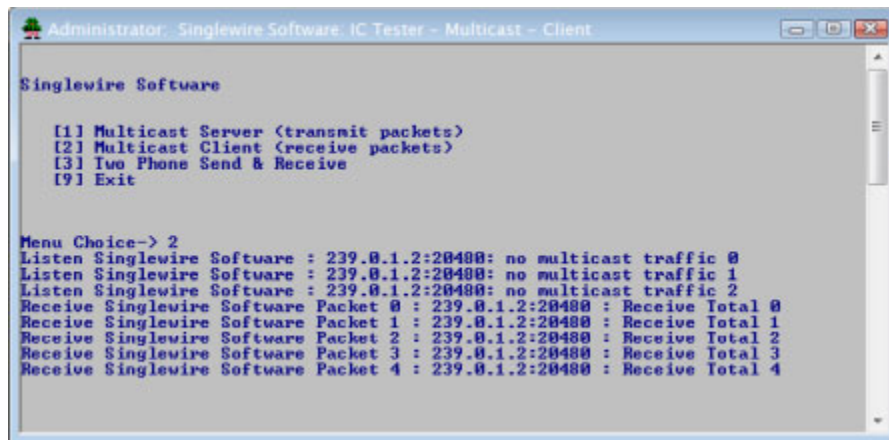
Administrator: Singlewire Software: IC Tester - Multicast

Singlewire Software

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

Menu Choice-> _
  
```

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



```

Administrator: Singlewire Software: IC Tester - Multicast - Client

Singlewire Software

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

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

If you receive a “no multicast traffic” result, you can try Option 3, follow the recommendations in “Review Multicast Configuration” on page 2-6, or see “Multicast” on page 9-1.

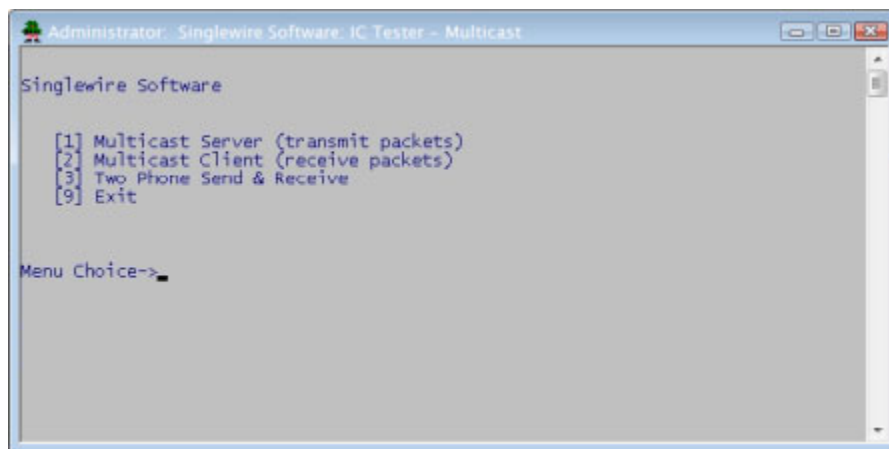
*Use Option 3*

Use the following steps to have the Multicast Testing Tool “hijack” two Cisco IP phones for Unified CM: one to receive packets and the other to transmit them.



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

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



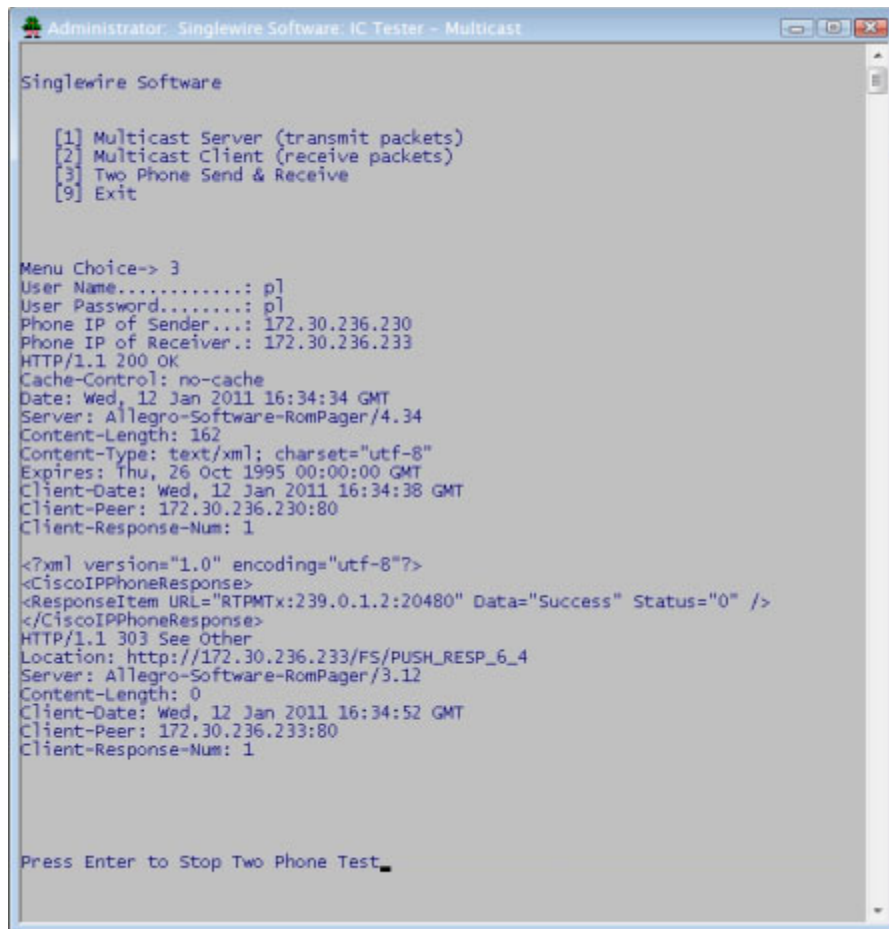
**Step 2** Enter **3** at the **Menu Choice** prompt and press the **Enter** key.

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

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

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

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



```

Administrator: Singlewire Software: IC Tester - Multicast
Singlewire Software

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

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

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

Press Enter to Stop Two Phone Test_

```

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

If you can't hear any audio, follow the recommendations in "Review Multicast Configuration" on page 2-6 or see "Multicast" on page 9-1.

## Review Multicast Configuration

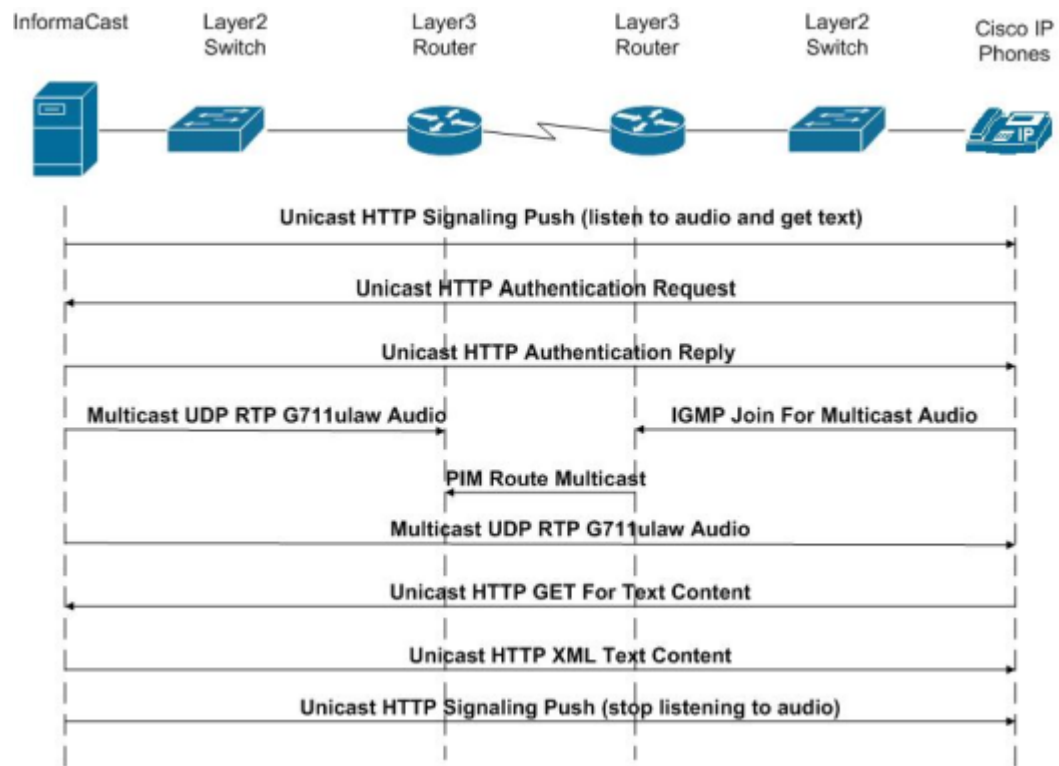
Multicast must be configured in order for InformaCast broadcasts to properly play on your recipients. The following recommendations can also apply:

- 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.



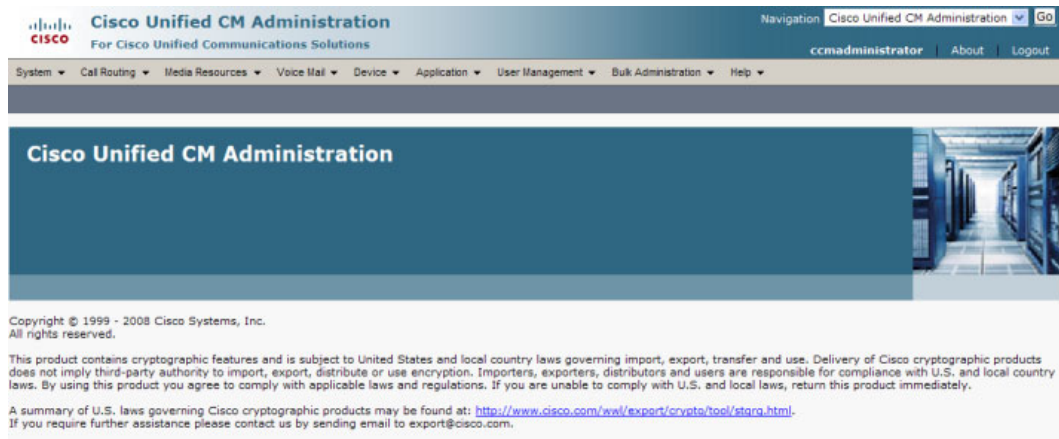
Now that you are familiar with the traffic flow created by InformaCast, you can use a protocol analyzer, such as Wireshark, to sniff the traffic on the network to see that multicast is enabled.

### Obtain a Network Traffic Capture

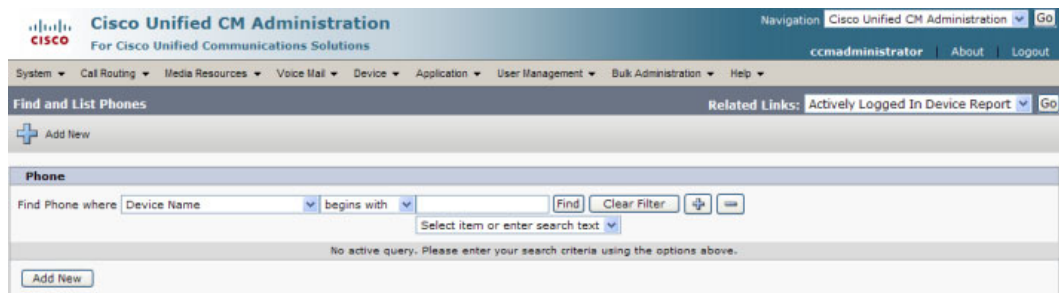
Use the following steps to obtain a network traffic capture from a Cisco IP phones for Unified CM to determine if multicast traffic is routing to that network segment.

- Step 1** Download and install a protocol analyzer like [Wireshark](#) on a PC that's attached to a Cisco IP phones for Unified CM on your network on which you want to obtain a traffic capture.

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

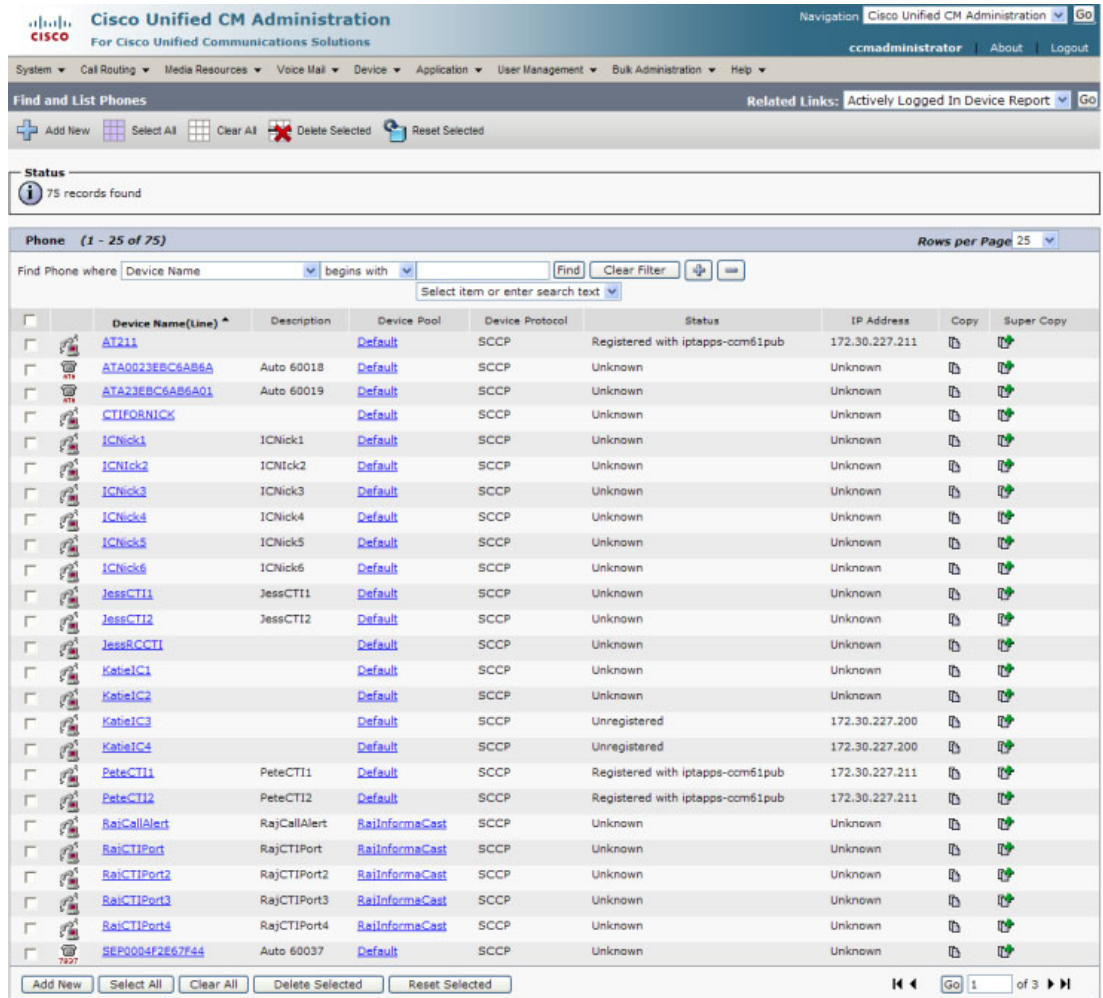


- Step 3** Go to **Device | Phone**. The Find and List Phone page appears.



**Step 4** Use the filter fields at the top of the page to narrow your list of phone results.

**Step 5** Click the **Find** button. The Find and List Phones page refreshes.



**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration Go  
ccadministrator About Logout

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

**Find and List Phones** Related Links: Actively Logged In Device Report Go

+ Add New Select All Clear All Delete Selected Reset Selected

**Status**  
75 records found

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

Find Phone where Device Name begins with Find Clear Filter

Select item or enter search text

	Device Name(Line) ^	Description	Device Pool	Device Protocol	Status	IP Address	Copy	Super Copy
<input type="checkbox"/>	AT211		Default	SCCP	Registered with iptapps-ccm61pub	172.30.227.211		
<input type="checkbox"/>	ATA0023EBC6AB6A	Auto 60018	Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	ATA23EBC6AB6A01	Auto 60019	Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	CTIPORNICX		Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	ICNick1	ICNick1	Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	ICNick2	ICNick2	Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	ICNick3	ICNick3	Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	ICNick4	ICNick4	Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	ICNick5	ICNick5	Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	ICNick6	ICNick6	Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	JessCTI1	JessCTI1	Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	JessCTI2	JessCTI2	Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	JessRCCTI		Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	KatieLC1		Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	KatieLC2		Default	SCCP	Unknown	Unknown		
<input type="checkbox"/>	KatieLC3		Default	SCCP	Unregistered	172.30.227.200		
<input type="checkbox"/>	KatieLC4		Default	SCCP	Unregistered	172.30.227.200		
<input type="checkbox"/>	PeteCTI1	PeteCTI1	Default	SCCP	Registered with iptapps-ccm61pub	172.30.227.211		
<input type="checkbox"/>	PeteCTI2	PeteCTI2	Default	SCCP	Registered with iptapps-ccm61pub	172.30.227.211		
<input type="checkbox"/>	RajCallAlert	RajCallAlert	RajInformaCast	SCCP	Unknown	Unknown		
<input type="checkbox"/>	RajCTIPort	RajCTIPort	RajInformaCast	SCCP	Unknown	Unknown		
<input type="checkbox"/>	RajCTIPort2	RajCTIPort2	RajInformaCast	SCCP	Unknown	Unknown		
<input type="checkbox"/>	RajCTIPort3	RajCTIPort3	RajInformaCast	SCCP	Unknown	Unknown		
<input type="checkbox"/>	RajCTIPort4	RajCTIPort4	RajInformaCast	SCCP	Unknown	Unknown		
<input type="checkbox"/>	SEP0004F2867F44	Auto 60037	Default	SCCP	Unknown	Unknown		

Add New Select All Clear All Delete Selected Reset Selected

Go 1 of 3

**Step 6** Click the **Device Name** link of the phone attached to the PC on which you downloaded Wireshark. The Phone Configuration page for that phone appears.

The screenshot shows the Cisco Unified CM Administration interface for a Cisco 7937 phone. The page is titled "Phone Configuration" and includes a navigation menu at the top. The main content area is divided into several sections:

- Status:** Ready
- Association Information:** A table with 16 rows. Row 1 is "Line [1] - 60028 (no partition)". Rows 2-12 are "None". Rows 13-16 are "Line [2] - Add a new DN", "Add a new SD", "Privacy", and "None".
- Phone Type:** Product Type: Cisco 7937, Device Protocol: SCCP
- Device Information:** A list of configuration parameters with dropdown menus and checkboxes. Parameters include Registration, IP Address, MAC Address (0004F2E67F44), Description (Auto 60028), Device Pool (Default), Common Device Configuration (< None >), Phone Button Template (\* -- Not Selected --), Softkey Template (< None >), Common Phone Profile (\* Standard Common Phone Profile), Calling Search Space (Phones), Media Resource Group List (< None >), User Hold MOH Audio Source (< None >), Network Hold MOH Audio Source (< None >), Location\* (Hub\_None), User Locale (< None >), Network Locale (< None >), Built In Bridge\* (Default), Privacy\* (Default), Device Mobility Mode\* (Default), Owner User ID (< None >), and Phone Load Name. Checkboxes include "Ignore Presentation Indicators (internal calls only)", "Allow Control of Device from CTI" (checked), "Logged Into Hunt Group" (checked), and "Remote Device".
- Product Specific Configuration Layout:** A section with a question mark icon. Parameters include Settings Access\* (Enabled), Gratuitous ARP\* (Enabled), PC Voice VLAN Access\* (Enabled), Web Access\* (Enabled), Load Server (empty text box), and SSH Access\* (Disabled).

At the bottom of the page, there are buttons for Save, Delete, Copy, Reset, and Add New. A legend indicates that asterisks (\*) denote required items, double asterisks (\*\*) denote items not required for Packet Capture Mode and Duration changes, and triple asterisks (\*\*\*) denote items with additional CAPF settings.

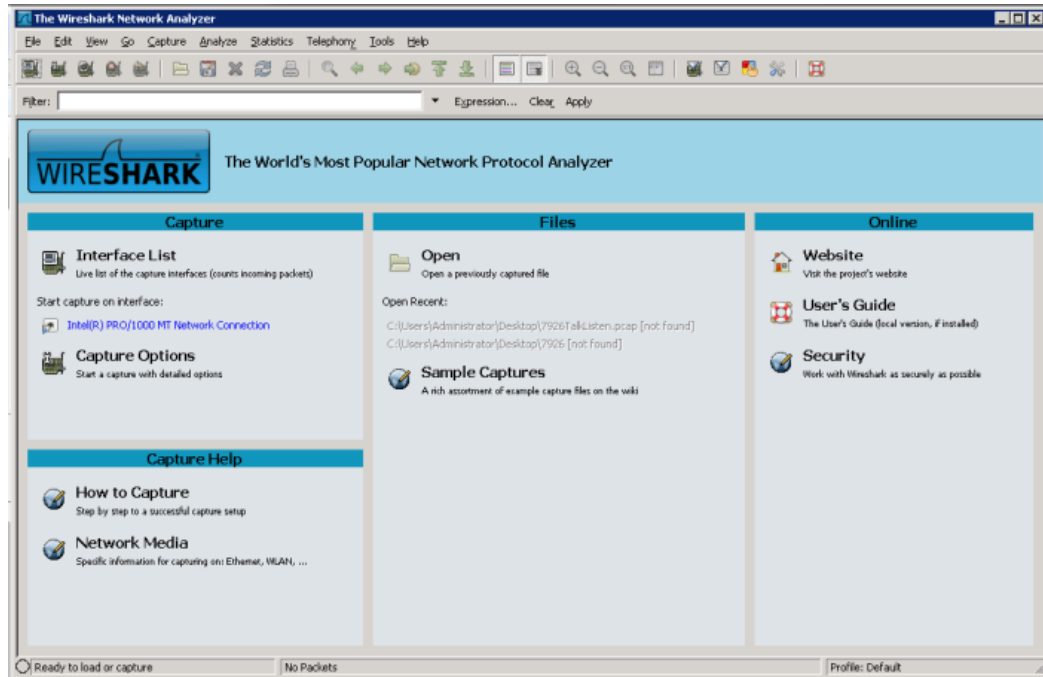
**Step 7** Scroll down to the *Product Specific Configuration Layout* area.

**Step 8** Make sure that both the **Web Access** and **Span to PC Port** dropdown menus have **Enabled** selected.

**Step 9** Click the **Reset** button.



**Step 10** Start Wireshark. The Wireshark window appears.



**Step 11** Send an InformaCast broadcast to the phone attached to the PC with Wireshark on it.

**Step 12** 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:

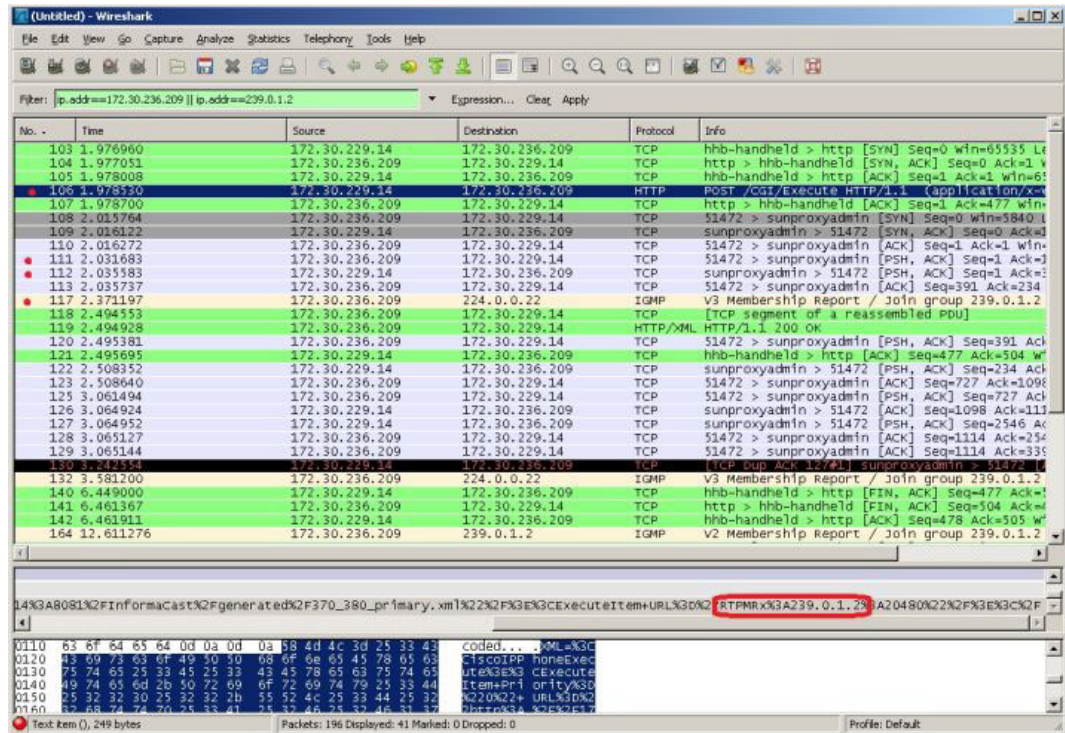
- A unicast HTTP command from InformaCast to the recipient to join the multicast group
- Successful authentication
- An IGMP join from the recipient to the multicast group
- A multicast audio stream

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.

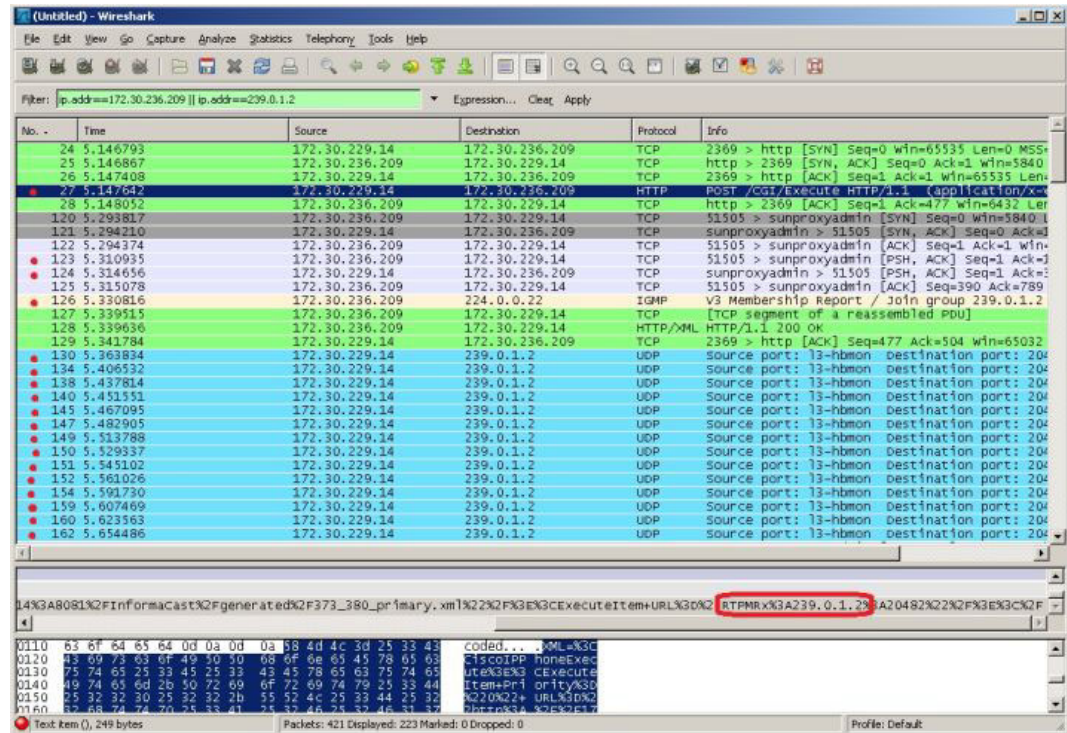
Each of the things to look for are marked with red in the following graphic.



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.

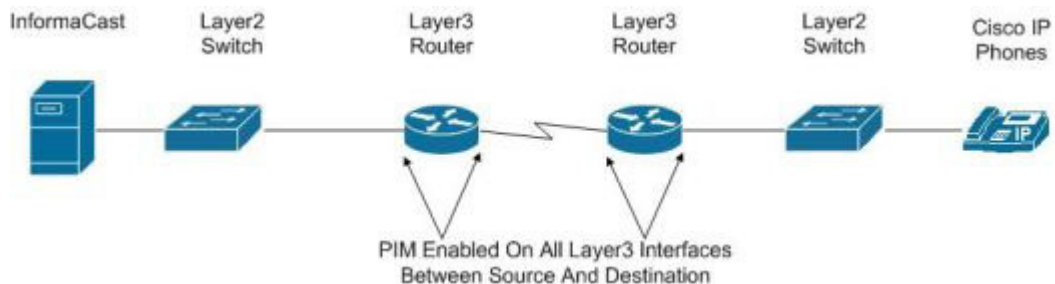


If multicast isn't working, troubleshoot the problems singly by frame(s). Work with your network administrator to configure multicast appropriately.

*Verify PIM is Configured on All Layer 3 Interfaces*

For audio broadcast traffic to route from a source (InformaCast) to a destination (Cisco IP phones for Unified CM), 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 Cisco IP phones for Unified CM and InformaCast.



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

```

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

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

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

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

IPTAPPS-SW3560-2#

```

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

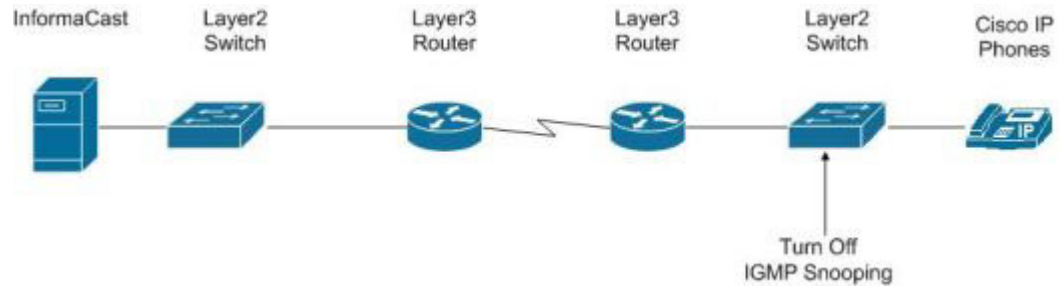
### *Verify your MPLS Provider Routes Multicast*

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

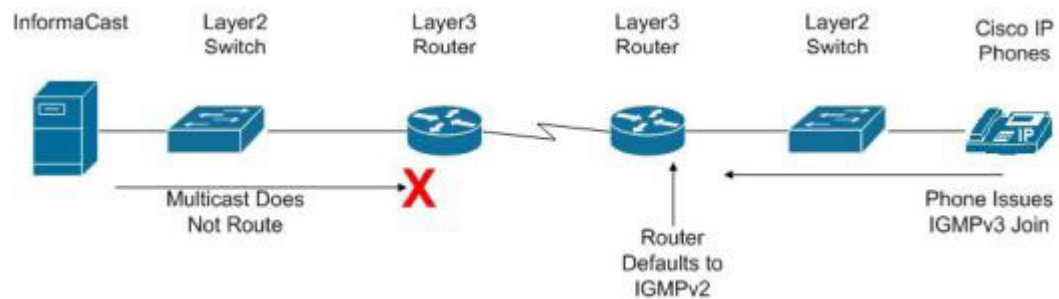
IGMP snooping has been seen to cause issues with Layer 2 switches. For this reason, if there are issues receiving the multicast audio stream at the Cisco IP phones for Unified CM, it would be worth testing if turning off IGMP snooping on the switches where phones are connected solves the problem. The 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 models of Cisco IP phones for Unified CM 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 2-7). In the capture, the phone will issue an IGMP join to listen to the multicast audio.



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

The image shows a Wireshark network traffic capture window. The filter is set to `ip.addr==172.30.236.209 || ip.addr==239.0.1.2`. The packet list pane shows a series of packets, with packet 117 highlighted in yellow and circled in red. The details pane for packet 117 shows the following information:

No.	Time	Source	Destination	Protocol	Info
117	2.371197	172.30.236.209	224.0.0.22	IGMP	V3 Membership Report / Join group 239.0.1.2

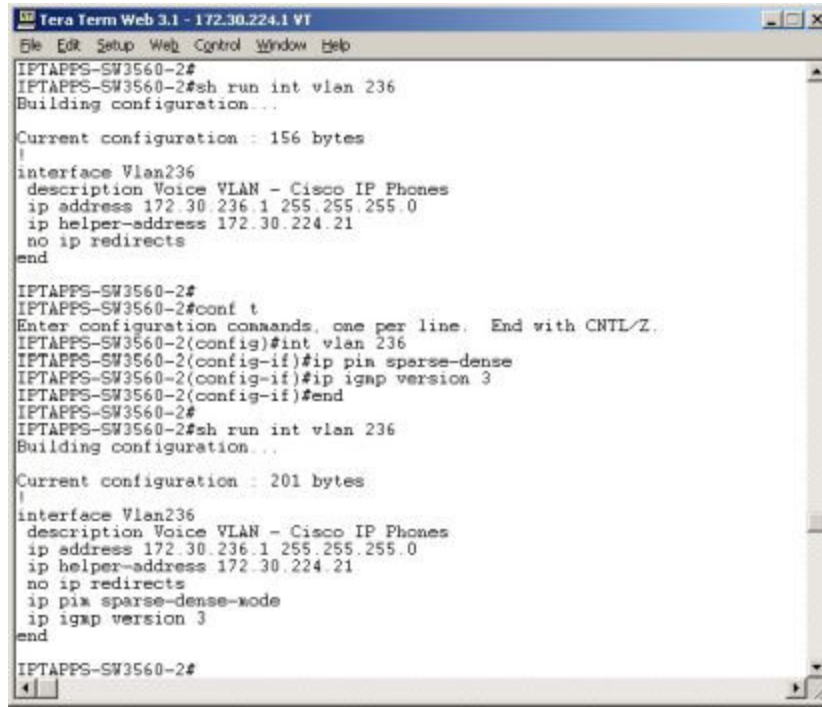
The details pane for packet 117 shows the following information:

```

V3 Membership Report / Join group 239.0.1.2
  Version: 3
  Type: Membership Report
  Group Address: 239.0.1.2
  Reserved: 0
  Max Resp Time: 0
  Report Flags: 0
  Source Address: 172.30.236.209
  
```

The packet bytes pane shows the raw data of the packet, including the IP header and the IGMP message.

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



```

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

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

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

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

IPTAPPS-SW3560-2#

```

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

## Deploy InformaCast

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



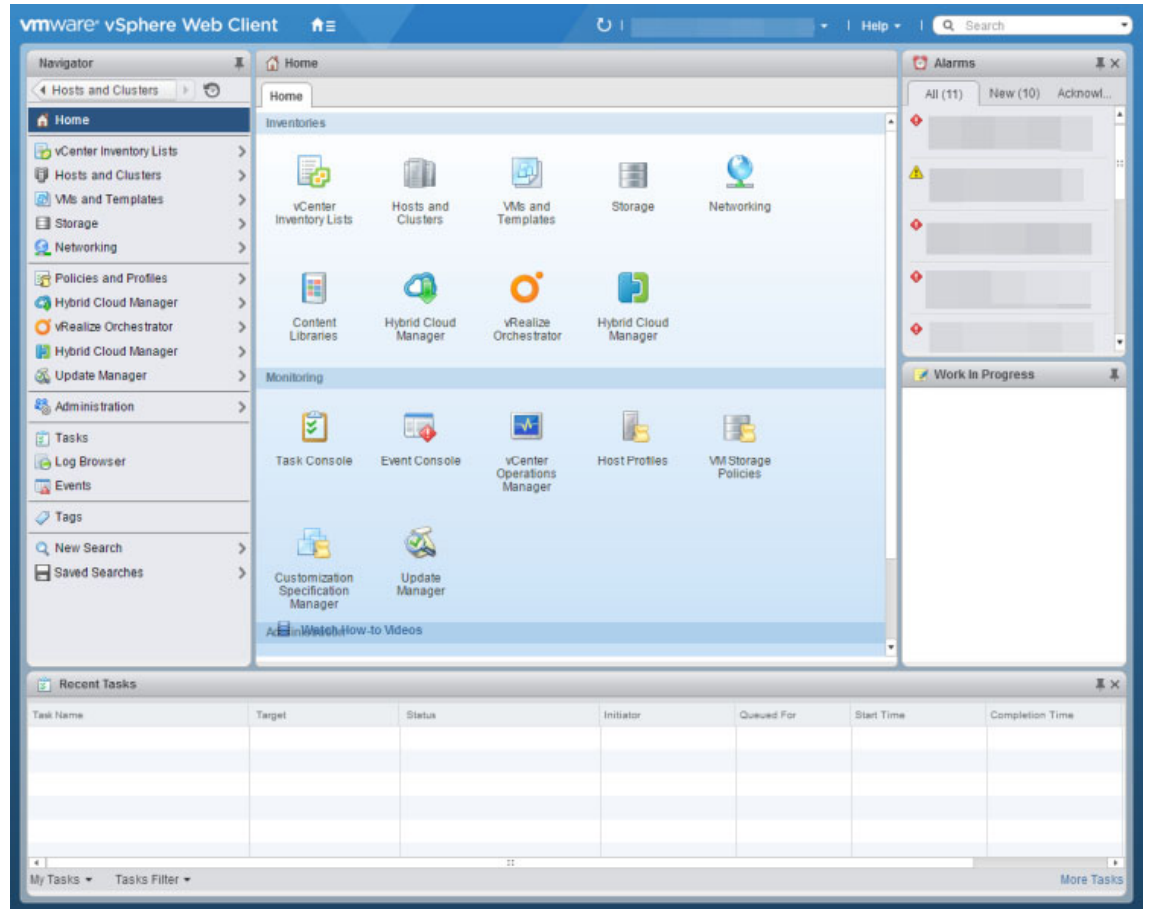
**Note** InformaCast Appliance is also supported as a physical machine, but that is not offered with Basic InformaCast.

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



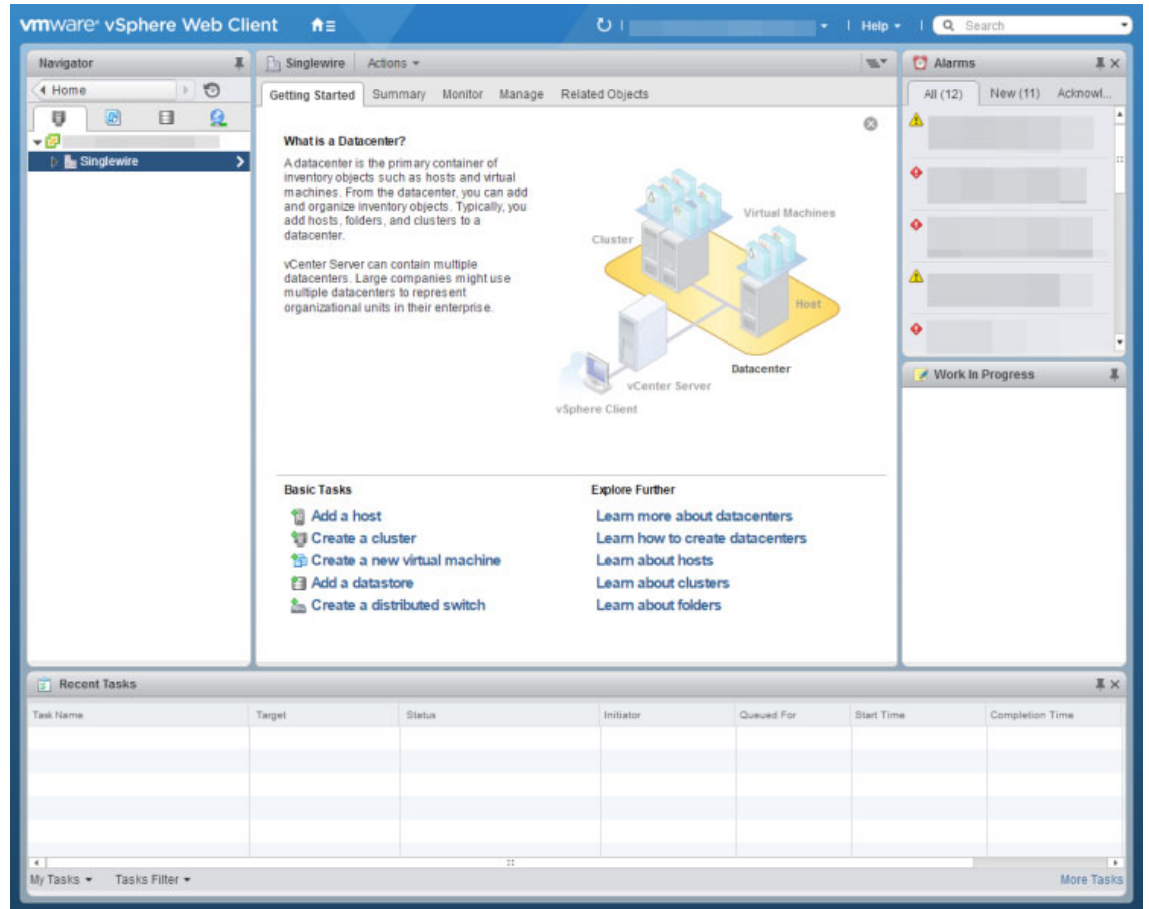
**Note** If you are using InformaCast on the Cisco Unified CM Business Edition 6000, you will be supplied with a DVD in a package with an OVA on it (physical media).

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

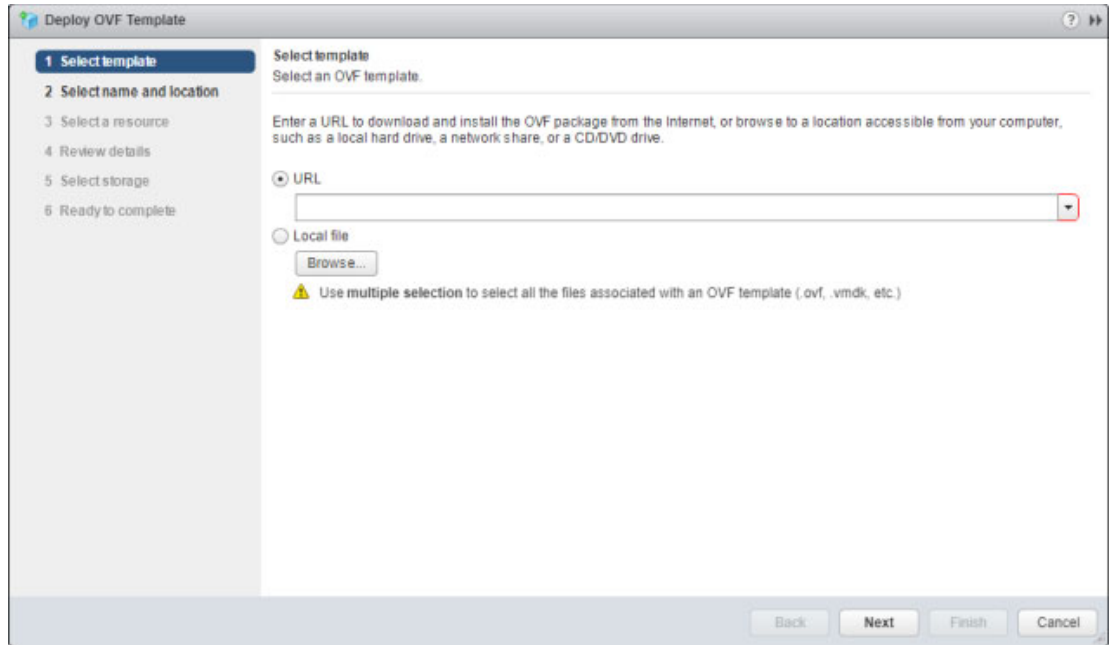




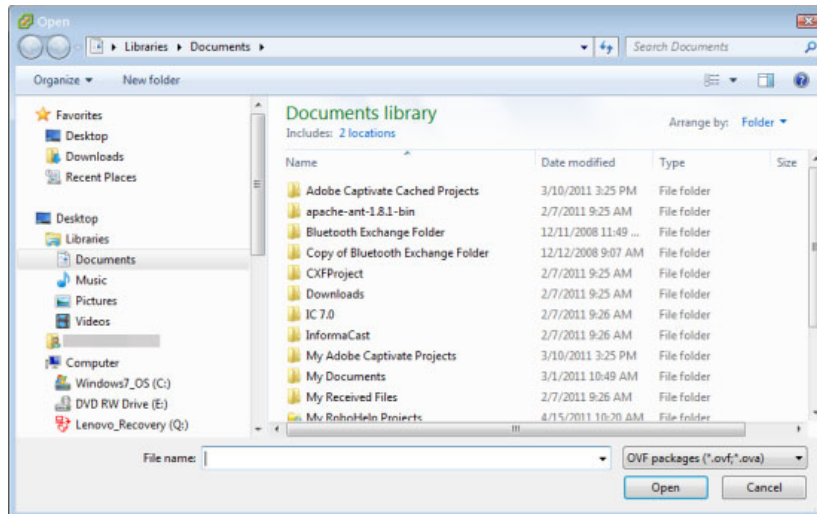
**Step 3** Click the **Hosts and Clusters** icon. The vSphere Web Client page refreshes.



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

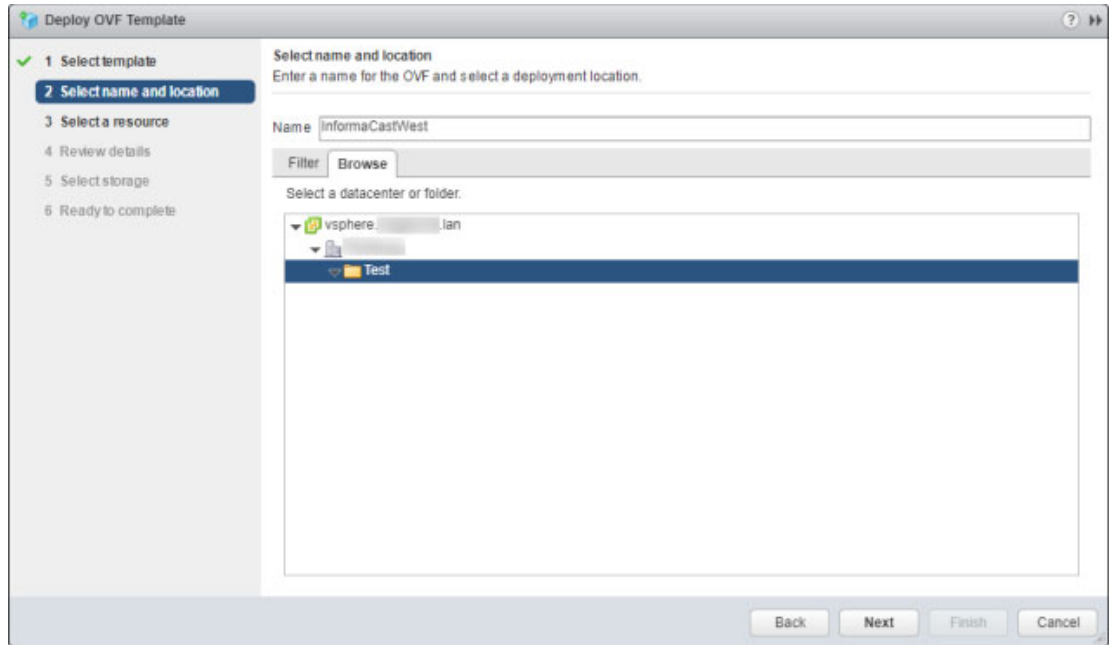


**Step 5** Click the **Local File** radio button and click its **Browse** button. The Open dialog box appears.



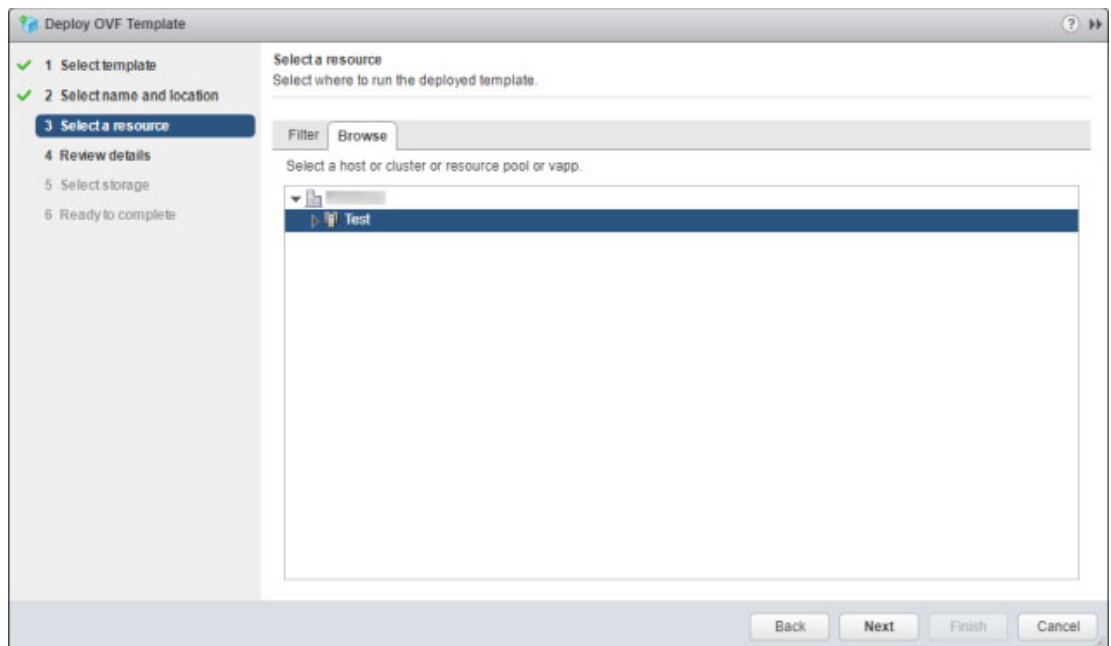
**Step 6** Navigate to where you saved the OVA file (or to the OVA file on the supplied DVD), select it, and click the **Open** button.

**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.

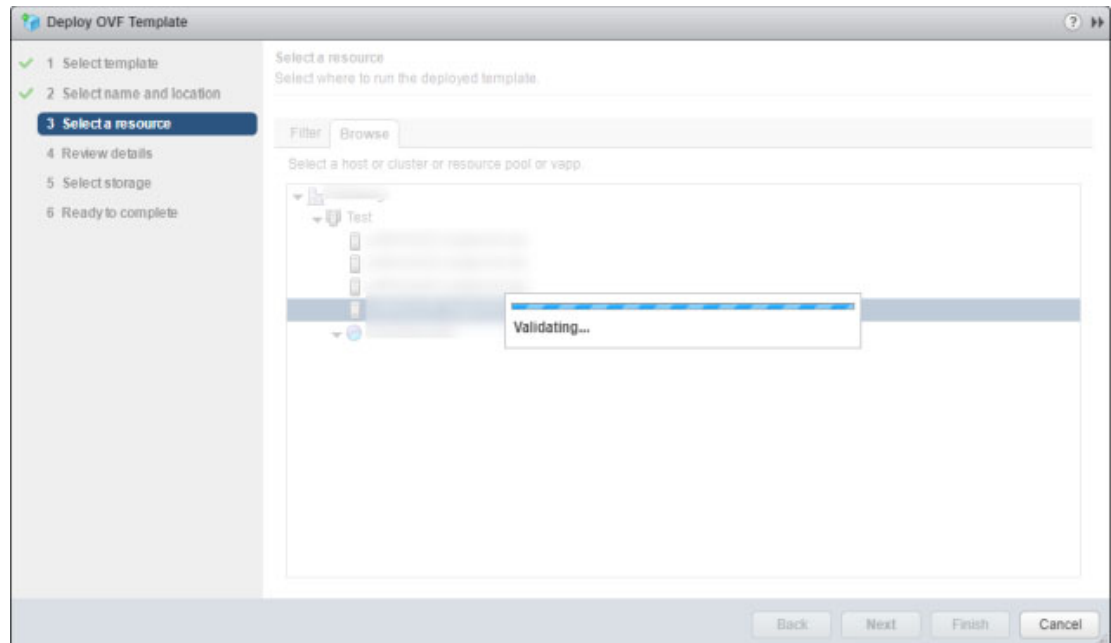
**Step 9** Select a deployment location for your virtual machine from the **Browse** tab and click the **Next** button. The Deploy OVF Template pop-up window refreshes



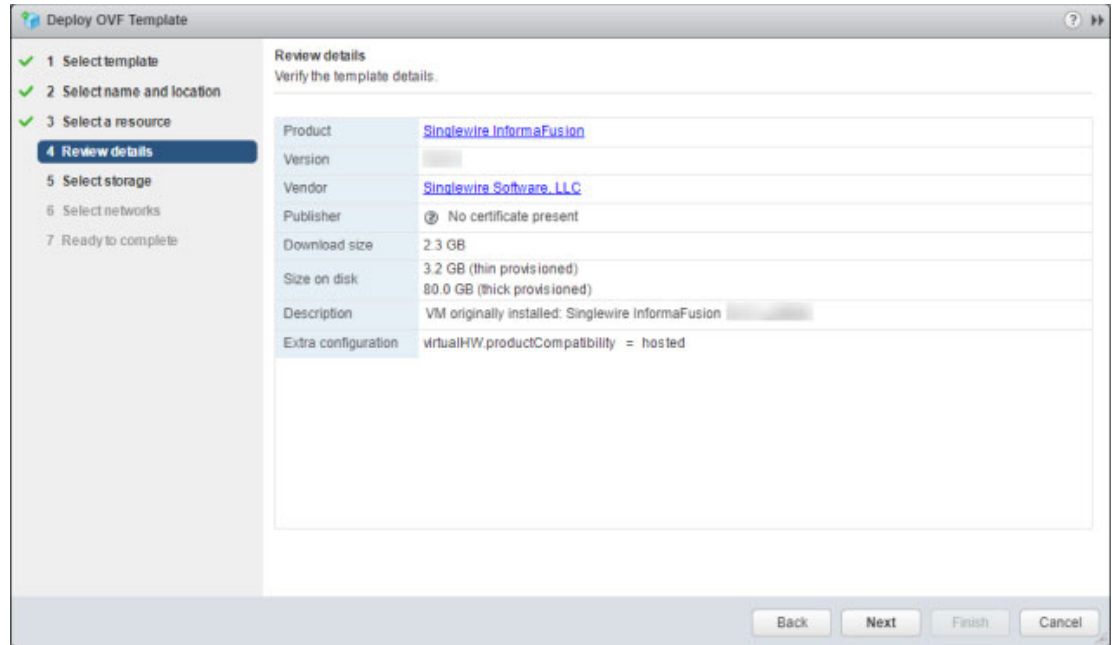
**Tip**

It is good practice to place the InformaCast Appliance on the same VLAN as your Cisco Unified CM.

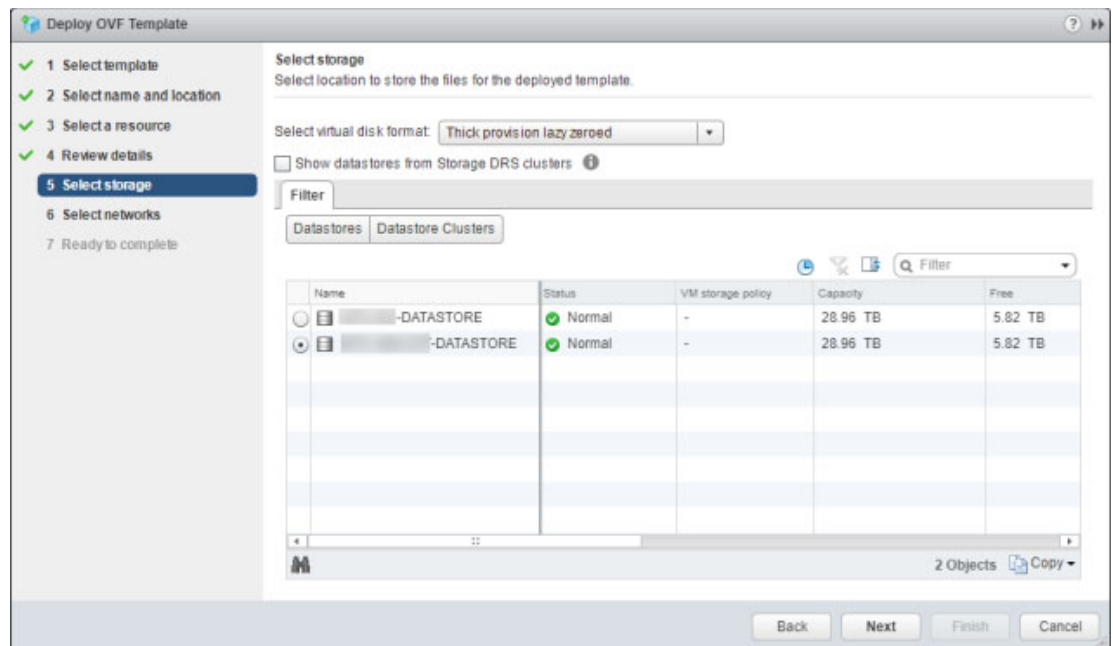
- Step 10** Select a location from which to run your deployed template from the **Browse** tab and click the **Next** button. The Deploy OVF template dialog box refreshes.



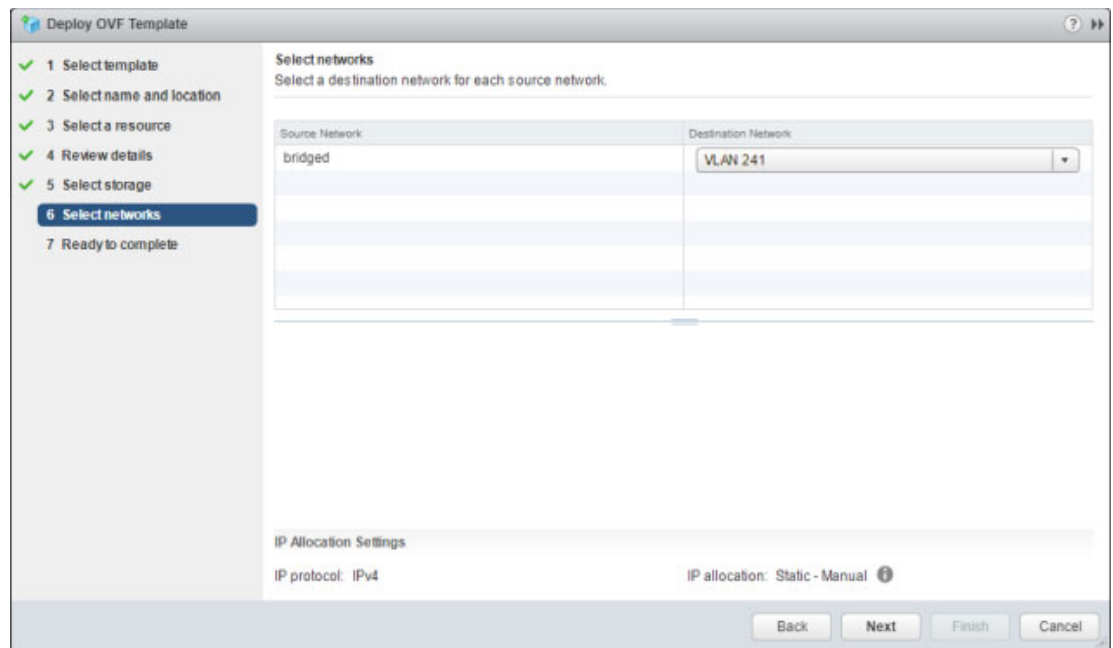
Once validation is complete, the Deploy OVF template dialog box refreshes.



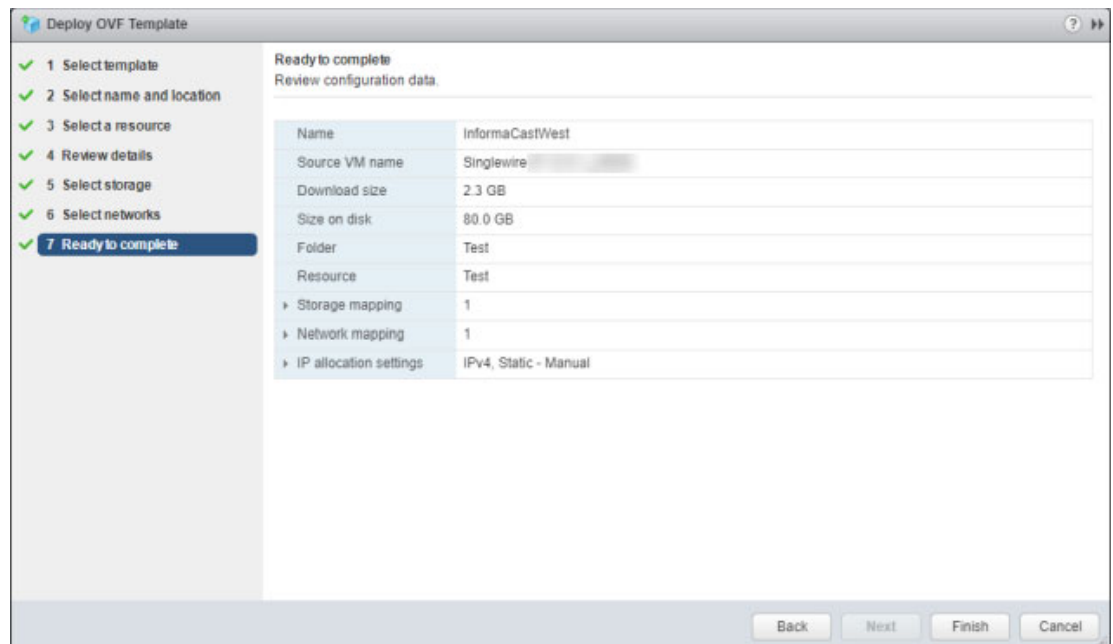
**Step 11** Click the **Next** button. The Deploy OVF Template pop-up window refreshes.



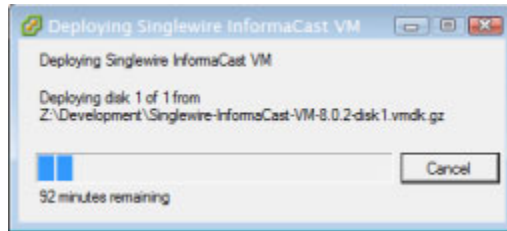
**Step 12** Select a format and storage location for your deployed template and click the **Next** button. The Deploy OVF Template pop-up window refreshes.



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

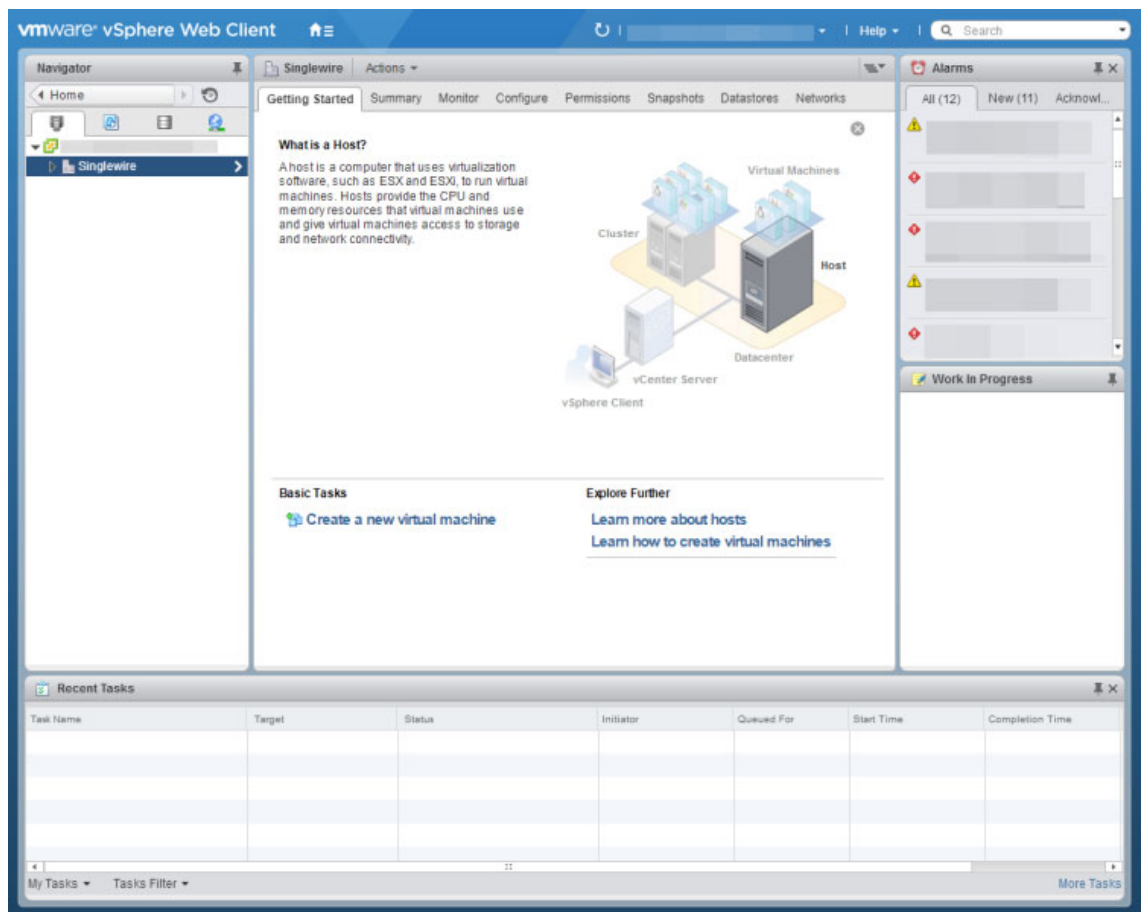


**Step 14** Review your information and click the **Finish** button. InformaCast Appliance will begin importing.

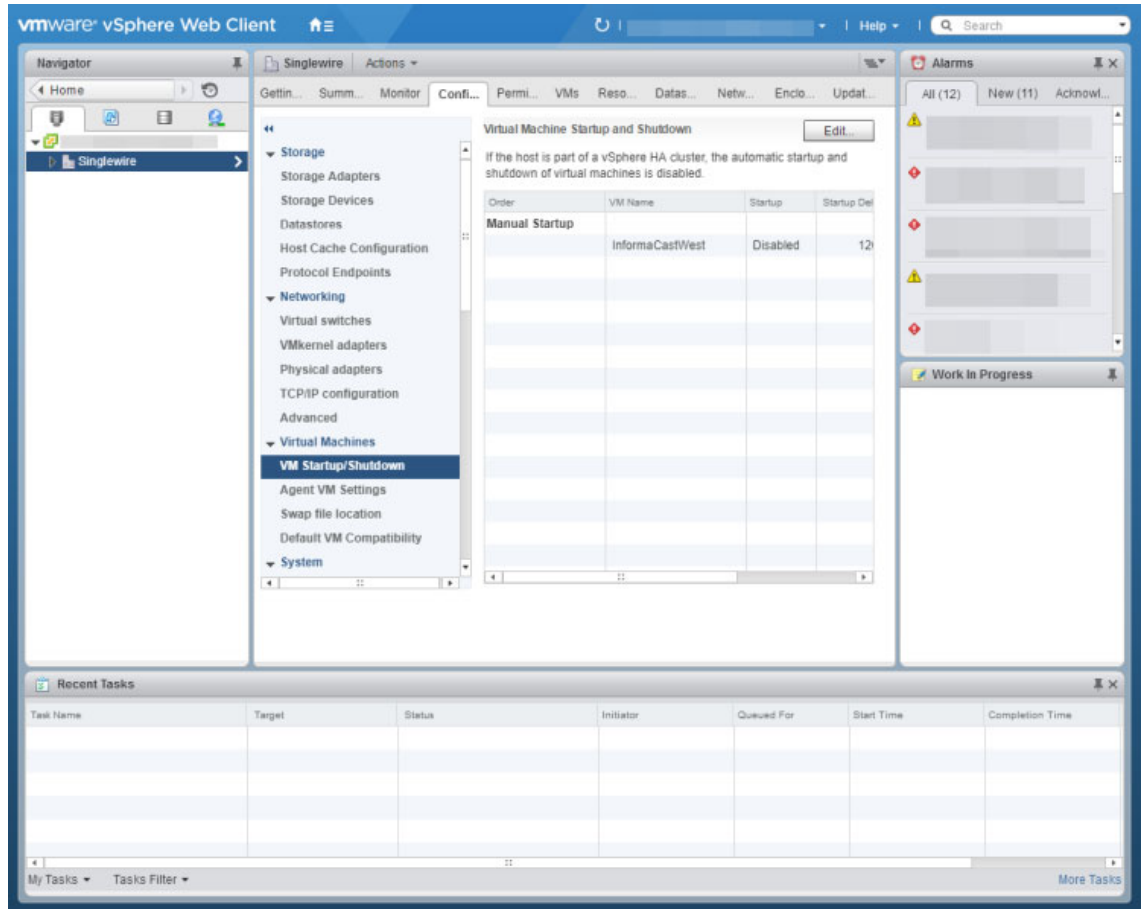


When it's finished, click the **Close** button.

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

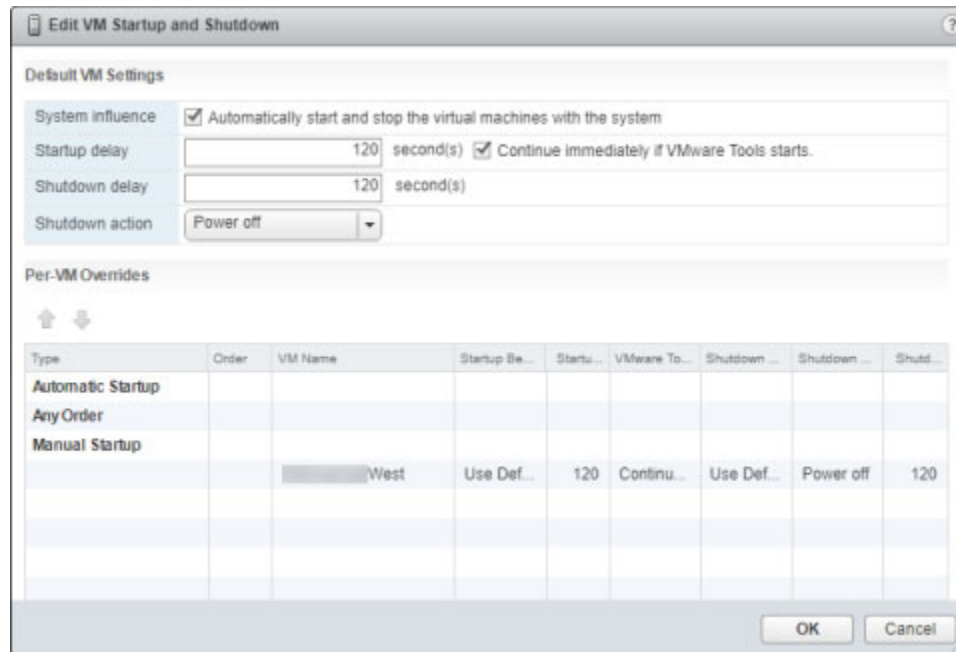


**Step 16** Click the **Configure** tab. The vSphere Web Client window's right pane refreshes.





**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.

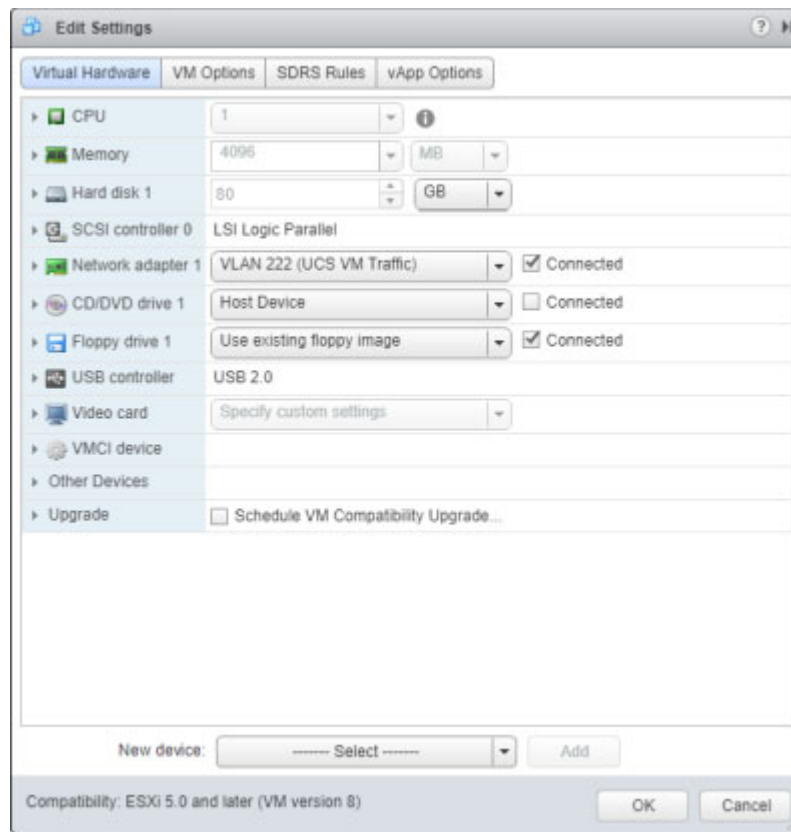


**Step 18** Ensure the **Automatically start and stop the virtual machines with the system** checkbox is selected.

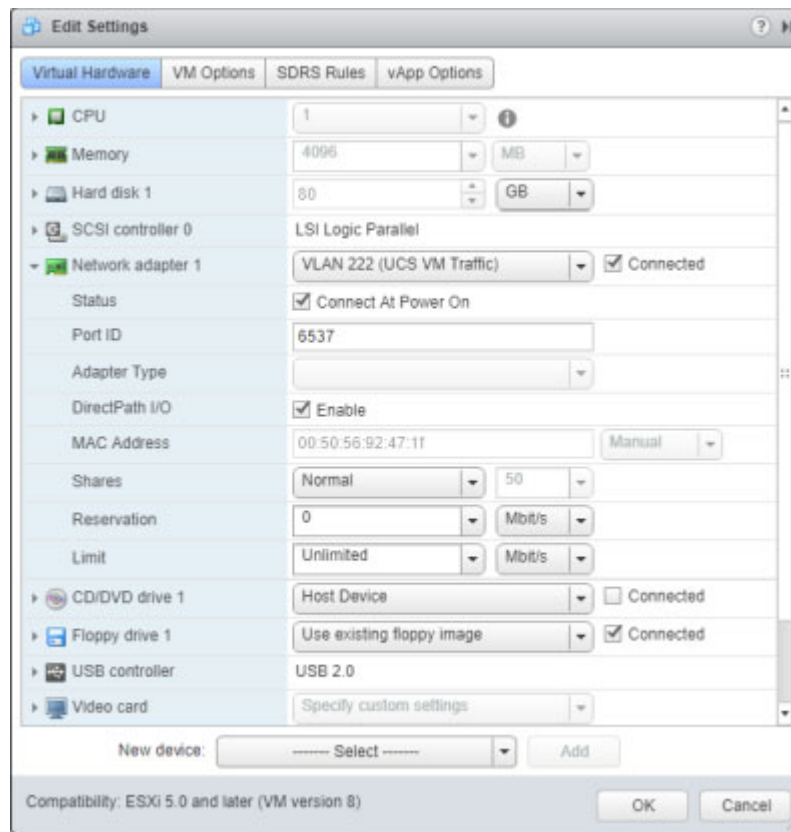
**Step 19** Select your virtual machine in the table and click the **Up** arrow to move it from **Manual Startup** to **Automatic Startup**.

**Step 20** Click the **OK** button in the Edit VM Startup and Shutdown pop-up window to save your changes. The InformaCast 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.



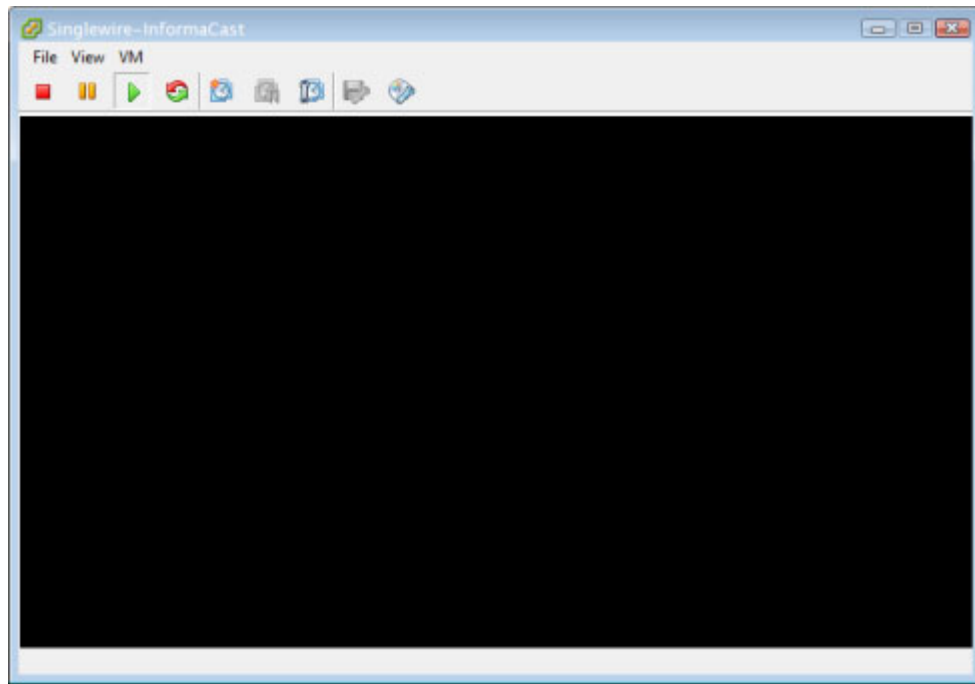
**Step 22** Click the **Network adaptor 1** dropdown arrow on the **Virtual Hardware** tab. The Edit Settings pop-up window refreshes.



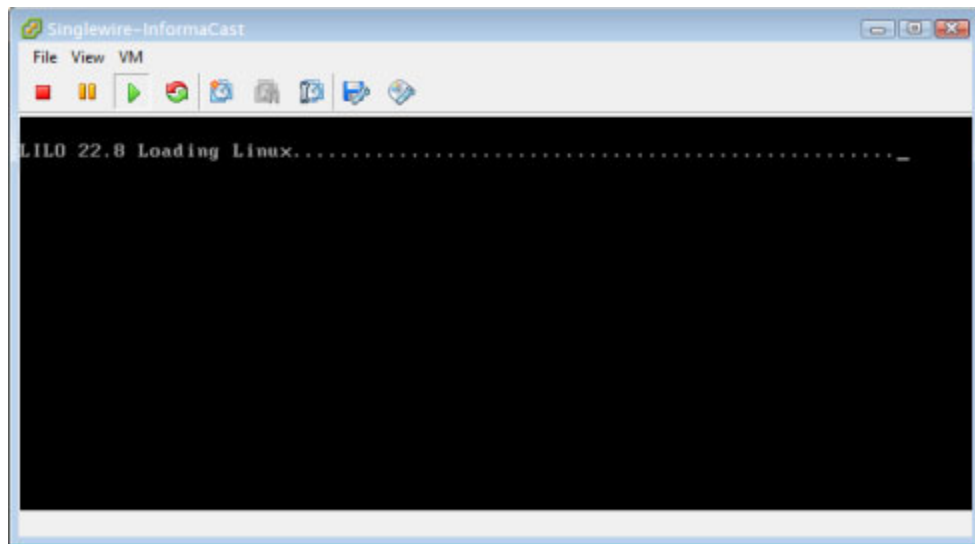
**Step 23** Ensure the **Connect At Power On** checkbox is selected.

**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 console window appears.

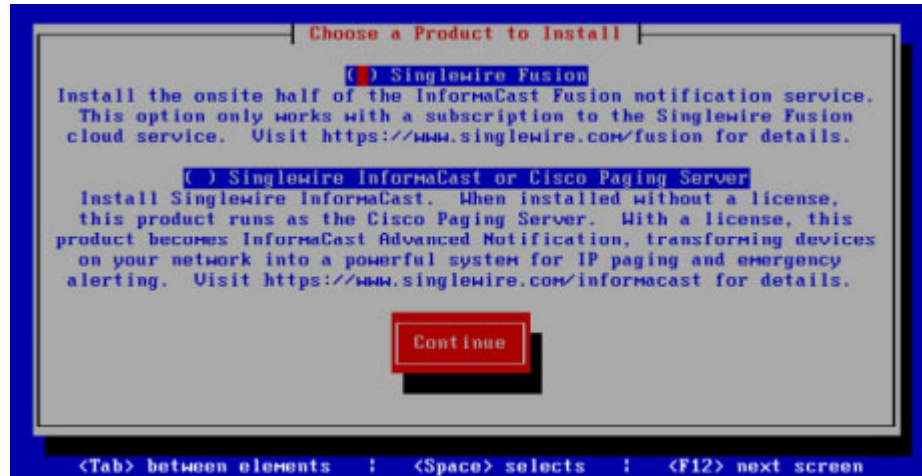


**Step 26** Click the green arrow button to turn on the virtual machine. The Singlewire InformaCast console window begins booting the virtual machine.



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

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

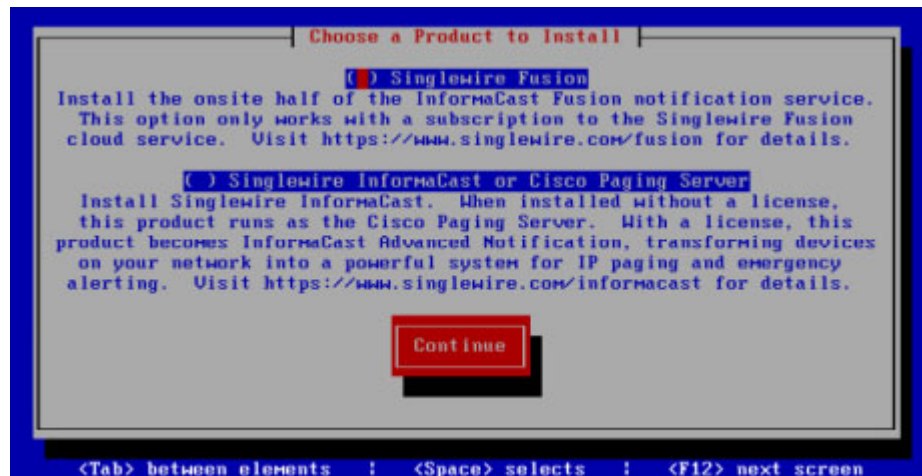


- Step 27** Leave your Singlewire InformaCast console window open and continue with “Set the Initial Configuration.”

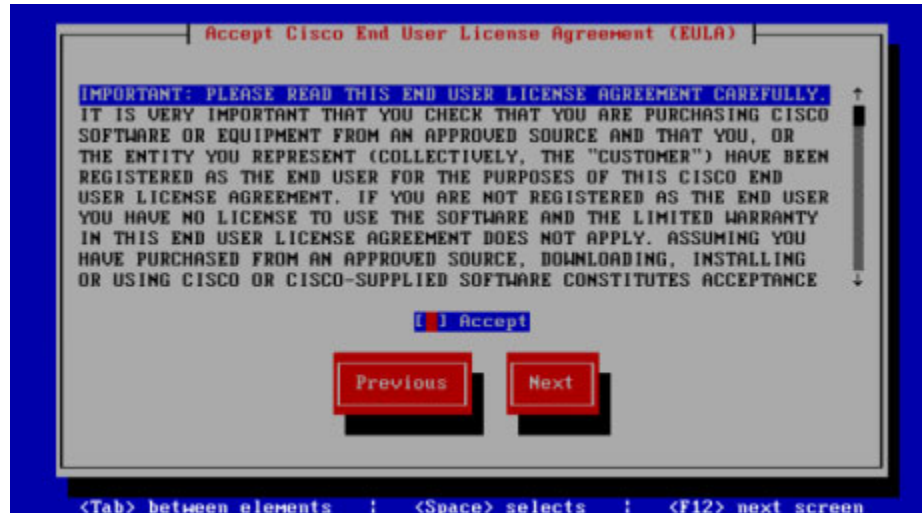
## Set the Initial Configuration

Once you have completed the steps in “Deploy InformaCast” on page 2-17, you will need to set InformaCast’s initial network configuration.

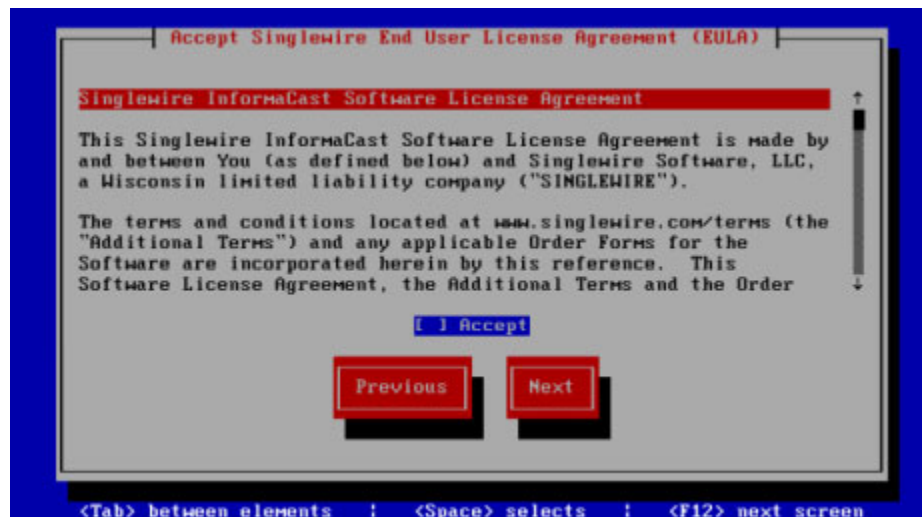
- Step 1** Return to your Singlewire InformaCast console window. You should see a request to select your product.



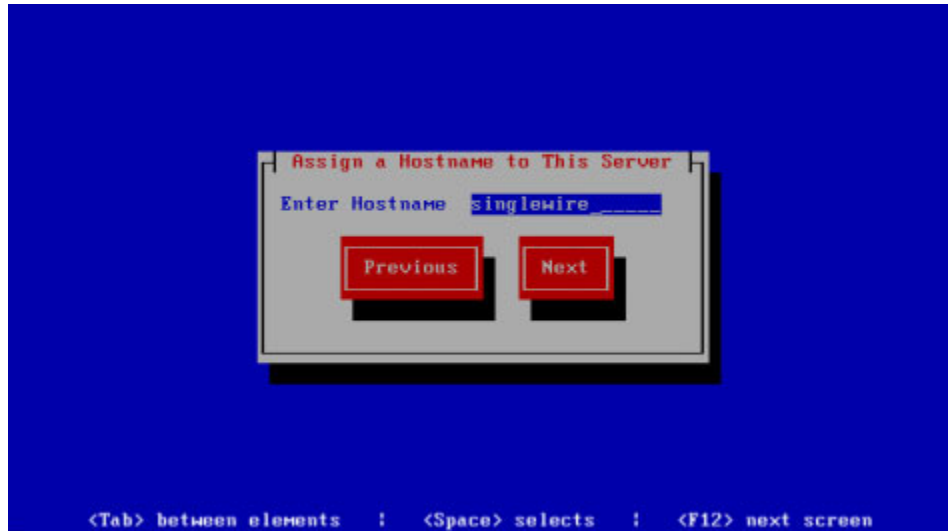
- Step 2** Press the **Tab** key followed by the **Spacebar** to select **Cisco Paging Server**.
- Step 3** Press the **Tab** key once to highlight the **Continue** button, then press the **Spacebar** to select it. You will be prompted to accept Cisco's End User License Agreement (EULA).



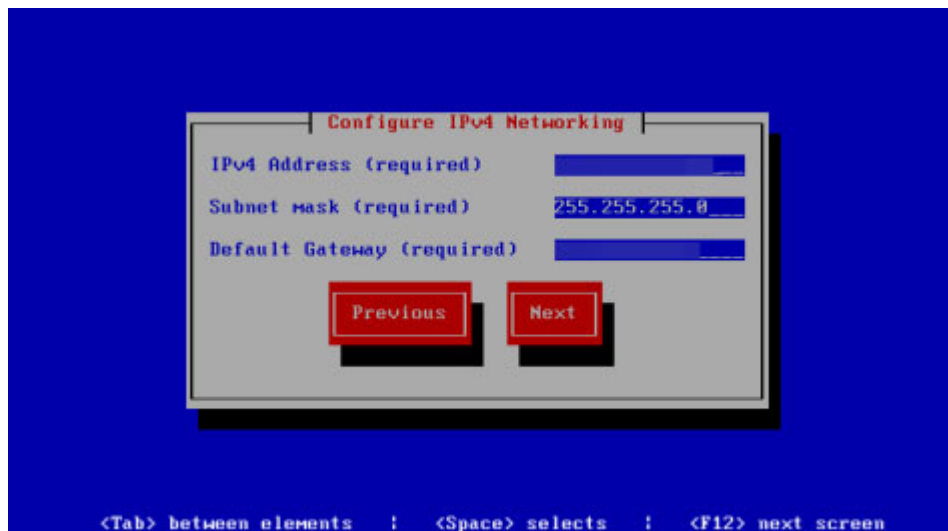
- Step 4** Press the **Tab** key to highlight the **Accept** checkbox, then press the **Spacebar** to accept the EULA.
- Step 5** Press the **Tab** key twice to highlight the **Next** button, then press the **Spacebar** to select it. You will be prompted to accept Singlewire's End User License Agreement.



- 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.

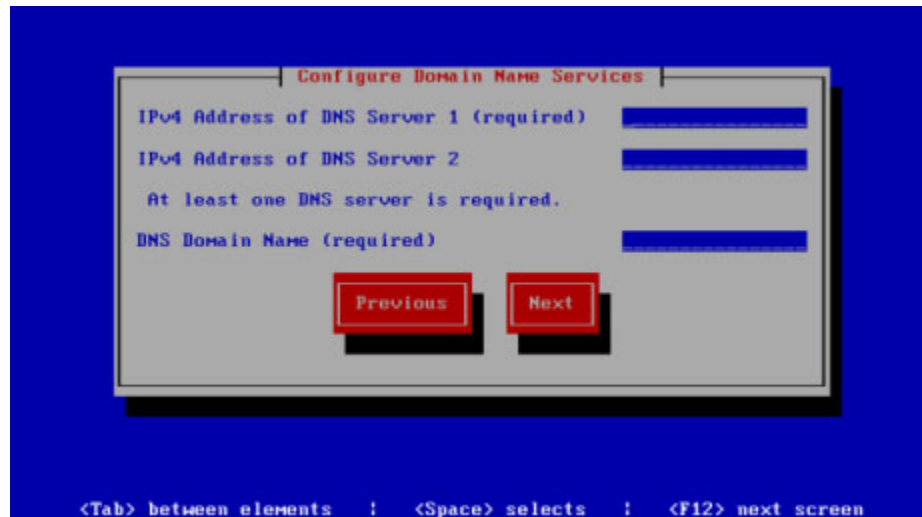


- Step 8** Enter a hostname for your InformaCast Appliance in the **Enter Hostname** field, e.g. InformaCastWest. This hostname will appear in Webmin's user interface.
- Step 9** Press the **Tab** key to highlight the **Next** button, then the **Spacebar** to select it. The InformaCast Appliance then attempts to use DHCP to find suitable IP addresses on your network. The Singlewire InformaCast console window refreshes.

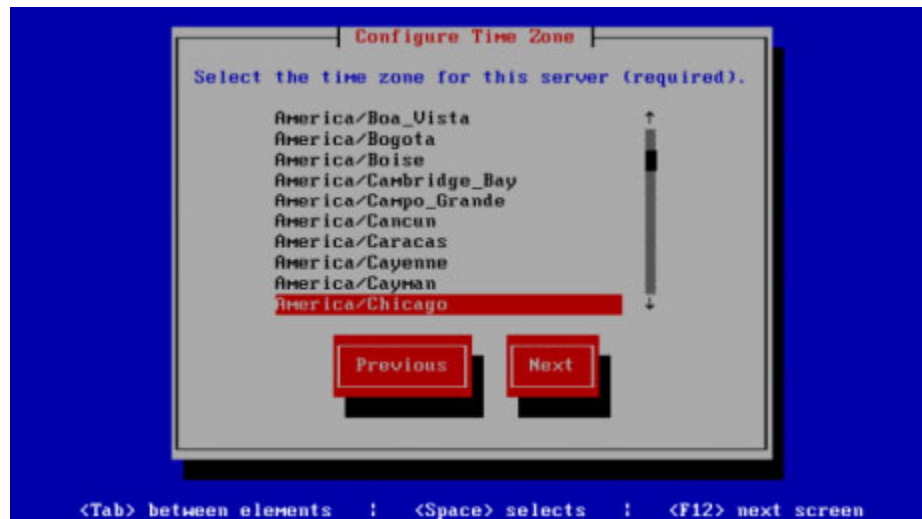


- Step 10** Accept these IP addresses or provide valid ones of your own in the **IPv4 Address**, **Subnet Mask**, and **Default Gateway** fields.

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



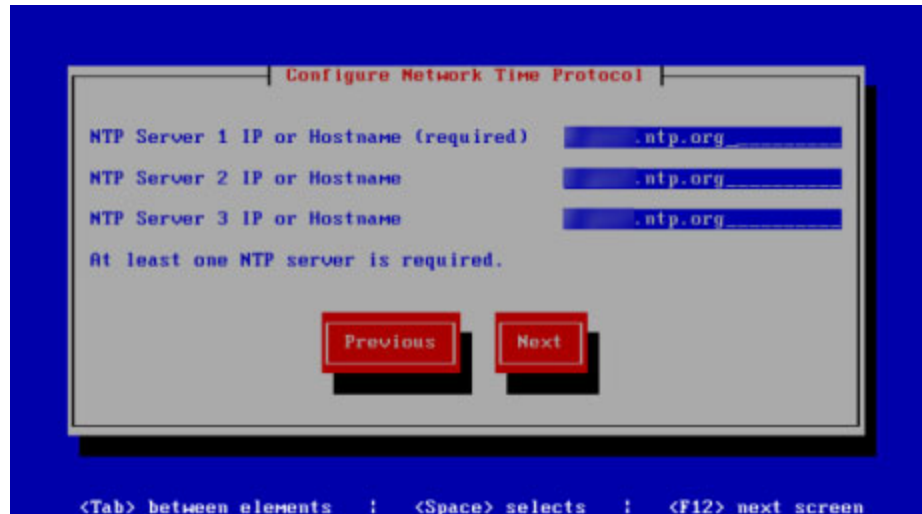
**Step 12** Enter at least one DNS server IP address in the field provided or accept the one provided to you and enter a DNS domain name. Press the **Tab** key to highlight the **Next** button, then the **Spacebar** to select it. The Singlewire InformaCast console window refreshes.



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

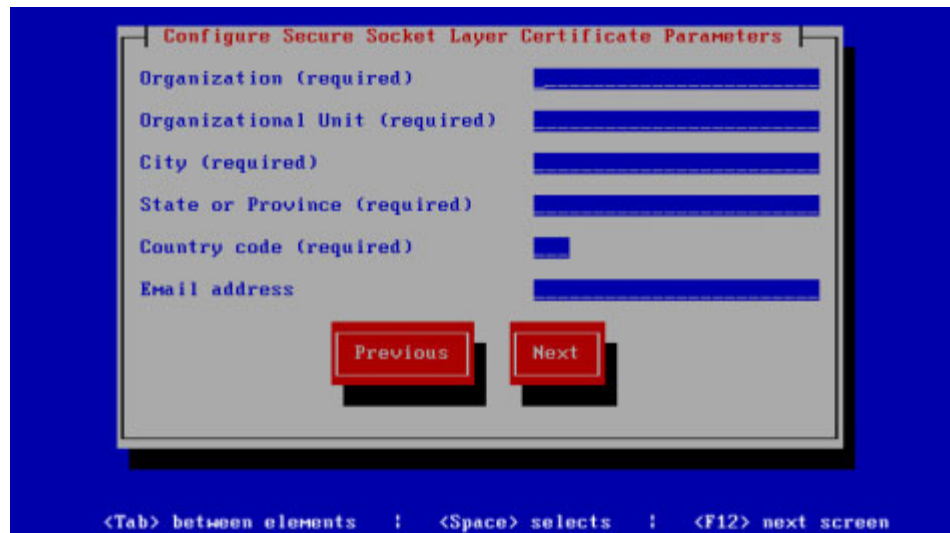


**Step 14** Press the **Tab** key to highlight the **Next** button, then the **Spacebar** to select it. The InformaCast Appliance then attempts to find an NTP server on your network. The Singlewire InformaCast console window refreshes.



**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 console window refreshes.



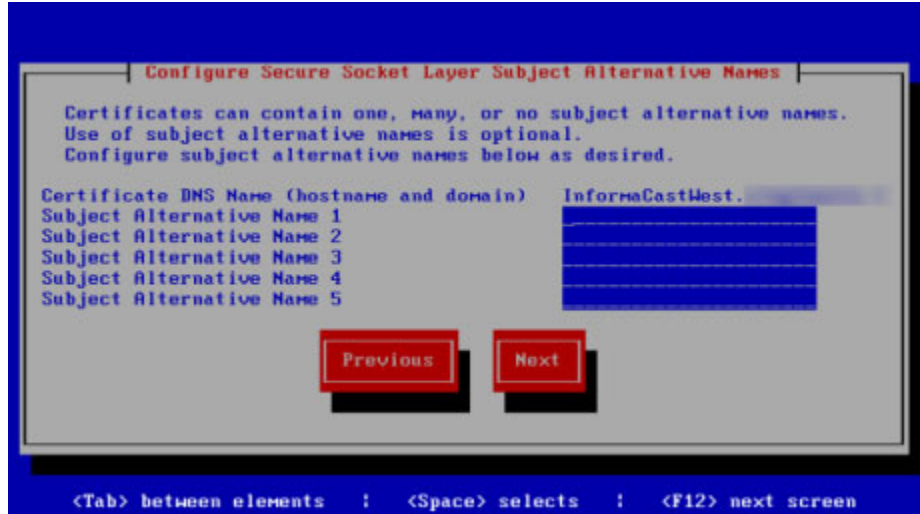
**Step 17** Enter the information necessary for a signed certificate (while the information is required, signing the certificate is not). A signed certificate, which can protect against Man-in-the-Middle (MITM) attacks, is an electronic document that proves ownership of a public key; it includes information 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 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 console window refreshes.

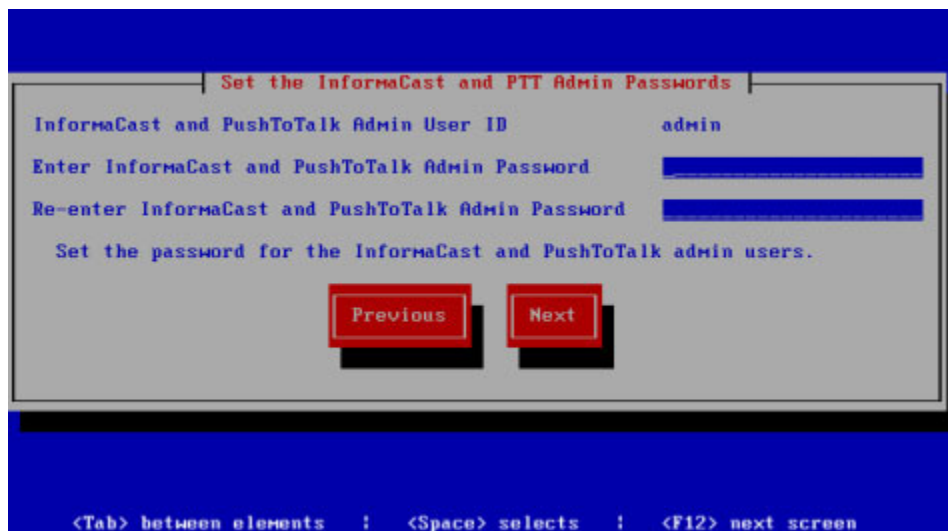


**Step 21** Enter a password in the **Enter OS Admin Password** field, press the **Tab** key, and enter the password again in the **Re-enter OS Admin Password** field. Your OS credentials are used to enter Webmin and Control Center and when using SSH to access the InformaCast Appliance.



**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 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 console window refreshes.

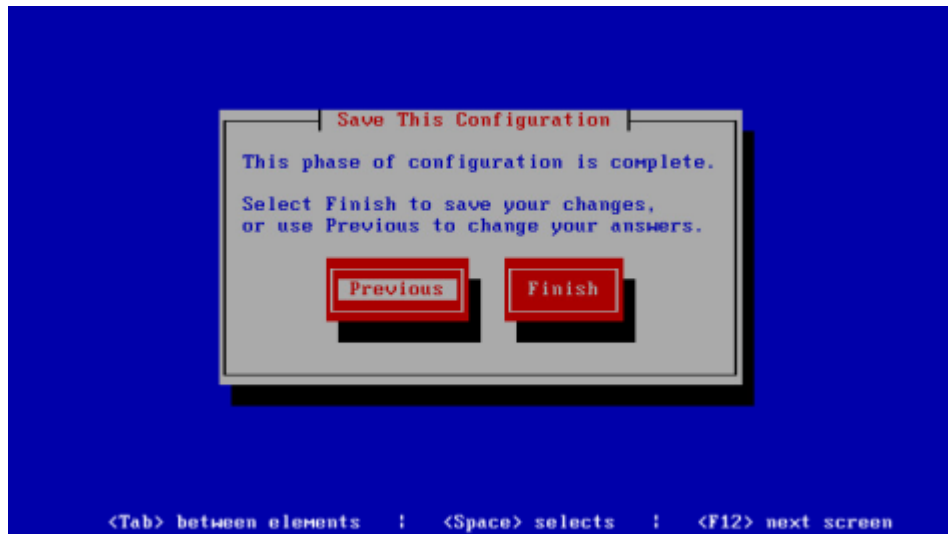


**Step 25** Enter a security passphrase in the **Enter Security Passphrase** and **Re-enter Security Passphrase** fields. This passphrase is used to secure your backups of the InformaCast Appliance. You must remember this passphrase. Singlewire Support personnel cannot recover it for you if it’s lost; however, you can reset it (see “Manage Password Recovery for the InformaCast Appliance” on page 13-101).

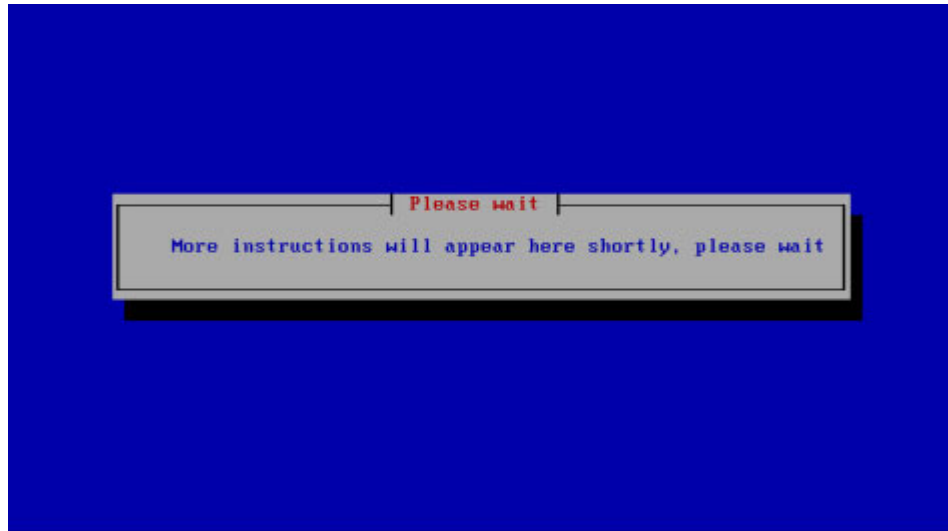


**Note** Your passphrase must follow the same character requirements as your OS admin password.

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

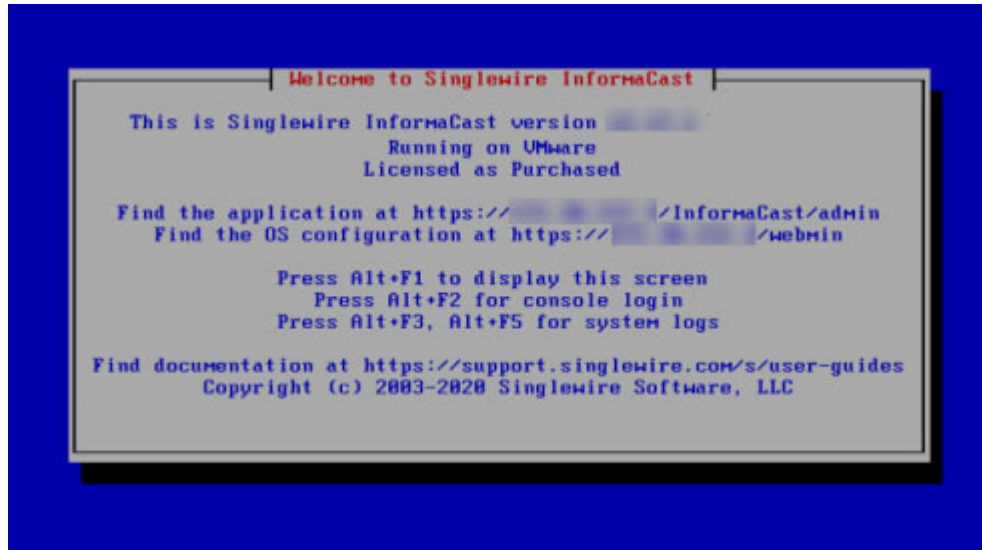


**Step 27** Press the **Tab** key to highlight the **Finish** button, then the **Spacebar** to select it. The Singlewire InformaCast console window refreshes.



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

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



- Step 28** Make a note of the displayed IP address. This is the IP address of the InformaCast Appliance's landing page, which you will use to access the InformaCast Appliance, Control Center, and Webmin web user interfaces.
- Step 29** Close your open console window.
-



## Interface Access

When using the InformaCast Appliance, you have access to several interfaces that control different facets of the server and application:

- **InformaCast Appliance landing page.** Contains links to InformaCast and the Control Center.
- **InformaCast.** Allows you to send a live audio stream to Cisco IP phones for Unified CM.



---

**Note** If this is your first time logging into InformaCast, follow the steps in “Log into InformaCast for the First Time” on page 3-3.

---

- **PushToTalk.** Facilitates communication between multiple parties (or on a one-to-one basis) through talk/listen or intercom functionality on supported Cisco IP phones for Unified CM.



---

**Note** While visible on the InformaCast Appliance landing page, PushToTalk is not supported by InformaCast Basic Paging. Please [contact Singlewire](#) for an upgrade to Advanced Notification.

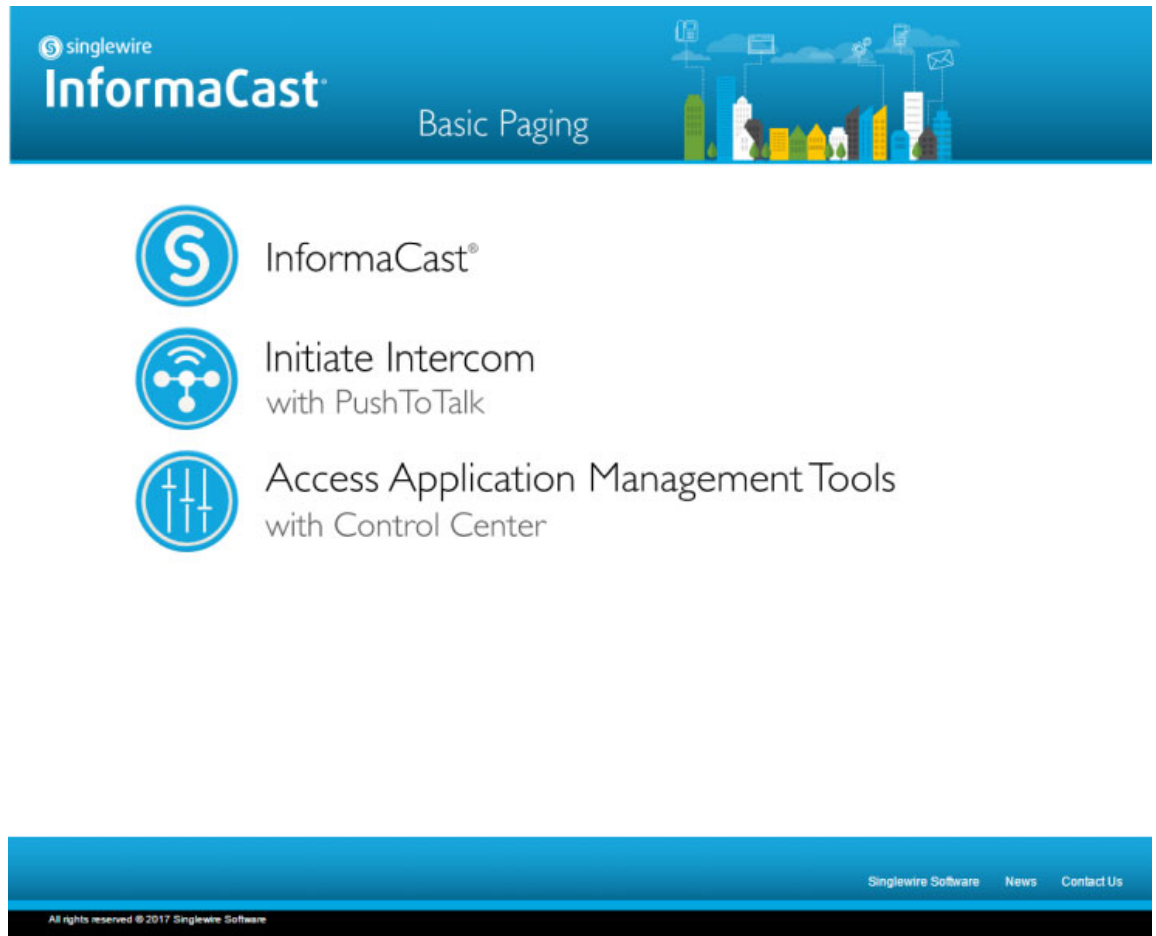
---

- **Control Center.** Houses abilities not contained in the InformaCast application's user interface: view InformaCast's status or access the License Manager to update your Basic license with an Advanced version. You can also access Webmin.
- **Webmin.** Administers the underlying operating system of the InformaCast Appliance, e.g. changing its password, restarting the server or its application, upgrading versions, and collecting/viewing logs.
- **Command line.** Used for support issues and some configuration procedures, e.g. those that require manual editing of files or the running of scripts, the CLI also allows you to perform the same administrative functions that available through Webmin.
- **Keyboard and monitor.** Displays version information and interface and documentation links for an InformaCast Appliance, and allows you to view system logs or open a console to the command-line interface.

## Access the InformaCast Appliance Landing Page

If you completed all of the steps in “Deploy InformaCast” on page 2-17 and “Set the Initial Configuration” on page 2-31, the InformaCast Appliance should be running and you can access the InformaCast Appliance landing page, which houses the links to the InformaCast Appliance's user interfaces, e.g. InformaCast, the Control Center, etc.

Open a web browser, enter the IP address of the InformaCast Appliance, which you made note of in Step 28 on page 2-40, and press the **Enter** key. The InformaCast Appliance landing page appears.



The InformaCast Appliance landing page allows you to easily access all of your 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 InformaCast Appliance and bookmark it for future use.



**Note**

When you access the InformaCast 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. The InformaCast Appliance is a locally-installed server rather than a global, public internet site; there is no practical way for web browsers to recognize its encryption certificate as safe. To permanently bypass this error, you can install a signed certificate (see “Create and Install a Signed Certificate” on page 13-125).



## Log into InformaCast for the First Time

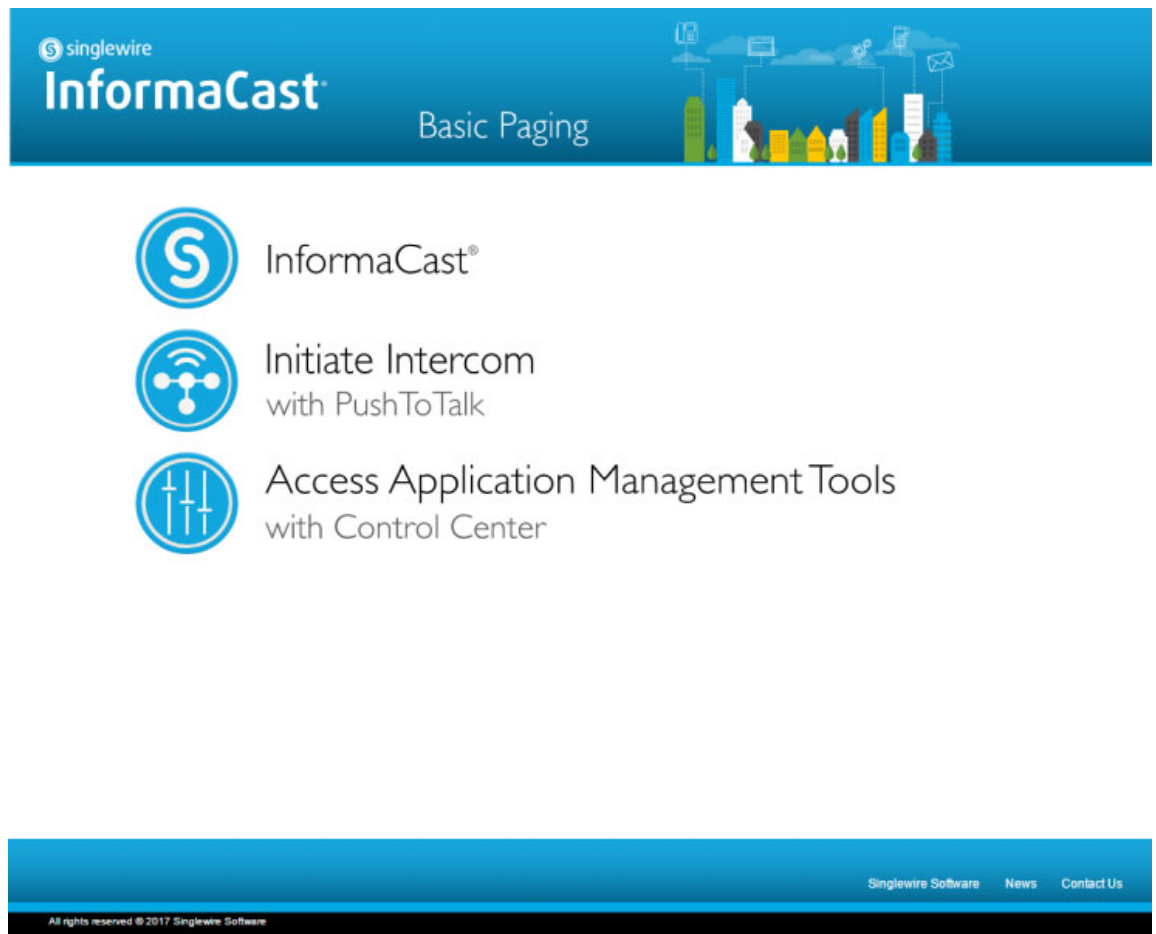


### Note

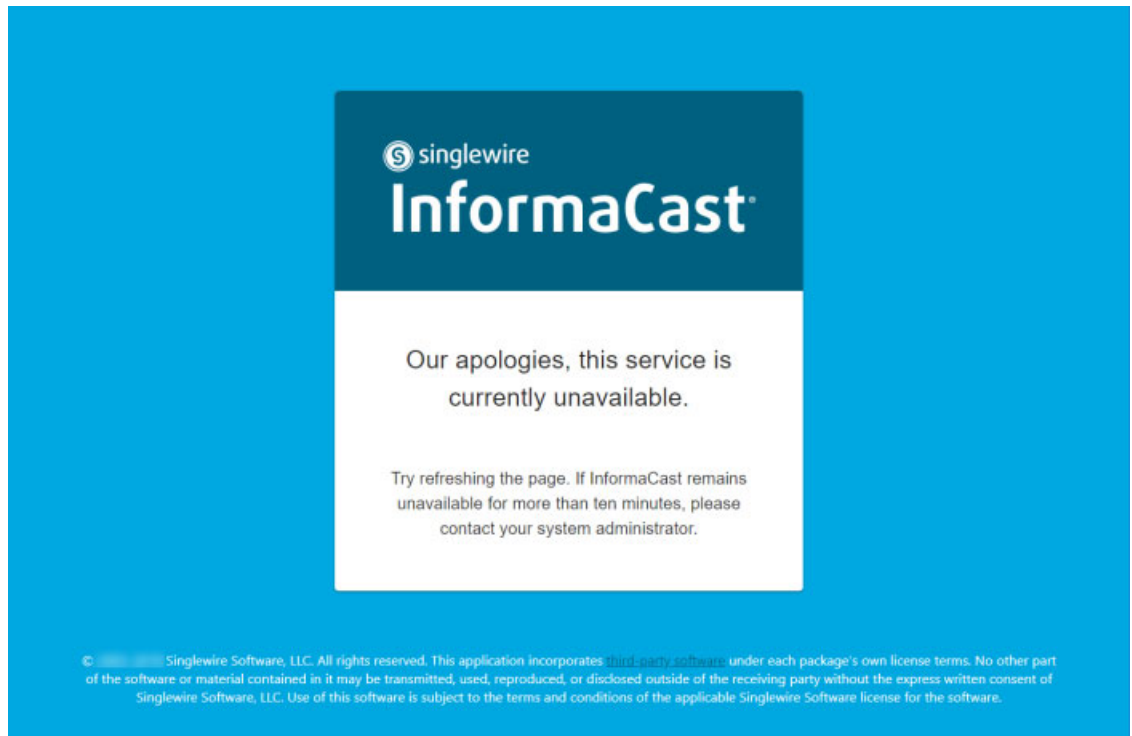
Before proceeding with configuring InformaCast, you must have properly configured your environment for multicast and successfully installed InformaCast Appliance (see and “Installation” on page 2-1). Do not continue with configuring InformaCast until you have completed these steps.

InformaCast’s web interface—where you will set up your InformaCast environment, e.g. recipient groups, SIP functionality, DialCasts, etc.—is accessed through the InformaCast Appliance landing page.

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

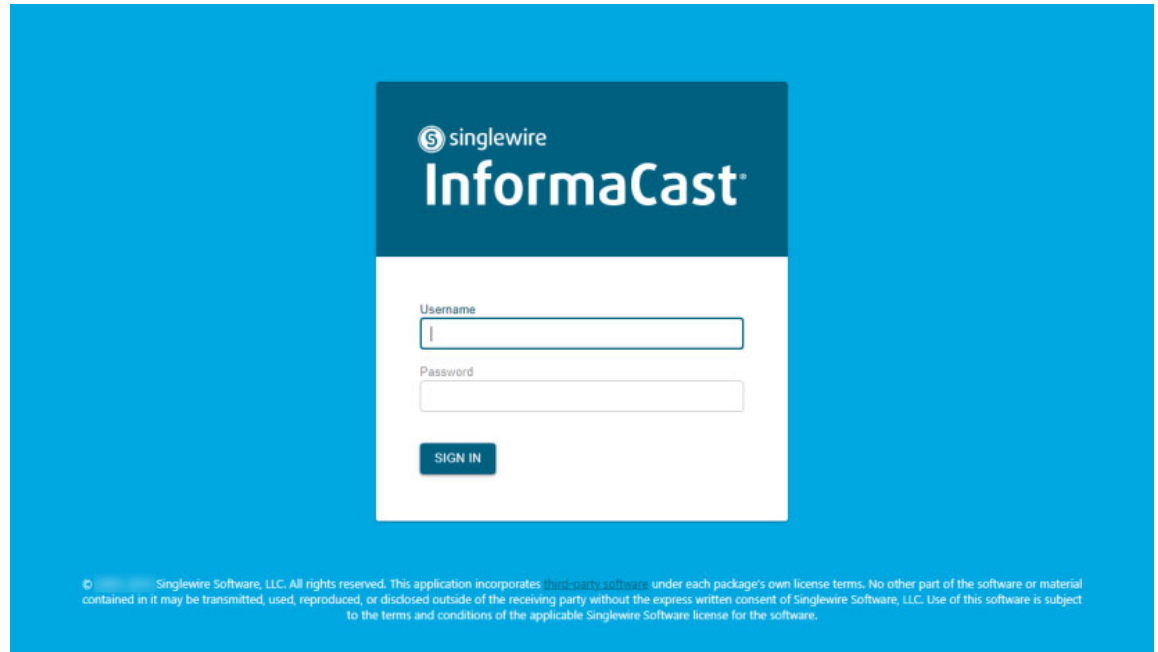


- Step 2** Click the **InformaCast** link. A separate tab/window opens to InformaCast’s Startup page. Depending on your system, there may be a delay of several minutes while InformaCast initializes.

**Note**

You may receive an error, “There is a problem with this website’s security certificate.” Since InformaCast, like Cisco Unified CM, 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 SSL certificate (see “Create and Install a Signed Certificate” on page 13-125).

Once InformaCast initializes, you will be presented with InformaCast’s Sign In page.



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

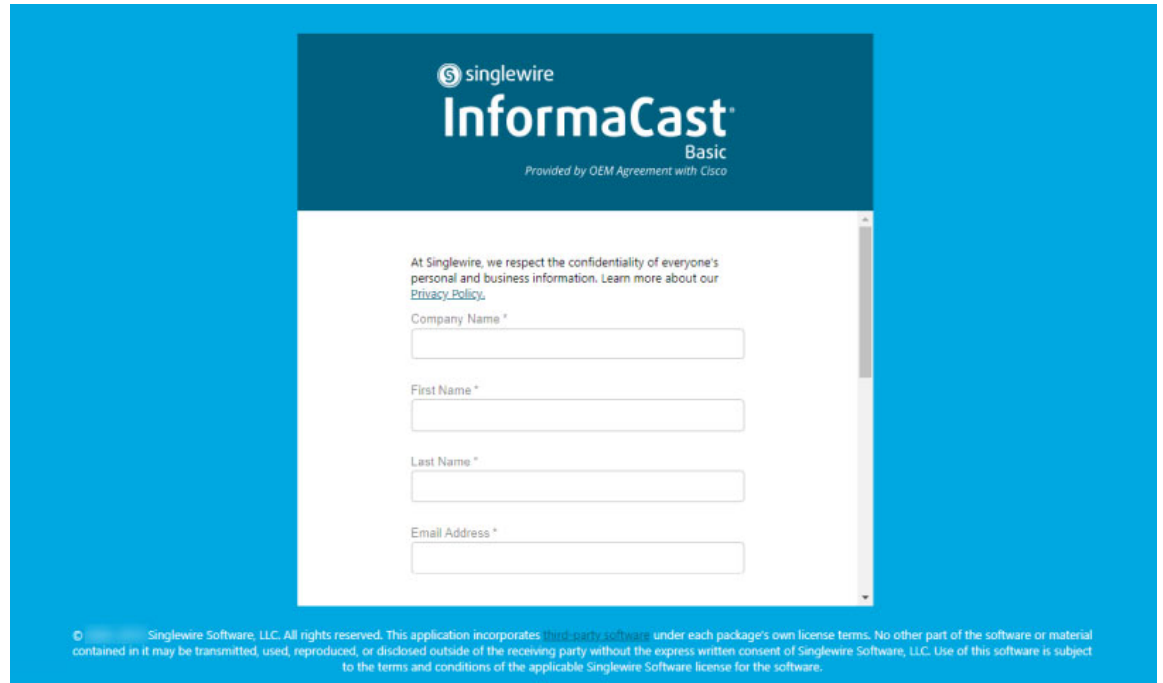
**Step 4** Enter your application password in the **Password** field. The **Password** field is also case sensitive.



**Note** These are your default credentials that you set in “Set the Initial Configuration” on page 2-31.

**Step 5** Click the **Sign In** button.

If the machine on which InformaCast is installed has internet access, a form appears.



The screenshot shows a web interface for InformaCast Basic. At the top, there is a dark blue header with the Singlewire logo and the text "InformaCast Basic" and "Provided by OEM Agreement with Cisco". Below the header is a white registration form with the following fields:

- Company Name \*
- First Name \*
- Last Name \*
- Email Address \*

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

**Note**

With internet access, 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 Dashboard page.

**Dashboard**

**Welcome to InformaCast**  
**Basic Paging (Cisco Paging Server)**

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
- Create unlimited recipient groups of 50 phones or less

[Technical Support](#)  
[User Guide](#)

**Reach More People and Devices**

Upgrade to InformaCast Advanced and enjoy a full-featured emergency notification solution that allows you to reach an unlimited number of phones as well as a variety of other endpoints, send text and live or pre-recorded audio as messages, add broadcast confirmations, and much more.

Click the Buy button to begin the process of obtaining an InformaCast Advanced license. You can also click the Try button to start your free 60-day InformaCast Advanced trial. If you would like more information, click the Demo button to request a demo.

**InformaCast Advanced**

[BUY](#) [TRY](#) [DEMO](#)

**Features Include:**

- Live audio paging between Cisco IP Phones, with no limit on the number of phones per group
- Integration to existing overhead paging systems
- Text and audio (live or pre-recorded) to Cisco IP Phones and other endpoints
- Audio broadcasts to IP Speakers
- 911/emergency call monitoring/alerting/recording
- Automated weather notifications
- Dynamically-triggered emergency conference calls
- Pre-recorded/scheduled broadcasts(school bells/shift changes)
- Notification to computer desktops (Windows and MacOS) via [InformaCast Desktop Notifier](#)
- Integrate with digital signage solutions and 3rd-party mass notification providers
- Notification and confirmation to mobile devices (Apple, Android, and SMS) with [InformaCast Fusion](#)
- Trigger notification to/from other systems (panic/duress buttons, door locks, lights, etc.)
- And More

**Learn More**

- [InformaCast Details](#)

Skip to Step 7 on page 3-8.

**Step 6** Fill out the form and click the **Submit** button. The InformaCast Dashboard page appears.

**Dashboard**

## Welcome to InformaCast Basic Paging (Cisco Paging Server)

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
- Create unlimited recipient groups of 50 phones or less

[Technical Support](#)  
[User Guide](#)

### Reach More People and Devices

Upgrade to InformaCast Advanced and enjoy a full-featured emergency notification solution that allows you to reach an unlimited number of phones as well as a variety of other endpoints, send text and live or pre-recorded audio as messages, add broadcast confirmations, and much more.

Click the Buy button to begin the process of obtaining an InformaCast Advanced license. You can also click the Try button to start your free 60-day InformaCast Advanced trial. If you would like more information, click the Demo button to request a demo.

**InformaCast Advanced**

[BUY](#) [TRY](#) [DEMO](#)

### Features Include:

- Live audio paging between Cisco IP Phones, with no limit on the number of phones per group
- Integration to existing overhead paging systems
- Text and audio (live or pre-recorded) to Cisco IP Phones and other endpoints
- Audio broadcasts to IP Speakers
- 911/emergency call monitoring/alerting/recording
- Automated weather notifications
- Dynamically-triggered emergency conference calls
- Pre-recorded/scheduled broadcasts(school bells/shift changes)
- Notification to computer desktops (Windows and MacOS) via [InformaCast Desktop Notifier](#)
- Integrate with digital signage solutions and 3rd-party mass notification providers
- Notification and confirmation to mobile devices (Apple, Android, and SMS) with [InformaCast Fusion](#)
- Trigger notification to/from other systems (panic/duress buttons, door locks, lights, etc.)
- And More

### Learn More

- [InformaCast Details](#)

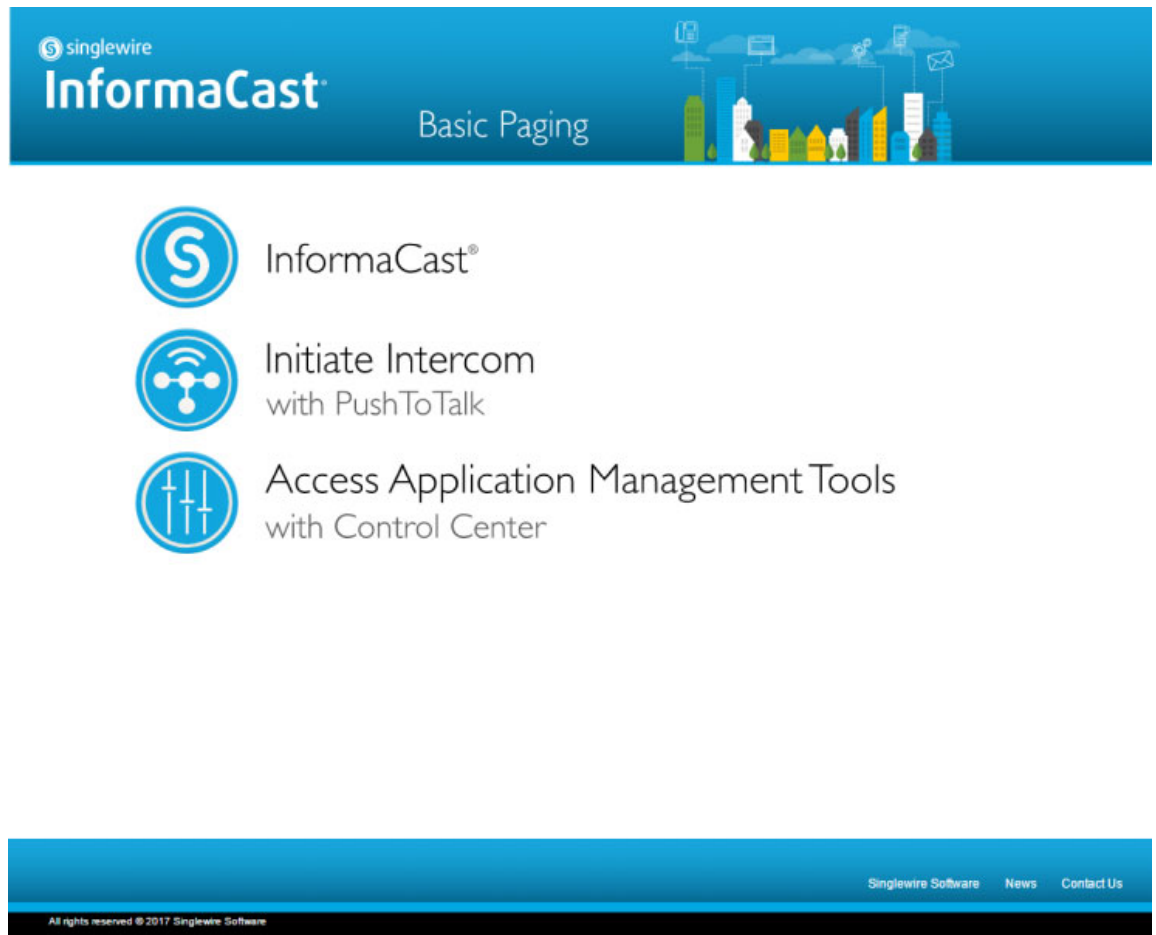
Now that you've logged into InformaCast for the first time, you'll follow the steps in “Log into InformaCast” on page 3-9 for every subsequent login.

**Step 7** Continue with “Broadcast Parameters Management” on page 7-1.

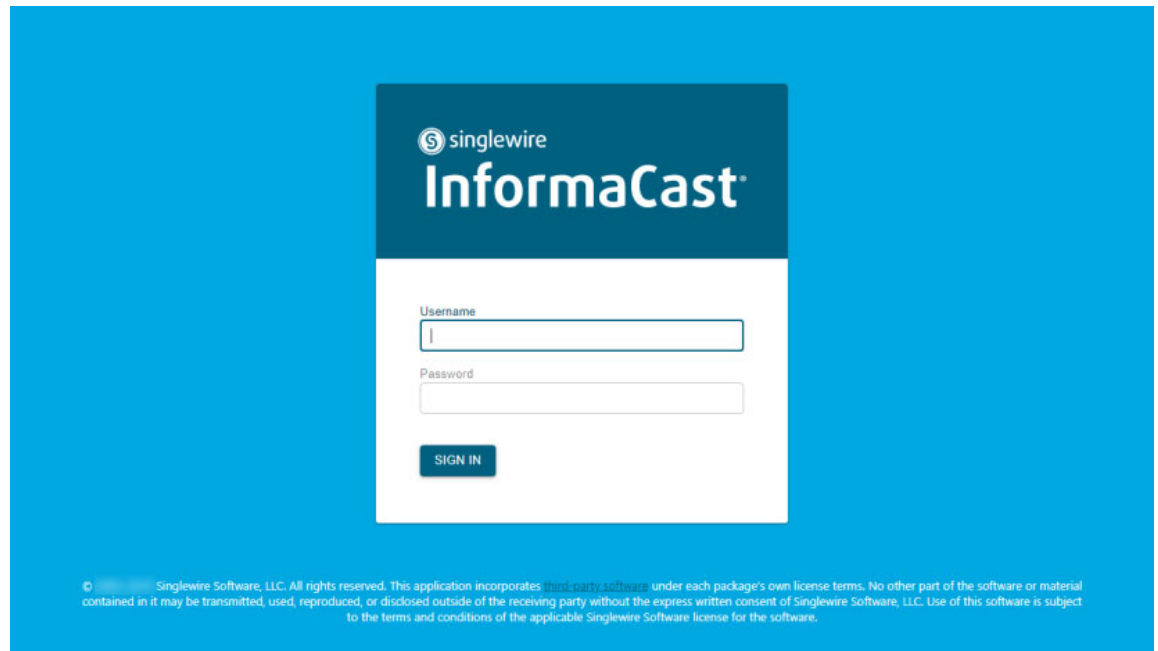
## Log into InformaCast

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 Appliance, and press the **Enter** key. The InformaCast Appliance landing page appears.



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



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

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



**Step 4** Click the **Sign In** button. InformaCast’s Dashboard page appears.

**Dashboard**

**Welcome to InformaCast  
Basic Paging (Cisco  
Paging Server)**

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
- Create unlimited recipient groups of 50 phones or less

[Technical Support](#)  
[User Guide](#)

**Reach More People and Devices**

Upgrade to InformaCast Advanced and enjoy a full-featured emergency notification solution that allows you to reach an unlimited number of phones as well as a variety of other endpoints, send text and live or pre-recorded audio as messages, add broadcast confirmations, and much more.

Click the Buy button to begin the process of obtaining an InformaCast Advanced license. You can also click the Try button to start your free 60-day InformaCast Advanced trial. If you would like more information, click the Demo button to request a demo.

**InformaCast Advanced**

[BUY](#) [TRY](#) [DEMO](#)

**Features Include:**

- Live audio paging between Cisco IP Phones, with no limit on the number of phones per group
- Integration to existing overhead paging systems
- Text and audio (live or pre-recorded) to Cisco IP Phones and other endpoints
- Audio broadcasts to IP Speakers
- 911/emergency call monitoring/alerting/recording
- Automated weather notifications
- Dynamically-triggered emergency conference calls
- Pre-recorded/scheduled broadcasts(school bells/shift changes)
- Notification to computer desktops (Windows and MacOS) via [InformaCast Desktop Notifier](#)
- Integrate with digital signage solutions and 3rd-party mass notification providers
- Notification and confirmation to mobile devices (Apple, Android, and SMS) with [InformaCast Fusion](#)
- Trigger notification to/from other systems (panic/duress buttons, door locks, lights, etc.)
- And More

**Learn More**

- [InformaCast Details](#)

## 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 Cisco IP phone for Unified CM or the side button of the 7921G wireless Cisco 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.

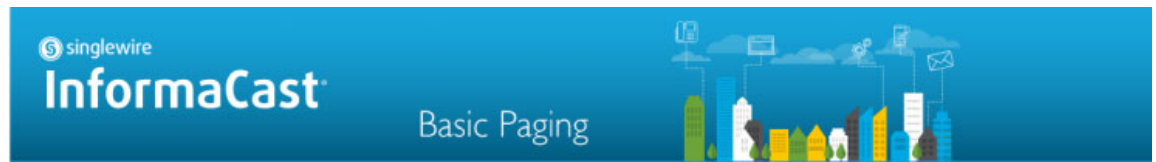
**Note**

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 InformaCast 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 Appliance landing page, and press the **Enter** key. The InformaCast Appliance landing page appears.



InformaCast®



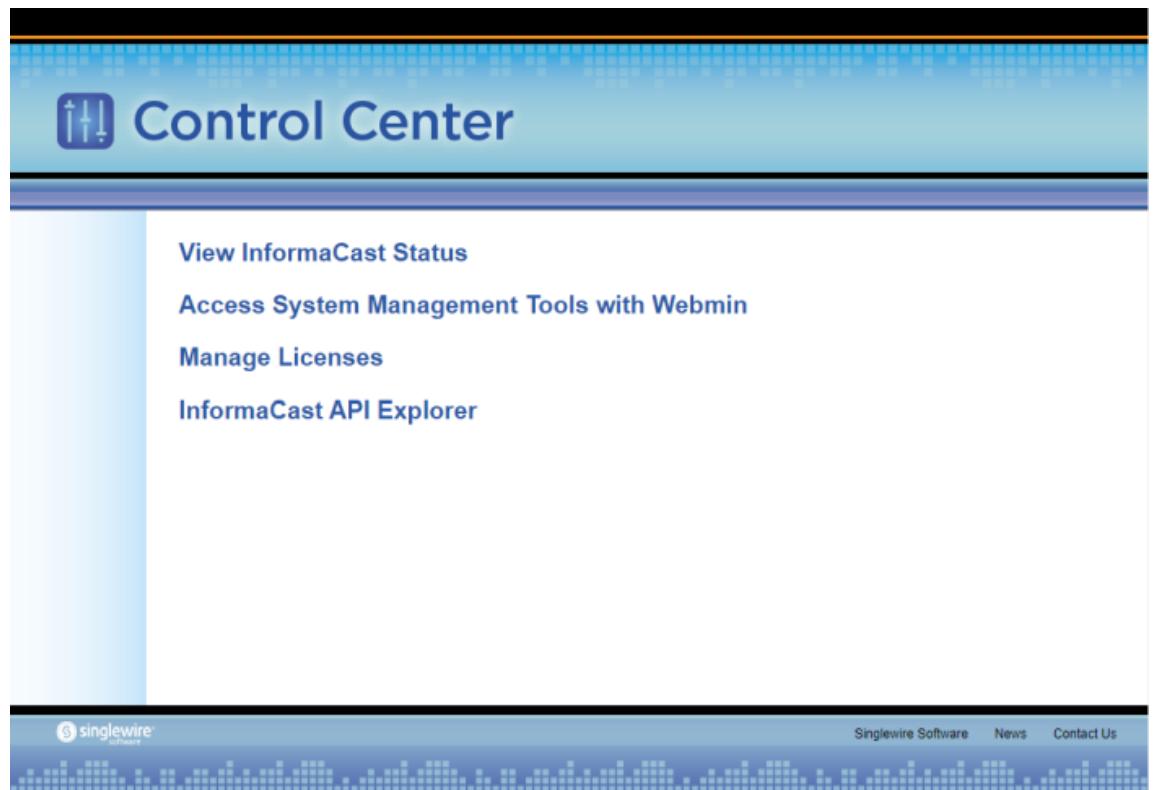
Initiate Intercom  
with PushToTalk



Access Application Management Tools  
with Control Center



**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.

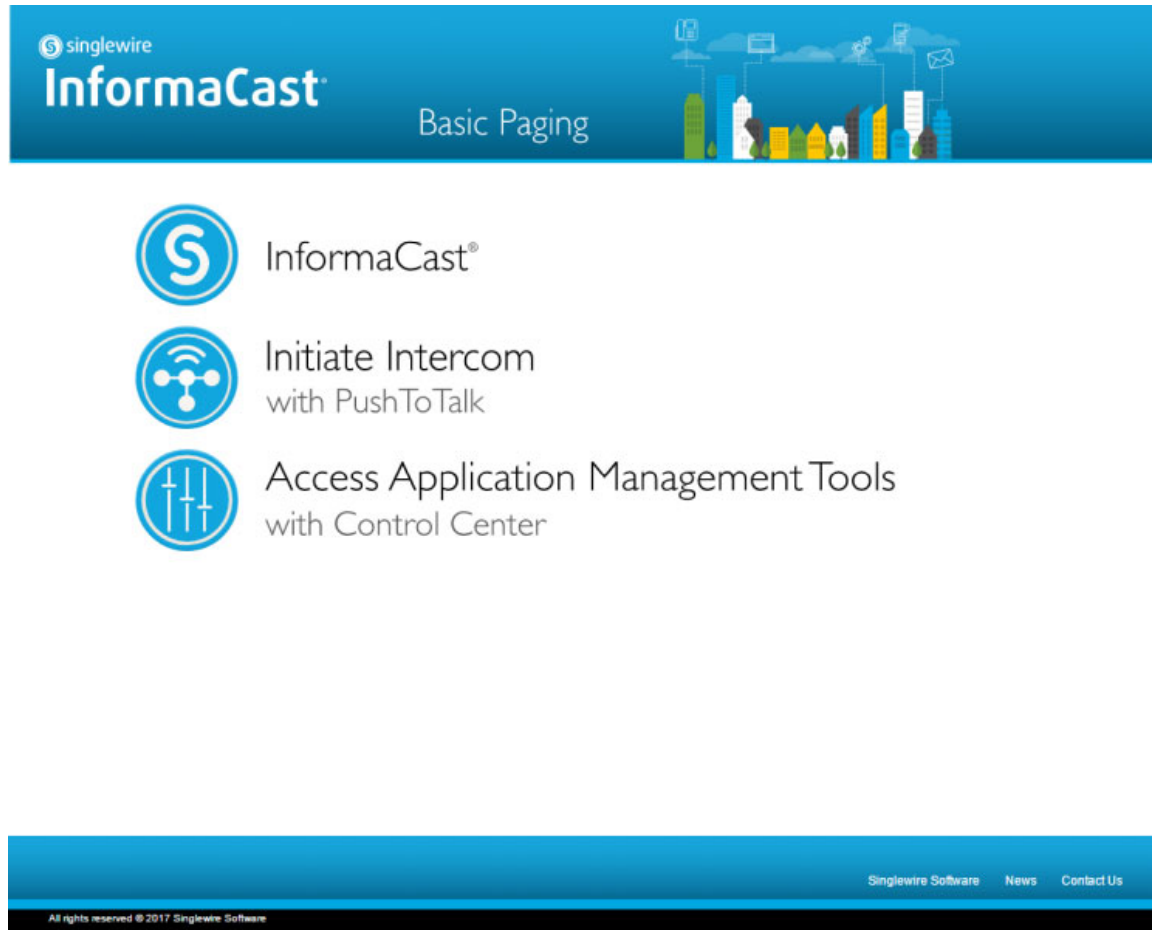
From the Control Center menu page, you can access InformaCast Appliance's accessory actions:

- Webmin access (see "Log into Webmin" on page 3-14)
- License key management (see "License Key Management" on page 4-1)
- [API Explorer](#)

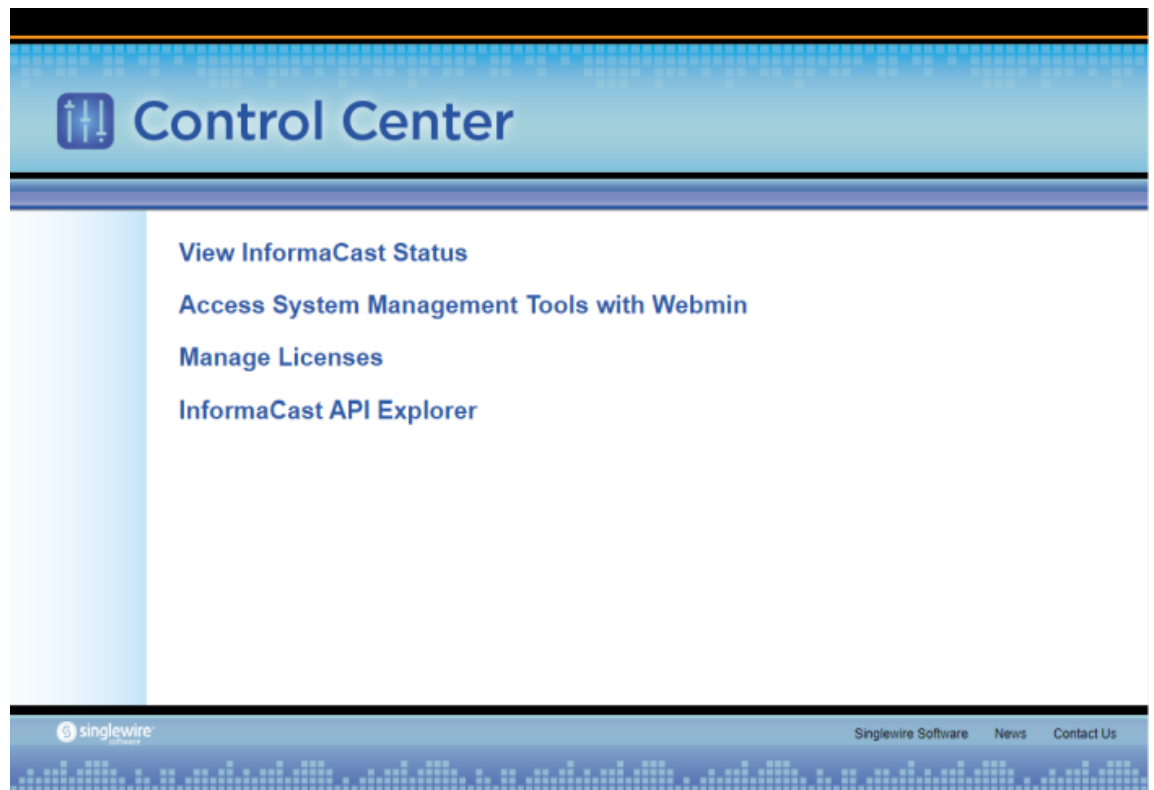
## Log into Webmin

Webmin's interface is used primarily for installing new software packages, collecting and viewing logs, starting/stopping/restarting applications' services, rebooting the InformaCast Appliance server, capturing network traffic, etc.

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

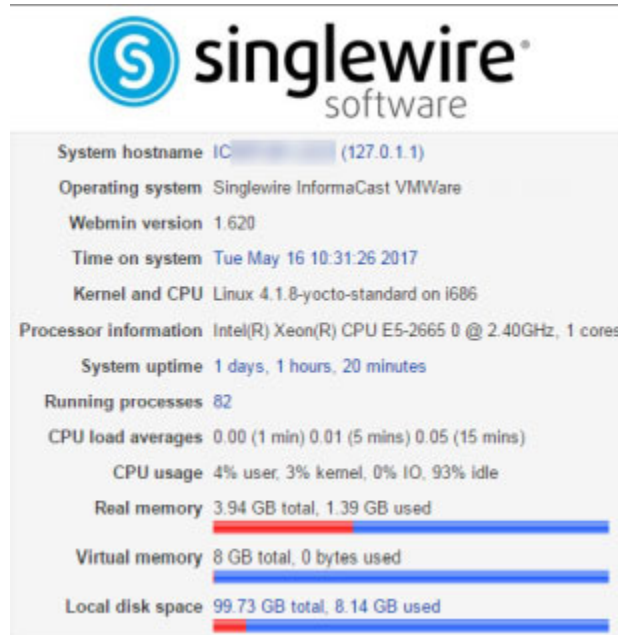


- Step 3** Click the **Access System Management Tools with Webmin** link. A separate tab/window opens to the Login to Webmin page.

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

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

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



The Webmin homepage displays version information and CPU and disk statistics about the InformaCast Appliance.

The table in “System Management” on page 13-1 provides you with summaries of the actions you can take within Webmin.

## 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 InformaCast 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](#).



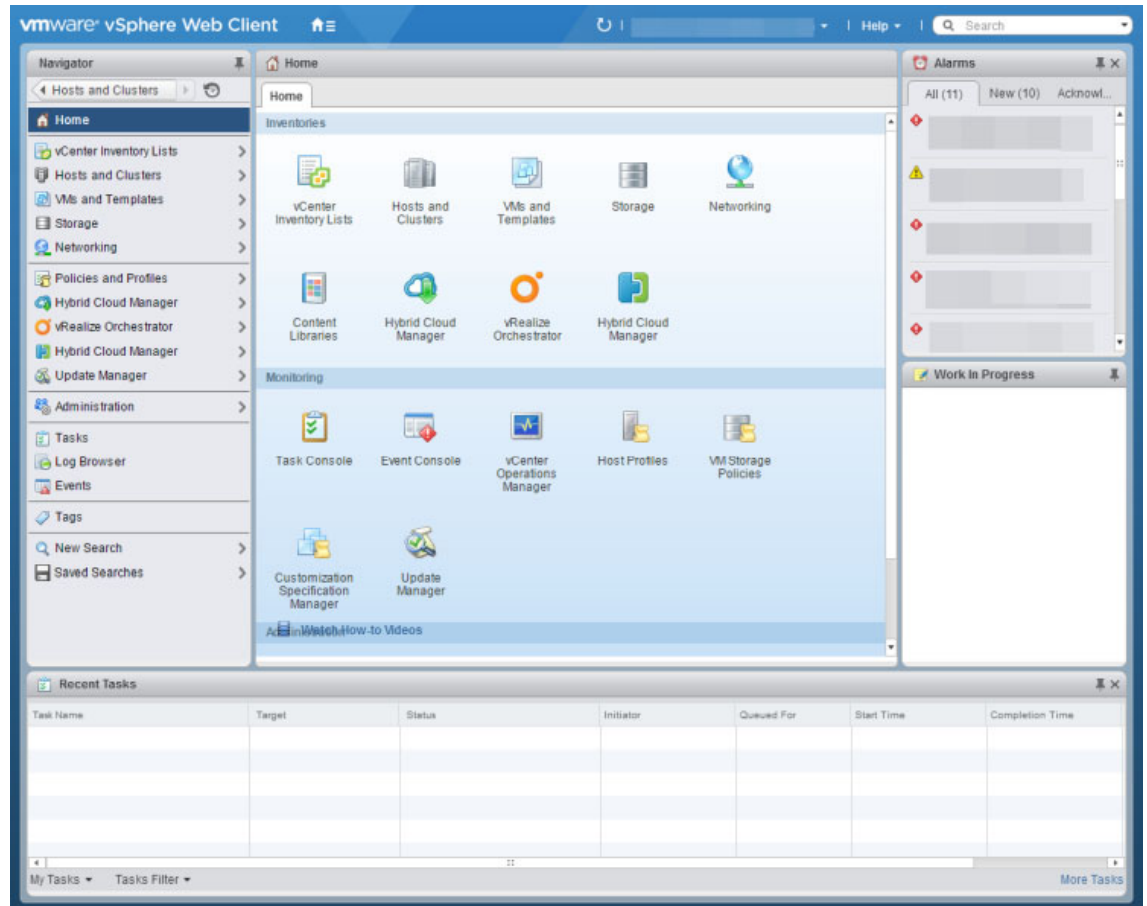
### Note

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

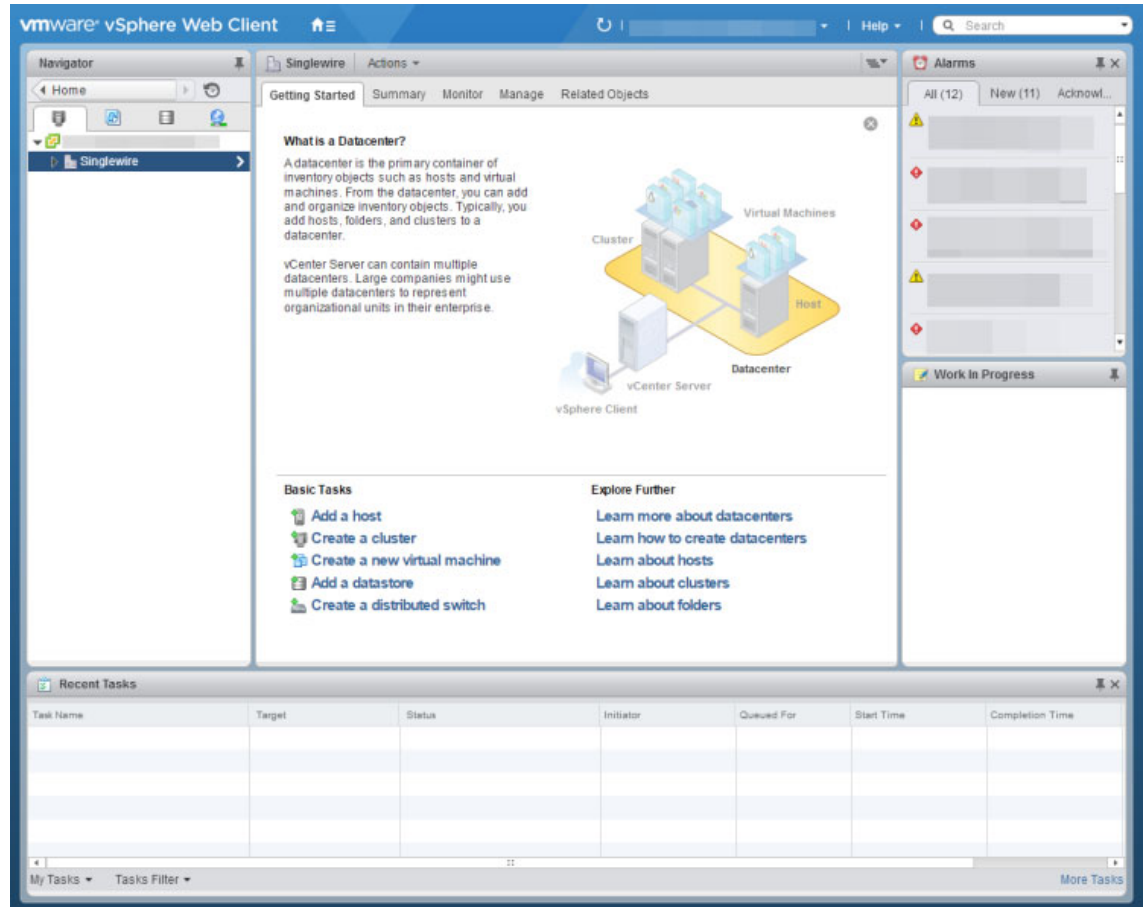
## Use a Virtual Machine Console Window

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

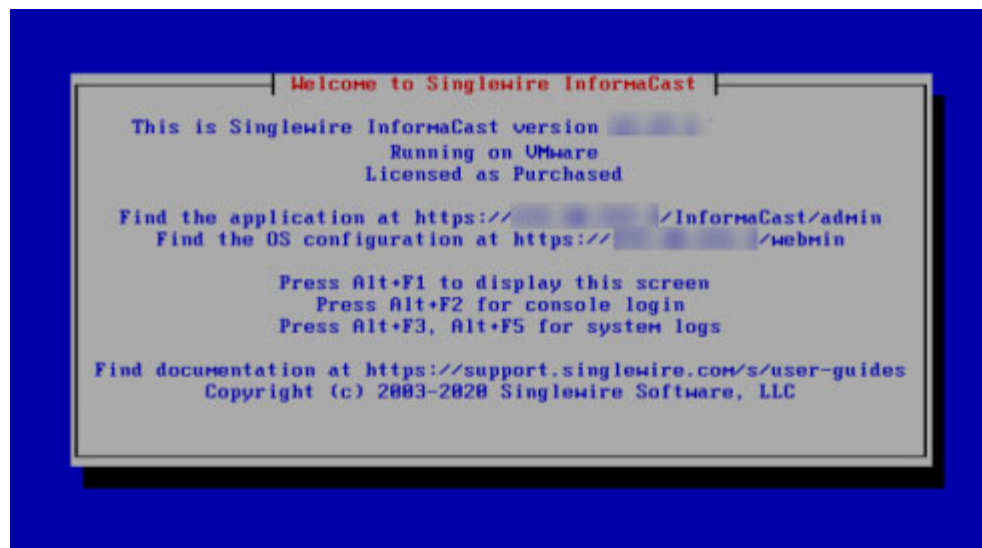
**Step 1** Open a web browser and log into your vSphere web client. The vSphere Web Client page appears.



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



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





Upon opening a console, the InformaCast 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.

```
Singlewire InformaCast/VMware
singlewire login: _
```

- 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.

```
Singlewire InformaCast/VMware
singlewire login: admin
Password:

Welcome to Singlewire InformaCast version
Running on VMware
Licensed as Subscription

admin@singlewire:~$ _
```

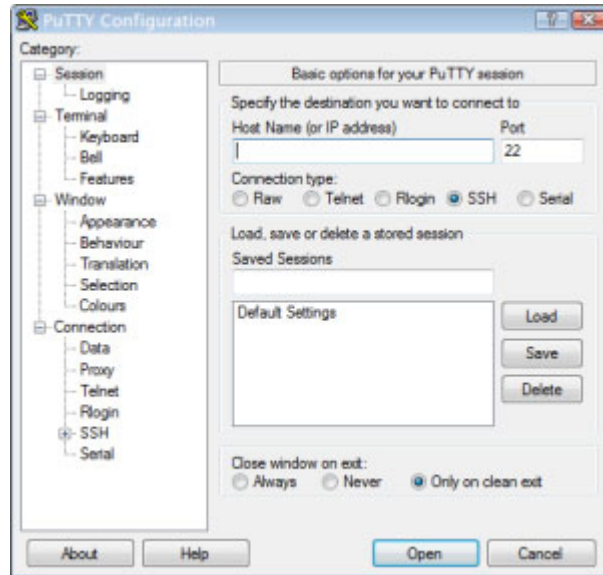


**Tip** Press the **Alt + F3** or **Alt + F5** keys to see the logs available through the Status screen.

## 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.

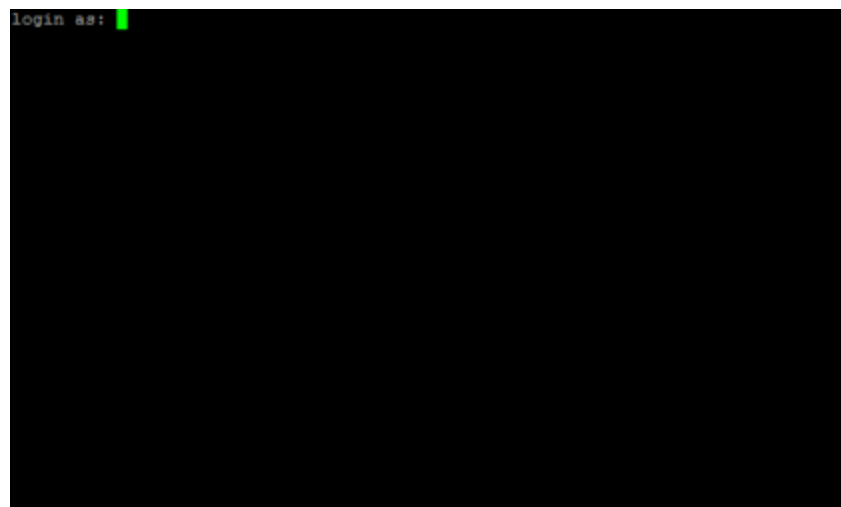


**Step 2** Enter your InformaCast Appliance's IP address in the **Host Name (or IP address)** field.

**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 InformaCast 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.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$
```



## License Key Management

The InformaCast Appliance'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:

- 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 for Unified CM
- InformaCast Advanced Notification functionality includes the ability to:
  - Send different types of broadcasts to a wide variety of recipients
  - Receive confirmations from recipients when broadcasts are sent
  - Attach scripts to broadcasts to create a customized integration with an outside system
  - Send patterns of tones to alert students to changing classes or workers to changing shifts, etc.

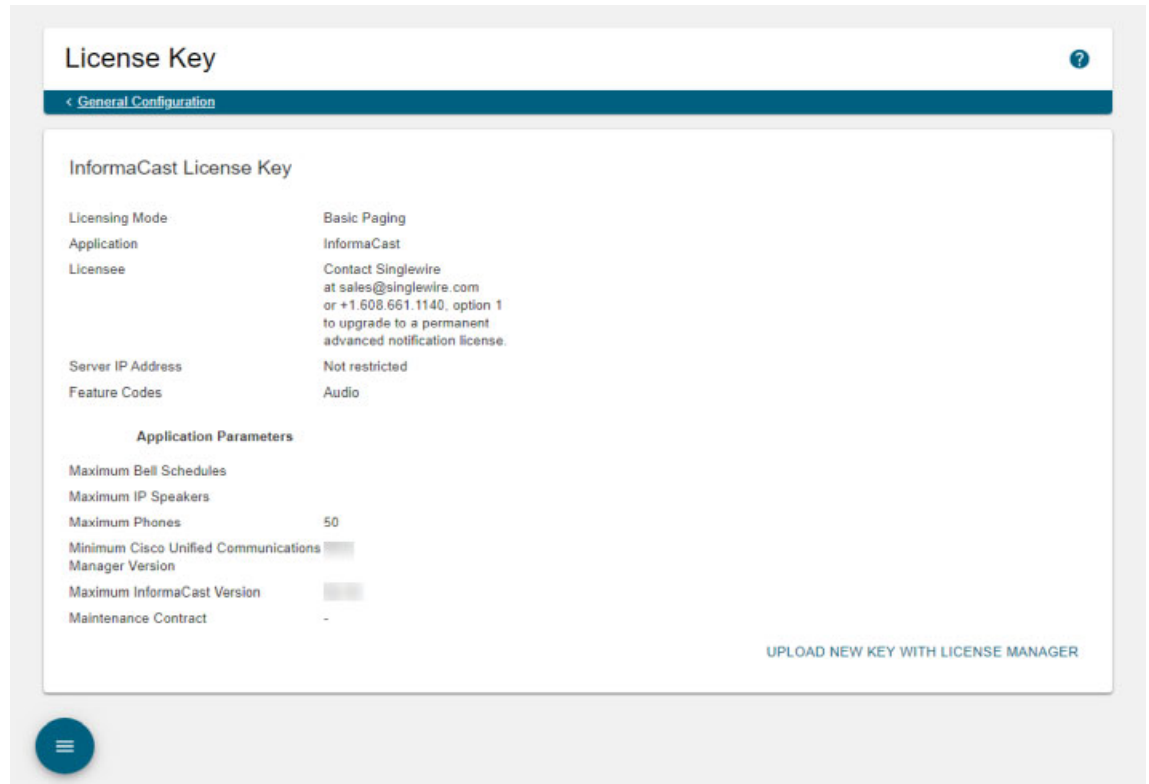
It's a good idea to view your license's functionality (see “View Your License Key” on page 4-2) and ensure you've got the level of access you expect. If you need to add InformaCast functionality, you'll need to [contact Singlewire](#) to obtain a new license and then upload it (see “Upload a New License” on page 4-2).

For a further discussion of how licensing works in InformaCast, see “Licensing Information” on page 1-7.

## View Your License Key

Your InformaCast license key contains your designated functionality for InformaCast, e.g. Basic vs. Advanced, the number of Cisco IP phones for Unified CM to which you can broadcast, trial vs. demonstration vs. subscription vs. perpetual, etc.

**Step 1** Go to **System Administration | General Configuration | License Key**. The License Key page appears.



**Step 2** Ensure that the following are correct:

- Basic Paging appears as your licensing mode
- Audio appears as your feature code
- The maximum InformaCast version is equal to or greater than your current version (visible on the Overview page)

## Upload a New License

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.

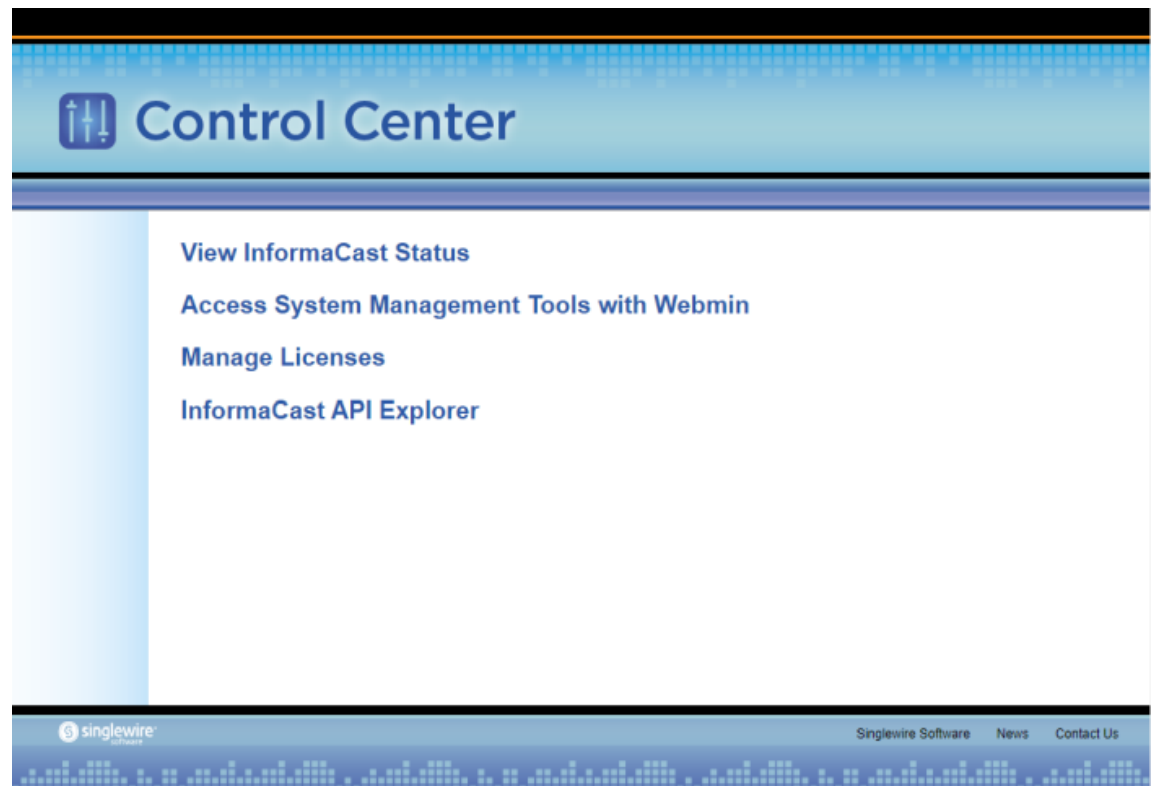
Before you can perform these steps, you must have an InformaCast Appliance license, which will be in the form of an XML file that was sent to you by email from a Singlewire sales representative. If your salesperson has not already provided one to you, [contact Singlewire](#) and request that a license be emailed to you. Make sure to save this XML 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 3-12 for specific steps).



**Note** For versions of InformaCast Appliance prior to 8.4, you will need to go to <https://<InformaCast Appliance IP Address>/LicenseManager>, where <InformaCast Appliance IP Address> is the InformaCast Appliance’s statically configured IP address. Skip to Step 3 on page 4-4.

A separate tab/window opens to the Control Center page.



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



The screenshot shows the License Manager interface. At the top, there is a blue header with the text "License Manager" and a sub-header "Manage your license keys for all Singlewire products." On the right side of the header, there is a "Log Out" link. Below the header, there is a navigation menu with a "Return to Control Center Menu" link. The main content area contains a login form with "Login" and "Password" input fields and a "LOGIN" button. The footer includes the Singlewire logo, navigation links for "Singlewire Software", "News", and "Contact Us", and a copyright notice: "© 2003–2017 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software."

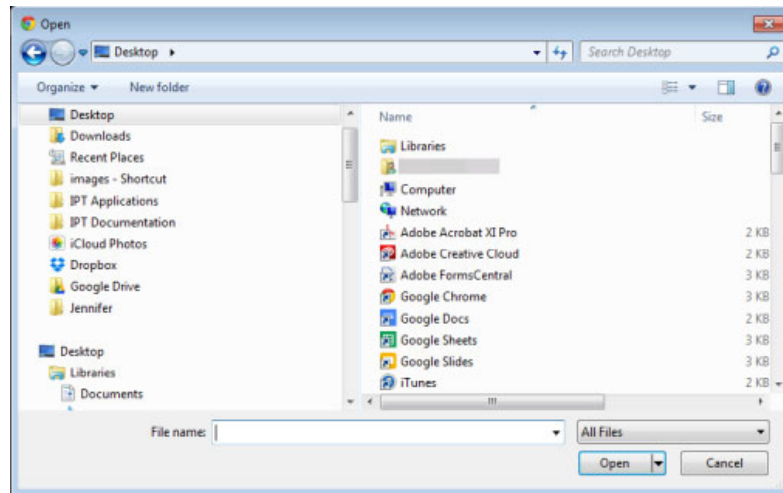
**Step 3** Enter your OS credentials in the **Login** and **Password** fields.

**Step 4** Click the **Login** button. The Upload a New License page appears.



The screenshot shows the License Manager interface after clicking the "Login" button. The main content area now displays "Upload a New License". Below this heading, there is a note: "Note: If you have questions about your license, the [Licensing FAQ](#) may help you. If you need a new license or assistance with your current one, please contact [licensing@singlewire.com](mailto:licensing@singlewire.com)." Below the note, there is a form for uploading a license file, consisting of a text input field labeled "Upload Your License File:" and a "Browse..." button. A blue "UPLOAD" button is positioned below the form. The footer is identical to the previous screenshot, including the Singlewire logo, navigation links, and copyright notice.

**Step 5** Click the **Browse** button. The Open dialog box 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 appears with a confirmation that the license has been uploaded.

**License Manager**  
Manage your license keys for all Singlewire products Log Out

[Return to Control Center Menu](#)

### License Status

**License file installed.** Restart any running applications that do not automatically reload their license.

**Note:** If you have questions about your license, the [Licensing FAQ](#) may help you. If you need a new license or assistance with your current one, please contact [licensing@singlewire.com](mailto:licensing@singlewire.com).

**Warning:** Uploading a license that indicates Advanced Notification *may* cause an automatic and immediate restart of InformaCast. Please refer to your documentation for more information.

The currently installed License Keys contain the following features:

[InformaCast](#)

**Issuer:** [Redacted]  
**Created:** Tue Apr 25 10:09:17 CDT 2017  
**Licensee:** \*\*\* LAB USE ONLY \*\*\*  
 Singlewire Test License Generated by [Redacted]  
 \*\*\* LAB USE ONLY \*\*\*

**IP Restriction:** Not restricted  
**Expiration:** No expiration  
**Features:** Audio, MessageConfirmation, Resiliency  
**Parameters:** MaintenanceContract=12345, MaxBellSchedules=1000, MaxIPSpeakers=1000, MaxPhones=1000, MaxVersion=13.0, Scheme=Purchased

[IC Plugin: Paging Gateway](#)

**Issuer:** [Redacted]  
**Created:** Tue Apr 25 10:09:17 CDT 2017  
**Licensee:** \*\*\* LAB USE ONLY \*\*\*  
 Singlewire Test License Generated by [Redacted]  
 \*\*\* LAB USE ONLY \*\*\*

**IP Restriction:** Not restricted  
**Expiration:** No expiration  
**Features:**  
**Parameters:** maxPagingGateways=1000

[IC Plugin: CallAware](#)

**Issuer:** [Redacted]  
**Created:** Tue Apr 25 10:09:17 CDT 2017  
**Licensee:** \*\*\* LAB USE ONLY \*\*\*  
 Singlewire Test License Generated by [Redacted]  
 \*\*\* LAB USE ONLY \*\*\*

**IP Restriction:** Not restricted  
**Expiration:** No expiration  
**Features:**  
**Parameters:**

[IC Plugin: Night Bell](#)

**Issuer:** [Redacted]  
**Created:** Tue Apr 25 10:09:17 CDT 2017  
**Licensee:** \*\*\* LAB USE ONLY \*\*\*  
 Singlewire Test License Generated by [Redacted]  
 \*\*\* LAB USE ONLY \*\*\*

**IP Restriction:** Not restricted  
**Expiration:** No expiration  
**Features:**  
**Parameters:**

Replace Your License(s)  No file chosen

© 2003–2017 Singlewire Software, LLC. All rights reserved. This application incorporates third-party software under each package's own license terms. No other part of the software or material contained in it may be transmitted, used, reproduced, or disclosed outside of the receiving party without the express written consent of Singlewire Software, LLC. Use of this software is subject to the terms and conditions of the applicable Singlewire Software license for the software.

**Note**

---

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** Restart the affected service, e.g. the singlewireInformaCast service (see “Restart a Service on the InformaCast Appliance” on page 13-10).

It may take a moment for the application to restart.

---



## InformaCast Summary and Diagnostics

InformaCast's Overview page displays various statistics associated with the configuration of InformaCast, such as the amount of time for which the current session of InformaCast has been running, your version of InformaCast, the health of your connection to Cisco Unified CM; the CTI

route points and ports you configured and their status with Cisco Unified CM; and whether your backups and Cisco IP phone for Unified CM updates have been configured.

The screenshot displays the 'Overview' page of the InformaCast system. At the top, there are two summary cards: '1 Recipient Groups' and '1 Messages'. Below these are four log links: 'API LOG', 'PERFORMANCE LOG', 'SIP STACK LOG', and 'SUMMARY LOG'. The main content area is divided into several sections:

- InformaCast Server:** Shows 'Version: [redacted] - 105 Basic Paging license', 'Application Mode: Stand-alone', and 'Backup Activated: No'.
- SIP:** Shows 'User Agent Status: User Agent is running' and 'Calls: None'.
- Multicast Ports:** Shows 'Number of Ports Configured: 301', 'Audio Broadcast Ports: 0', 'Talk and Listen Message Ports: 0', and 'Number of Unused Ports: 301'.
- JTAPI:** Shows 'JTAPI Version: Cisco Jtapi version 12.0(0.98000)-3 Release', 'Send Commands by JTAPI: Yes', 'Create Telephony Terminals for All Phones: Yes', 'Maximum Devices per Provider: 2000', 'Terminals Requested: 19', and 'Terminals Created: 0'.
- Phone Updates:** Shows 'Last Attempted Rebuild: 2020-09-10 16:10:00', 'Last Successful Rebuild: 2020-09-10 16:19:03', 'Next Phone Rebuild: 2020-09-10 17:10:00', 'Last Attempted Refresh: Never', 'Last Successful Refresh: Never', 'Phones Retrieved: 49946', 'Phones Used/Licensed: 0/50', and 'Refresh Interval (minutes): Disabled'.
- Cisco Unified Communications Manager Clusters:** A table with columns: Description, CTI Provider Secure, CTI Provider, and Version.
 

Description	CTI Provider Secure	CTI Provider	Version
Default configuration	No	[redacted]	12.0.1.10000-10
- CTI Port:** A table with columns: Name, DDI, State, Registered Address, Active Calls, Marked for Deletion, and User Description. It shows 'No Data'.
- Route Point:** A table with columns: Name, DDI, State, and Active Calls. It shows 'No Data'.
- SIP Calls:** A table with columns: Start Time, From, and To. It shows 'No Data'.

Use the Overview page for troubleshooting purposes, or as an indicator that certain configuration changes have taken place, i.e. backups have been configured or Cisco Unified CM can communicate with InformaCast.



## Log Directory

The Log Directory page allows you to view a list of InformaCast's logs and download them, as needed. InformaCast's logs contain a variety of information on its activities and the activities you've performed while interacting with InformaCast, as well as the activities of external services with which InformaCast interacts.

**Step 1** Go to the **User** dropdown menu | **Help** | **Log Directory**. The Log Directory page appears.

Name	Size (KB)	Last Modified	Download
audit.log	34.0 kB	2020/05/21/ 08:10:00	↓
CiscoJtapi.index	85 B	2020/05/15/ 14:10:00	↓
CiscoJtapi001.log	0 B	2020/05/15/ 14:10:00	↓
meta.log	0 B	2020/05/14/ 23:12:28	↓
performance.log	8.0 MB	2020/05/21/ 08:56:21	↓
pool.log	1.0 kB	2020/05/15/ 13:48:08	↓
pool.logpid	32 B	2020/05/15/ 13:46:47	↓
pool2.log	0 B	2020/05/14/ 23:12:28	↓
pool2.logpid	0 B	2020/05/14/ 23:12:28	↓
ras-20200515-000000.log.gz	174 B	2020/05/15/ 13:46:08	↓

On the Log Directory page, you will find the following logs:

- **audit.log**. A record of the changes that have been made to InformaCast.

- **CiscoJtapi.index.** Cisco JTAPI stores the index of the current CiscoJtapiXXX.log file in this log.
- **CiscoJtapi###.log.** Cisco JTAPI records its activities in these logs. In production, there may be up to 100 of these files.
- **meta.log.** The Business Intelligence and Reporting Tools (BIRT) reporting tool uses this file for logging its activities.
- **performance.log.** The general information/debugging log. It's most commonly used by Singlewire Support when looking for errors and warnings in the user interface or API.
- **pool.log.** The Berbee Reusable Lightweight Architecture Project (BRLAP) library uses this file for logging its database connection pool activities.
- **pool.logpid.** The PID log file for the BRLAP database connection pool.
- **ras-yyyymmdd-000000.log.** A log file of the rust activation service's activities. This service runs on the virtual machine to provide high-speed phone authentication services.
- **restApi.json.** A log of incoming and outgoing API requests, which includes the request verb, e.g. HTTP GET, PUT, POST, etc. Successful requests mostly log the status code, e.g. 20x, and errors generally log the full return response.
- **sipOptions.log.** The SIP OPTIONS requests sent from InformaCast to other SIP servers, e.g. LPI SIP server groups and SIP speaker telephony providers, and the SIP OPTIONS requests sent to InformaCast by other SIP servers.
- **sipStack.log.** The National Institute of Standards and Technology (NIST) SIP stack records its activities in this log (minus SIP OPTIONS requests, which are in the sipOptions.log). In production, there may be up to 100 of these files.
- **summary.log.** A short, concise location where broadcasts' timing and status, e.g. successful and failed recipient activation and sending events, can be found.

**Step 2** Click a log's **Download** icon to download the log from InformaCast and view it.



**Tip**

---

You may also find InformaCast logs through Webmin or the CLI (see “Access the InformaCast Appliance’s Logs” on page 13-62 for more information).

---



## Broadcast Parameters Management

Ensure that there is a valid multicast IP address (or range of addresses) for InformaCast's use and allow the DialCast IVR to send RTP packets that contain silence to the caller after the IVR has finished interacting with it.

- Step 1** Go to **System Administration | General Configuration | Broadcast Parameters**. The Broadcast Parameters page appears.

The screenshot shows the 'Broadcast Parameters' configuration page. At the top, there is a title 'Broadcast Parameters' and a breadcrumb trail '< General Configuration'. Below the title is a section for 'General Details' with a descriptive paragraph and a link for 'ADDITIONAL MULTICAST INFORMATION'. The 'Phone' section includes a 'Multicast' subsection with a warning: 'Warning: If you have Paging Gateway, changing the values of these settings may cause them to gracefully reset.' There are three input fields: 'Starting Multicast IP Address \*' with the value '239.0.1.2', 'Ending Multicast IP Address \*' with the value '239.0.1.12', and 'Multicast TTL \*' with the value '16'. The 'Broadcast Settings' section has a checkbox for 'Send Silence with DialCast IVR' which is currently unchecked. At the bottom right, there are 'CANCEL' and 'SAVE' buttons. A hamburger menu icon is visible in the bottom left corner.

- Step 2** 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 Cisco IP phones for Unified CM. 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 the InformaCast Appliance 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 the InformaCast server as having the highest priority.



---

**Note** See the [IPv4 Multicast Address Space Registry](#) for information on how multicast addresses are assigned.

---

- Step 3** 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 4** 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 5** Click the **Save** button to save your changes.
- Step 6** Continue with "Add a Cisco Unified CM Cluster" on page 9-1.
-





## Configuration Pathways

InformaCast has many features available to you. Some of these features require more configuration than others, and sometimes a set of configuration steps applies to more than one feature.

If you're not using these features, there's no need for you to be concerned with configuring them; however if you are using them, configuring them early and getting their complexity out of the way will ensure a smooth InformaCast installation.

InformaCast features that require extra configuration include:

- Sending broadcasts to Cisco IP phones for Unified CM requires integrating Cisco Unified CM with InformaCast
- Ensuring that both the communication between InformaCast and Cisco Unified CM is secure, as well as between InformaCast and its Cisco IP phones for Unified CM requires configuring CTI security
- Requiring InformaCast to validate certificates for all outbound communication via SSL and TLS requires configuring host trust
- Dialing the number of a Cisco IP phone for Unified CM and sending a broadcast to a preconfigured group of recipients, e.g. DialCasts, requires configuring Session Initiation Protocol



---

**Note**

If you are using more than one of the preceding features, it is best for you to configure them in the order they are listed.

---

The following sections provide you with the configuration order you should follow to ensure a successful installation of InformaCast.

## Broadcast to Cisco IP Phones for Unified CM

Use the steps in the following sections to configure InformaCast broadcast to Cisco IP phones for Unified CM.

- 
- Step 1** “Deploy InformaCast” on page 2-17.
  - Step 2** “Set the Initial Configuration” on page 2-31.
  - Step 3** “Log into InformaCast for the First Time” on page 3-3.
  - Step 4** “Broadcast Parameters Management” on page 7-1.
  - Step 5** “Integrate Cisco Unified CM” on page 8-3.

**Step 6** Continue with:

- One of the other configuration pathways (optional)
  - “Add a Cisco Unified CM Cluster” on page 9-1.
- 

## Secure CTI Communication

Use the steps in the following sections to ensure that both the communication between InformaCast and Cisco Unified CM is secure, as well as between InformaCast and its Cisco IP phones for Unified CM.

**Step 1** “Deploy InformaCast” on page 2-17.

**Step 2** “Set the Initial Configuration” on page 2-31.

**Step 3** “Log into InformaCast for the First Time” on page 3-3.

**Step 4** “Broadcast Parameters Management” on page 7-1.

**Step 5** “Integrate Cisco Unified CM” on page 8-3.

**Step 6** “Manage CTI Security” on page 8-49 (if you're using secure outbound communication).

**Step 7** Continue with:

- One of the other configuration pathways (optional)
  - “Add a Cisco Unified CM Cluster” on page 9-1.
- 

## Validate Certificates for Secure, Outbound Communication

Use the steps in the following sections to require InformaCast to validate certificates for all outbound communication via SSL and TLS.

**Step 1** “Deploy InformaCast” on page 2-17.

**Step 2** “Set the Initial Configuration” on page 2-31.

**Step 3** “Log into InformaCast for the First Time” on page 3-3.

**Step 4** “Broadcast Parameters Management” on page 7-1.

**Step 5** “Integrate Cisco Unified CM” on page 8-3.

**Step 6** “Manage CTI Security” on page 8-49

**Step 7** “Configure Host Trust” on page 8-48.

**Step 8** Continue with:

- One of the other configuration pathways (optional)
  - “Add a Cisco Unified CM Cluster” on page 9-1.
-

## Send a Preconfigured Broadcast

Use the steps in the following sections to dial the number of a Cisco IP phone for Unified CM and send a broadcast to a preconfigured group of recipients.

- 
- Step 1** “Deploy InformaCast” on page 2-17.
  - Step 2** “Set the Initial Configuration” on page 2-31.
  - Step 3** “Log into InformaCast for the First Time” on page 3-3.
  - Step 4** “Broadcast Parameters Management” on page 7-1.
  - Step 5** “Integrate Cisco Unified CM” on page 8-3.
  - Step 6** “Manage CTI Security” on page 8-49 (if you want to ensure that both the communication between InformaCast and Cisco Unified CM is secure, as well as between InformaCast and its Cisco IP phones for Unified CM).
  - Step 7** “Configure Host Trust” on page 8-48 (if you're using secure outbound communication).
  - Step 8** “Manage SIP Functionality” on page 8-56.
  - Step 9** Continue with:
    - One of the other configuration pathways (optional)
    - “Add a Cisco Unified CM Cluster” on page 9-1.
  - Step 10** “Manage DialCasts” on page 10-1.
- 

## Integrate Cisco Unified CM

Before you can begin sending broadcasts to Cisco IP phones for Unified CM, you must configure your version of Cisco Unified Communications Manager:

- “Configure Cisco Unified CM SNMP” on page 8-4
- “Set the Default Codec to G.711” on page 8-12
- “Create a Device Pool” on page 8-14
- “Create a Route Partition” on page 8-16
- “Create a Calling Search Space” on page 8-17
- “Create CTI Ports” on page 8-19
- “Create an Access Control Group” on page 8-24
- “Create an Application User” on page 8-28
- “Create an Application User CAPF Profile” on page 8-31
- “Enable Web Access for Cisco IP Phones” on page 8-32
- “Set Your Authentication URL” on page 8-40
- “Set the Authentication Method for API Browser Access” on page 8-42
- “Reboot Your Phones” on page 8-43

- “Test Your Phones” on page 8-45

**Tip**

When naming your Cisco Unified CM 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 10-1 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 8-56 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 Cisco Unified CM SNMP

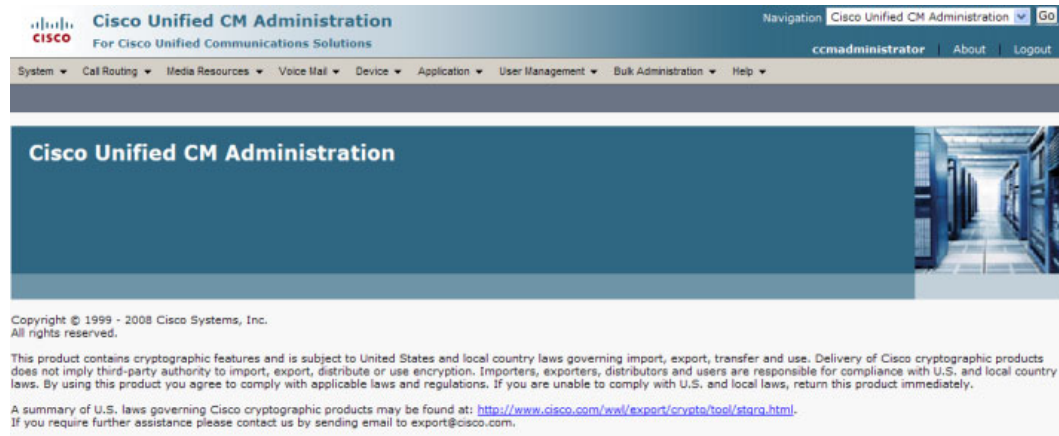
InformaCast uses SNMP to gather phone information from Cisco Unified CM. Depending on whether you are using SNMP v2 or v3, you will follow different steps:

- **SNMP v2.** Follow the steps in “Enable SNMP on Cisco Unified CM Cluster Nodes” on page 8-4 and “Create an InformaCast SNMP v2 Community String” on page 8-7.
- **SNMP v3.** Follow the steps in “Enable SNMP on Cisco Unified CM Cluster Nodes” on page 8-4 and “Create an SNMP v3 User” on page 8-9.

### *Enable SNMP on Cisco Unified CM Cluster Nodes*

You must enable SNMP on Cisco Unified CM cluster nodes that will function with InformaCast.

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

The screenshot displays the Cisco Unified Serviceability interface for Service Activation. At the top, the navigation bar includes the Cisco logo and the text 'Cisco Unified Serviceability For Cisco Unified Communications Solutions'. The user is logged in as 'ccmadministrator'. The 'Service Activation' page shows a 'Status' of 'Ready' and a 'Select Server' dropdown menu set to 'IPTCUCM613'. Below this, there are several sections of services, each with a table of service names and their activation status. The services are categorized into CM Services, CTI Services, CDR Services, Database and Admin Services, Performance and Monitoring Services, Security Services, and Directory Services. The 'Save' button is visible at the bottom of the page.

Service Name	Activation Status
<input checked="" type="checkbox"/> Cisco CallManager	Activated
<input checked="" type="checkbox"/> Cisco Tftp	Activated
<input type="checkbox"/> Cisco Messaging Interface	Deactivated
<input type="checkbox"/> Cisco Unified Mobile Voice Access Service	Deactivated
<input type="checkbox"/> Cisco IP Voice Media Streaming App	Deactivated
<input checked="" type="checkbox"/> Cisco CTIManager	Activated
<input checked="" type="checkbox"/> Cisco Extension Mobility	Activated
<input type="checkbox"/> Cisco Extended Functions	Deactivated
<input type="checkbox"/> Cisco Dialed Number Analyzer	Deactivated
<input type="checkbox"/> Cisco DHCP Monitor Service	Deactivated
<b>CTI Services</b>	
<input type="checkbox"/> Cisco CallManager Attendant Console Server	Deactivated
<input type="checkbox"/> Cisco IP Manager Assistant	Deactivated
<input type="checkbox"/> Cisco WebDialer Web Service	Deactivated
<b>CDR Services</b>	
<input type="checkbox"/> Cisco SOAP - CDRonDemand Service	Deactivated
<input type="checkbox"/> Cisco CAR Web Service	Deactivated
<b>Database and Admin Services</b>	
<input checked="" type="checkbox"/> Cisco AXL Web Service	Activated
<input type="checkbox"/> Cisco UXL Web Service	Deactivated
<input checked="" type="checkbox"/> Cisco Bulk Provisioning Service	Activated
<input type="checkbox"/> Cisco TAPS Service	Deactivated
<b>Performance and Monitoring Services</b>	
<input type="checkbox"/> Cisco Serviceability Reporter	Deactivated
<input checked="" type="checkbox"/> Cisco CallManager SNMP Service	Activated
<b>Security Services</b>	
<input type="checkbox"/> Cisco CTL Provider	Deactivated
<input type="checkbox"/> Cisco Certificate Authority Proxy Function	Deactivated
<b>Directory Services</b>	
<input type="checkbox"/> Cisco DirSync	Deactivated

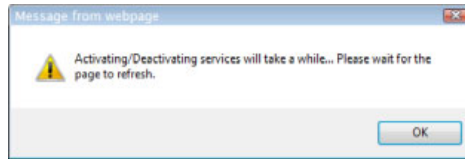


**Note** If you have more than one server, you'll have to select your server from the **Server** dropdown menu and click the **Go** button. The Service Activation page for that server will then appear.

**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

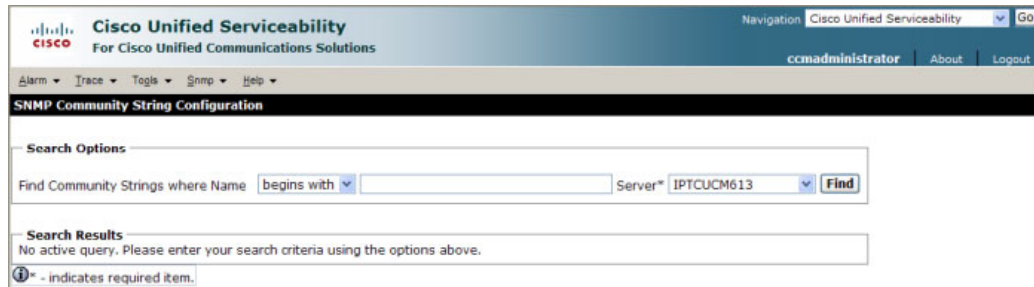
Follow these steps to create an SNMP v2 InformaCast SNMP community string.



#### Note

Skip this section if you're using SNMP v3 and go to "Create an SNMP v3 User" on page 8-9.

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



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

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

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

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

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

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

- Step 4** Enter **ICVA** into the **Community String Name** field. You will need to remember this name when you edit InformaCast's SNMP configuration in "Add a Cisco Unified CM Cluster" on page 9-1.



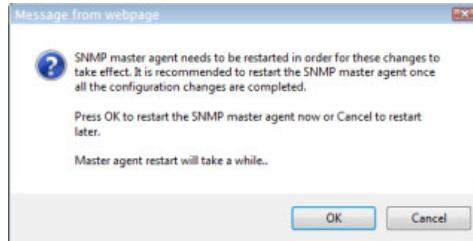


**Note** For additional security, click the **Accept SNMP packets only from these hosts** radio button and enter the InformaCast Appliance's IP address in the **Host IP Address** field.

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

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

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



### Create an SNMP v3 User

Follow these steps to create an SNMP v3 user.



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

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



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

**Search Options**

Find Users where Name  Server\*  **Find**  
 (Users where Name begins with any)

**Search Results**

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

Apply To All Nodes

**Help:**

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

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

The screenshot shows the Cisco Unified Serviceability web interface for configuring an SNMP user. The page includes the following sections and controls:

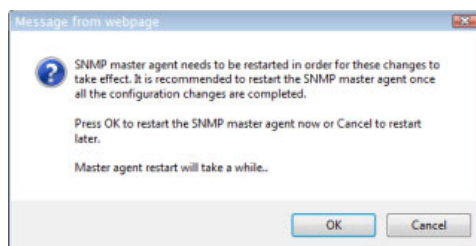
- Status:** A text field showing "Status : Ready".
- Server:** A dropdown menu currently set to "-pub--CUCM Voice/Video".
- User Information:** A text field for "User Name".
- Authentication Information:**
  - Authentication Required
  - Fields for "Password" and "Reenter Password".
  - Protocol selection:  MDS,  SHA.
- Privacy Information:**
  - Privacy Required
  - Fields for "Password" and "Reenter Password".
  - Protocol selection:  DES,  AES128,  AES192,  AES256.
- Host IP Addresses Information:**
  - Accept SNMP Packets from any host
  - Accept SNMP Packets only from these hosts
  - Field for "Host IP Address" with an "Insert" button.
  - A list box for "Host IP Addresses" with a "Remove" button.
- Access Privileges:**
  - Dropdown menu: "Access Privileges" with "-- Select Access Privilege --".
  - Information icon: "Notify access privilege is required in order to configure Notification Destinations."
- Apply To All Nodes
- Buttons: "Save", "Clear All", "Cancel".
- Legend: "i" - indicates required item.

**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.

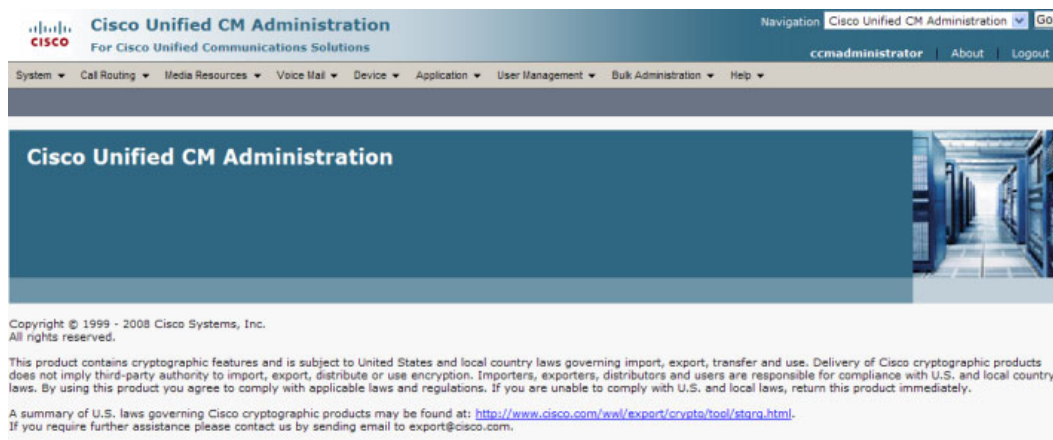
- Step 5** Select the **Authentication Required** checkbox.
- Step 6** Enter an authentication password for your user in the Password and Reenter Password fields. The password must contain at least eight characters and no more than 64.
- Step 7** Select the **SHA** radio button.
- Step 8** Select the **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 and no more than 64.
- 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 InformaCast Appliance requires that audio streams be in G.711  $\mu$ Law format. Because most Cisco Unified CM deployments use G.729 across the WAN, you need to create a region for the InformaCast 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 InformaCast 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 Cisco Unified CM. In order to have those components use the newly created G.711  $\mu$ Law region, you must first create a device pool.

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

The screenshot shows the Cisco Unified CM Administration web interface. The page title is "Find and List Device Pools". At the top, there is a navigation menu with options like System, Call Routing, Media Resources, Voice Mail, Device, Application, User Management, Bulk Administration, and Help. Below the navigation menu, there is a search bar for "Device Pool" with a dropdown menu set to "Device Pool Name" and a "begins with" filter. There are "Find", "Clear Filter", and "Add New" buttons. The page also displays "No active query. Please enter your search criteria using the options above."

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

The screenshot displays the Cisco Unified CM Administration interface for configuring a new Device Pool. The page is titled "Device Pool Configuration" and includes a navigation bar at the top with options like "System", "Call Routing", "Media Resources", "Voice Mail", "Device", "Application", "User Management", "Bulk Administration", and "Help". The user is logged in as "ccadministrator".

The configuration sections are as follows:

- Status:** Ready
- Device Pool Information:** Device Pool: New
- Device Pool Settings:**
  - Device Pool Name\* (text input)
  - Cisco Unified Communications Manager Group\* (dropdown: -- Not Selected --)
  - Calling Search Space for Auto-registration (dropdown: < None >)
  - Reverted Call Focus Priority (dropdown: Default)
  - Local Route Group (dropdown: < None >)
- Roaming Sensitive Settings:**
  - Date/Time Group\* (dropdown: -- Not Selected --)
  - Region\* (dropdown: -- Not Selected --)
  - Media Resource Group List (dropdown: < None >)
  - Location (dropdown: < None >)
  - Network Locale (dropdown: < None >)
  - SRST Reference\* (dropdown: -- Not Selected --)
  - Connection Monitor Duration\*\*\* (text input)
  - Single Button Barge\* (dropdown: Default)
  - Join Across Lines\* (dropdown: Default)
  - Physical Location (dropdown: < None >)
  - Device Mobility Group (dropdown: < None >)
- Device Mobility Related Information\*\*\*\*:**
  - Device Mobility Calling Search Space (dropdown: < None >)
  - AAR Calling Search Space (dropdown: < None >)
  - AAR Group (dropdown: < None >)
  - Calling Party Transformation CSS (dropdown: < None >)
  - Called Party Transformation CSS (dropdown: < None >)
- Incoming Calling Party Settings:**

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

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

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

At the bottom, there is a "Save" button and a legend for the asterisks used in the field labels:

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

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



**Tip**

Make sure that the Cisco Unified CM group you choose contains the Cisco Unified CM with which the InformaCast Appliance will communicate.

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

**Tip**

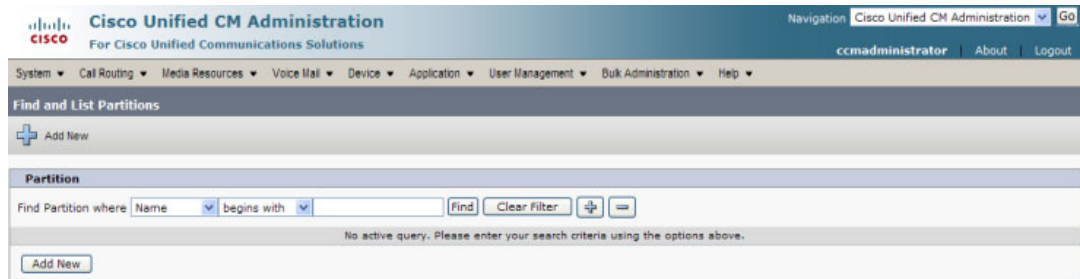
Select **CMLocal** unless you are performing dialing restrictions/re-routing by time of day.

- 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 8-12.
- 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.

The screenshot shows the Cisco Unified CM Administration interface for Partition Configuration. At the top, there's a navigation bar with 'Cisco Unified CM Administration' and 'Go'. Below that, a breadcrumb trail shows 'System > Call Routing > Media Resources > Voice Mail > Device > Application > User Management > Bulk Administration > Help'. The main heading is 'Partition Configuration' with a 'Related Links: Back To Find/List' and 'Go' button. A 'Save' button is visible. The 'Status' section shows 'Status: Ready'. The 'Partition Information' section includes instructions: 'To enter multiple partitions, use one line for each partition entry. You can enter up to 75 partitions; the names and descriptions can have up to a total of 1475 characters. The partition name cannot exceed 50 characters. Use a comma (",") to separate the partition name and description on each line. If a description is not entered, Cisco Unified Communications Manager uses the partition name as the description. For example: << partitionName >> , << description >>'. Below this, there are two examples: 'CiscoPartition, Cisco employee partition' and 'DallasPartition'. A text area labeled 'Name\*' is provided for input. At the bottom, there's another 'Save' button and a note: '\* - indicates required item.'

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

**Step 4** Click the **Save** button.

## Create a Calling Search Space

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

The screenshot shows the Cisco Unified CM Administration interface for Find and List Calling Search Spaces. At the top, there's a navigation bar with 'Cisco Unified CM Administration' and 'Go'. Below that, a breadcrumb trail shows 'System > Call Routing > Media Resources > Voice Mail > Device > Application > User Management > Bulk Administration > Help'. The main heading is 'Find and List Calling Search Spaces' with an 'Add New' button. Below that, there's a search section with a dropdown for 'CSS Name' and a 'begins with' dropdown. Below the search section, there's a message: 'No active query. Please enter your search criteria using the options above.' and an 'Add New' button.

**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 8-16
- 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.



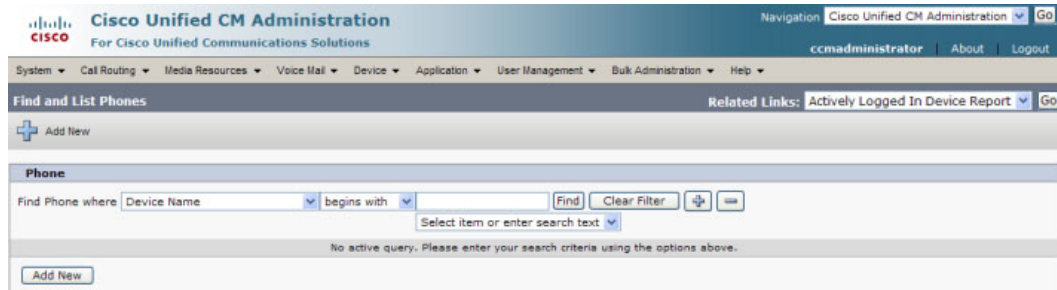
**Tip** Do not add your voicemail platform to the *Selected Partitions* area.

**Step 6** Click the **Save** button.

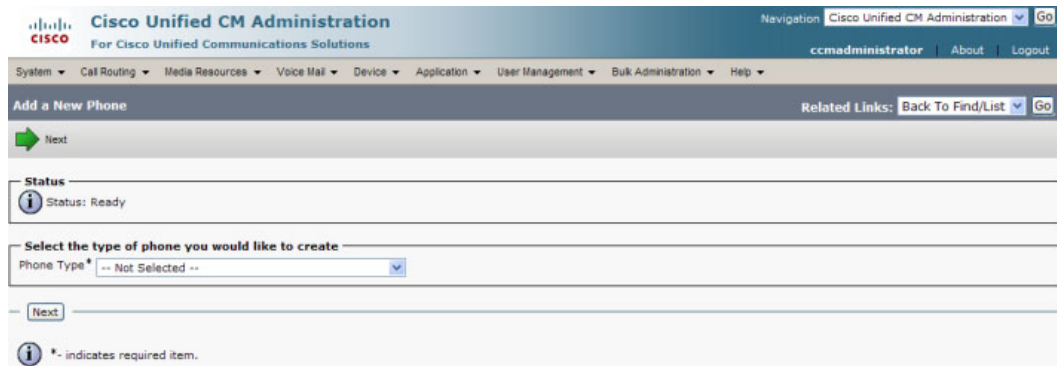
## Create CTI Ports

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.

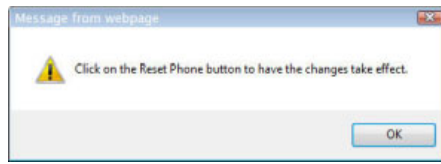
**Step 5** Enter a description in the **Description** field, e.g. InformaCast Port.

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



**Note** The device pool must use a region that will allow a G.711  $\mu$ Law call to phones.

- Step 7** Select **ICVA** from the **Calling Search Space** dropdown menu. This calling search space must allow calls to the partitions in which phones reside. Calling search spaces are unable to detect when voicemail answers a phone. If a phone extension is called with the expectation that the person answering will dictate a message, InformaCast will end up broadcasting the voicemail prompt until the broadcast is canceled.
- Step 8** Select the **Anonymous/Public Shared Space** radio button above the **Owner User ID** field, which will remove the required setting from the **Owner User ID** field.
- Step 9** Scroll to the *Protocol Specific Information* area and select **Cisco CTI Port - Standard SCCP Non-Secure Profile** from the **Device Security Profile** dropdown menu.
- Step 10** Click the **Save** button. A warning dialog box appears.



**Step 11** Click the **OK** button if you are prompted to restart the CTI port. The Phone Configuration page refreshes, and you are given the opportunity to create a Directory Number (DN) for the new port.

The screenshot displays the Cisco Unified CM Administration interface for configuring a CTI Port. The page is titled "Phone Configuration" and shows a successful status message: "Add successful".

**Association Information:**

- 1 [Line \[1\] - Add a new DN](#)
- 2 [Intercom \[1\] - Add a new Intercom](#)

**Phone Type:** Product Type: CTI Port, Device Protocol: SCCP

**Device Information:**

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

**Protocol Specific Information:**

Presence Group*	Standard Presence group
Device Security Profile*	Cisco CTI Port - Standard SCCP Non-Secure Profil
SUBSCRIBE Calling Search Space	< None >
<input type="checkbox"/> Unattended Port	

At the bottom of the page, there are buttons for Save, Delete, Copy, Reset, and Add New. A legend explains the asterisks: \*

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

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

The screenshot displays the Cisco Unified CM Administration interface for configuring a Directory Number. The page is titled "Directory Number Configuration" and includes a navigation menu at the top. The main content area is divided into several sections:

- Status:** Shows "Status: Ready".
- Directory Number Information:** Includes fields for "Directory Number\*", "Route Partition" (set to "< None >"), "Description", "Alerting Name", and "ASCII Alerting Name". There is a checked "Active" checkbox.
- Directory Number Settings:** Includes dropdown menus for "Voice Mail Profile" (set to "< None >"), "Calling Search Space" (set to "< None >"), "Presence Group\*" (set to "Standard Presence group"), "User Hold MOH Audio Source" (set to "< None >"), and "Network Hold MOH Audio Source" (set to "< None >").
- AAR Settings:** Includes a "Voice Mail" section with an "AAR" checkbox and a "Retain this destination in the call forwarding history" checkbox (checked). It also has fields for "AAR Destination Mask" and "AAR Group" (set to "< None >").
- MLPP Alternate Party Settings:** Includes fields for "Target (Destination)", "MLPP Calling Search Space" (set to "< None >"), and "MLPP No Answer Ring Duration (seconds)".
- Line Settings for All Devices:** Includes fields for "Hold Reversion Ring Duration (seconds)" and "Hold Reversion Notification Interval (seconds)".
- Line 1 on Device ICVA-IC-1:** Includes fields for "Display (Internal Caller ID)", "ASCII Display (Internal Caller ID)", and "External Phone Number Mask".
- Multiple Call/Call Waiting Settings on Device InformaCast:** Includes fields for "Maximum Number of Calls\*" (set to 5000) and "Busy Trigger\*" (set to 4500).
- Forwarded Call Information Display on Device InformaCast:** Includes checkboxes for "Caller Name" (checked), "Caller Number", "Redirected Number", and "Dialed Number" (checked).

At the bottom of the page, there is a "Save" button and two informational icons: one indicating that asterisks (\*) denote required items, and another indicating that double asterisks (\*\*) denote changes that require a restart.

**Step 13** Enter a value in the **Directory Number** field that will not be used for any other purpose at your organization, and which is not within a direct-inward-dialing range. Nothing will call this number. It's purely for InformaCast's use when placing calls.

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

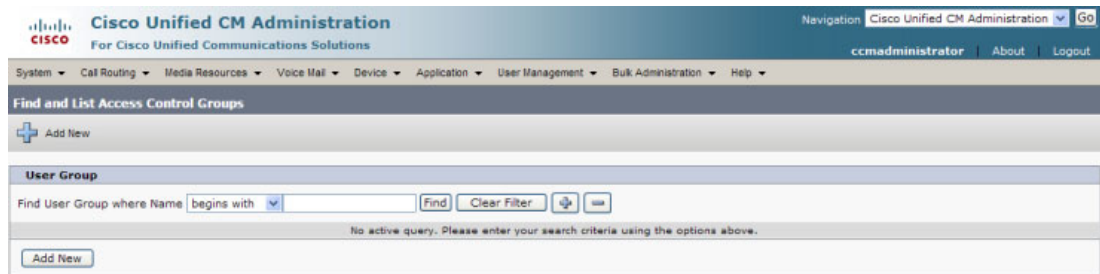
**Step 15** Scroll to the *Line 1 on Device ICVA-IC-001* area and enter **InformaCast** in the **Display (Internal Caller ID)** field.

- Step 16** Enter **InformaCast** in the **ASCII Display (Caller ID)** field. This will cause “from InformaCast” to display on phones when they are called by InformaCast.
- Step 17** Click the **Save** button to add the directory number.
- Step 18** Repeat Steps 1 through 17 as many times as needed to create the number of CTI ports that you need (minimum two).

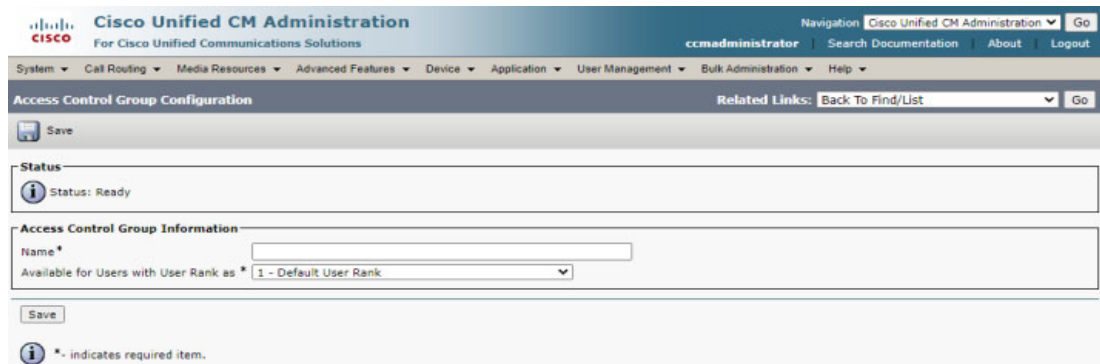
## Create an Access Control Group

In “Create an Application User” on page 8-28, 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.

The screenshot shows the Cisco Unified CM Administration interface. The page title is "Access Control Group Configuration". The "Name" field is filled with "ICVA User Group". The "Related Links" dropdown menu is set to "Back To Find/List". The "Status" section shows "0 records found". The "User Group Information" section shows the "Name" field with "ICVA User Group". The "User" section has a search filter set to "User ID" and "begins with". The "Add End Users to Group", "Add App Users to Group", "Select All", "Clear All", and "Delete Selected" buttons are visible. The "Save", "Delete", "Copy", and "Add New" buttons are also present.

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

The screenshot shows the Cisco Unified CM Administration interface. The page title is "Find and List Access Control Groups". The "Add New" button is visible. The "User Group" section has a search filter set to "Name" and "begins with". The "Add New" button is visible. The "No active query. Please enter your search criteria using the options above." message is displayed.

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

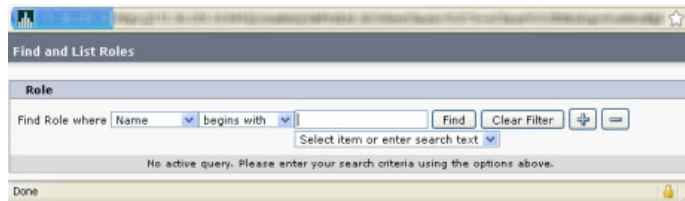
The screenshot shows the 'Find and List Access Control Groups' page in Cisco Unified CM Administration. The page title is 'Find and List Access Control Groups'. Below the title, there are buttons for 'Add New', 'Select All', 'Clear All', and 'Delete Selected'. A status bar indicates '23 records found'. The main content area is titled 'User Group (1 - 23 of 23)' and includes a search filter 'Find User Group where Name begins with' and a 'Find' button. Below the search bar is a table with the following columns: Name, Roles, and Copy. The table lists 23 user groups, with the first one, 'ICVA User Group', highlighted in blue. The Roles column contains an information icon (i) for each group. At the bottom of the table, there are buttons for 'Add New', 'Select All', 'Clear All', and 'Delete Selected'.

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

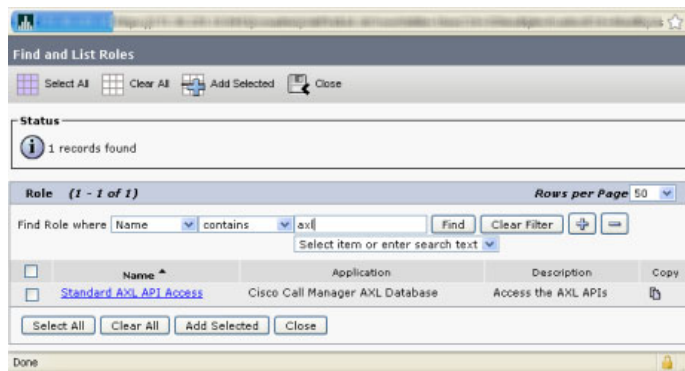
The screenshot shows the 'Access Control Group Configuration' page for the 'ICVA User Group'. The page title is 'Access Control Group Configuration'. Below the title, there is a 'Save' button and a status bar indicating 'Status: Ready'. The main content area is titled 'User Group Information' and shows the 'Name' as 'ICVA User Group'. Below this is the 'Role Assignment' section, which has a 'Role' field and buttons for 'Assign Role to Group' and 'Delete Role Assignment'. At the bottom of the page, there is a 'Save' button and a legend for information icons (i):

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

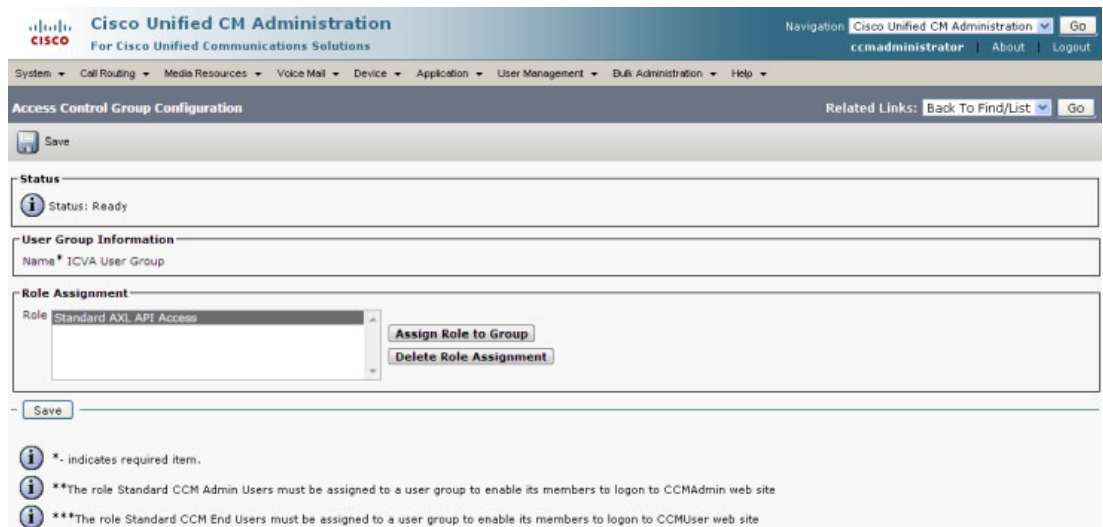
**Step 7** Click the **Assign Role to Group** button. The Find and List Roles window appears.



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



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



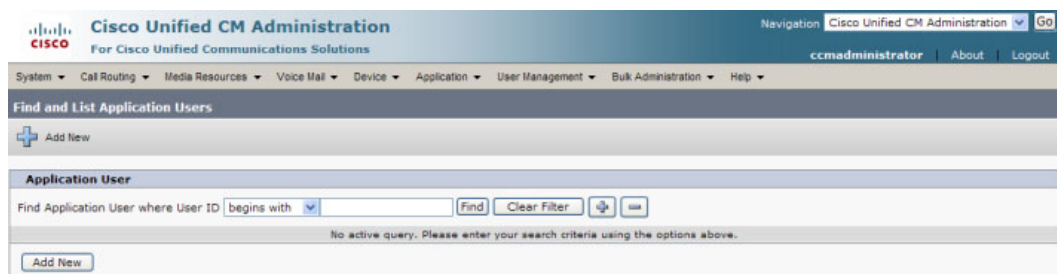
**Step 10** Click the **Save** button.

## Create an Application User

needs an application user set in Cisco Unified CM so that it can establish a CTI connection and gain access to the telephony features Cisco Unified CM offers, e.g. making calls to Cisco IP phones for Unified CM, 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 8-24.
- **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 (see “Set JTAPI or HTTP Configuration” on page 9-7), 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 8-32.
- **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 Allow Reception of SRTP Key Material.** Allows CTI applications to access and distribute SRTP key material, e.g. secure RTP packets containing call audio. This role is only necessary if you are configuring CTI security between InformaCast and Cisco Unified CM.
- **Standard CTI Enabled.** Enables users to execute CTI applications that control/monitor devices.
- **Standard CTI Secure Connection.** Enables a secure CTI connection to Cisco Unified CM. This role is only necessary if you are configuring CTI security between InformaCast and Cisco Unified CM.

**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.

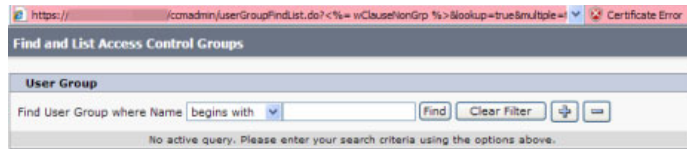


**Note** The password can be up to 64 characters in length.

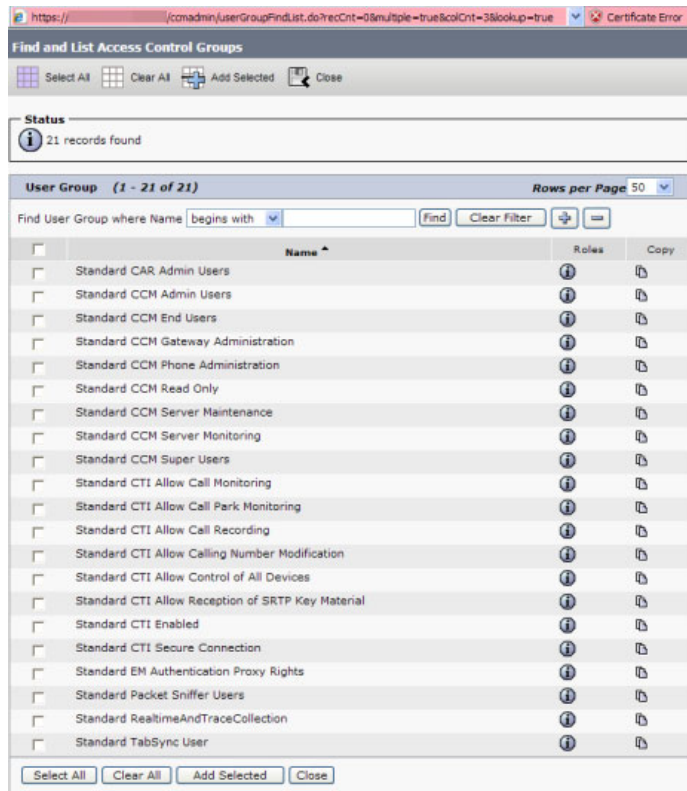
You will need to remember the user ID and password values because you will enter them into InformaCast's own Edit Telephony Configuration page once you install InformaCast (see "Add a Cisco Unified CM Cluster" on page 9-1).

**Step 5** Select the CTI ports (created in "Create CTI Ports" on page 8-19) 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 following checkboxes and click the **Add Selected** button:

- 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
- Standard CTI Allow Reception of SRTP Key Material (if you're using CTI security)
- Standard CTI Enabled
- Standard CTI Secure Connection

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.

## Create an Application User CAPF Profile

If you're configuring CTI security (see “Manage CTI Security” on page 8-49), you should create a Certificate Authority Proxy Function (CAPF) profile and assign it to your application user (see “Create an Application User” on page 8-28). Cisco Unified CM uses CAPF profiles to authenticate application user certificate downloads from its CAPF server. InformaCast then uses this certificate to establish a secure connection with Cisco Unified CM.

- Step 1** Go to **User Management | User Settings | Application User CAPF Profile**. The Find and List Application User CAPF Profiles page appears.

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

- Step 3** Select the application user you created in “Create an Application User” on page 8-28 from the **Application User** dropdown menu, e.g. ICVA.
- Step 4** Enter a description of your profile in the **Instance Id** field, e.g. InformaCastCAPFProfile.
- Step 5** Select **Install/Upgrade** from the **Certificate Operation** dropdown menu.
- Step 6** Leave **By Authentication String** selected in the **Authentication Mode** dropdown menu.
- Step 7** Enter between four and 10 numerals in the **Authentication String** field.
- Step 8** Select **EC Preferred, RSA Backup** from the **Key Order** dropdown menu.
- Step 9** Select **4096** from the **RSA Key Size** dropdown menu.
- Step 10** Select **256** from the **EC Key Size** dropdown menu.
- Step 11** Use the **Operation Completes By** fields to specify a future date by which time the install/upgrade certificate operation must be completed.
- Step 12** Make note of your instance ID and authentication string. You will need them later when installing your CTI certificate (see “Install a CTI Certificate” on page 8-51).
- Step 13** 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.

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

Save

\* - indicates required item.

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

- Step 3** Click the **Save** button.

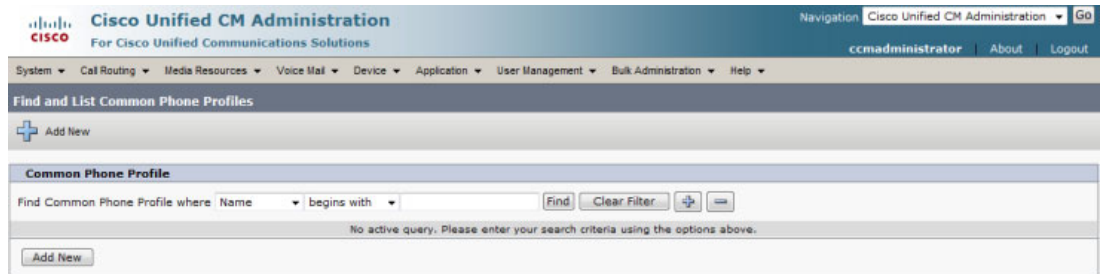


**Note** You will need to reboot your phones for this change to take effect; however, you will also need to reboot your phones after performing the steps in “Set Your Authentication URL” on page 8-40. If you have a lot of phones, this process can be time-consuming. If you only want to reset your phones once, wait to do so until prompted in “Reboot Your Phones” on page 8-43.

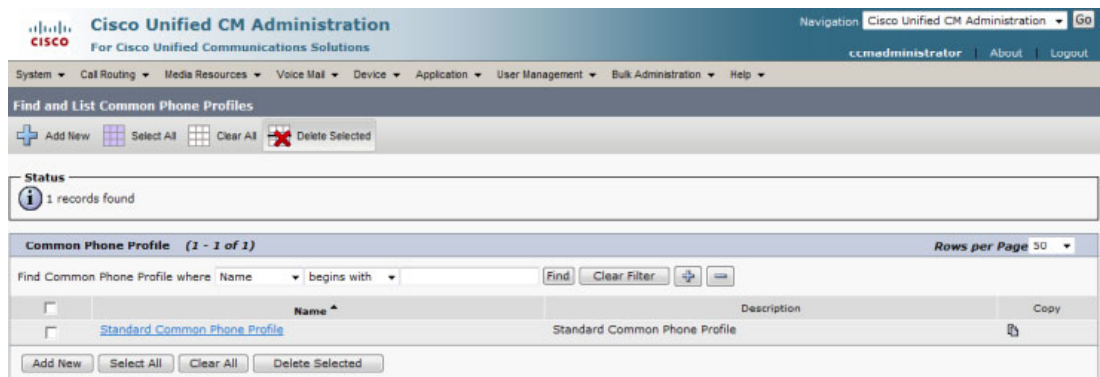
### Enable Web Access for Multiple Phones by Changing Their Profiles

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 Cisco Unified CM 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.

The screenshot displays the Cisco Unified CM Administration interface for the 'Common Phone Profile Configuration' page. The page is organized into several sections:

- Status:** Shows 'Status: Ready'.
- Common Phone Profile Information:** Includes fields for Name, Description, Local Phone Unlock Password, DND Option (set to Ringer Off), DND Incoming Call Alert (set to Beep Only), and Feature Control Policy (set to < None >). There is a checkbox for 'Enable End User Access to Phone Background Image Setting' which is checked.
- Secure Shell Information:** Fields for Secure Shell User and Secure Shell Password.
- Phone Personalization Information:** Fields for Phone Personalization, Always Use Prime Line, Always Use Prime Line for Voice Message, and Services Provisioning, all set to Default.
- Product Specific Configuration Layout:** A table with three columns: Param, Override Common Settings, and a third column for values. The 'Web Access' parameter is highlighted in blue.
 

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

At the bottom of the page, there are buttons for Save, Delete, Copy, Reset, Apply Config, and Add New. A note indicates that an asterisk (\*) denotes a required item.

- Step 4** Scroll down to the *Product Specific Configuration Layout* area and select **Enabled** from the **Web Access** dropdown menu.
- Step 5** Click the **Save** button.



**Note** You will need to reboot your phones for this change to take effect; however, you will also need to reboot your phones after performing the steps in “Set Your Authentication URL” on page 8-40. 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 8-43.

### Enable Web Access for Individual Phones

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

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

The screenshot displays the Cisco Unified CM Administration interface. The main heading is "Find and List Phones". Below this, there is a search section with a dropdown menu set to "Device Name" and a filter set to "begins with". There are buttons for "Find", "Clear Filter", and "Add New". A message at the bottom of the search section reads: "No active query. Please enter your search criteria using the options above." The top navigation bar includes "System", "Call Routing", "Media Resources", "Voice Mail", "Device", "Application", "User Management", "Bulk Administration", and "Help". The user is logged in as "ccmadministrator".

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

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

Device Name (Line)	Description	Device Pool	Device Protocol	Status	IP Address	Copy	Super Copy
AT211		Default	SCCP	Registered with iptapps-ccm61pub	172.30.227.211		
ATA0023EBC6A86A	Auto 60018	Default	SCCP	Unknown	Unknown		
ATA23EBC6A86A01	Auto 60019	Default	SCCP	Unknown	Unknown		
CTIFORNICX		Default	SCCP	Unknown	Unknown		
ICNick1	ICNick1	Default	SCCP	Unknown	Unknown		
ICNick2	ICNick2	Default	SCCP	Unknown	Unknown		
ICNick3	ICNick3	Default	SCCP	Unknown	Unknown		
ICNick4	ICNick4	Default	SCCP	Unknown	Unknown		
ICNick5	ICNick5	Default	SCCP	Unknown	Unknown		
ICNick6	ICNick6	Default	SCCP	Unknown	Unknown		
JessCTI1	JessCTI1	Default	SCCP	Unknown	Unknown		
JessCTI2	JessCTI2	Default	SCCP	Unknown	Unknown		
JessRCCTI		Default	SCCP	Unknown	Unknown		
KatieLC1		Default	SCCP	Unknown	Unknown		
KatieLC2		Default	SCCP	Unknown	Unknown		
KatieLC3		Default	SCCP	Unregistered	172.30.227.200		
KatieLC4		Default	SCCP	Unregistered	172.30.227.200		
PeteCTI1	PeteCTI1	Default	SCCP	Registered with iptapps-ccm61pub	172.30.227.211		
PeteCTI2	PeteCTI2	Default	SCCP	Registered with iptapps-ccm61pub	172.30.227.211		
RajCallAlert	RajCallAlert	RajInformaCast	SCCP	Unknown	Unknown		
RajCTIPort	RajCTIPort	RajInformaCast	SCCP	Unknown	Unknown		
RajCTIPort2	RajCTIPort2	RajInformaCast	SCCP	Unknown	Unknown		
RajCTIPort3	RajCTIPort3	RajInformaCast	SCCP	Unknown	Unknown		
RajCTIPort4	RajCTIPort4	RajInformaCast	SCCP	Unknown	Unknown		
SEP0004F2E67F44	Auto 60037	Default	SCCP	Unknown	Unknown		

**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.

The screenshot displays the Cisco Unified CM Administration interface for configuring a phone. The main content area is divided into four sections:

- Association Information:** A list of lines and SDs. Line 1 is selected, showing 'Line [1] - 60028 (no partition)'. Other lines are 'None' or 'Add a new SD'.
- Phone Type:** Product Type: Cisco 7937, Device Protocol: SCCP.
- Device Information:** A table of settings:
 

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

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

At the bottom, there are buttons for Save, Delete, Copy, Reset, and Add New. A legend explains the asterisks: \* indicates required item, \*\* indicates device reset is not required, and \*\*\* indicates security profile settings.

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

**Step 5** Click the **Save** button.

**Note**

---

You will need to reboot your phones for this change to take effect; however, you will also need to reboot your phones after performing the steps in “Set Your Authentication URL” on page 8-40. 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 8-43.

---



## 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 Cisco Unified CM's Authentication URL to InformaCast.

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

The screenshot displays the Cisco Unified CM Administration interface for Enterprise Parameters Configuration. The page is organized into several sections, each with a list of parameters, their current values, and suggested default values. The 'Authentication Method for API Browser Access' parameter is highlighted, showing it is currently set to 'Basic'.

Parameter Name	Parameter Value	Suggested Value
Cluster ID *	qa-ucm120	StandAloneCluster
Max Number of Device Level Trace *	12	12
DSCP for Phone-based Services *	default DSCP (000000)	default DSCP (000000)
DSCP for Phone Configuration *	CS3(precedence 3) DSCP (011000)	CS3(precedence 3) DSCP (011000)
DSCP for Cisco CallManager to Device Interface *	CS3(precedence 3) DSCP (011000)	CS3(precedence 3) DSCP (011000)
Connection Monitor Duration *	120	120
Auto Registration Phone Protocol *	SCCP	SCCP
Auto Registration Legacy Mode *	True	False
SLF For Call Lists *	Disabled	Disabled
Advertise G.722 Codes *	Enabled	Enabled
Phone Personalization *	Disabled	Disabled
Services Provisioning *	Internal	Internal
Feature Control Policy	< None >	< None >
Wi-Fi Hotspot Profile	< None >	< None >
IMS Inter Operator Id *	IMS Inter Operator Identification	IMS Inter Operator Identification
URL Lookup Policy *	Case Sensitive	Case Sensitive
<b>CCMAdmin Parameters</b>		
Max List Box Items *	250	250
Max Lookup Items *	1000	1000
Enable Discontinuity Records *	True	False
Auto select DN on any Partition *	False	False
<b>Security Parameters</b>		
Cluster Security Mode *	0	Insecure
IMS Security Mode *	Insecure	Insecure
CAPE Phone Port *	3804	3804
CAPE Operation Expires in (days) *	10	10
TFTP File Signature Algorithm *	SHA-1	SHA-1
Enable Caching *	True	True
Authentication Method for API Browser Access *	Basic	Basic
TLS Ciphers *	All Ciphers RSA Preferred	All Ciphers RSA Preferred
SRTP Ciphers *	Medium - AEAD AES-256 GCM, AEAD AES-128 GCM cipl	All Supported Ciphers
HTTPS Ciphers *	RSA Ciphers Only	RSA Ciphers Only
Trusted List of Hosts in HTTP referer header		
<b>Phone URL Parameters</b>		
URL Authentication		
URL Directories	http://qa-ucm120-pub.singlewire.lan:8080/ccm/cip/xmldir	
URL Idle		
URL Idle Time	0	0
URL Information	http://qa-ucm120-pub.singlewire.lan:8080/ccm/cip/GetTel	
URL Messages		
IP Phone Proxy Address		
URL Services	http://qa-ucm120-pub.singlewire.lan:8080/ccm/cip/getser	
<b>Secure Phone URL Parameters</b>		
Secure Authentication URL		
Secure Directory URL (XML)	https://qa-ucm120-pub.singlewire.lan:8443/ccm/cip/xmldir	
Secure Contact Search URL (UDS)	https://qa-ucm120-pub.singlewire.lan:8443/cucm-uds/us	
Secure Idle URL		
Secure Information URL	https://qa-ucm120-pub.singlewire.lan:8443/ccm/cip/GetTel	
Secure Messages URL		
Secure Services URL	https://qa-ucm120-pub.singlewire.lan:8443/ccm/cip/getse	
<b>Cisco Directory Number Alias</b>		
DSCP for LDAP (all services using Directory Number Alias Entry) *	default DSCP (000000)	default DSCP (000000)
<b>SSO and OAuth Configuration</b>		
OAuth Access Token Expiry Timer (minutes) *	60	60
OAuth Refresh Token Expiry Timer (days) *	60	60
Redirect URIs for Third Party SSO Client *		
SSO Login Behavior for iOS *	Use embedded browser (WebView)	Use embedded browser (WebView)
OAuth with Refresh Login Flow *	Disabled	Disabled
Use SSO for RTMT *	True	True

Buttons: Save, Set to Default, Reset, Apply Config

Legend:  
 \* - indicates required item.  
 \*\* The Set-to-Default button restores all parameters that have been modified to their original default values.



### 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 “Add a Cisco Unified CM Cluster” on page 9-1.
- Step 4** Enter **http://<InformaCast Appliance IP Address>:8081/InformaCast/phone/auth** in the **URL Authentication** field, where <InformaCast Appliance IP Address> is replaced with your InformaCast 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 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 8-43.

---

## Set the Authentication Method for API Browser Access



### Note

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

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

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

The screenshot shows the Cisco Unified CM Administration console. The main content area is titled "Enterprise Parameters Configuration". It contains several sections of configuration parameters:

- Enterprise Parameters Configuration:** A table with columns for Parameter Name, Parameter Value, and Suggested Value. Parameters include Cluster ID, Max Number of Device Level Traces, DSCP for Phone-based Services, DSCP for Phone Configuration, DSCP for Cisco CallManager to Device Interface, Connection Monitor Duration, Auto Registration Phone Protocol, Auto Registration Legacy Mode, RLP for Call Lists, Advertise SIP Codecs, Phone Personalization, Services Provisioning, Feature Control Policy, Wi-Fi Hotspot Profile, IMS Inter-Operator Id, and URL Lookup Policy.
- CCMAdmin Parameters:** Parameters include Max List Box Items, Max Lookup Items, Enable Dependency Records, and Auto select DN on any Partition.
- Security Parameters:** Parameters include Cluster Security Mode, LBM Security Mode, CAPF Phone Port, CAPF Operation Expires in (days), TFTP File Signature Algorithm, Enable Caching, Authentication Method for API Browser Access (set to Basic), SRTP Ciphers, HTTPS Ciphers, and Trusted List of Hosts in HTTP referer header.
- Phone URL Parameters:** Parameters include URL Authentication, URL Directories, URL Idle, URL Idle Time, URL Information, URL Messages, IP Phone Proxy Address, and URL Services.
- Secure Phone URL Parameters:** Parameters include Secure Authentication URL, Secure Directory URL (XML), Secure Contact Search URL (UDS), Secure Idle URL, Secure Information URL, Secure Messages URL, and Secure Services URL.
- Cisco Directory Number Alias:** Parameter DSCP for LDAP (all services using Directory Number Alias port).
- SSO and OAuth Configuration:** Parameters include OAuth Access Token Expiry Timer (minutes), OAuth Refresh Token Expiry Timer (days), Redirect URIs for Third Party SSO Client, SSO Login Behavior for iOS, OAuth with Refresh Login Flow, and Use SSO for RTMT.

At the bottom of the page, there are buttons for "Save", "Set to Default", "Reset", and "Apply Config". Below the buttons, there are two informational icons: one indicating that an asterisk (\*) denotes a required item, and another indicating that the "Set-to-Default" button restores all parameters to their original default values.

**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.

The screenshot shows the Cisco Unified CM Administration interface. The page title is "Find and List Phones". The search criteria are "Device Pool" and "begins with" "icva". The table displays 155 records. The columns are: Device Name(Line), Description, Device Pool, Device Protocol, Status, IPv4 Address, Copy, and Super Copy. The "Reset Selected" button is highlighted at the bottom of the table.

	Device Name(Line)	Description	Device Pool	Device Protocol	Status	IPv4 Address	Copy	Super Copy
<input type="checkbox"/>	LanAccCTI04	InformaCast CTI port	ICVA	SCCP	Registered with qa-ucm105-pub	172.30.227.226		
<input type="checkbox"/>	SEP00115C979921	Auto 105030	ICVA	SCCP	Registered with qa-ucm105-pub	172.30.223.7		
<input type="checkbox"/>	LanAccCTI12	Conference Call CTI port	ICVA	SCCP	Registered with qa-ucm105-pub	172.30.227.226		
<input type="checkbox"/>	LanBcaCTI01	CallAware CTI port	ICVA	SCCP	None	None		
<input type="checkbox"/>	LanBccCTI09	Conference Call CTI port	ICVA	SCCP	Unregistered	172.30.223.3		
<input type="checkbox"/>	JenkCccConf01	Conference Call CTI port (Jenkins C)	ICVA	SCCP	None	None		
<input type="checkbox"/>	LanAccCTI15	Conference Call CTI port	ICVA	SCCP	Registered with qa-ucm105-pub	172.30.227.226		
<input type="checkbox"/>	SEP0026085BE26A	Auto 105190	ICVA	SCCP	Registered with qa-ucm105-pub	172.30.227.74		
<input type="checkbox"/>	LanBccCTI01	InformaCast CTI port	ICVA	SCCP	Registered with qa-ucm105-pub	172.30.223.3		
<input type="checkbox"/>	LanBccCTI12	Conference Call CTI port	ICVA	SCCP	Unregistered	172.30.223.3		
<input type="checkbox"/>	SEP001E138C7D81	Auto 105032	ICVA	SCCP	Registered with qa-ucm105-pub	172.30.227.22		
<input type="checkbox"/>	SEP04FE7F6911B9	Auto 105015	ICVA	SCCP	Registered with qa-ucm105-pub	172.30.227.81		
<input type="checkbox"/>	LanBccCTI11	Conference Call CTI port	ICVA	SCCP	Unregistered	172.30.223.3		
<input type="checkbox"/>	SEP001D45E95D12	Auto 105040	ICVA	SIP	Registered with qa-ucm105-pub	172.30.227.27		
<input type="checkbox"/>	SEPSCAFC8FE72CA	Auto 105035	ICVA	SCCP	Registered with qa-ucm105-pub	172.30.223.5		
<input type="checkbox"/>	LanAccCTI11	Conference Call CTI port	ICVA	SCCP	Registered with qa-ucm105-pub	172.30.227.226		
<input type="checkbox"/>	LanAccCTI14	Conference Call CTI port	ICVA	SCCP	Registered with qa-ucm105-pub	172.30.227.226		
<input type="checkbox"/>	LanBicCTI02	InformaCast CTI port	ICVA	SCCP	Registered with qa-ucm105-pub	172.30.223.3		

**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.

The screenshot shows the "Device Reset" dialog box. The status is "Ready". The "Reset Information" section states "Selected Device: 1 devices selected" and provides instructions on how to reset or restart a device. The "Reset" button is highlighted.

**Device Reset**

Reset Restart

**Status**

Status: Ready

**Reset Information**

**Selected Device: 1 devices selected**

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

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

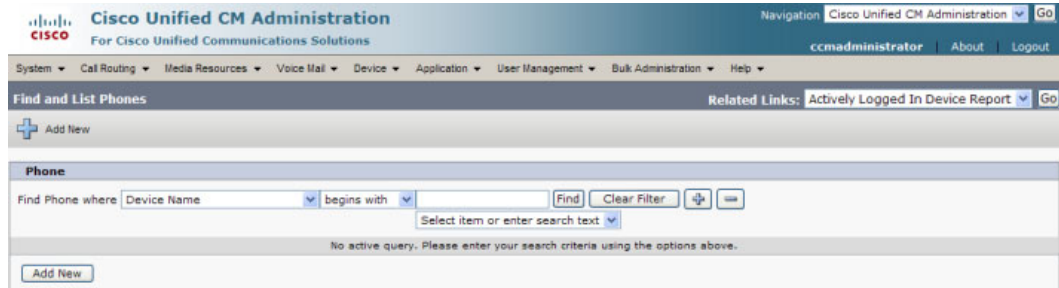
Reset Restart Close

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

## Test Your Phones

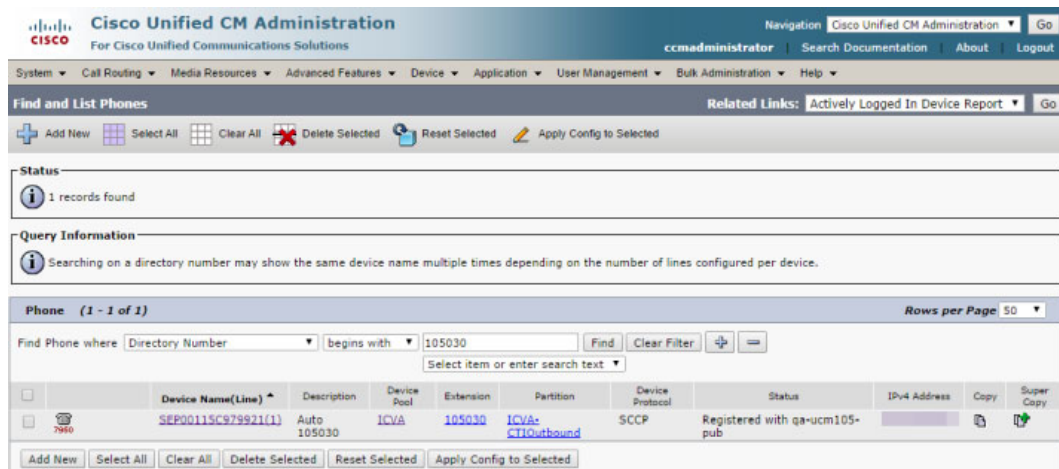
Rebooting your phones should have caused them to pick up their new settings. You can verify their new settings through a web browser.

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




**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 8-32 for more information).

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

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

The screenshot displays the Network Configuration page for a Cisco IP Phone CP-7960G (SEP00115C979921). The page is organized into a sidebar with navigation links and a main content area with configuration parameters.

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

**Step 6** Scroll down the page until you come to Authentication URL. It should list the IP address you entered in the **URL Authentication** field in Step 4 on page 8-41. If it does not, see “Set Your Authentication URL” on page 8-40.

## 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. InformaCast uses its trust store to establish trust with hosts it talks to over SSL or TLS. The InformaCast trust store is seeded with root certificates included by Oracle in the JVM.

In the *System Certificates* area on the Settings page, 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:

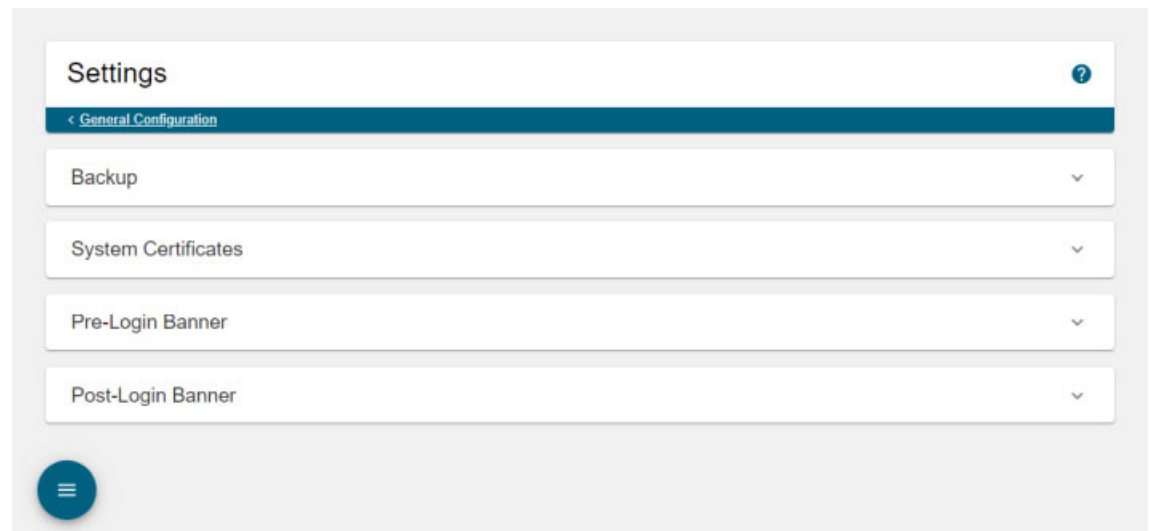
- **The Cisco Unified CM cluster.** You can see which Cisco Unified CM certificates are currently trusted, whether automatic certificate importation is enabled/disabled, and select which certificates should be imported for use in future SSL/TLS communications between InformaCast and Cisco Unified CM.
- **SIP certificates.** SIP functionality is handled separately within InformaCast and unaffected by the *System Certificates* area (see “Manage SIP Functionality” on page 8-56 for more information).



### Note

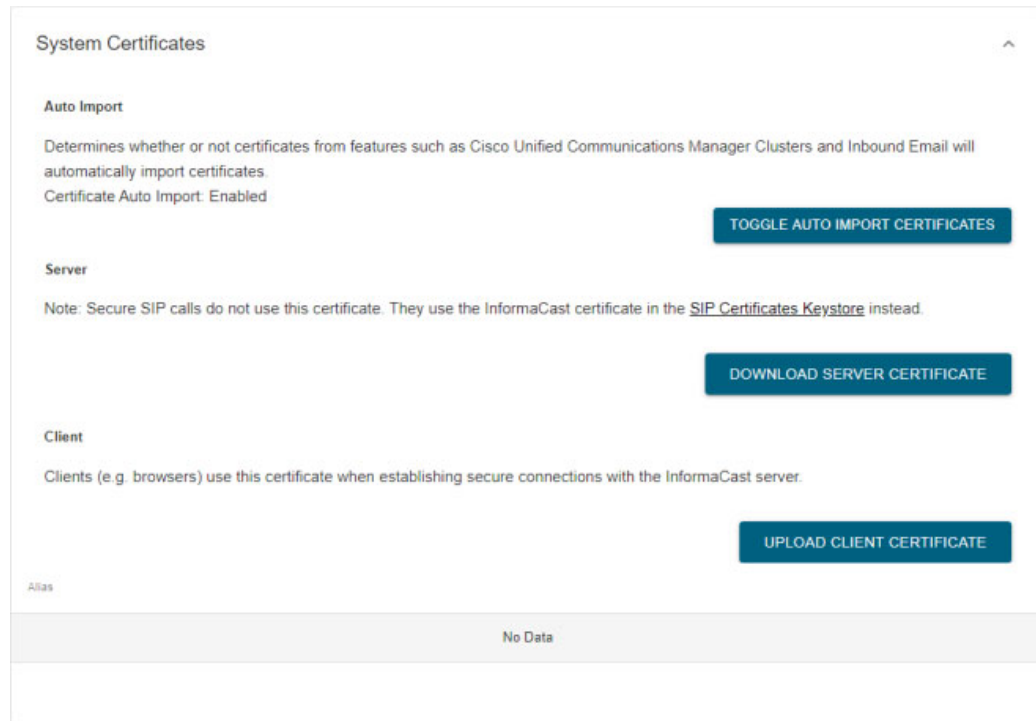
InformaCast will only negotiate an SSL session with a host that supports AES cipher suites; negotiation with hosts that support only 3DES will fail.

- Step 1** Go to **System Administration | General Configuration | System Settings**. The Settings page appears.





**Step 2** Expand the *System Certificates* area, if it's not already visible.



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

- **Automatically Import SSL Certificates.** Leave Certificate Auto Import listed as Enabled. By default, SSL certificates are automatically imported, and if you were running InformaCast prior to InformaCast 12.0.1, this is how InformaCast worked previously.
- **Manually Import SSL Certificates.** Click the **Toggle Auto Import Certificates** button so that Certificate Auto Import is listed as Disabled.

Disabling the automatic import of SSL certificates means you will need to explicitly trust the SSL certificate supplied by your Cisco Unified CM cluster (see “Add a Cisco Unified CM Cluster” on page 9-1 for more information).

## Manage CTI Security

CTI security involves configuring Computer Telephony Integration over Transport Layer Security (CTI over TLS) and CTI with Secure Real-Time Transport Protocol (CTI with SRTP). CTI over TLS ensures that communication between InformaCast and Cisco Unified CM is secure, and CTI with SRTP ensures that communication between InformaCast and its Cisco IP phones for Unified CM is secure.

In addition, if you'd like to use InformaCast in Cisco's Hosted Collaboration Solution for Government (HCS-G), which is a secure, reliable, and scalable cloud-based collaboration space for government organizations, you must configure InformaCast with both CTI over TLS and CTI with SRTP.

By configuring a Cisco Unified CM cluster with CTI security, you secure all of InformaCast's CTI connections (see “Add a Cisco Unified CM Cluster” on page 9-1 for more information).

However, if you don't also install the proper CTI certificates for InformaCast, your broadcasts will fail (see “Install a CTI Certificate” on page 8-51 for more information).

Before completing the following steps, ensure:

- You have a properly configured Cisco Unified CM 12.5.1 SU 1 or later with JTAPI 12.5 or later installed
- You're running Cisco Unified CM in mixed mode
- The phones that will receive InformaCast's broadcasts are [supported Cisco IP phones for Unified CM](#)

**Note**

A CTI over TLS connection to a Cisco Unified CM through certificates signed by third-party Certificate Authorities cannot be established without Cisco Unified CM configuration modifications. Please refer to Cisco issue CSCuc76331, which contains several work-arounds to this issue, one of which you will need to apply before continuing.

- 
- Step 1** Enable the **Send Commands to Phones by JTAPI** checkbox (see “Set JTAPI or HTTP Configuration” on page 9-7 for more information).
- Step 2** Ensure that InformaCast’s application user has the Standard CTI Allow Reception of SRTP Key Material and Standard CTI Secure Connection roles assigned to it (see “Create an Application User” on page 8-28 for more information).
- Step 3** Check that a CAPF profile is associated with your InformaCast application user (see “Create an Application User CAPF Profile” on page 8-31 for more information).
- Step 4** Declare an outage window and ensure that it falls outside of regular business hours. The following steps will cause service interruptions.
- Step 5** Make sure the **Use Secure Connection** checkbox is selected and the **Cisco Unified CM CAPF Address**, **Cisco Unified CM CAPF Port**, **Cisco Unified CM TFTP Address**, and **Cisco Unified CM TFTP Port** fields are configured for your Cisco Unified CM cluster (see “Add a Cisco Unified CM Cluster” on page 9-1 for more information).
- You may see an error when you click the **Save** button on your Cisco Unified CM cluster. This error will resolve itself once you install CTI certificates discussed in Step 6.
- Step 6** Install the proper CTI certificate for InformaCast (see “Install a CTI Certificate” on page 8-51 for more information).
- Step 7** Restart the singlewireInformaCast service (see “Restart a Service on the InformaCast Appliance” on page 13-10 for more information).
- Step 8** Verify that you have a secure CTI connection (see “Verify a Secure CTI Connection” on page 8-55 for more information).
-

## Manage CTI Certificates

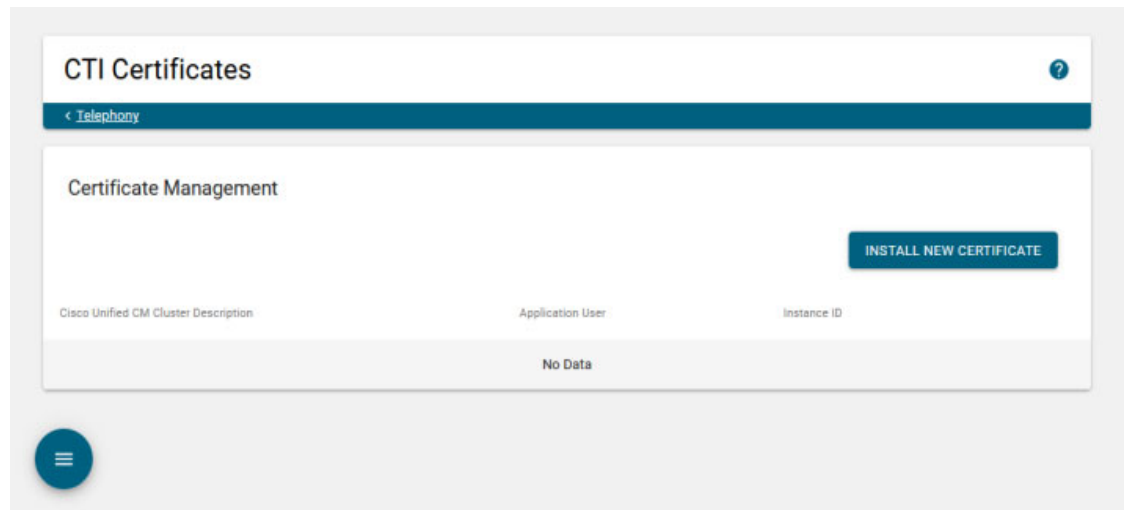
Once you've configured a Cisco Unified CM cluster with CTI security (see “Add a Cisco Unified CM Cluster” on page 9-1 for more information), JTAPI is used to install the certificates required by the TLS connections made between InformaCast and Cisco Unified CM.

### *Install a CTI Certificate*

JTAPI is used to install the certificates required by the TLS connections made between InformaCast and Cisco Unified CM.

Ensure you complete the steps in this topic before the date specified in the **Operation Completes By** field of your CAPF profile (see “Create an Application User CAPF Profile” on page 8-31).

**Step 1** Go to **System Administration | Telephony | CTI Certificates**. The CTI Certificates page appears.



**Step 2** Click the **Install New Certificate** button. The Install CTI Certificate page appears.

**Install CTI Certificates** ?

< Telephony < CTI Certificates

**General Details**

Installation of CTI certificates requires Unified Communications Manager 12.5.1 SU 1 or later running in mixed mode.

Application User \*

Application User CAPF Profile Instance ID \*

Application User CAPF Profile Authentication String \*

CAPF Address \*

CAPF Port \*

3804

TFTP Address \*

TFTP Port \*

69

CANCEL SAVE

- Step 3** Enter the name of the application user you created in “Create an Application User” on page 8-28 in the **Application User** field, e.g. ICVA.
- Step 4** Enter the application user CAPF profile instance ID you created in “Create an Application User CAPF Profile” on page 8-31 in the **Application User CAPF Profile Instance ID** field, e.g. InformaCastCAPFProfile.
- Step 5** Enter the authentication string you created in “Create an Application User CAPF Profile” on page 8-31 in the **Application User CAPF Profile Authentication String** field.
- Step 6** Enter the IP address of the Cisco Unified CM you're using as a Certificate Authority Proxy Function server in the **CAPF Address** field.
- Step 7** Enter the port number at which your Cisco Unified CM is listening for CAPF communication in the **CAPF Port** field. The default is 3804.
- Step 8** Enter the IP address of the Cisco Unified CM you're using as a TFTP server in the **TFTP Address** field.
- Step 9** Enter the port number at which your Cisco Unified CM is listening for TFTP traffic in the **TFTP Port** field. The default is 69.

**Note**

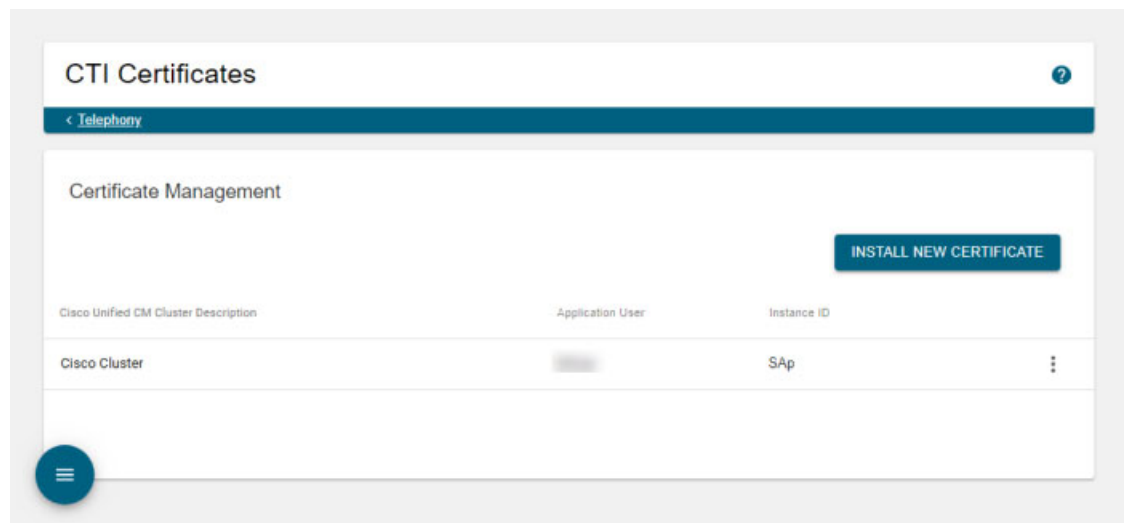
The field values in Steps 4 through 9 should match the values you entered when you configured a Cisco Unified CM cluster.

**Step 10** Click the **Save** button. Your certificate is installed.

### *View an Installed CTI Certificate*

Once you've installed a CTI certificate, you may need to view/verify its information.

**Step 1** Go to **System Administration | Telephony | CTI Certificates**. The CTI Certificates page appears.



**Step 2** Click the **More | View** icon of the CTI certificate you want to view. The Certificate pop-up window appears and you can see your CTI certificate's information.

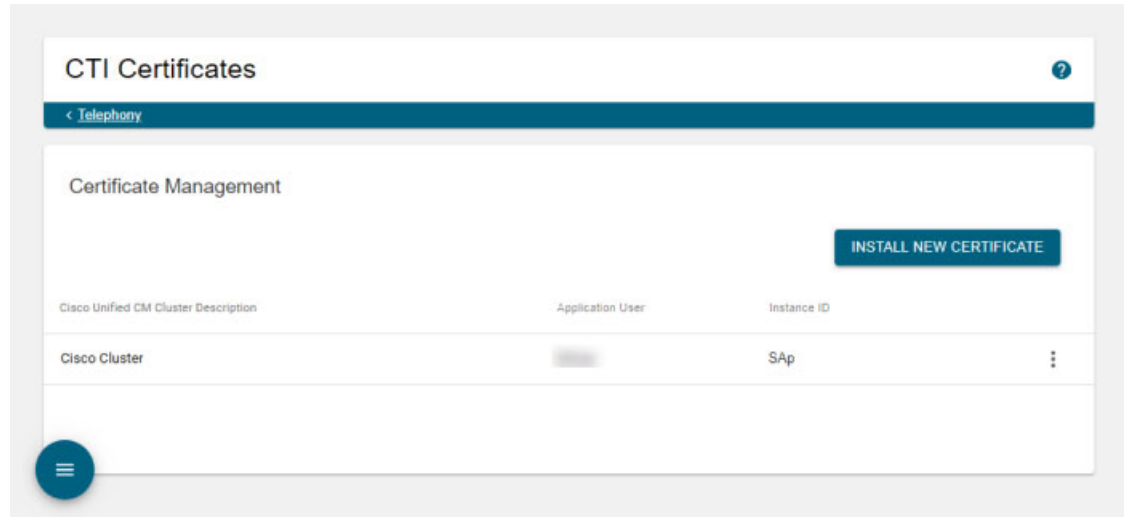


**Step 3** Click the **OK** button when you are finished.

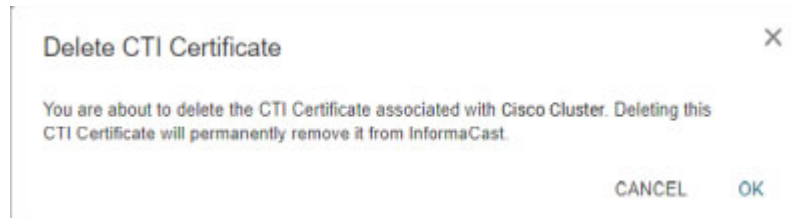
### Delete an Installed CTI Certificate

As your needs change, you may need to remove installed CTI certificates from InformaCast.

- Step 1** Go to **System Administration | Telephony | CTI Certificates**. The CTI Certificates page appears.



- Step 2** Click the **More | Delete** icon of the CTI certificate you want to remove. The Delete CTI Certificate pop-up window appears.



- Step 3** Click the **OK** button. The CTI certificate is deleted.

### Verify a Secure CTI Connection

Once you have completed all the requirements and steps in “Manage CTI Security” on page 8-49, the last step is to verify that you have a secure CTI connection.

- Step 1** Go to **Home | Overview** and scroll down to the Cisco Unified CM Clusters area.

Cisco Unified CM Clusters			
Description	CTI Provider Secure	CTI Provider	Version
Cisco Cluster	Yes	[Redacted]	11.5.1.21900-40

**Step 2** Verify that Yes appears in the CTI Provider Secure column.

---

## Manage SIP Functionality

In order to use DialCasts (see “Manage DialCasts” on page 10-1), you must first configure Session Initiation Protocol (SIP), which provides InformaCast with the capability to receive SIP calls, allowing other SIP devices, such as those managed by Cisco Unified Communications Manager, to locate and call InformaCast.

### SIP Features

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 telephony providers when sending a request.



#### Note

If you are running Cisco Unified CM in mixed mode and you want calls to and from InformaCast to use encrypted media, you must configure SRTP support or CTI security (see “Enable SIP Call Security” on page 8-88).

---

### Connection Path

When configuring SIP communication between InformaCast and your telephony provider, the first thing you'll want to do is configure a SIP trunk connection (see “Configure a SIP Trunk Connection” on page 8-57).

### InformaCast Parameters

Once you're done configuring your SIP connection(s), you'll want to set other SIP parameters within InformaCast:

- **Allow/Deny SIP access.** Set InformaCast to allow or deny all incoming SIP calls, and add exceptions to counteract their setting, e.g. deny all incoming SIP calls with the exception of a certain host or subnet (see “Allow/Deny SIP Access to InformaCast” on page 8-85).
- **Enable SIP call security.** Control the level of security imposed on the content of SIP calls made and received by InformaCast (see “Enable SIP Call Security” on page 8-88).
- **Enable digest authentication with SIP user credentials.** Enter valid credentials for each SIP realm where you expect InformaCast to be challenged when registering or terminating SIP calls (see “Enable Digest Authentication with SIP User Credentials” on page 8-93).



- **Manage the SIP stack.** Set certain parameters that govern InformaCast's fundamental low-level SIP functionality, such as transaction handling, dialogs, utilities for SIP headers, maintenance of SIP timers, etc. (see “Manage the SIP Stack” on page 8-99).
- **Restart SIP.** Restart the SIP stack to ensure certain SIP changes take effect (see “Restart SIP” on page 8-101).

## Configure a SIP Trunk Connection

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

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

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

- “Add a SIP Trunk Security Profile” on page 8-58
- “Add a SIP Profile” on page 8-60
- “Add a SIP Trunk” on page 8-62
- “Add a Route Pattern” on page 8-83

For a secure SIP trunk connection, the TLS protocol provides secure signaling 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 on 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 create a SIP trunk security profile and SIP trunk that uses 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 and a common name assigned to it. You can see both the alias and common name for each certificate in the *Certificates* area of the SIP page.

For a secure SIP trunk connection, follow these steps:

- Declare an outage window and ensure that it falls outside of regular business hours.  
Exchanging certificates between InformaCast and Cisco Unified CM causes SIP to restart and all SIP calls to be dropped, i.e. any callers interacting with the DialCast IVR will have their calls dropped.
- “Create and Install a Signed Certificate” on page 13-125 and “Import a Signed SSL Certificate to InformaCast's SIP Certificate Store” on page 13-122 (optional)
- “Install the InformaCast SIP Certificate on Cisco Unified CM” on page 8-64
- “Add a SIP Trunk Security Profile That Uses TLS” on page 8-71
- “Add a SIP Profile” on page 8-60

- “Add a SIP Trunk That Uses TLS” on page 8-74
- “Install Cisco Unified CM Certificates on InformaCast” on page 8-77
- “Add a Route Pattern” on page 8-83

### Add a SIP Trunk Security Profile

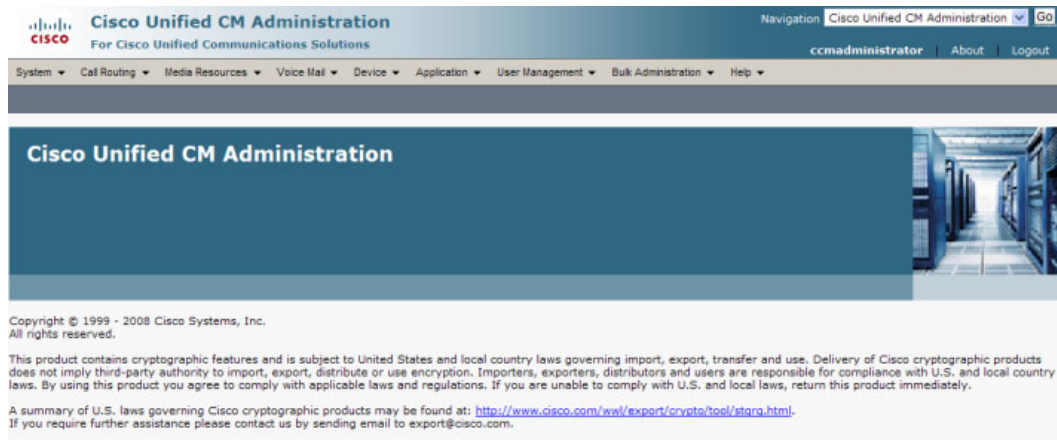
A SIP trunk security profile specifies the transport protocol to be used in SIP communication, the port on which to communicate, whether digest authentication should be performed, etc.



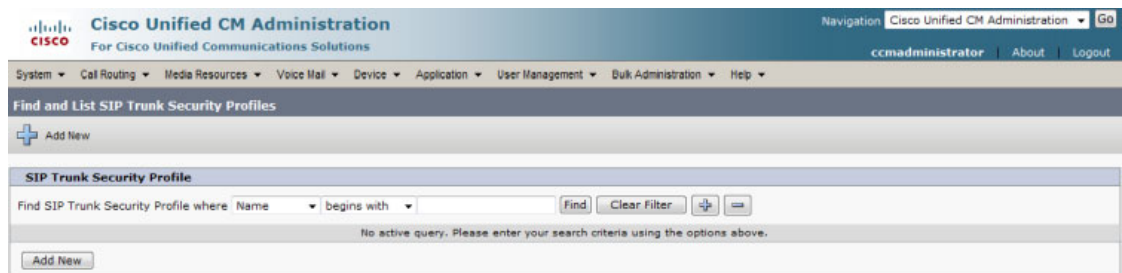
#### Note

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 8-71.

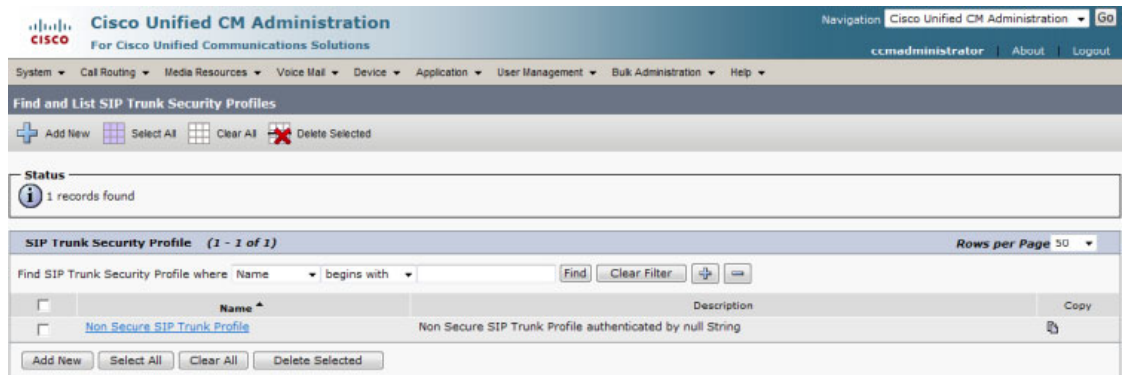
- Step 1** Open a web browser and log into the administration interface of the Cisco Unified CM server (the address will be similar to <https://<Cisco Unified CM IP Address>/ccmadmin>). The Cisco Unified CM Administration page appears.



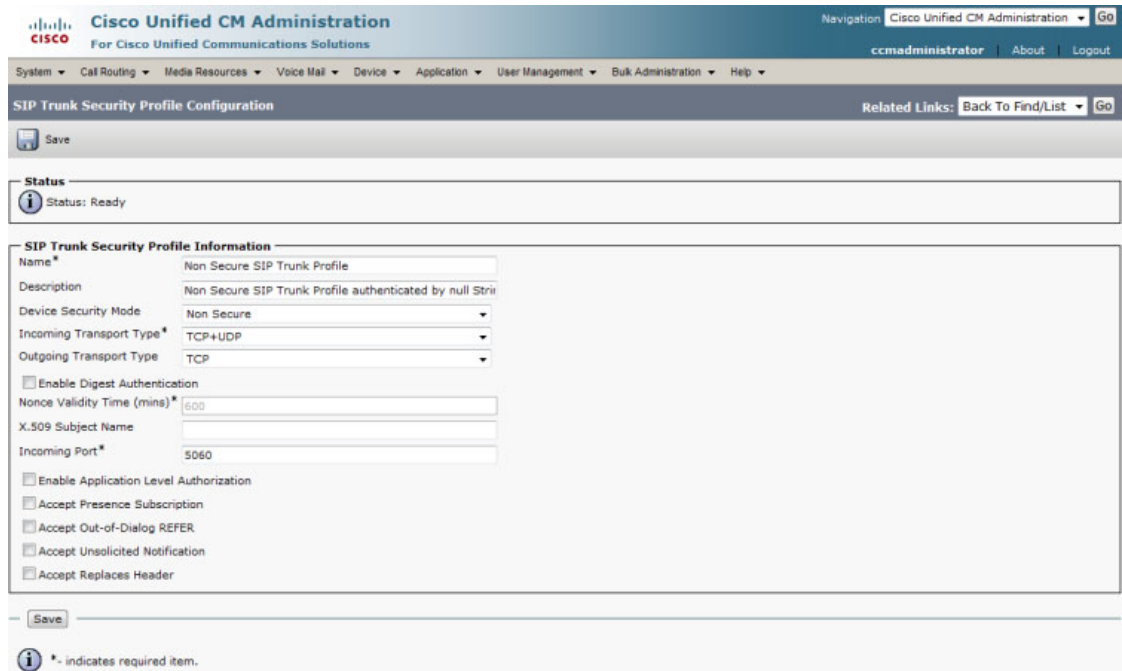
- Step 2** Go to **System | Security | SIP Trunk Security Profile**. The Find and List SIP Trunk Security Profiles page appears.



- 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**.

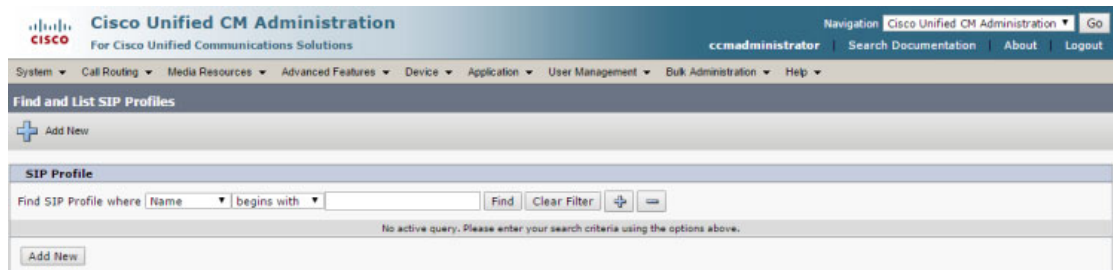
- Step 10** Select the **Accept Unsolicited Notification** checkbox.

**Step 11** Click the **Save** button.

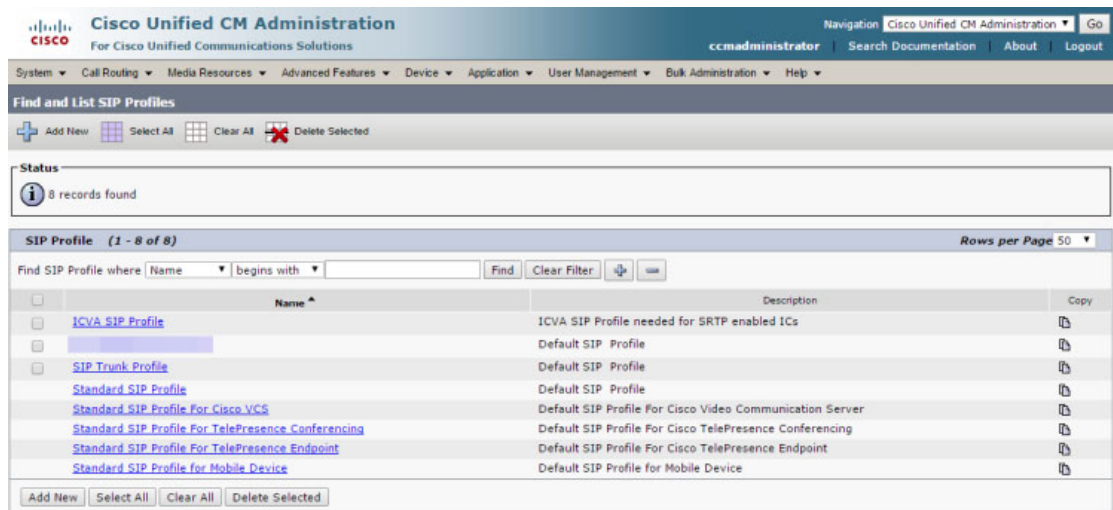
### Add a SIP Profile

The **Early Offer support for voice and video calls** parameter, available through a SIP profile, should be set to **Best Effort (no MTP inserted)** 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 **Copy** icon in the Standard SIP Profile's row. The SIP Profile Configuration page appears.

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

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

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

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

Copy | Reset | Apply Config | Add New

**Status**

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

**SIP Profile Information**

Name\* Standard SIP Profile  
Description Default SIP Profile  
Default MTP Telephony Event Payload Type\* 101  
Early Offer for G.Clear Calls\* Disabled  
User-Agent and Server header information\* Send Unified CM Version Information as User-Agen  
Version in User Agent and Server Header\* Major And Minor  
Dial String Interpretation\* Phone number consists of characters 0-9, \*, =, anc  
Confidential Access Level Headers\* Disabled

Redirect by Application  
 Disable Early Media on 180  
 Outgoing T.38 INVITE include audio mline  
 Use Fully Qualified Domain Name in SIP Requests  
 Assured Services SIP conformance

**SDP Information**

SDP Session-level Bandwidth Modifier for Early Offer and Re-invites\* TIAS and AS  
SDP Transparency Profile < None >  
Accept Audio Codec Preferences in Received Offer\* Default

Require SDP Inactive Exchange for Mid-Call Media Change  
 Allow RR/RS bandwidth modifier (RFC 3556)

**Trunk Specific Configuration**

Reroute Incoming Request to new Trunk based on\* Never  
RSVP Over SIP\* Local RSVP  
Resource Priority Namespace List < None >  
 Fall back to local RSVP  
SIP RelXX Options\* Disabled  
Video Call Traffic Class\* Mixed  
Calling Line Identification Presentation\* Default  
Session Refresh Method\* Invite  
Early Offer support for voice and video calls\* Disabled (Default value)

Enable ANAT  
 Deliver Conference Bridge Identifier  
 Allow Passthrough of Configured Line Device Caller Information  
 Reject Anonymous Incoming Calls  
 Reject Anonymous Outgoing Calls  
 Send ILS Learned Destination Route String

Copy | Reset | Apply Config | Add New

**i** \* indicates required item.

**Step 4** Enter a name for your SIP profile in the **Name** field, e.g. ICVA SIP Profile.

**Step 5** Enter a description of your SIP profile in the **Description** field, e.g. SIP Profile for SRTP.

**Step 6** 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.

**Step 7** Click the **Save** button.



**Note** If you're configuring a secure SIP trunk, skip to "Add a SIP Trunk That Uses TLS" on page 8-74. For non-secure SIP trunks, continue with "Add a SIP Trunk" on page 8-62

## 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 8-74.

**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 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. InformaCast.
- Step 8** Select the device pool you created in “Create a Device Pool” on page 8-14 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 8-17 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 8-59.
- Step 13** Select the SIP trunk security profile that you created in “Add a SIP Trunk Security Profile” on page 8-58 from the **SIP Trunk Security Profile** dropdown menu.
- Step 14** Select the SIP profile you created in “Add a SIP Profile” on page 8-60 from the **SIP Profile** dropdown menu.
- Step 15** Click the **Save** button.
- Step 16** Proceed to “Add a Route Pattern” on page 8-83.
- 

### *Install the InformaCast SIP Certificate on Cisco Unified CM*

To use the TLS protocol between your telephony provider and InformaCast, you will need to install InformaCast’s SIP certificate on all nodes in the Cisco Unified CM group used by your SIP trunk’s device pool (see “Add a SIP Trunk That Uses TLS” on page 8-74 for more information).

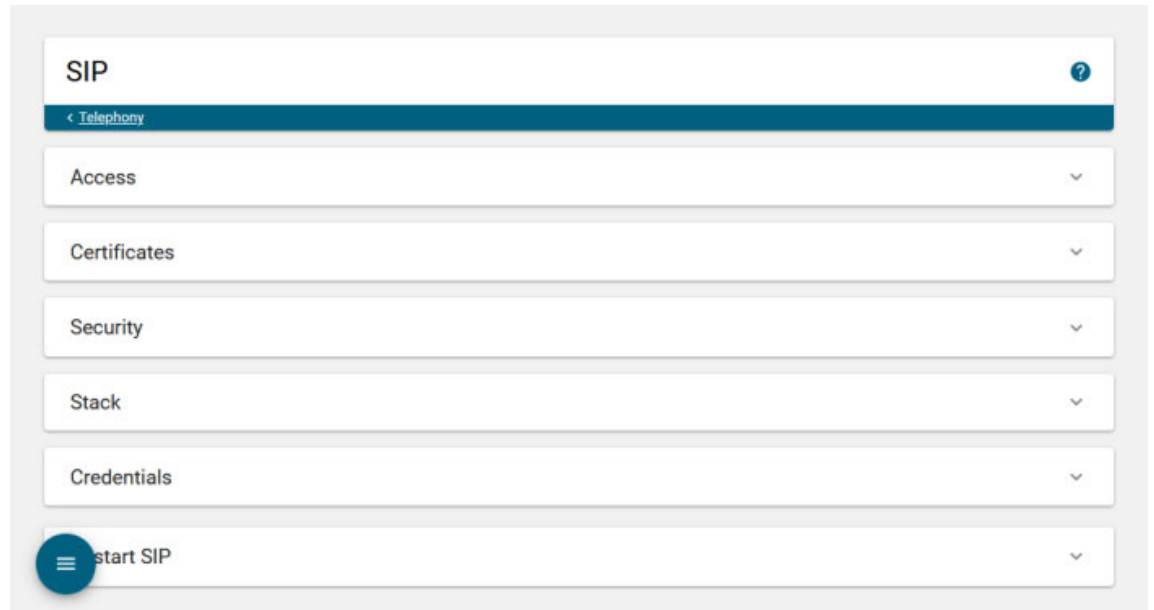
**Note**

TLS certificates are regenerated whenever InformaCast is installed, its IP address is changed, or Cisco Unified CM is installed, which means the steps in this section will need to be repeated if either InformaCast or Cisco Unified CM is restored from backup or re-installed, or if InformaCast's IP address changes.

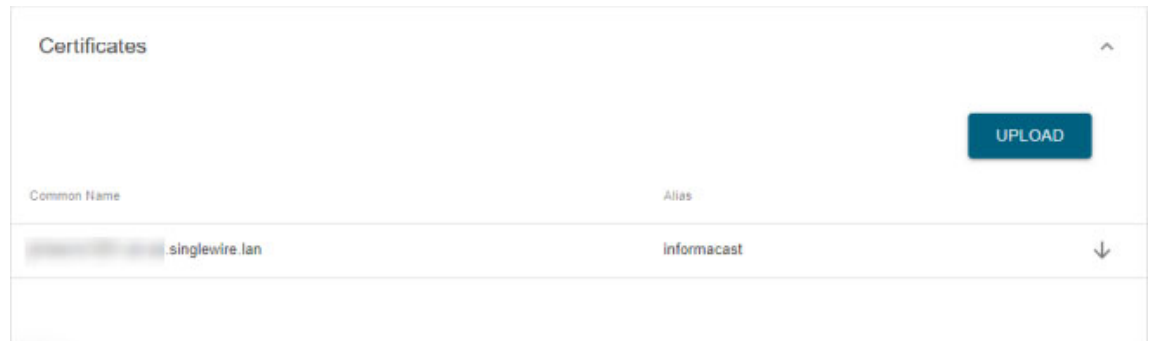
---



**Step 1** Go to **System Administration | Telephony | SIP**. The SIP page appears.



**Step 2** Expand the *Certificates* area, if it's not already visible.



**Step 3** Click the **Download** icon and save the PEM file to a location accessible to your Cisco Unified CM server(s).

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



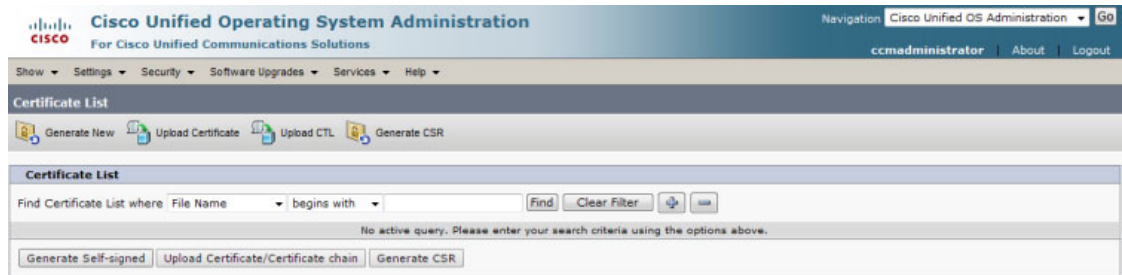
- Step 5** Select **Cisco Unified OS Administration** from the **Navigation** dropdown menu and click the **Go** button. The Cisco Unified Operating System Administration page appears.



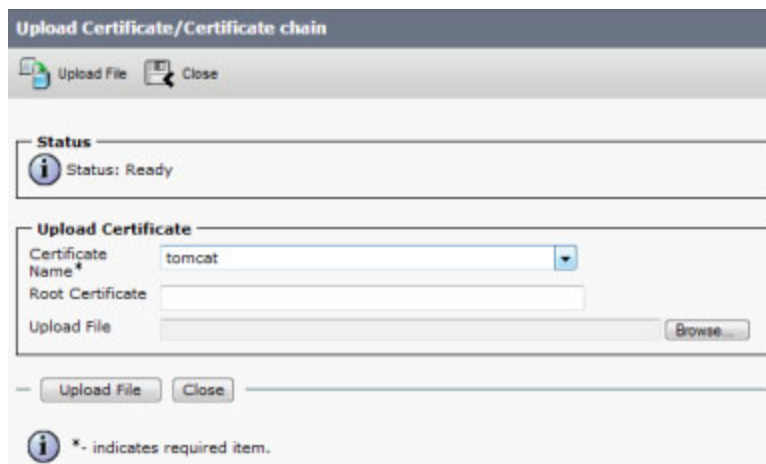
- Step 6** Enter your Operating System Administration username and password in the **Username** and **Password** fields, respectively, and click the **Login** button. The Cisco Unified Operating System Administration page refreshes.



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

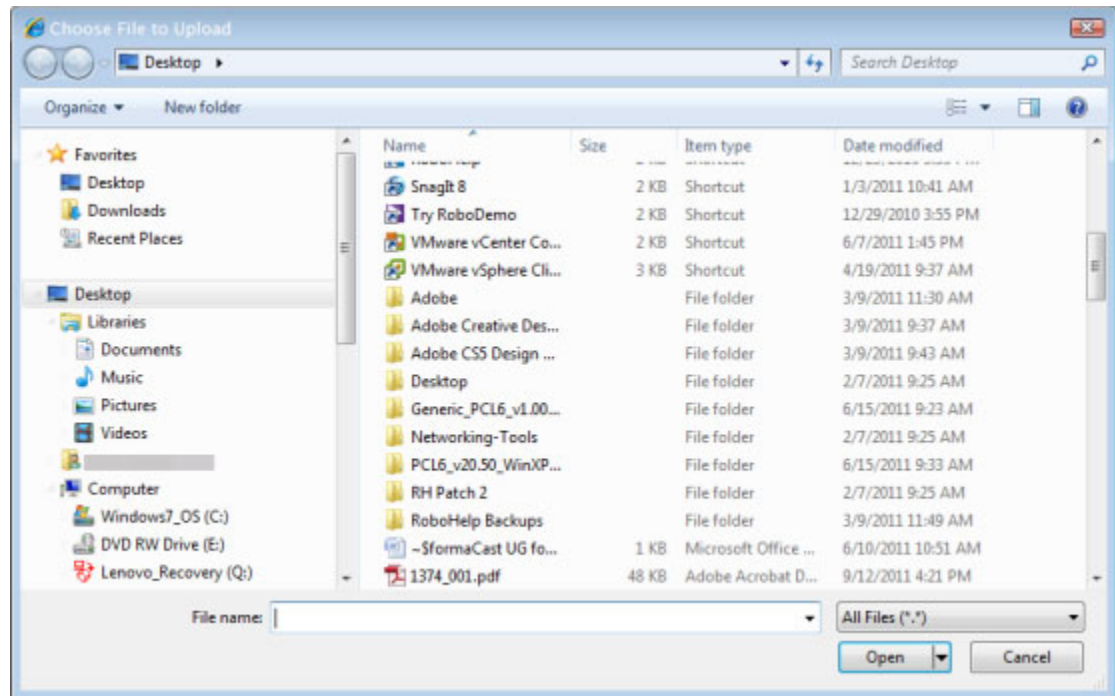


- Step 8** Click the **Upload Certificate/Certificate chain** button. The Upload Certificate/Certificate chain window appears.



- 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 Cisco Unified CM server used by the SIP trunk.



**Note** The following steps require you to restart Cisco Unified CM. Plan to perform them during a maintenance window to avoid disrupting your users. Your certificate will not take effect until Cisco Unified CM is restarted.

**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 Cisco Unified CM again.

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



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

**Control Center - Feature Services**

Navigation: Cisco Unified Serviceability Go

ccadministrator About Logout

Alarm Trace Tools Smp CallHome Help

Related Links: Service Activation Go

Start Stop Restart Refresh Page

Status: Ready

Select Server

Server: dev-ucm90-pub Go

**Database and Admin Services**

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

**Performance and Monitoring Services**

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

**Directory Services**

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

**CM Services**

Service Name	Status	Activation Status	Start Time	Up Time
<input type="radio"/> Cisco CallManager	Started	Activated	Wed Oct 16 00:26:20 2013	140 days 04:54:15
<input type="radio"/> Cisco Messaging Interface	Not Running	Deactivated		
<input type="radio"/> Cisco Unified Mobile Voice Access Service	Not Running	Deactivated		
<input type="radio"/> Cisco IP Voice Media Streaming App	Started	Activated	Tue Feb 19 09:30:13 2013	379 days 02:50:30
<input type="radio"/> Cisco CTIManager	Started	Activated	Wed Jan 15 13:49:07 2014	48 days 22:31:36
<input type="radio"/> Cisco Extension Mobility	Started	Activated	Tue Mar 4 16:07:11 2014	0 days 20:13:32
<input type="radio"/> Cisco DHCP Monitor Service	Not Running	Deactivated		
<input type="radio"/> Cisco Intercluster Lookup Service	Not Running	Deactivated		
<input type="radio"/> Cisco Location Bandwidth Manager	Not Running	Deactivated		
<input type="radio"/> Cisco Dialed Number Analyzer Server	Not Running	Deactivated		
<input type="radio"/> Cisco Tftp	Started	Activated	Thu Jun 27 09:46:41 2013	251 days 03:34:02

**CTI Services**

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

**Voice Quality Reporter Services**

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

**CDR Services**

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

**Security Services**

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

Start Stop Restart Refresh

i\* - indicates required item.

**Step 18** Scroll to the *CM Services* area.

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

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

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

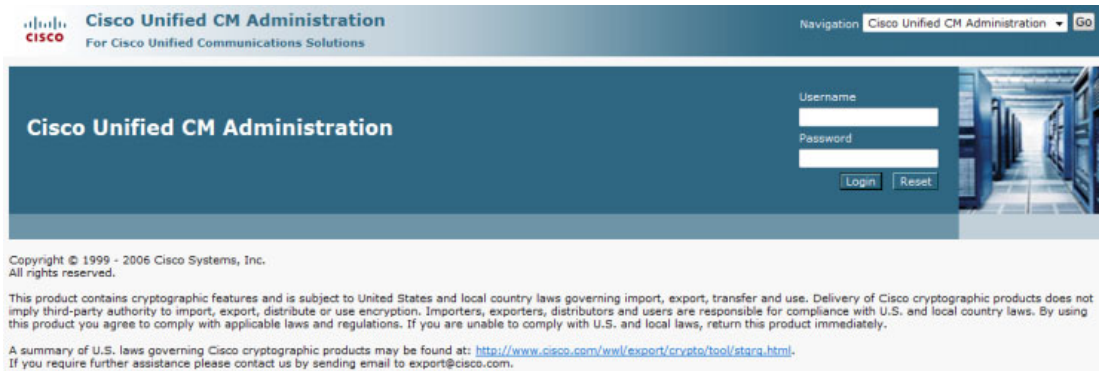


- Step 22** Scroll to the top of the page and repeat Steps 17 through 21 for each Cisco Unified CM server used by the SIP trunk.

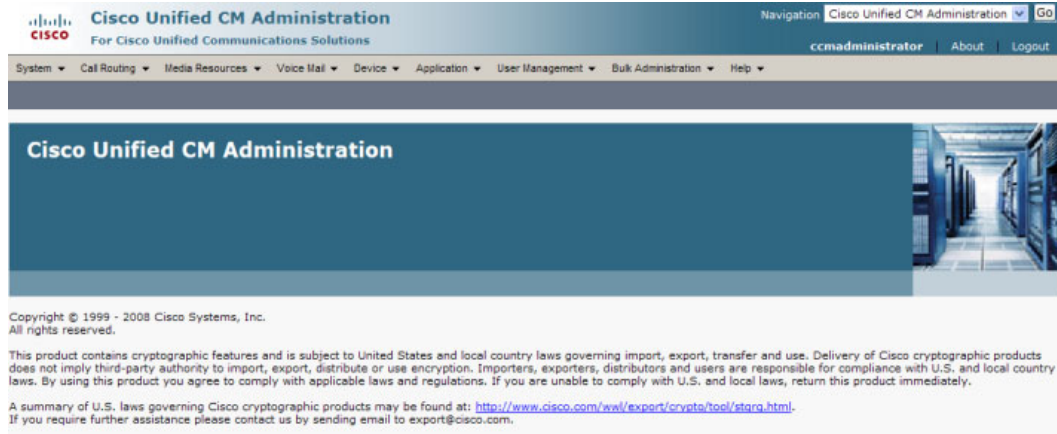
### Add a SIP Trunk Security Profile That Uses TLS

After installing the InformaCast SIP certificate on Cisco Unified CM, use the following steps to create a SIP trunk security profile that uses TLS.

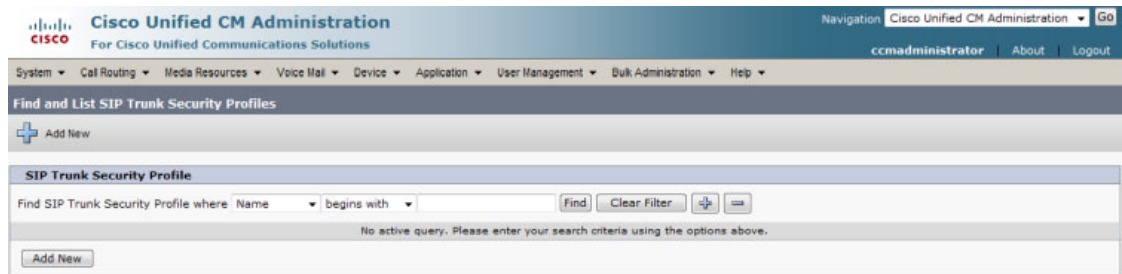
- Step 1** Select **Cisco Unified CM Administration** from the **Navigation** menu and click the **Go** button. The Cisco Unified CM Administration page appears.



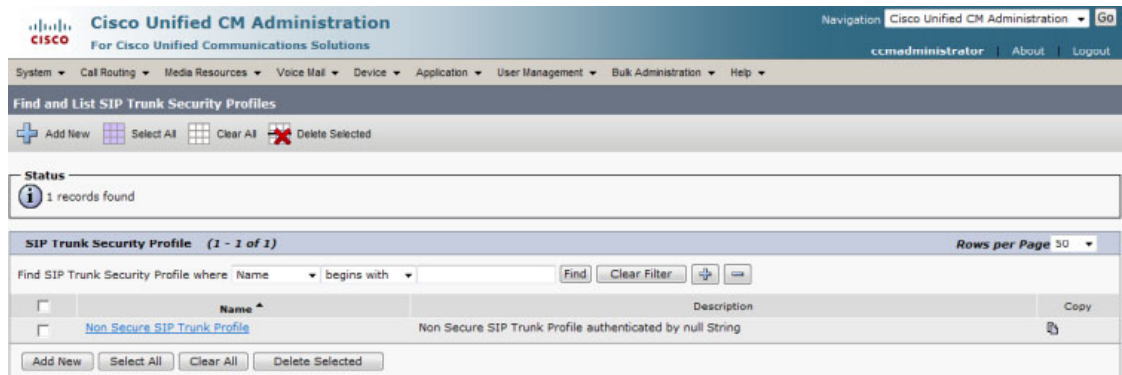
- Step 2** Enter your administrative username and password in the **Username** and **Password** fields, respectively, and click the **Login** button. The Cisco Unified CM Administration page refreshes.



**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.

The screenshot shows the Cisco Unified CM Administration interface for configuring a SIP Trunk Security Profile. The page title is "SIP Trunk Security Profile Configuration" and it includes a "Save" button. The "SIP Trunk Security Profile Information" section contains the following fields and options:

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

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

- 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 the certificate common name assigned to your InformaCast 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.

```

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

  Key: Sun RSA public key, 1024 bits
  modulus:
1183697121016984262124186139075525433477849254894024690612744900000173735735326922621
1540857756645914171069876103438026520403470446582208459226084141271592141747568141928
7976525350321996019091283029028515297515845874347643393471135200295957930875774977221
915286745498762127423199339533477897994916941166934273
  public exponent: 65537
  Validity: [From: Wed Nov 16 20:13:12 CST 2011,
            To: Sat Apr 02 21:13:12 CDT 2039]
  Issuer: CN=InformaCast-172.30.227.212
  SerialNumber: [ 4ec46db8]
]
Algorithm: [SHA1withRSA]
Signature:
0000: 77 22 26 DF 15 E8 95 DD 8E 5C 50 FC 9C F6 ED BC w*&.....P.....
0010: 36 9E 31 CC EF 2F 4A 11 52 F6 1E 4C 57 AB 79 4E 6.1..J.R.LW.yN

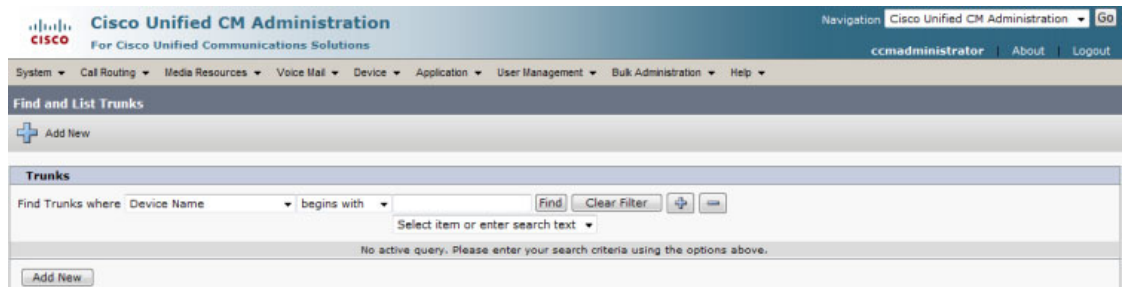
```

- Step 11** Enter **5061** in the **Incoming Port** field.
- Step 12** Select the **Accept Unsolicited Notification** checkbox.
- Step 13** Click the **Save** button.
- Step 14** Continue with “Add a SIP Profile” on page 8-60.

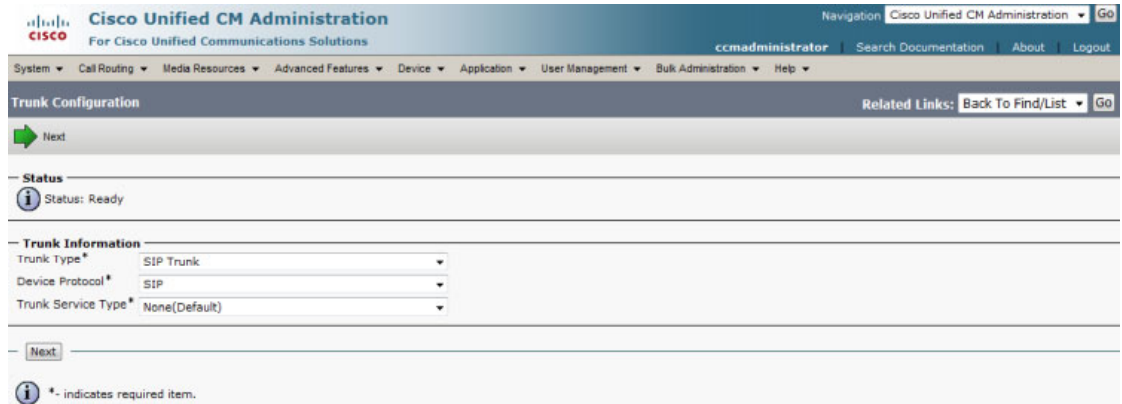
### Add a SIP Trunk That Uses TLS

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 8-71.

- 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.



The screenshot shows the Cisco Unified CM Administration interface for configuring a trunk. The page title is "Trunk Configuration". At the top, there is a navigation menu with options like "System", "Call Routing", "Media Resources", "Advanced Features", "Device", "Application", "User Management", "Bulk Administration", and "Help". The user is logged in as "ccmadministrator". Below the navigation, there is a "Next" button with a green arrow. The "Status" section shows "Status: Ready". The "Trunk Information" section contains three dropdown menus: "Trunk Type\*" (set to "SIP Trunk"), "Device Protocol\*" (set to "SIP"), and "Trunk Service Type\*" (set to "None(Default)"). A "Next" button is located below the dropdowns. At the bottom, there is an information icon and a note: "\*- indicates required item."

**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\*  
Common Device Configuration  
Call Classification\*  
Media Resource Group List  
Location\*  
AAR Group  
Tunneled Protocol\*  
QSIG Variant\*  
ASN.1 ROSE OID Encoding\*  
Packet Capture Mode\*  
Packet Capture Duration

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\*  
Route Class Signaling Enabled\*  
Use Trusted Relay Point\*  
 PSTN Access  
 Run On All Active Unified CM Nodes

**Call Routing Information**

Remote-Party-Id  
 Asserted-Identity  
Asserted-Type\*  
SIP Privacy\*

**Inbound Calls**

Significant Digits\*  
Connected Line ID Presentation\*  
Connected Name Presentation\*  
Calling Search Space  
AAR Calling Search Space  
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\*  
BLF Presence Group\*  
SIP Trunk Security Profile\*  
Rerouting Calling Search Space  
Out-Of-Dialog Refer Calling Search Space  
SUBSCRIBE Calling Search Space  
SIP Profile\*  
DTMF Signaling Method\*

Save

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

- Step 7** Enter a name for your SIP trunk in the **Device Name** field, e.g. InformaCast/TLS.
- Step 8** Select the device pool you created in “Create a Device Pool” on page 8-14 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 8-17 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 8-74).
- 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 8-71 from the **SIP Trunk Security Profile** dropdown menu.
- Step 14** Select the SIP profile you created in “Add a SIP Profile” on page 8-60 from the **SIP Profile** dropdown menu.
- Step 15** Click the **Save** button.

### *Install Cisco Unified CM Certificates on InformaCast*

To use the TLS protocol between Cisco Unified CM and InformaCast, you will need to install on InformaCast two certificates from each node of the Cisco Unified CM group used by the SIP trunk’s device pool: CallManager and CallManager-ECDSA.

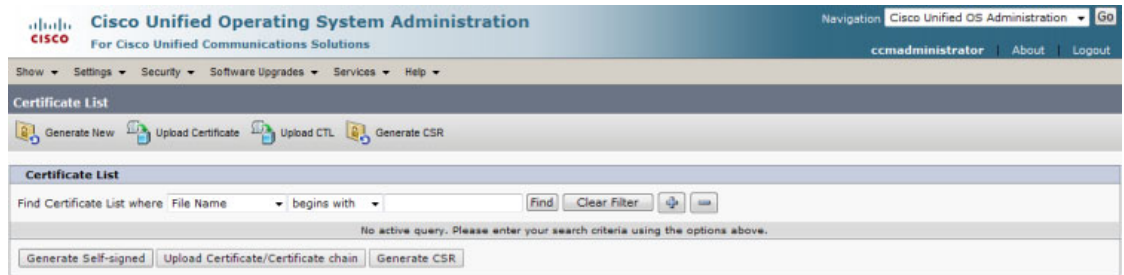
- Step 1** Select **Cisco Unified OS Administration** from the **Navigation** dropdown menu and click the **Go** button. The Cisco Unified Operating System Administration page appears.



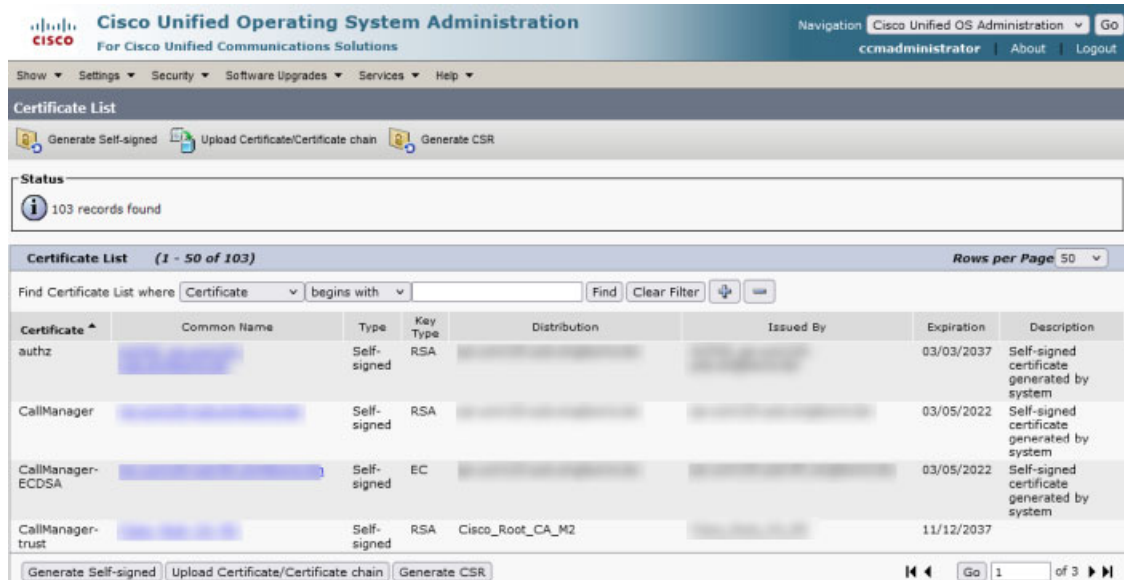
**Step 2** Enter your Operating System Administration username and password in the **Username** and **Password** fields, respectively, and click the **Login** button. The Cisco Unified Operating System Administration page refreshes.



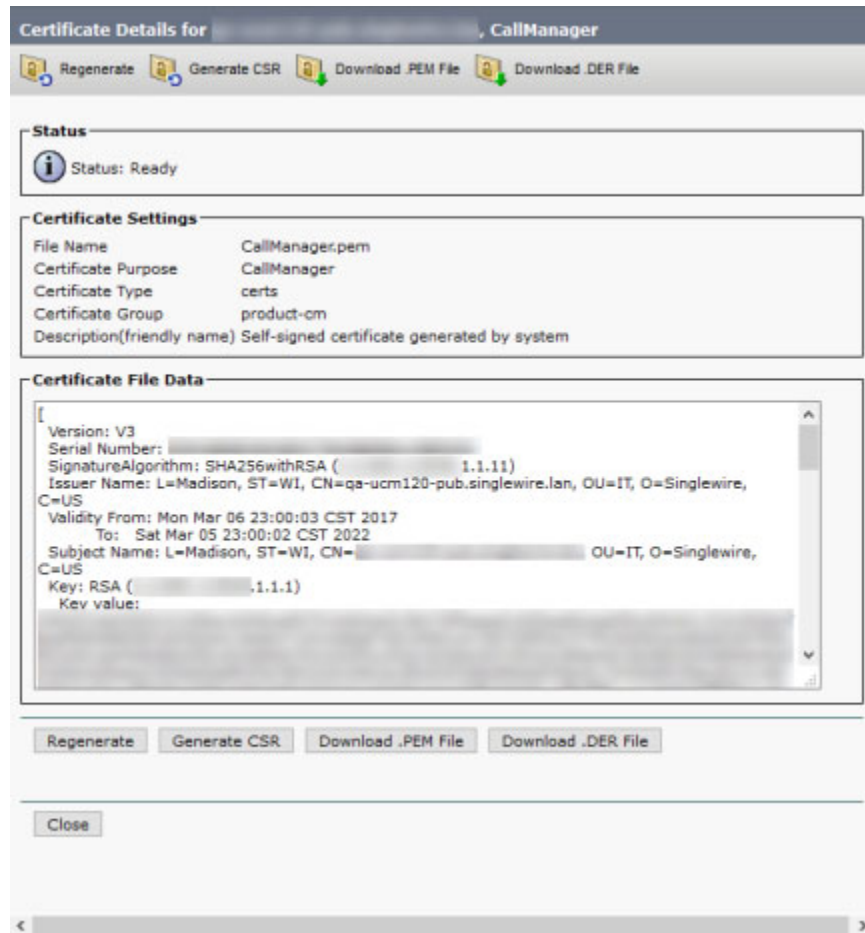
**Step 3** Go to **Security | Certificate Management**. The Certificate List page appears.



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



- Step 5** Click the **Common Name** link of the certificate that displays “CallManager” in the Certificate column. The Certificate Details pop-up window appears.



- Step 6** Click the **Download .PEM File** button.

Depending on your browser, Cisco Unified CM may download the certificate to a common downloads folder or ask you for a location in which to place the certificate. Select a location accessible to your InformaCast server and click the **Save** button.



**Note** Repeat these download steps for each Cisco Unified CM server that will be communicating with InformaCast.

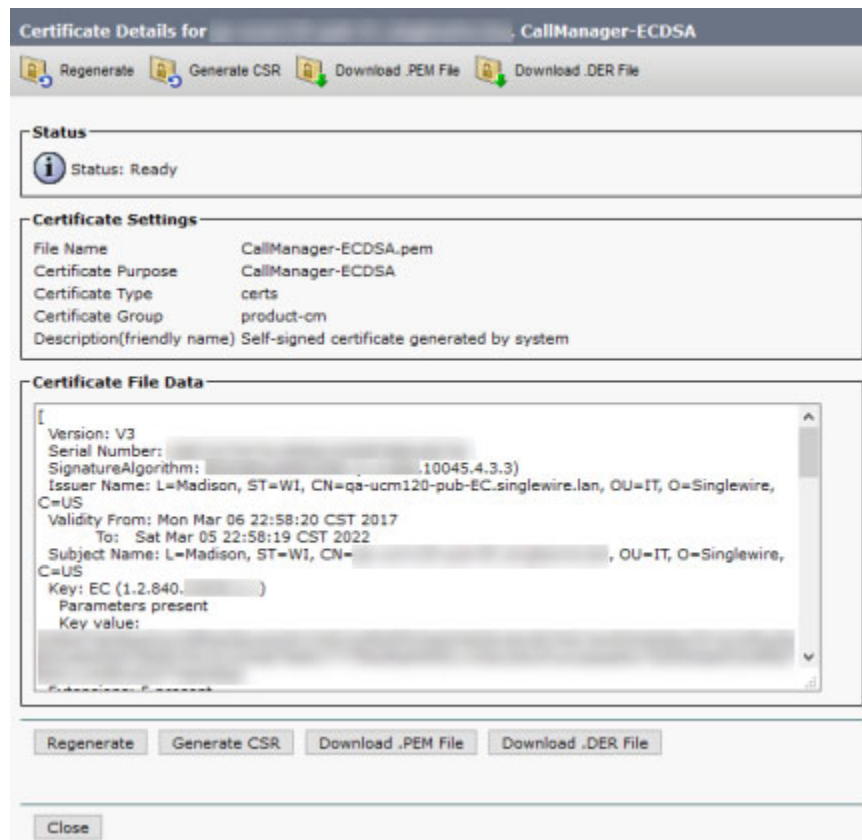
- Step 7** Return to the Certificate List page.



**Note** You may need to click the **Find** button again to display all the certificates about which Cisco Unified CM knows.



- Step 8** Click the **Common Name** link of the certificate that displays "CallManager-ECDSA" in the Certificate column. The Certificate Details pop-up window appears.



- Step 9** Click the **Download .PEM File** button.

Depending on your browser, Cisco Unified CM may download the certificate to a common downloads folder or ask you for a location in which to place the certificate. Select a location accessible to your InformaCast server and click the **Save** button.

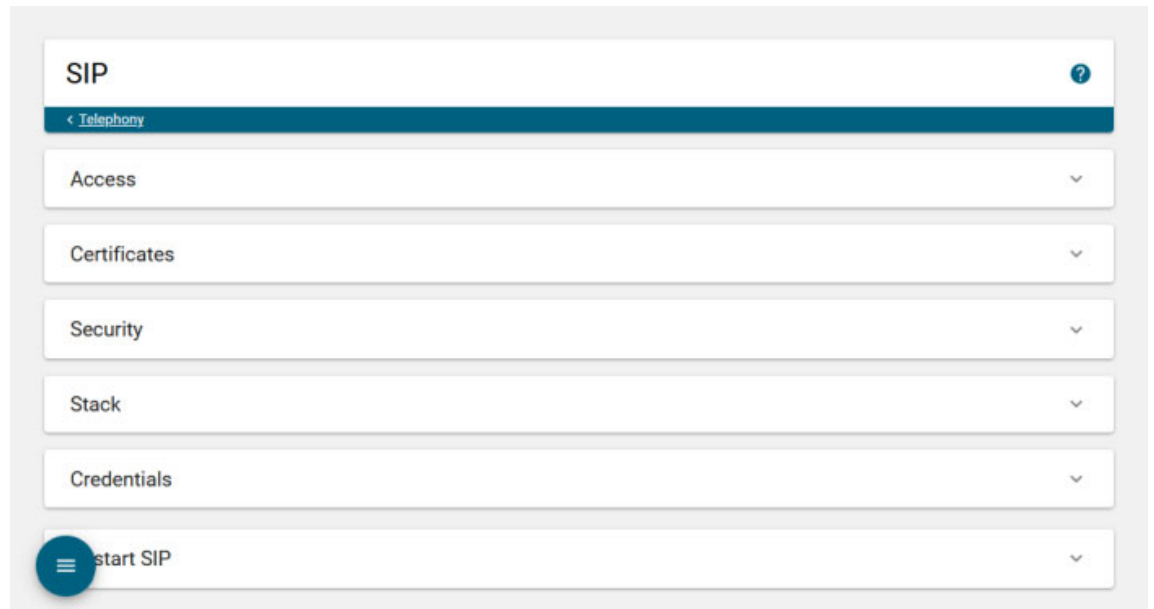


**Note** Repeat these download steps for each Cisco Unified CM server that will be communicating with InformaCast.

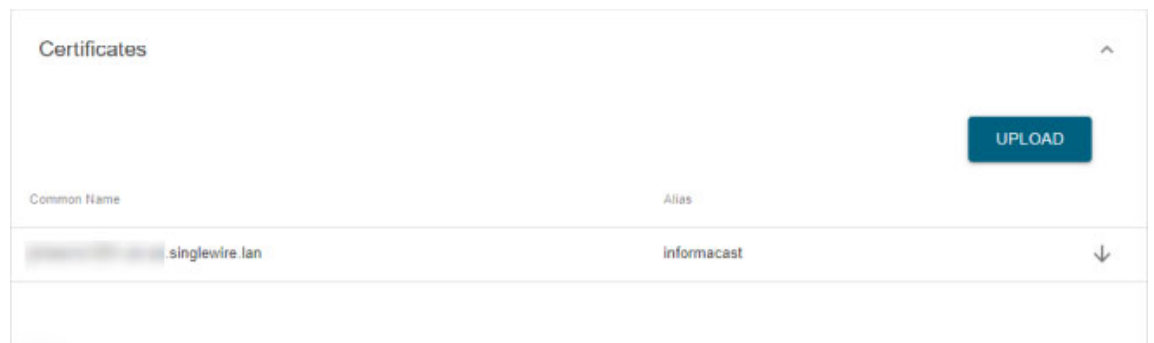
- Step 10** Go back to your InformaCast window.



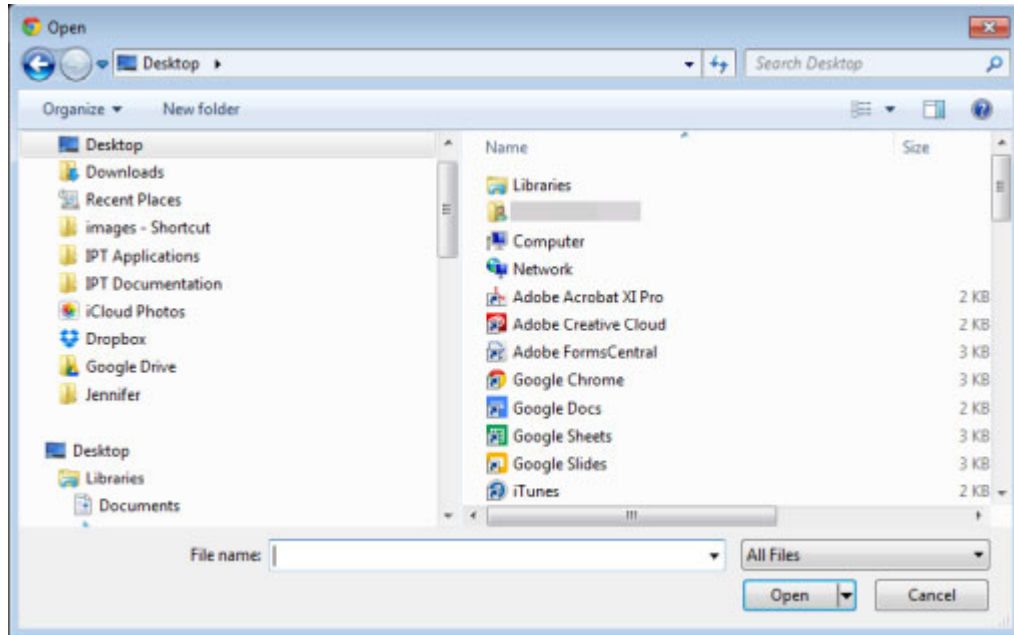
**Step 11** Go to **System Administration | Telephony | SIP**. The SIP page appears.



**Step 12** Expand the *Certificates* area, if it's not already visible.



**Step 13** Click the **Upload** button. The Open dialog box appears.



**Step 14** Navigate to where you saved your CallManager.pem and CallManager-ECDSA.pem files, select one, and click the **Open** button. InformaCast uploads your certificate. Select the other .pem file and click the **Open** button. InformaCast uploads your certificate.

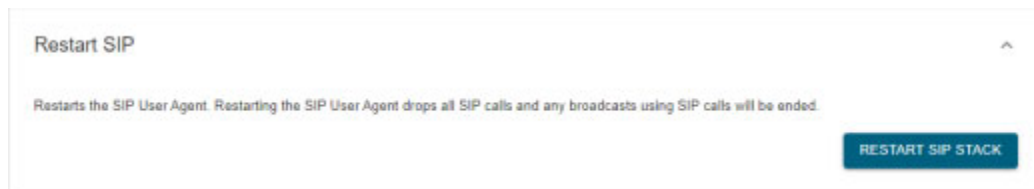
**Step 15** Upload each CallManager.pem and CallManager-ECDSA.pem file you downloaded. The Certificates area refreshes with each certificate you add.

**Step 16** Perform Steps 13 through 15 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 17** Expand the *Restart SIP* area, if it's not already visible.



**Step 18** Click the **Restart SIP Stack** button. It may take a few moments for SIP to restart.

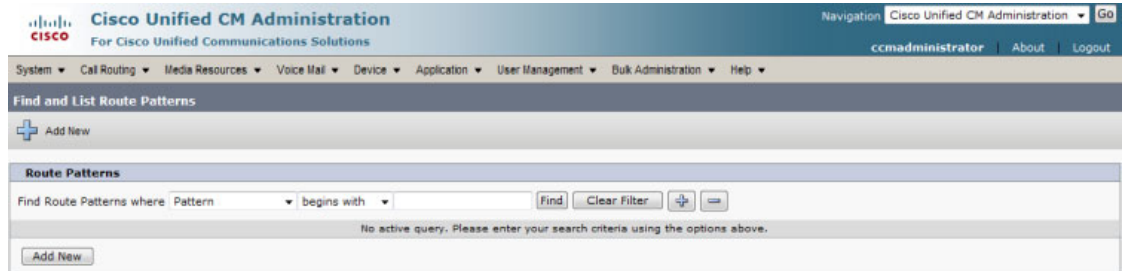


**Caution** Restarting SIP causes all SIP calls to be dropped, i.e. any callers interacting with the DialCast IVR will have their calls dropped. Live broadcasts using SIP calls will be stopped.

### 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 8-62 or “Add a SIP Trunk That Uses TLS” on page 8-74. In your route pattern, specify a range of DNs that, when called, use the SIP trunk or wild card patterns to match a range of numbers.

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



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

The screenshot displays the 'Route Pattern Configuration' page in the Cisco Unified CM Administration interface. The page is titled 'Route Pattern Configuration' and includes a 'Save' button at the top left. The configuration is organized into several sections:

- Status:** Ready
- Pattern Definition:**
  - Route Pattern\* (text input)
  - Route Partition (dropdown menu, currently '< None >')
  - Description (text input)
  - Numbering Plan (dropdown menu, currently '-- Not Selected --')
  - Route Filter (dropdown menu, currently '< None >')
  - MLPP Precedence\* (dropdown menu, currently 'Default')
  - Gateway/Route List\* (dropdown menu, currently '-- Not Selected --', with an '(Edit)' link)
  - Route Option (radio buttons for 'Route this pattern' (selected) and 'Block this pattern', with a 'No Error' dropdown)
  - Call Classification\* (dropdown menu, currently 'OffNet')
  - Checkboxes: Allow Device Override, Provide Outside Dial Tone (checked), Allow Overlap Sending, Urgent Priority
  - Require Forced Authorization Code (checkbox)
  - Authorization Level\* (text input, currently '0')
  - Require Client Matter Code (checkbox)
- Calling Party Transformations:**
  - Use Calling Party's External Phone Number Mask (checkbox)
  - Calling Party Transform Mask (text input)
  - Prefix Digits (Outgoing Calls) (text input)
  - Calling Line ID Presentation\* (dropdown menu, currently 'Default')
  - Calling Name Presentation\* (dropdown menu, currently 'Default')
- Connected Party Transformations:**
  - Connected Line ID Presentation\* (dropdown menu, currently 'Default')
  - Connected Name Presentation\* (dropdown menu, currently 'Default')
- Called Party Transformations:**
  - Discard Digits (dropdown menu, currently '< None >')
  - Called Party Transform Mask (text input)
  - Prefix Digits (Outgoing Calls) (text input)
- ISDN Network-Specific Facilities Information Element:**
  - Network Service Protocol (dropdown menu, currently '-- Not Selected --')
  - Carrier Identification Code (text input)
  - Network Service (dropdown menu, currently '-- Not Selected --')
  - Service Parameter Name (dropdown menu, currently '< Not Exist >')
  - Service Parameter Value (text input)

A 'Save' button is located at the bottom left of the form. A legend at the bottom indicates that an asterisk (\*) denotes a required item.

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

**Step 4** Select a route partition from the **Route Partition** dropdown menu. This partition should be reachable from the Cisco IP phones for Unified CM 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 8-62 or “Add a SIP Trunk That Uses TLS” on page 8-74 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

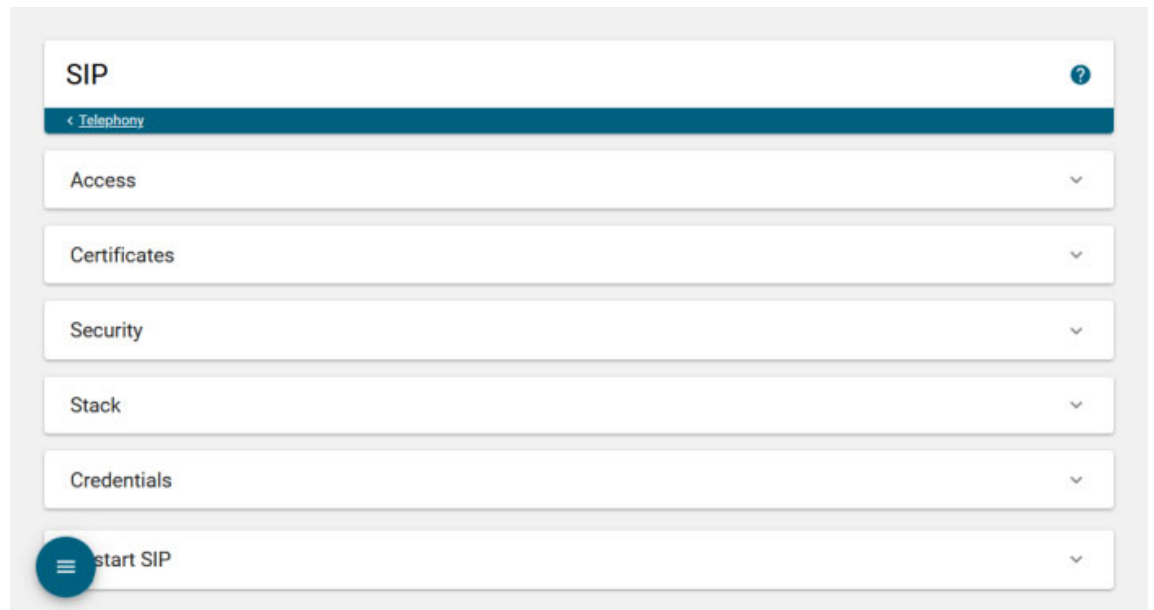
InformaCast's SIP access permits you to either allow or deny incoming SIP calls. The all-or-nothing scope of these buttons can be tuned by adding exceptions that counteract their setting. For example, when all incoming SIP calls are denied, exceptions serve to *allow* calls to be answered from the hosts 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. As the message is routed to its destination, additional Via headers are added at each hop. When the message arrives at its final destination, one or more Via headers are present in the request. Via headers are used by SIP to ensure that responses are routed back to the caller through the same hosts 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 **System Administration | Telephony | SIP**. The SIP page appears.



**Step 2** Expand the *Access* area, if it's not already visible.

The screenshot shows the 'Access' configuration page. Under 'Incoming SIP Access', the 'Allow' radio button is selected. The 'Exceptions' section is currently empty, with a 'CREATE' button visible. The page also includes 'RESET CONFIGURATION' and 'SAVE' buttons.



**Note** By default, SIP access is denied.

**Step 3** Click the **Create** button in the *Exceptions* area to add exceptions to the SIP calls that are denied. The Create SIP Access Exception page appears.

The screenshot shows the 'Create SIP Access Exception' page. The breadcrumb trail is '< General Configuration < SIP'. The 'General Details' section has a text input field for 'Host or Subnet \*'. The 'CANCEL' and 'SAVE' buttons are located at the bottom right of the form.

**Step 4** 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.example.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 5** Click the **Save** button. The SIP page appears and when you expand the *Access* area, you can see your new exception.

The screenshot shows a configuration page for SIP access. At the top, there's a section titled 'Access' with a collapse arrow. Below it, 'Incoming SIP Access:' has two radio buttons: 'Allow' (selected) and 'Deny'. To the right are 'RESET CONFIGURATION' and 'SAVE' buttons. Below that is the 'Exceptions' section, which is currently empty and has a 'CREATE' button. At the bottom, there's a 'Host or Subnet' input field. At the very bottom of the page, there's a pagination control showing 'Rows per page: 10' and '1-1 of 1' with navigation arrows.



**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.



**Tip** Delete an exception by clicking its **More | Delete** icon.



---

**Tip** Click the **Reset Configuration** 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, 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.

If your installation of InformaCast is integrated with Cisco Unified Communications Manager, you should ensure your Cisco Unified CM is also operating in mixed mode.

- **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.

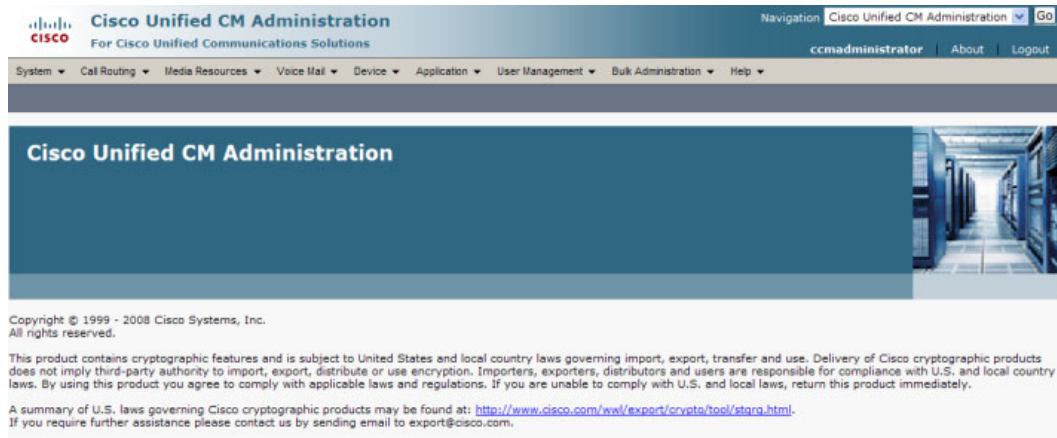
First you'll obtain Cisco Unified CM's SIP realm and authentication credentials. Then, you'll add them to InformaCast.



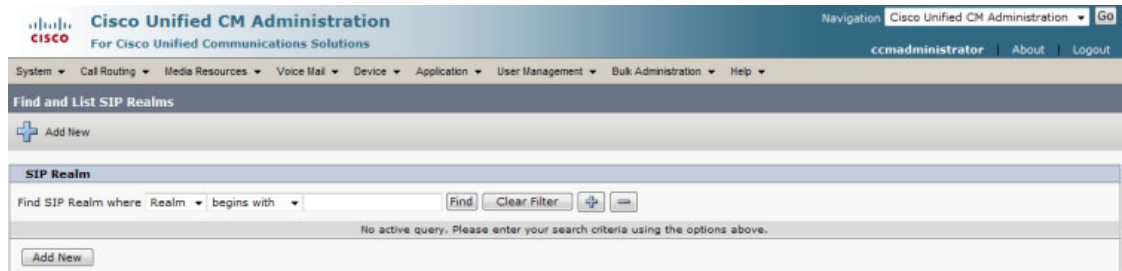
## Obtain Realm and Credentials Information from Cisco Unified CM

Use the following steps to obtain realm and credentials information from Cisco Unified CM.

- Step 1** Open a web browser and log into the administration interface of the Cisco Unified CM server (the address will be similar to `https://<Cisco Unified CM 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 1 on page 8-91.

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.

The screenshot shows the Cisco Unified CM Administration interface for SIP Realm Configuration. The page title is "SIP Realm Configuration" and it includes a "Save" button at the top left. Below the title bar, there is a "Status" section showing "Status: Ready". The main configuration area is titled "SIP Realm Information" and contains four required fields: "Realm\*", "User\*", "Digest Credentials\*", and "Confirm Digest Credentials\*". Each field has a corresponding input box. A "Save" button is located at the bottom left of the form. A legend at the bottom indicates that an asterisk (\*) denotes a required item.

**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.

## Add Realm and Credentials Information to InformaCast

Use the following steps to add realm and credentials information to InformaCast.

**Step 1** Log into InformaCast. The InformaCast Dashboard appears.

**Dashboard**

**Welcome to InformaCast**  
**Basic Paging (Cisco**  
**Paging Server)**

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
- Create unlimited recipient groups of 50 phones or less

[Technical Support](#)  
[User Guide](#)

**Reach More People and Devices**

Upgrade to InformaCast Advanced and enjoy a full-featured emergency notification solution that allows you to reach an unlimited number of phones as well as a variety of other endpoints, send text and live or pre-recorded audio as messages, add broadcast confirmations, and much more.

Click the Buy button to begin the process of obtaining an InformaCast Advanced license. You can also click the Try button to start your free 60-day InformaCast Advanced trial. If you would like more information, click the Demo button to request a demo.

**InformaCast Advanced**

[BUY](#) [TRY](#) [DEMO](#)

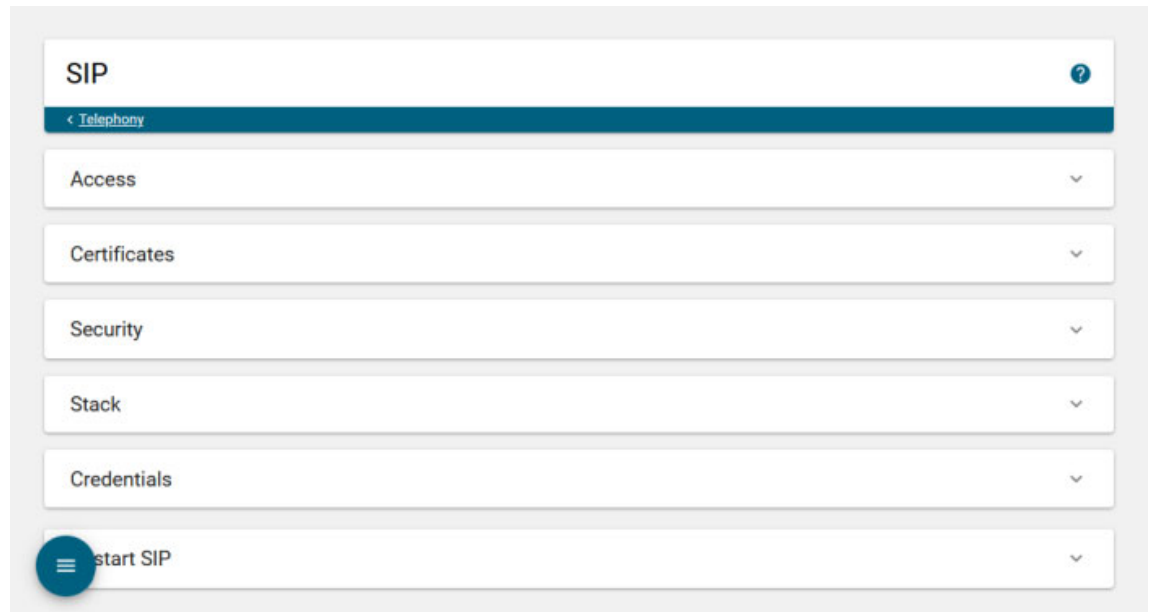
**Features Include:**

- Live audio paging between Cisco IP Phones, with no limit on the number of phones per group
- Integration to existing overhead paging systems
- Text and audio (live or pre-recorded) to Cisco IP Phones and other endpoints
- Audio broadcasts to IP Speakers
- 911/emergency call monitoring/alerting/recording
- Automated weather notifications
- Dynamically-triggered emergency conference calls
- Pre-recorded/scheduled broadcasts(school bells/shift changes)
- Notification to computer desktops (Windows and MacOS) via [InformaCast Desktop Notifier](#)
- Integrate with digital signage solutions and 3rd-party mass notification providers
- Notification and confirmation to mobile devices (Apple, Android, and SMS) with [InformaCast Fusion](#)
- Trigger notification to/from other systems (panic/duress buttons, door locks, lights, etc.)
- And More

**Learn More**

- [InformaCast Details](#)

**Step 2** Go to **System Administration | Telephony | SIP**. The SIP page appears.



**Step 3** Expand the *Security* area, if it's not already visible.



**Note** By default, all call security is disabled.

**Step 4** Select the **Secure Signaling Required** checkbox if you want to use the TLS transport protocol to send your SIP messages. Once selected, the **Secure RTP Allowed** checkbox becomes accessible.

**Step 5** 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).

With the **Secure RTP Allowed** checkbox selected, you should also ensure you've configured a secure SIP trunk connection (see "Configure a SIP Trunk Connection" on page 8-57).



---

**Note** You must also have your Cisco Unified CM running in mixed mode.

---

**Step 6** Select the **Authenticate Incoming Requests** checkbox to enable SIP authentication.

**Step 7** Enter values in the **Realm**, **Authentication Username**, and **Authentication Password** fields that match the values you entered in Steps 5 through 8.

**Step 8** 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 9** Click the **Save** button. Your changes are saved.

---

### Enable Digest Authentication with SIP User Credentials



---

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

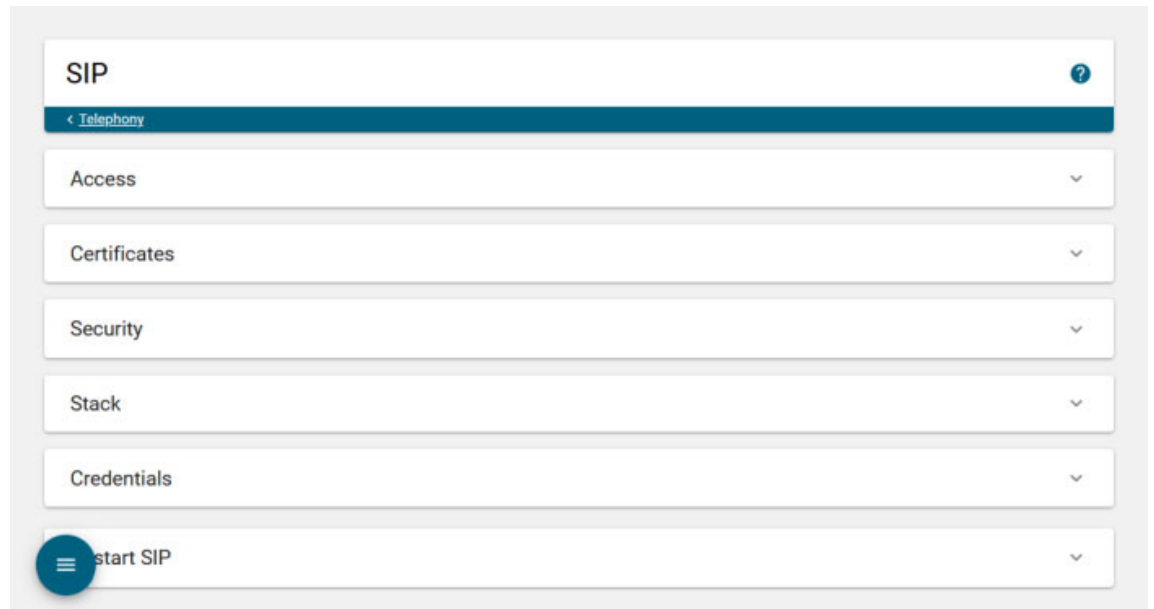
---

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.

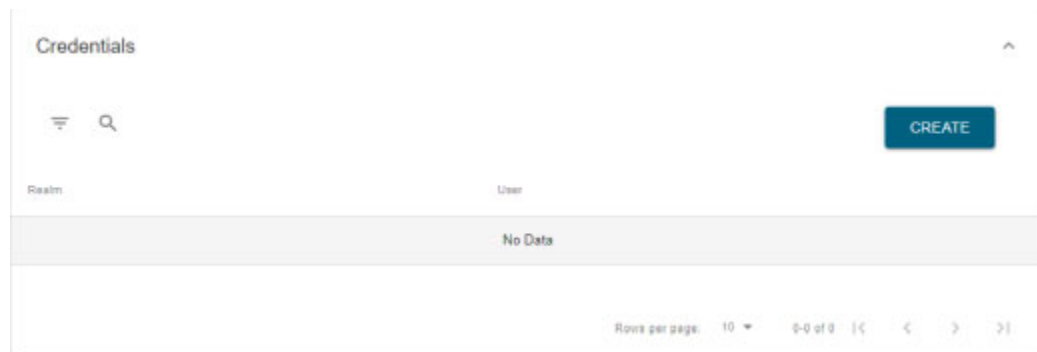
### Add SIP User Credentials

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

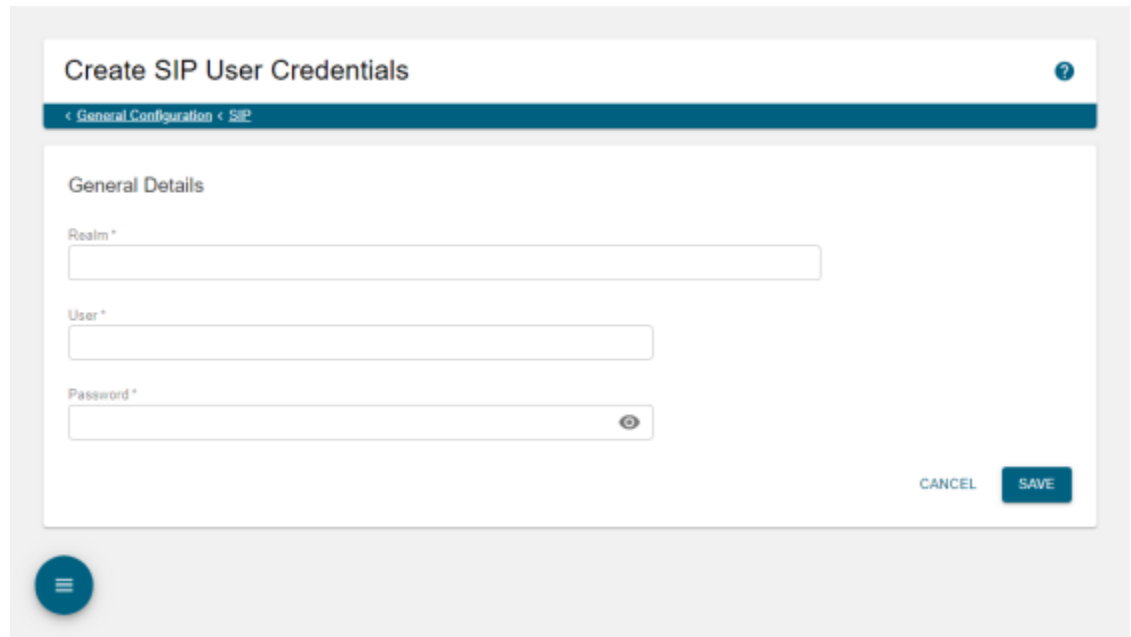
- Step 1** Go to **System Administration | Telephony | SIP**. The SIP page appears.



- Step 2** Expand the *Credentials* area, if it's not already visible.



**Step 3** Click the **Create** button. The Create SIP User Credentials page appears.



The screenshot shows a web interface titled "Create SIP User Credentials". At the top, there is a breadcrumb trail: "< General Configuration < SIP?". Below this is a section titled "General Details" containing three input fields: "Realm\*", "User\*", and "Password\*". The "Password\*" field has a toggle icon to its right. At the bottom right of the form are two buttons: "CANCEL" and "SAVE". A blue circular menu icon is visible in the bottom left corner of the page.

**Step 4** Enter the name of your SIP peer's SIP realm in the **Realm** field.

**Step 5** Enter the username associated with the SIP peer's SIP realm in the **User** field.

**Step 6** Enter the password of the username associated with the SIP peer's SIP realm in the **Password** field.



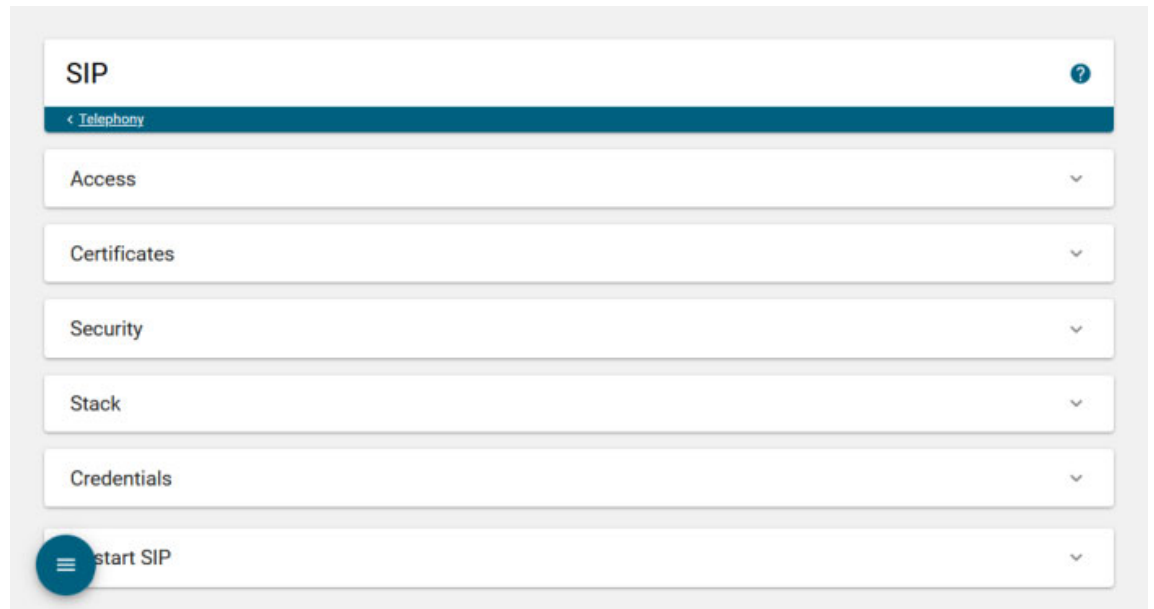
**Note** The password can be up to 64 characters in length.

**Step 7** Click the **Save** button. Your SIP user credentials are saved.

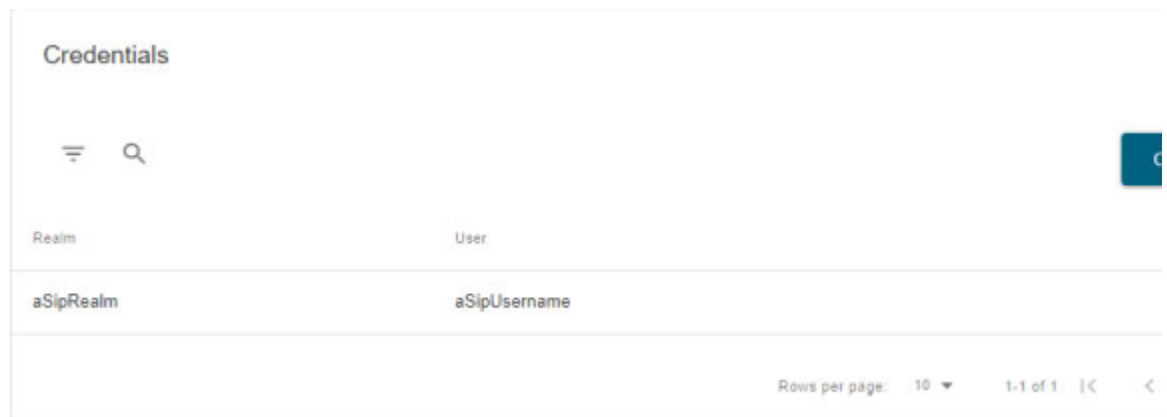
### Edit SIP User Credentials

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

**Step 1** Go to **System Administration | Telephony | SIP**. The SIP page appears.



**Step 2** Expand the *Credentials* area, if it's not already visible.





- Step 3** Click the table row or **More** | **Edit** icon of the user credentials you want to modify. The Edit SIP User Credentials page appears.

The screenshot shows the 'Edit SIP User Credentials' page. The page title is 'Edit SIP User Credentials' with a help icon. Below the title is a breadcrumb trail: '< General Configuration < SIP'. The main content area is titled 'General Details' and contains three input fields: 'Realm \*' with the value 'aSipRealm', 'User \*' with the value 'aSipUsername', and 'Password \*' with masked characters '\*\*\*\*\*' and a toggle icon. At the bottom right of the form are 'CANCEL' and 'SAVE' buttons. A blue circular menu icon is visible at the bottom left of the page.

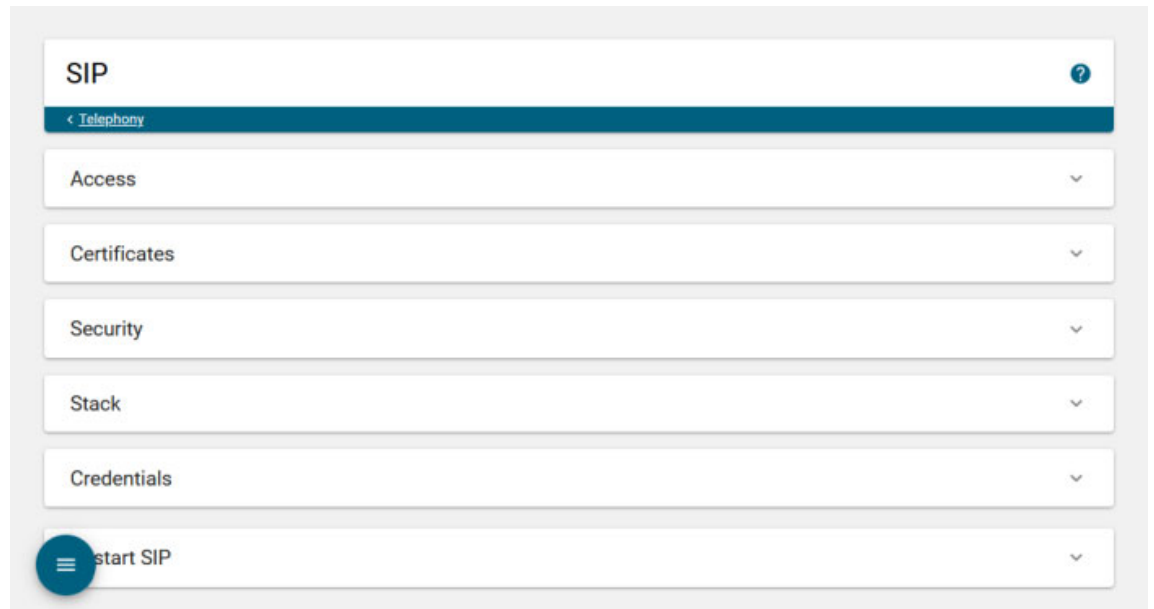
On the Edit SIP User Credentials page, you can change the name of your SIP peer's SIP realm or enter a different username and password.

- Step 4** Make your desired changes.
- Step 5** Click the **Save** button. Your changes are saved.

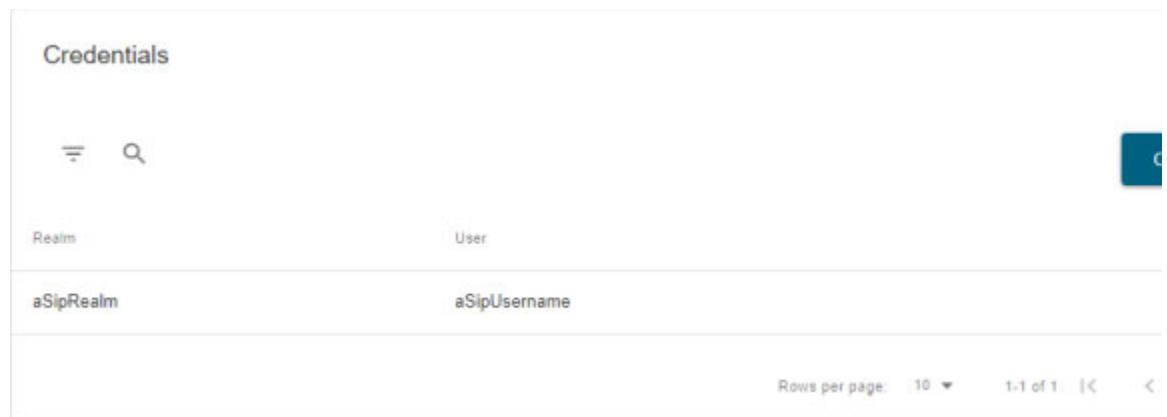
### Delete SIP User Credentials

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

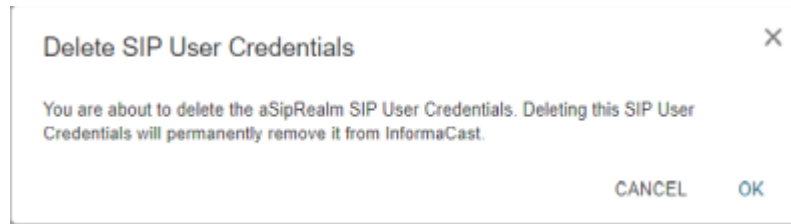
- Step 1** Go to **System Administration | Telephony | SIP**. The SIP page appears.



- Step 2** Expand the *Credentials* area, if it's not already visible.



- Step 3** Click the **More | Delete** icon of the SIP user credentials you want to delete. The Delete SIP User Credentials pop-up window appears.



- Step 4** Click the **OK** 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

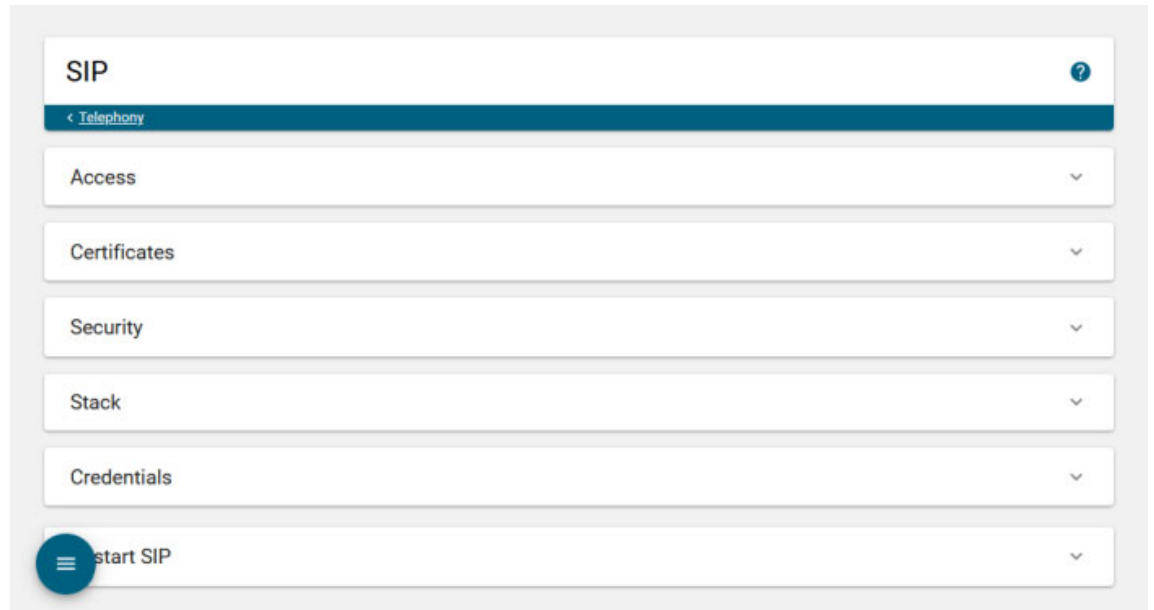
The log generated for the SIP stack, sipStack.log, is accessible through the Log Directory page (**User** dropdown menu | **Help** | **Log Directory**). sipStack.log can reach 10MB in size; at which point, sipStack.log.1 will be created to house the original contents of sipStack.log and sipStack.log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



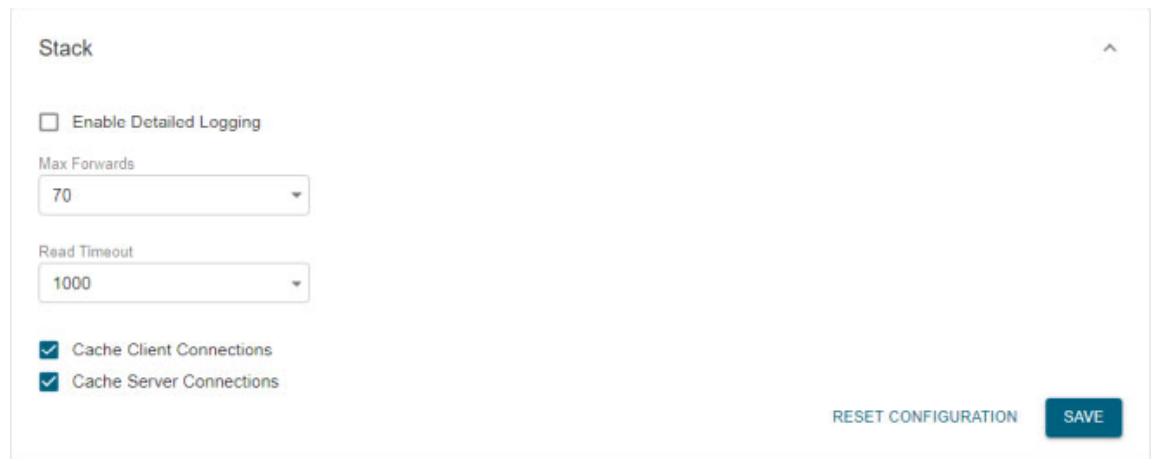
### Caution

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 **System Administration | Telephony | SIP**. The SIP page appears.



**Step 2** Expand the *Stack* area, if it's not already visible.



**Note**

Most values on this page should not ever need to be changed. The value most likely to be changed is the **Enable Detailed 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 3** Make your desired changes and click the **Save** button. Your changes are saved.



---

**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.

---



---

**Tip** Click the **Reset Configuration** button to return to your default settings.

---

## 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.

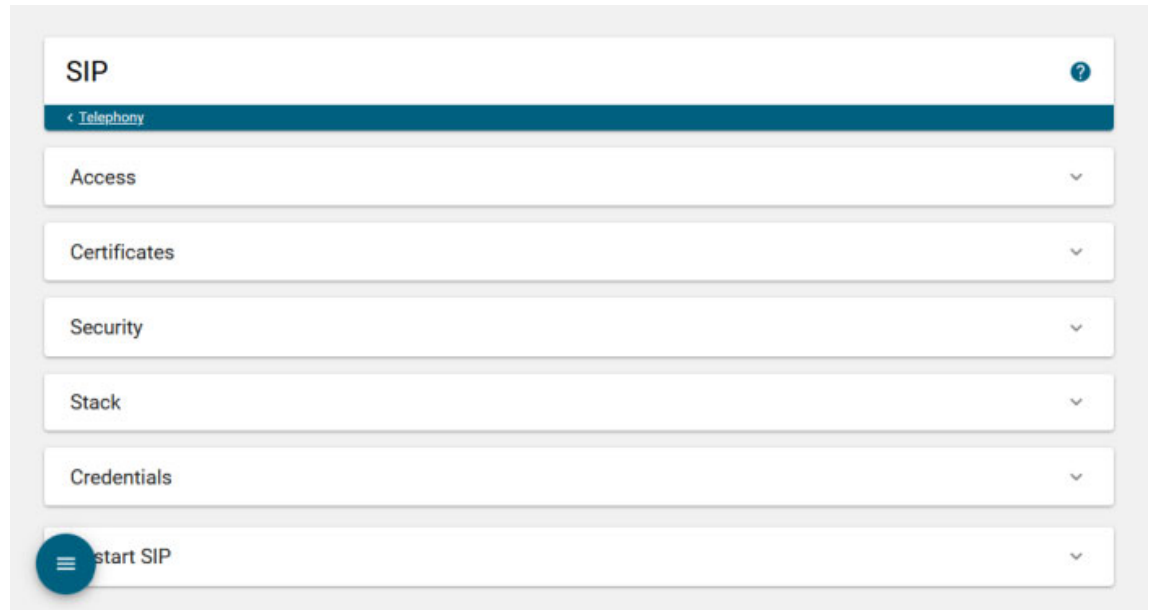


---

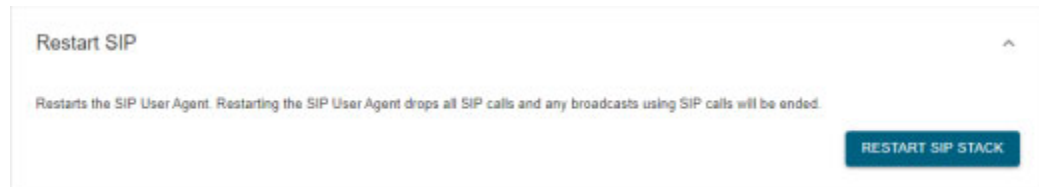
**Caution** Restarting SIP causes all SIP calls to be dropped, i.e. any callers interacting with the DialCast IVR will have their calls dropped. Broadcasts using SIP calls will also be impacted by a restart. Live broadcasts using SIP calls will be stopped.

---

**Step 1** Go to **System Administration | Telephony | SIP**. The SIP page appears.



**Step 2** Expand the *Restart SIP* area, if it's not already visible.



**Step 3** Click the **Restart** button. It may take a few moments for SIP to restart.



## Recipient Management

Basic InformaCast has only one type of eligible recipient, Cisco IP phones for Unified CM, which can receive live audio broadcasts through InformaCast's DialCast functionality (see “Manage DialCasts” on page 10-1) combined with proper session initiation protocol (SIP) configuration (see “Manage SIP Functionality” on page 8-56).

Recipient groups allow you to organize your IP phones into groups that will receive the broadcasts sent to them (see “Manage Recipient Groups” on page 9-17).

By default, InformaCast initially creates an “(All Recipients)” group, which contains all the IP phones that can be discovered. However, you may find it helpful to send to smaller groups.

Recipient administration covers a number of topics that pertain the administration of your Cisco IP phones for Unified CM (see “Manage Recipient Administration” on page 9-47).

## Manage IP Phones

Many models of [Cisco IP phones for Unified CM](#) are eligible recipients for InformaCast's broadcasts. Broadcasts sent to Cisco IP phones will activate the phones over CTI or HTTP. Their handsets (or external speakers) play the audio component of broadcasts in an RTP stream over multicast while their screens display the text component and any images or confirmations. In order for InformaCast to interact with IP phones, it must be configured to communicate with the Cisco Unified Communications Manager you set up in “Integrate Cisco Unified CM” on page 8-3.

The following sections cover setting up your IP phones' communication with InformaCast:

- “Add a Cisco Unified CM Cluster” on page 9-1
- “Edit Your Default Cluster” on page 9-11
- “Delete a Cisco Unified CM Cluster” on page 9-14
- “Manage Phone Updates” on page 9-15

### Add a Cisco Unified CM Cluster

In order for InformaCast to interact with Cisco IP phones for Unified CM, e.g. place calls, use JTAPI for monitoring busy states of associated phones, etc., it must be configured to communicate with the Cisco Unified CM you set up in “Integrate Cisco Unified CM” on page 8-3.

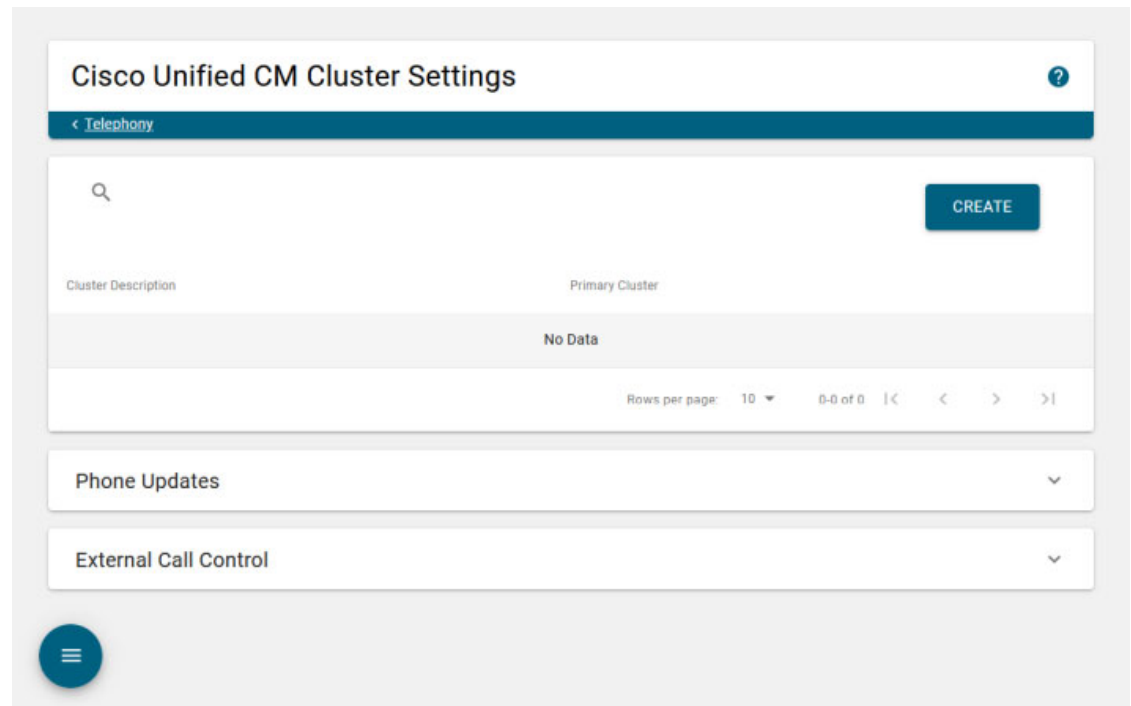
Before proceeding with the steps in this topic, there are several points of note:

- These steps should be performed by your Cisco Unified CM administrator.
- You must have an established CTI connection. If you followed the required topics in Integrate Cisco Unified CM, your CTI connection should already be established.
- You are only allowed one Cisco Unified CM cluster.

### Set Telephony Configuration

Use the following steps to set your Cisco Unified CM cluster's telephony configuration.

- Step 1** Go to **System Administration | Telephony | Cisco Unified CM Cluster**. The Cisco Unified CM Cluster Settings page appears.





**Step 2** Click the **Create** button. The Create Cisco Unified CM Cluster page appears.

## Create Cisco Unified CM Cluster

?

[< Telephony](#) < [Cisco Unified CM Cluster Settings](#)

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

### Telephony Configuration

Cisco Unified CM Cluster Description \*

Cisco Unified CM Application User \*

Cisco Unified CM Application Password \*

Use Application User for AXL

Cisco Unified CM AXL User \*

Cisco Unified CM AXL Password \*

AXL IP Address(es), comma-separated

Cisco Unified CM Address(es), comma-separated \*

Choose SNMP Version \*

SNMP v2

SNMP v3

SNMP v2 Community Name \*

Use Secure Connection

Send Commands to Phones by JTAPI

Create Telephony Terminals for All Phones

**XML Push Authentication**

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

Next Authentication URL

If empty, non-InformaCast authentication requests from phones in this cluster will be sent to the default Cisco Unified CM authentication page.

CANCEL
SAVE

- Step 3** Enter a name for your cluster in the **Cisco Unified CM Cluster Description** field.
- Step 4** Enter your application user's username in the **Cisco Unified CM Application User** field.
- Step 5** Enter your application user's password in the **Cisco Unified CM Application Password** field.

### Set AXL Configuration

Use the following steps to set your Cisco Unified CM cluster's AXL configuration.

- Step 1** Decide if you will use your application user or AXL user's credentials.

Using your AXL credentials means that potentially more people have administrative access to Cisco Unified CM, which may pose a security risk. To close this potential security hole, your Cisco Unified CM 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 Cisco Unified CM.

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 4.

For AXL credentials, continue with the following steps.

- Step 2** Enter the Cisco Unified CM administrator's username in the **Cisco Unified CM AXL User** field.



**Note** This is the same username you use to access the Cisco Unified CM Administration interface, often CCMAdministrator.

The username and password of the administrative login to the Cisco Unified CM server are required for gathering phone information to enable InformaCast to broadcast messages to Cisco IP phones.

- Step 3** Enter the Cisco Unified CM administrator's password in the **Cisco Unified CM AXL Password** field.



**Note** This is the same password you use to access the Cisco Unified CM Administrator interface, and it can be up to 64 characters in length.

The username and password of the administrative login to the Cisco Unified CM server are required for gathering phone information to enable InformaCast to broadcast messages to Cisco IP phones.

- Step 4** 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 Cisco Unified CM, 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 5** Enter the IP address of the Cisco Unified CM server(s) in the **Cisco Unified CM Address(es)** field, which will be used when establishing a CTI (JTAPI) connection with Cisco Unified CM. You can enter any and all Cisco Unified CMs running the CTI Manager service. Use the numeric IP addresses rather than DNS names.

When InformaCast needs to interact with the Cisco Unified CM, 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.

### Set SNMP Configuration

Use the following steps to set your Cisco Unified CM cluster's SNMP configuration.

- Step 1** 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 Create Cisco Unified CM Cluster page refreshes with new fields.

The screenshot shows a configuration form with the following elements:

- Choose SNMP Version \***: Two radio buttons are present. The first is labeled "SNMP v2" and is unselected. The second is labeled "SNMP v3" and is selected (indicated by a blue dot).
- SNMP v3 Username \***: A text input field below the radio buttons.
- SNMP v3 Authentication Password \***: A text input field below the username field, featuring a small eye icon on the right side to toggle password visibility.

- Step 2** Enter the correct information depending on your version of SNMP (you configured this in “Configure Cisco Unified CM SNMP” on page 8-4):

- **SNMP v2.** Enter the name of your community string in the **SNMP v2 Community Name** field.
- **SNMP v3.** Enter your SNMP v3 user's name in the **SNMP v3 Username** field, your authentication password in the **SNMP v3 Authentication Password** field, and your privacy password in the **SNMP v3 Privacy Password** field.

The SNMP v3 authentication and privacy passwords must contain at least eight characters and no more than 64.

### Set Secure CTI Configuration

Use the following steps to set your Cisco Unified CM cluster's secure CTI configuration.

- Step 1** Select the **Use Secure Connection** checkbox if you want to configure CTI over TLS for the communication between InformaCast and Cisco Unified CM (see “Manage CTI Security” on page 8-49 for more information). The Create Cisco Unified CM Cluster page refreshes with additional fields.

The screenshot shows a configuration form with the following elements:

- Choose SNMP Version \***: Radio buttons for **SNMP v2** and **SNMP v3** (selected).
- SNMP v3 Username \***: An empty text input field.
- SNMP v3 Authentication Password \***: A password input field with a toggle icon.
- SNMP v3 Privacy Password \***: A password input field with a toggle icon.
- Use Secure Connection**: A checked checkbox.
- Cisco Unified CM CAPF Address \***: An empty text input field.
- Cisco Unified CM CAPF Port \***: A text input field containing the value **3804**.
- Cisco Unified CM TFTP Address \***: An empty text input field.
- Cisco Unified CM TFTP Port \***: A text input field containing the value **69**.

- Step 2** Enter the IP address of the Cisco Unified CM you're using as a Certificate Authority Proxy Function server in the **Cisco Unified CM CAPF Address** field.
- Step 3** Enter the port number at which your Cisco Unified CM is listening for CAPF communication in the **Cisco Unified CM CAPF Port** field. The default is 3804.
- Step 4** Enter the IP address of the Cisco Unified CM you're using as a TFTP server in the **Cisco Unified CM TFTP Address** field.
- Step 5** Enter the port number at which your Cisco Unified CM is listening for TFTP traffic in the **Cisco Unified CM TFTP Port** field. The default is 69.



**Note** Saving this information ensures that communication between InformaCast and Cisco Unified CM is secure, but further configuration is necessary to ensure that communication between InformaCast and its Cisco IP phones is secure. See “Manage CTI Security” on page 8-49 for more information.

### Set JTAPI or HTTP Configuration

Use the following steps to set your Cisco Unified CM cluster's JTAPI or HTTP configuration.

- Step 1** Determine whether InformaCast will activate your IP phones over HTTP or through JTAPI:
- **HTTP.** If you leave the **Send Commands to Phones by JTAPI** checkbox unselected, InformaCast activates your IP phones over HTTP. Each time InformaCast sends a broadcast to a phone, it validates its communication through a digitally encrypted token that is valid for one minute before expiring. These tokens enhance the security of the HTTP communication between InformaCast and your IP phones by requiring that the InformaCast Appliance sending the activation request decrypts the payload and verifies that the token has not expired. If you leave the **Send Commands to Phones by JTAPI** checkbox unselected, you must have also enabled web access for your phones (see “Enable Web Access for Cisco IP Phones” on page 8-32).
  - **JTAPI.** If you select the **Send Commands to Phones by JTAPI** checkbox, InformaCast uses JTAPI to communicate with your Cisco Unified CM 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” on page 8-28).



---

**Note** If you are configuring InformaCast with CTI security, selecting the **Send Commands to Phones by JTAPI** checkbox is required.

---

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 accessible.

- Step 2** Select the **Create Telephony Terminals for all Phones** checkbox if you want to create CTI terminals for all phones in the cluster, which can improve phone activation times during broadcasts (optional). 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 any phones no longer in the cache will have their terminals destroyed.



---

**Note** If you disable the **Create Telephony Terminals for all Phones** or **Send Commands to Phones by JTAPI** checkbox after having saved this cluster with the checkboxes enabled, all CTI terminals will be destroyed.

---

**Note**

Cisco Unified CM limits a CTI application like InformaCast through its Maximum Devices Per Provider parameter. If your primary cluster contains more phones than allowed by this parameter 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 running the **show-log-performance** command in the CLI (see “Access the InformaCast Appliance’s Logs” on page 13-62).

### *Configure XML Push Authentication*

Enter the original value of Cisco Unified CM’s **URL Authentication** field in the **Next Authentication URL** field. You made note of this in “Set Your Authentication URL” on page 8-40.

### *Save and Optionally Set Cluster Security*

Use the following steps to save your Cisco Unified CM cluster and optionally set its cluster security.

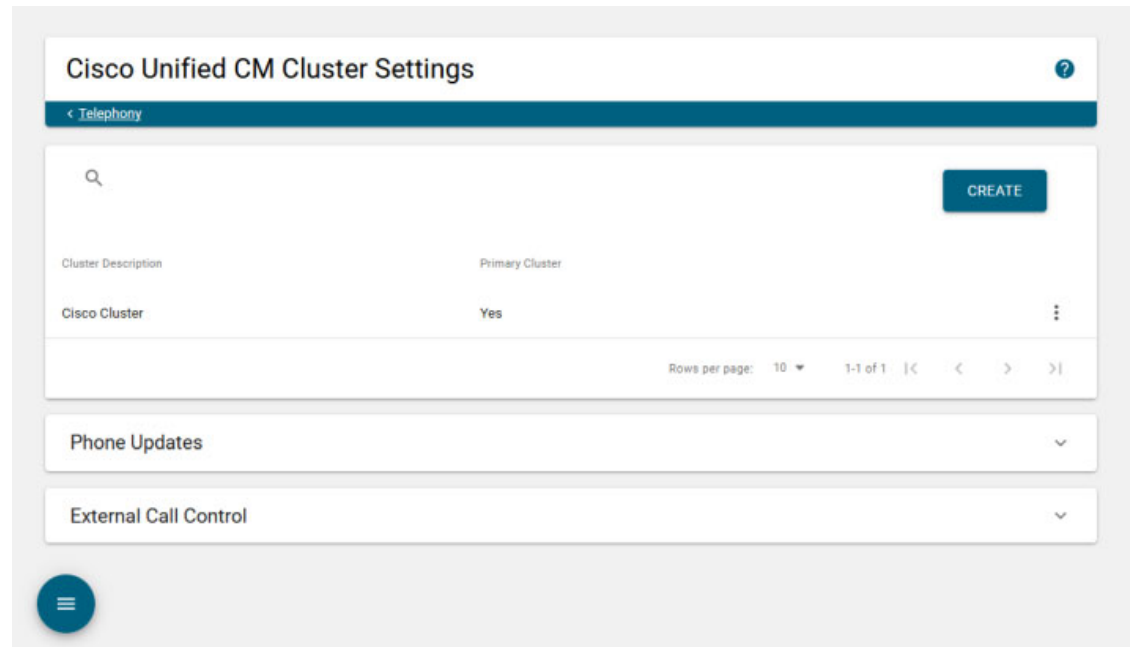
- Step 1** Click the **Save** button to save your changes.

**Note**

Saving your Cisco Unified CM cluster may require a restart of the InformaCast Appliance if InformaCast's installed version of JTAPI does not match the one provided by Cisco Unified CM, and you will have to log in again.

JTAPI updates (and InformaCast Appliance restarts) should not occur very often. Once JTAPI has been updated, it will remain in sync with Cisco Unified CM until Cisco Unified CM is upgraded.

Clicking the **Save** button redirects you to the Cisco Unified CM Cluster Settings page.



**Note**

If you disabled the automatic import of certificates in the *System Certificates* area on the Settings page (see “Configure Host Trust” on page 8-48 for more information), you must click the **Trust** checkbox for each certificate alias in the *Manage Cluster Security* area on the Edit Cisco Unified CM Cluster page to trust the cluster members' certificates detected by InformaCast. Continue with Step 2. If you left the automatic import of certificates enabled, skip to Step 1 on page 9-10.

The *Manage Cluster Security* area on the Edit Cisco Unified CM Cluster 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 Cisco Unified CM. Since you have disabled the automatic import of certificates, you will have to choose which of the certificates should be imported into InformaCast's trust store.

- Step 2** Verify that the SHA1 fingerprints displayed in the table match the SHA1 fingerprints of the actual certificates provided by the Cisco Unified CM cluster members and select the **Trust** checkbox for each match.



**Tip**

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 3** Click the **Save** button to save these certificates in InformaCast's trust store. By default, InformaCast stores its Cisco Unified CM certificates in `/usr/local/singlewire/InformaCast/certs/cucm.bcf`.

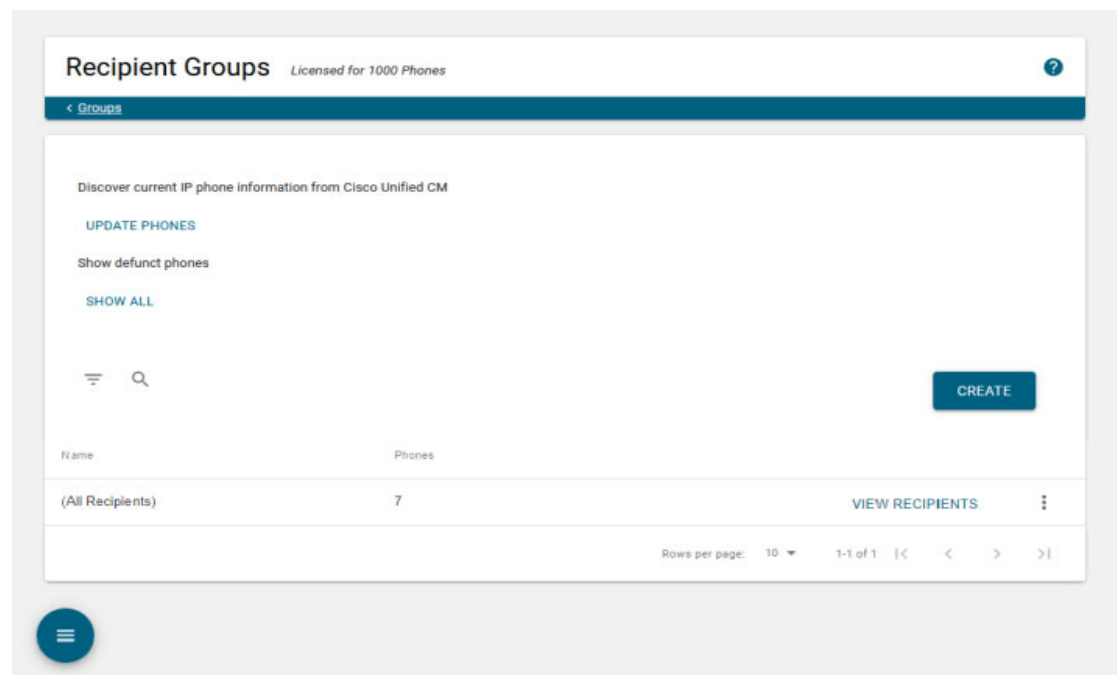


**Note** If your Cisco Unified CM cluster members change, you will need to return to the *Manage Cluster Security* area and mark the changed member as trusted.

### Update Recipients

Use the following steps to update your recipients now that you've set your Cisco Unified CM cluster's configuration.

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



**Step 2** Click the **Update Phones** button to refresh InformaCast's information pertaining to Cisco IP phones available for inclusion in recipient groups. This may take a few moments. InformaCast will update you with a success statement when it is finished.

Clicking the **Update Phones** button causes InformaCast to query Cisco Unified CM for a list of all known IP phones, which InformaCast then uses to build its phone cache, i.e. a list of registered IP phones. There is also a scheduled job that performs this work on a regular basis. By default, the job runs every hour, but you can configure it to suit your needs (see “Manage Phone Updates” on page 9-15).



## Update JTAPI

Use the following steps to ensure that you have the most up-to-date version of JTAPI.



### Note

Updating JTAPI is only necessary for the first Cisco Unified CM cluster you add (or if InformaCast's installed version of JTAPI does not match the one provided by Cisco Unified CM, as noted in “Save and Optionally Set Cluster Security” on page 9-8).

- 
- Step 1** Log into Webmin (see “Log into Webmin” on page 3-14). Webmin is administrative interface of InformaCast's server.
- Step 2** Restart the `singlewireInformaCast` service (see “Restart a Service on the InformaCast Appliance” on page 13-10). JTAPI automatically updates every time the `singlewireInformaCast` service is restarted.
- 

## Edit Your Default Cluster

Once you've added a Cisco Unified CM cluster, you may need to edit its information.

- Step 1** Go to **System Administration | Telephony | Cisco Unified CM Cluster**. The Cisco Unified CM Cluster Settings page appears.

**Step 2** Click the table row or **More** | **Edit** icon for your Cisco Unified CM cluster. The Edit Cisco Unified CM Cluster page appears.

### Edit Cisco Unified CM Cluster ?

< Telephony > Cisco Unified CM Cluster Settings

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

#### Telephony Configuration

Cisco Unified CM Cluster Description \*

Cisco Cluster

Cisco Unified CM Application User \*

\_jc

Cisco Unified CM Application Password \*

[password field]

Use Application User for AXL

AXL IP Address(es), comma-separated

[IP address field]

Cisco Unified CM Address(es), comma-separated \*

[IP address field]

Choose SNMP Version \*

SNMP v2

SNMP v3

SNMP v2 Community Name \*

[community name field]

Use Secure Connection

Send Commands to Phones by JTAPI

Create Telephony Terminals for All Phones

#### XML Push Authentication

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

http://[hostname]:8081/informaCast/phone/auth

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

Next Authentication URL

[URL field]

If empty, non-informaCast authentication requests from phones in this cluster will be sent to the default Cisco Unified CM authentication page, [http://\[hostname\]/ccmclp/authenticate.jsp](http://[hostname]/ccmclp/authenticate.jsp)

CANCEL SAVE

---

#### Manage Cluster Security

Trust	Certificate Alias	Certificate SHA1 (Hex)
<input checked="" type="checkbox"/>	[alias]	e8102558054d3c6e4dfb
<input checked="" type="checkbox"/>	[alias]	3aa4978453b7ba9bced2

SAVE

On the Edit Cisco Unified CM Cluster page, you can change the name of your cluster or the application user credentials attached to it, update the Cisco Unified CM IP addresses providing the CTI Manager service for your cluster, switch between using application user or AXL credentials, change the version of SNMP your cluster is using, ensure you have a secure connection between InformaCast and Cisco Unified CM (see “Manage CTI Security” on page 8-49), choose a different activation method for your cluster, e.g. JTAPI or HTTP, determine whether you will create CTI terminals for all phones in the primary cluster, and manage your cluster's security (see “Configure Host Trust” on page 8-48).

**Step 3** Make your desired changes.

Ensure your cluster's configuration matches that which you have set up in Cisco Unified CM.

**Step 4** Click the **Save** button.



**Note** Saving this Cisco Unified CM cluster may require a restart of the InformaCast Appliance if InformaCast's installed version of JTAPI does not match the one provided by Cisco Unified CM.

JTAPI updates (and InformaCast Appliance restarts) should not occur very often. Once JTAPI has been updated, it will remain in sync with Cisco Unified CM until Cisco Unified CM is upgraded.



**Note** If you disabled the automatic import of certificates in the *System Certificates* area on the Settings page (see “Configure Host Trust” on page 8-48), you must click the **Trust** checkbox for each certificate alias in the *Manage Cluster Security* area to trust the cluster members' certificates detected by InformaCast. Continue with Step 2. If you left the automatic import of certificates enabled, you are finished with the steps in this section.

The *Manage Cluster Security* area on the Edit Cisco Unified CM Cluster Settings 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 Cisco Unified CM. Since you have disabled the automatic import of certificates, you will have to choose which of the certificates should be imported into InformaCast's trust store.

**Step 5** Verify that the SHA1 fingerprints displayed in the table match the SHA1 fingerprints of the actual certificates provided by the Cisco Unified CM cluster members and select the **Trust** checkbox for each match.



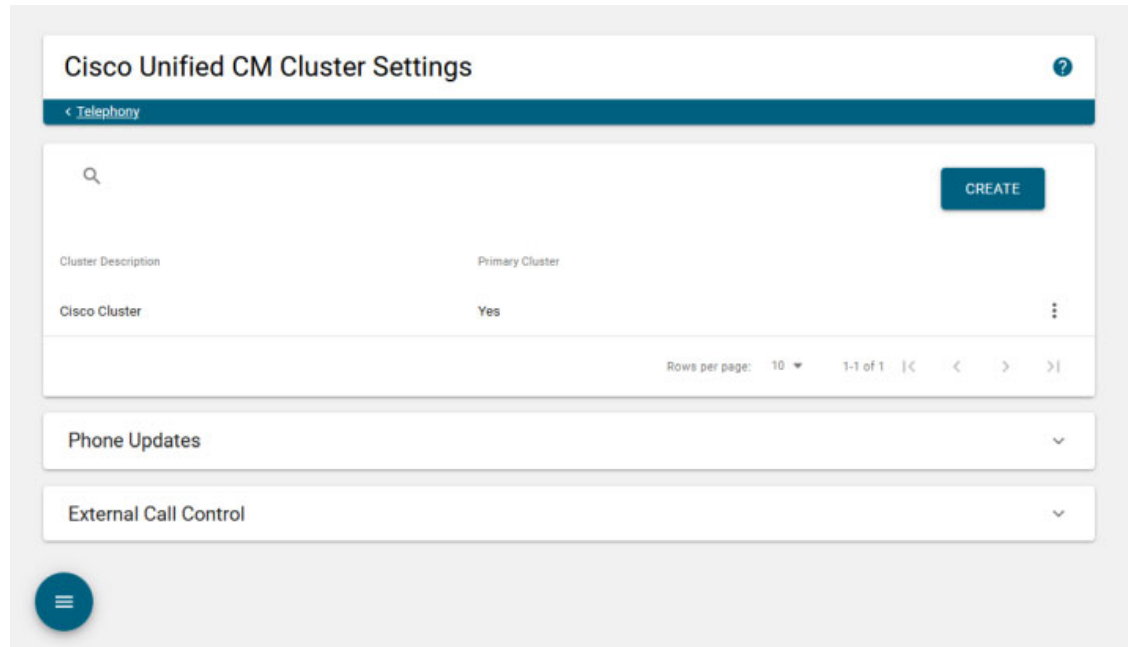
**Tip** Viewing certificate SHA1 fingerprints can be done through a browser and the steps for viewing them are browser dependent. For example, in Chrome, go to **Settings** | **More tools** | **Developer tools** | **Security** tab | **View certificate** button | **Details** tab.

**Step 6** Click the **Save** button to save these certificates in InformaCast's trust store.

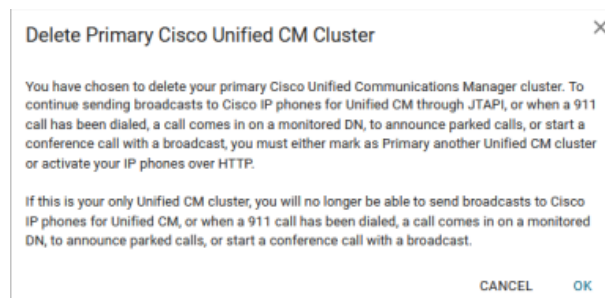
## Delete a Cisco Unified CM Cluster

As your needs change, you may want to remove Cisco Unified CM clusters from InformaCast.

- Step 1** Go to **System Administration | Telephony | Cisco Unified CM Cluster**. The Cisco Unified CM Cluster Settings page appears.



- Step 2** Click the **More | Delete** icon of the Cisco Unified CM cluster you want to delete. The Delete Primary Cisco Unified CM Cluster pop-up window appears.



**Note** If you delete your cluster, you will be unable to send broadcasts to Cisco IP phones.

- Step 3** Click the **OK** button. The cluster is deleted.  
You should update the recipients in your recipient groups.
- Step 4** Go to **Recipients | Groups | Recipient Groups**, and click the **Update Phones** button. This process may take some time.

## Manage Phone Updates

Configure the timing for two scheduled jobs that determine how and when InformaCast updates its information on Cisco IP phones for Unified CM.

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



### 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 build of registered phones.

Phone updates can be performed as frequently as once per minute or even disabled if desired.



### Note

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

**Step 1** Go to **System Administration | Telephony | Cisco Unified CM Cluster**. The Cisco Unified CM Cluster Settings page appears.

**Step 2** Expand the *Phone Updates* area, if it's not already visible.

### Phone Updates ^

**Build List of Registered Phones**

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

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

Hour (0-23)  Minute \*  Second \*

Month

Day

Week Day

**Refresh List of Registered Phones**

Configure the timing for how often InformaCast queries Cisco Unified CM for the changes to phones already in the list of registered phones. A refresh can be performed as frequently as once per minute.

Entering zero into this field indicates to InformaCast that no refresh should be performed.

Refresh Interval (minutes) \*

[SAVE PHONE UPDATE INFORMATION](#)

**Step 3** Enter numeric values in the **Hour**, **Minute**, and **Second** fields in the *Build a List of Registered Phones* area to specify the time of day you'd like InformaCast to build its list of registered phones.

**Step 4** Select **Every Month** or a specific month from the **Month** dropdown menu.

**Step 5** Enter a numeric value in the **Day** field if you'd like InformaCast to only rebuild its phone information on a specific day.

**Step 6** Select **Every Day** or a specific day from the **Week Day** dropdown menu.

**Step 7** Enter a numeric value in the **Refresh Interval (minutes)** field in the *Refresh List of Registered Phones* area. A positive numeric value enables updates. Zero or no value disables updates.

- Step 8** Click the **Save Phone Update Information** button. On the Overview page, you can see your changes reflected in the *Phone Updates* section.

JTAPI	
JTAPI Version:	Cisco Jtapi version 12.0(1.23900)-1 Release
Send Commands by JTAPI:	Yes
Create Telephony Terminals for All Phones:	Yes
Maximum Devices per Provider:	2000
Terminals Requested:	19
Terminals Created:	19
Phone Updates	
Last Attempted Rebuild:	2020-09-10 15:10:00
Last Successful Rebuild:	2020-09-10 15:11:02
Next Phone Rebuild:	2020-09-11 10:00:00
Last Attempted Refresh:	Never
Last Successful Refresh:	Never
Phones Retrieved:	19
Phones Used/Licensed:	0/1000
Refresh Interval (minutes):	60

## Manage Recipient Groups

Recipient groups allow you to organize your recipients into groups that will receive the broadcasts sent to them.

By default, InformaCast initially creates an “(All Recipients)” group, which contains all the recipients that it can discover. However, you may find it helpful to send to smaller groups of recipients.

There are three ways to group recipients:

- Select the recipients you want included as members, which is easiest for a small grouping of recipients
- Select multiple, existing recipient groups and combine them into one group, which is helpful when you have a large number of smaller recipient groups that will receive similar broadcasts
- Construct matching rules that specify the members of a group, which is useful when you have a large and/or changeable group of recipients

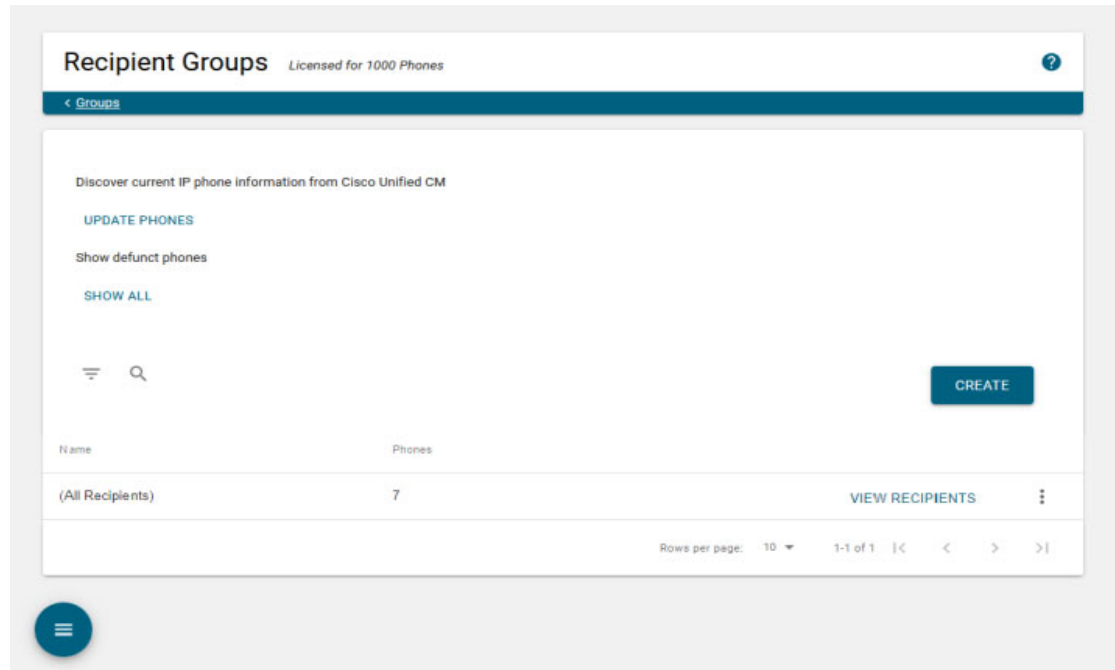
You can create groups that use one way, a combination of two, or all three ways.

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

## Create a Recipient Group

Use the following steps to create a recipient group.

- Step 1** Go to **Recipients | Groups | Recipient Groups**. The Recipient Groups page appears. This page shows the number of Cisco phones for Unified CM.





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

**Create Recipient Group**

< Groups < Recipient Groups

1 Details and Additions — 2 Add Rules Optional — 3 Select Exceptions Optional You must have filtered recipient groups or rules for exceptions — 4 Review Final Group

**General Details**

Name\*

Create as an exclusionary recipient group

Dial Code

Tags

**Select Individual Recipients**

Available Recipients

<input type="checkbox"/>	Cisco IP Phone: Auto 105021. DNs: 105021. 163668	<input type="button" value="🔍"/>
<input type="checkbox"/>	Cisco IP Phone: Auto 105054. DNs: 105054. D3D0E	<input type="button" value="🔍"/>
<input type="checkbox"/>	Cisco IP Phone: Auto 105122. DNs: 105122. 072FE6	<input type="button" value="🔍"/>
<input type="checkbox"/>	Cisco IP Phone: Auto 105141. DNs: 105141. 1C2AC	<input type="button" value="🔍"/>
<input type="checkbox"/>	Cisco IP Phone: Auto 105522. DNs: 105522. E63EE	<input type="button" value="🔍"/>
<input type="checkbox"/>	Cisco IP Phone: Auto 105537. DNs: 105537. 05AC5	<input type="button" value="🔍"/>
<input type="checkbox"/>	Cisco IP Phone: Auto 105543. DNs: 105543. B51E3	<input type="button" value="🔍"/>
<input type="checkbox"/>	Cisco IP Phone: Auto 105021. DNs: 105021. 163668	<input type="button" value="🔍"/>
<input type="checkbox"/>	Cisco IP Phone: Auto 105054. DNs: 105054. D3D0E	<input type="button" value="🔍"/>
<input type="checkbox"/>	Cisco IP Phone: Auto 105122. DNs: 105122. 072FE6	<input type="button" value="🔍"/>

Rows per page: 10 1-10 of 15 |< < > >|

**Filter with Recipient Groups**

Available Groups

(All Recipients)

Rows per page: 10 1-1 of 1 |< < > >|

The Create Recipient Group page will walk you through stages of configuring your recipient group.

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

**Step 4** Select a recipient group tag from the **Tags** dropdown menu (optional).

Recipient group tags allow you finer control over the display results for recipient groups throughout InformaCast's recipient-specific features.

**Step 5** Select checkboxes for individual recipients in the *Select Individual Recipients* area (optional).



**Tip**

Use the **Search** field to search for specific recipients. Click a recipient's **Info** icon to view its details.

Device Details
✕

---

**Device**  
Cisco IP Phone: Auto 105021; DN: 105021, 163668

**ID**  
CiscoPhone-55: 163668

**Description**  
Auto 105021

**Reported IPv4 Address**  
[Redacted]

**Unified Communications Manager Device Type**  
30018

**IC 4 style RegEx target**  
name=163668 desc=Auto 105021 css=informacast pool=Default  
addr=[Redacted] type=30018

**Unified Communications Manager Cluster Description**  
Default configuration

**Authentication URL**  
http://127.0.0.1:8081/InformaCast/phone/auth

**Unified Communications Manager Cluster Remote Description**  
qa-ucm115

**Name**  
163668

**Partition Names**  
[InformaCast]

**Can Display Text**  
true

**InformaCast Device Type**  
CiscoIPPhone

**Unified Communications Manager Device Pool**  
Default

**End User Identifier**

**Directory Numbers**  
[105021]

**IP Address**  
[Redacted]

**Unified Communications Manager Calling Search Space**  
informacast

**Location**  
Hub\_None

OK

- Step 6** Select checkboxes for existing recipient groups in the *Filter with Recipient Groups* area (optional).
- Step 7** Click the **Add Rules** button. The Create Recipient Groups page refreshes and you can see the *Filter with Rules* area.

The screenshot shows the 'Create Recipient Group' page. At the top, there is a breadcrumb trail: < Groups < Recipient Groups. Below this is a progress indicator with four steps: 1. Details and Additions, 2. Add Rules (Optional), 3. Select Exceptions (You must have filtered recipient groups or rules for exceptions) (Optional), and 4. Review Final Group. The main content area is titled 'Filter with Rules'. It features a 'Logic Type' dropdown menu set to 'ALL' and the text 'All of the following rules are true.' Below this is a 'Logical Expression' input field with the placeholder text 'e.g. 1 AND (2 OR 3)'. An 'ADD CONDITION' button is located at the bottom right of the 'Filter with Rules' section. At the bottom of the page, there is a navigation bar with a hamburger menu icon, a 'CANCEL' button, a 'PREVIOUS' button, and a 'REVIEW FINAL GROUP' button.

- Step 8** Add rules to your group (optional).  
If you don't want to add rules but you do want to add exceptions (and you added existing recipient groups through the *Filter with Recipient Groups* area), skip to Step 17 on page 9-25.  
If you don't want to add rules or exceptions, skip to Step 19 on page 9-26.
- Step 9** Select the manner in which rules will be applied to your recipient group from the **Logic Type** dropdown menu, e.g. **Any**, **All**, or **Logical Expression**.

**Any** will include recipients that match at least one of the rules you add. **All** will include recipients that match each rule you add. **Logical Expression** allows you to craft a regular expression where, to be included, your recipients must match a combination of rules based on their order in the table and the words “AND” and “OR.”

If you select **Logical Expression**, the **Logical Expression** field becomes accessible and you can create your regular expression, e.g. (1 or 2) and not (3 and 4 and not 5). **AND** means that your recipients have to match every rule you specify. **OR** means that your recipients must match at least one specified rule. See “Configure Advanced Matching for Recipient Groups” on page 9-48 for a discussion of regular expressions.

- Step 10** Click the **Add Condition** button. The *Filter with Rules* area refreshes with dropdown menus and fields for your new rule.

The screenshot shows the 'Create Recipient Group' interface. At the top, there is a breadcrumb trail: < Groups < Recipient Groups. Below this is a progress indicator with four steps: 1. Details and Additions, 2. Add Rules (Optional), 3. Select Exceptions (Optional), and 4. Review Final Group (Optional). Step 2 is currently active.

The main section is titled 'Filter with Rules'. It contains a 'Logic Type' dropdown menu set to 'ALL', with the text 'All of the following rules are true.' next to it. Below this is a 'Logical Expression' text input field containing the example 'e.g. 1 AND (2 OR 3)'. Underneath, there is a row of controls: the word 'AND', a dropdown menu for 'InformaCast Device Type', a dropdown menu for 'Does', a dropdown menu for 'Contain', an empty text input field, a dropdown menu for 'Ignor...', and a trash icon. A blue 'ADD CONDITION' button is located at the bottom right of this section.

At the bottom of the interface, there is a navigation bar with a hamburger menu icon on the left, and three buttons on the right: 'CANCEL', 'PREVIOUS', and 'SELECT EXCEPTIONS'.

**Step 11** Select a parameter from the first dropdown menu. The following table details the parameters available to you.

Matching Parameter	Description
Authentication URL	Cisco IP phones for Unified CM that match (or don't match) the specified authentication URL.
Cisco Unified CM Calling Search Space	Cisco IP phones for Unified CM that match (or don't match) the specified search space. <sup>a</sup>
Cisco Unified CM Cluster Description	Cisco IP phones for Unified CM that match (or don't match) the specified Cisco Unified CM cluster description.
Cisco Unified CM Device Pool	Cisco IP phones for Unified CM that match (or don't match) the specified device pool.
Cisco Unified CM Device Type	Cisco IP phones for Unified CM that match (or don't match) the specified model, as reported by Cisco Unified CM.
Cisco Unified CM Remote Description	Cisco IP phones for Unified CM that match (or don't match) the specified cluster ID from Cisco Unified CM's Enterprise Parameters page.
Can Display Text	Cisco IP phones for Unified CM that match (or don't match) in their ability to display text. <sup>b</sup>
Description	<p>Cisco IP phones for Unified CM that match (or don't match) the supplied description value. This is often a useful grouping tool because you have control over the description of the recipients in your system, so you can set up your descriptions in ways that facilitate grouping.</p> <p>The text you enter will be compared against the Device Description entries of phones registered with your Cisco Unified CM. Any recipients whose descriptions match with the rule you've specified will be considered part of the recipient group.</p>
Directory Numbers	Cisco IP phones for Unified CM that match (or don't match) the supplied phone number(s) assigned to them in Cisco Unified CM. <sup>b</sup>
IC 4 style RegEx target	Cisco IP phones for Unified CM that match (or don't match) the supplied string of device details, e.g. name=EXAMPLE_NAME desc=EXAMPLE_DESCRIPTION css=EXAMPLE_CSS pool=EXAMPLE_POOL.
IP Address	Cisco IP phones for Unified CM that match (or don't match) the supplied subnet boundaries. When choosing this parameter, you are given a new Comparison Type choice, <b>Belong to Subnet</b> , which allows you to enter a subnet mask like 172.17.30.0/8. See "Configure Advanced Matching for Recipient Groups" on page 9-48 for more information about this approach.
InformaCast Device Type	Cisco IP phones for Unified CM that match (or don't match) in their functionality as an IP phone.
Location	Cisco IP phones for Unified CM that match (or don't match) the supplied location value.

Matching Parameter	Description
MAC Address	Cisco IP phones for Unified CM that match (or don't match) the supplied network hardware address of the IP phone, which is guaranteed to be unique across your network.
Name	Cisco IP phones for Unified CM that match (or don't match) the supplied name. Like the <b>Description</b> parameter, you have control over names, so they may be useful for grouping, but should be concise.
Partition Names	Cisco IP phones for Unified CM 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 Cisco Unified CM.
Profile Description	Cisco IP phones for Unified CM that match (or don't match) the Cisco Unified CM'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 **Cisco Unified CM 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 IP phone must be currently registered for this parameter to match. InformaCast has no information about the detailed features of unregistered IP phones.

By default, **InformaCast Device Type** is selected in this dropdown menu.

**Step 12** Select **Does** or **Does Not** from the second dropdown menu.

**Step 13** Select the matching constraint from the third dropdown menu, which has parameter-specific choices. For example, if you select **IP Address** as the rule parameter to match, a choice of **Belong to Host Bitmask** 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.

**Step 14** Enter the criteria to be matched in the last field.



**Note** If you selected the **Equal** relationship, the criteria element may facilitate your selection by changing from a field to a dropdown menu.

**Step 15** Select **Ignore Case** or **Case Sensitive** from the last dropdown menu to further refine your recipients.

**Step 16** Decide if your rule is sufficient as it stands or follow Steps 10 through 15 to add another rule.



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

Depending on whether you added existing recipient groups and/or rules, you will see different buttons:

- **Existing Recipient Groups/Rules.** The **Select Exceptions** button appears and you can select recipients that had been included in your recipient group by a certain rule or through an existing recipient group to now be excluded. Continue with Step 17.
- **Individual Recipients.** The **Review Final Group** button appears and you can view the recipients included in your recipient group. Skip to Step 19.

**Step 17** Click the **Select Exceptions** button. The Create Recipient Groups page refreshes and you can see the *Select Recipient Exceptions* area.

**Create Recipient Group** ?

< Groups < Recipient Groups

1 Details and Additions — 2 Add Rules Optional — 3 **Select Exceptions** You must have filtered recipient groups or rules for exceptions Optional — 4 Review Final Group Optional

Select Recipient Exceptions

Available Recipients

<input type="checkbox"/>	Cisco IP Phone: Auto 105021; DN: 105021; 163668	i
<input type="checkbox"/>	Cisco IP Phone: Auto 105141; DN: 105141; 71C2AC	i
<input type="checkbox"/>	Cisco IP Phone: Auto 105522; DN: 105522; 43E63EE	i
<input type="checkbox"/>	Cisco IP Phone: Auto 105537; DN: 105537; F05AC5	i
<input type="checkbox"/>	Cisco IP Phone: Auto 105543; DN: 105543; FB51E3	i
<input type="checkbox"/>	Cisco IP Phone: Auto 105553; DN: 105553; FA3EA6	i
<input type="checkbox"/>	Cisco IP Phone: phone 105201 [alde.parker, ljw]; DN: 105201; 2AECA3	i

Rows per page: 10 1-8 of 8 |< < > >|

☰ CANCEL PREVIOUS REVIEW FINAL GROUP

The recipients displayed in the *Select Recipient Exceptions* area are the ones included by either your existing recipient group selection(s) or your rule configuration(s).

**Step 18** Select checkboxes for the recipients you don't want to include in your recipient group.

**Step 19** Click the **Review Final Group** button. The Create Recipient Groups page refreshes and you can see the *Review Included Devices* area.

**Create Recipient Group**

< Groups < Recipient Groups

1 Details and Additions — 2 Add Rules Optional — 3 Select Exceptions Optional You must have filtered recipient groups or rules for exceptions — 4 Review Final Group Optional

Review Included Devices

Available Recipients

Cisco IP Phone: Auto 105522; DNs: 105522; [redacted] E63EE	(i)
Cisco IP Phone: Auto 105537; DNs: 105537; [redacted] F05AC5	(i)
Cisco IP Phone: Auto 105543; DNs: 105543; [redacted] B51E3	(i)
Cisco IP Phone: Auto 105553; DNs: 105553; [redacted] A3EA6	(i)
Cisco IP Phone: phone 105201 [aide.parker, ljw]; DNs: 105201; [redacted] AECA3	(i)

Rows per page: 10 1-6 of 6 |< < > >|

CANCEL PREVIOUS SAVE

**Step 20** Verify that the recipients included in your recipient group are the ones you expect to see.

**Step 21** Click the **Save** button. Your recipient group is added to InformaCast.



## 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 | Groups | Recipient Groups**. The Recipient Groups page appears.

Recipient Groups Licensed for 50 Phones

< Groups

Discover current IP phone information from Cisco Unified CM

UPDATE PHONES

Show defunct phones

SHOW ALL

CREATE

Name	Phones	
(All Recipients)	14	VIEW RECIPIENTS
Managers	3	VIEW RECIPIENTS

Rows per page: 10 1-3 of 3

**Step 2** Click the **View Recipients** button of the recipient group for which you want to view recipients. The Edit Recipient Group page appears and you can see your included recipients in the *Review Included Devices* area.

The screenshot shows the 'Edit Recipient Group' page. At the top, there is a breadcrumb trail: < Groups < Recipient Groups. Below this is a progress indicator with four steps: 1. Details and Additions, 2. Add Rules (Optional), 3. Select Exceptions (You must have filtered recipient groups or rules for exceptions), and 4. Review Final Group (Optional). The 'Review Final Group' step is currently active. The main content area is titled 'Review Included Devices' and contains a search bar. Below the search bar, there is a section for 'Available Recipients' which lists five entries, each with a details icon (i):

Recipient Information	Action
Cisco IP Phone: Auto 105522; DN: 105522; [redacted] E63EE	(i)
Cisco IP Phone: Auto 105537; DN: 105537; [redacted] F05AC5	(i)
Cisco IP Phone: Auto 105543; DN: 105543; [redacted] B51E3	(i)
Cisco IP Phone: Auto 105553; DN: 105553; [redacted] A3EA6	(i)
Cisco IP Phone: phone 105201 [aide.parker, ljw]; DN: 105201; [redacted] AECA3	(i)

At the bottom of the list, there is a pagination control showing 'Rows per page: 10' and '1-6 of 6'. The bottom of the page features a hamburger menu icon on the left and three buttons: 'CANCEL', 'PREVIOUS', and 'SAVE'.

**Step 3** Click a recipient's **Info** icon to view its details. The Device Details pop-up window appears.



**Step 4** Click the **OK** button in the Device Details pop-up window to close it.

**Step 5** Use the steps in the following topics to change your recipient group:

- “Edit a Recipient Group” on page 9-31
- “Copy a Recipient Group” on page 9-37
- “Remove Defunct Phones from Recipient Groups” on page 9-42

- “Delete a Recipient Group” on page 9-43

## Find a Phone's Recipient Groups

The Find a Phone's Recipient Groups page allows you to enter the complete DN or IP address of a Cisco IP phone for Unified CM and display the recipient groups of which it is a member. Easily determining a Cisco IP phone's recipient groups can be useful when:

- Discovering why a Cisco IP phone is getting a certain broadcast
- Determining whether removing/moving a Cisco IP phone will affect people's ability to receive broadcasts
- Troubleshooting why a Cisco IP phone didn't get a broadcast

**Step 1** Go to **Recipients | Groups | Recipient Groups with Phone**. The Find a Phone's Recipient Groups page appears.

Name	Dial Code	Phones	Other Recipients	Speakers
No Data				

**Step 2** Select an attribute of a Cisco IP phone for Unified CM on which to search from the **Phone Attribute** dropdown menu, e.g. **DN** or **IP Address**.

**Step 3** Enter the complete DN or IP address of a Cisco IP phone for Unified CM in the **Value** field.

- Step 4** Click the **Show** button. The Find a Phone's Recipient Groups page refreshes with the recipient groups of which your Cisco IP phone is a member.

Find a Phone's Recipient Groups

< Groups

Enter a phone's DN or IP address and display the recipient groups of which it is a member.

Phone Attribute: DN Value: 01 SHOW CLEAR

Name	Dial Code	Phones	Other Recipients	Speakers
(All Recipients)	*	24	1	1
Security Staff		4	0	0
Executive Management		2	0	0



**Tip** Click the **Clear** button to clear the dropdown menu, field, and table of their contents.

### 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 Phones** button on the Recipient Groups page.

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

Recipient Groups *Licensed for 50 Phones*

< Groups

Discover current IP phone information from Cisco Unified CM

UPDATE PHONES

Show defunct phones

SHOW ALL

CREATE

Name	Phones	
(All Recipients)	14	VIEW RECIPIENTS
Managers	3	VIEW RECIPIENTS

Rows per page: 10 1-3 of 3

**Step 2** Click the table row or **More | Edit** icon next to the recipient group you'd like to edit. The Edit Recipient Group page appears.

**Edit Recipient Group**

< Groups < Recipient\_Groups

1 Details and Additions — 2 Add Rules (Optional) — 3 Select Exceptions (Optional) — 4 Review Final Group

*You must have filtered recipient groups or rules for exceptions*

### General Details

Name\*  
Managers

Create as an exclusionary recipient group

Dial Code

Tags

### Select Individual Recipients

Available Recipients

<input type="checkbox"/>	Cisco IP Phone: Auto 105021, DNs: 105021, 163668	
<input type="checkbox"/>	Cisco IP Phone: Auto 105054, DNs: 105054, D3D0E	
<input type="checkbox"/>	Cisco IP Phone: Auto 105122, DNs: 105122, 072FE6	
<input type="checkbox"/>	Cisco IP Phone: Auto 105141, DNs: 105141, 1C2AC	
<input type="checkbox"/>	Cisco IP Phone: Auto 105522, DNs: 105522, E63EE	
<input type="checkbox"/>	Cisco IP Phone: Auto 105537, DNs: 105537, 05AC5	
<input type="checkbox"/>	Cisco IP Phone: Auto 105543, DNs: 105543, B51E3	
<input type="checkbox"/>	Cisco IP Phone: Auto 105021, DNs: 105021, 163668	
<input type="checkbox"/>	Cisco IP Phone: Auto 105054, DNs: 105054, D3D0E	
<input type="checkbox"/>	Cisco IP Phone: Auto 105122, DNs: 105122, 072FE6	

Rows per page: 10 1-10 of 15

### Filter with Recipient Groups

Available Groups

(All Recipients)

Rows per page: 10 1-1 of 1

CANCEL ADD RULES

The Edit Recipient Group page will walk you through stages of configuring your recipient group. Immediately, you can select new individual recipients, remove old ones or add/remove existing recipient groups to/from the recipient group you're editing.

Clicking the **Add Rules** button advances the Edit Recipient Group page, and you can add new rules and modify or delete existing ones.

The screenshot displays the 'Edit Recipient Group' interface. At the top, there is a breadcrumb trail: < Groups < Recipient Groups. Below this is a progress indicator with four steps: 1. Details and Additions, 2. Add Rules (Optional), 3. Select Exceptions (You must have filtered recipient groups or rules for exceptions), and 4. Review Final Group (Optional). Step 2 is currently active.

The main section is titled 'Filter with Rules'. It includes a 'Logic Type' dropdown menu set to 'Logical...'. Below it is a 'Logical Expression' text input field containing '1 OR 2'. There are two rule conditions listed:

- Condition 1: InformaCast Device Type (dropdown) Does (dropdown) Equal (dropdown) Cisco IP Phone (dropdown) Ignor... (dropdown) with a delete icon.
- Condition 2: Can Record (dropdown) Does (dropdown) Equal (dropdown) Yes (dropdown) Ignor... (dropdown) with a delete icon.

An 'ADD CONDITION' button is located at the bottom right of the rule list. At the bottom of the page, there is a navigation bar with a hamburger menu icon on the left, and three buttons: 'CANCEL', 'PREVIOUS', and 'SELECT EXCEPTIONS'.



If your recipient group either uses rules and/or has added existing recipient groups, clicking the **Select Exceptions** button allows you to exclude recipients that had been added to your group through rule or existing group additions. Clicking the **Review Final Group** button will advance the Edit Recipient Group page again.

**Edit Recipient Group**

< Groups < Recipient Groups

1 Details and Additions — 2 Add Rules Optional — 3 **Select Exceptions** You must have filtered recipient groups or rules for exceptions — 4 Review Final Group Optional

Select Recipient Exceptions

Available Recipients

<input type="checkbox"/>	Cisco IP Phone: Auto 105021; DN: 105021; 163668	(i)
<input type="checkbox"/>	Cisco IP Phone: Auto 105141; DN: 105141; 71C2AC	(i)
<input type="checkbox"/>	Cisco IP Phone: Auto 105522; DN: 105522; 43E63EE	(i)
<input type="checkbox"/>	Cisco IP Phone: Auto 105537; DN: 105537; F05AC5	(i)
<input type="checkbox"/>	Cisco IP Phone: Auto 105543; DN: 105543; FB51E3	(i)
<input type="checkbox"/>	Cisco IP Phone: Auto 105553; DN: 105553; FA3EA6	(i)
<input type="checkbox"/>	Cisco IP Phone: phone 105201 [aide.parker, ljw]; DN: 105201; 2AECA3	(i)

Rows per page: 10 1-8 of 8 |< < > >|

CANCEL PREVIOUS **REVIEW FINAL GROUP**

If your recipient group doesn't use rules or existing recipient groups, clicking the **Review Final Group** button will advance the Edit Recipient Group page again.

This last area of the Edit Recipient Group page allows you to view the recipients included in your recipient group.

**Edit Recipient Group** ?

< Groups < Recipient Groups

1 Details and Additions — 2 Add Rules Optional — 3 Select Exceptions You must have filtered recipient groups or rules for exceptions Optional — 4 Review Final Group Optional

**Review Included Devices**

Q

Available Recipients

Cisco IP Phone: Auto 105522; DNs: 105522; [redacted] E63EE	(i)
Cisco IP Phone: Auto 105537; DNs: 105537; [redacted] F05AC5	(i)
Cisco IP Phone: Auto 105543; DNs: 105543; [redacted] B51E3	(i)
Cisco IP Phone: Auto 105553; DNs: 105553; [redacted] A3EA6	(i)
Cisco IP Phone: phone 105201 [aide.parker, ljw]; DNs: 105201; [redacted] AECA3	(i)

Rows per page: 10 ▾ 1-6 of 6 |< < > >|

CANCEL PREVIOUS **SAVE**

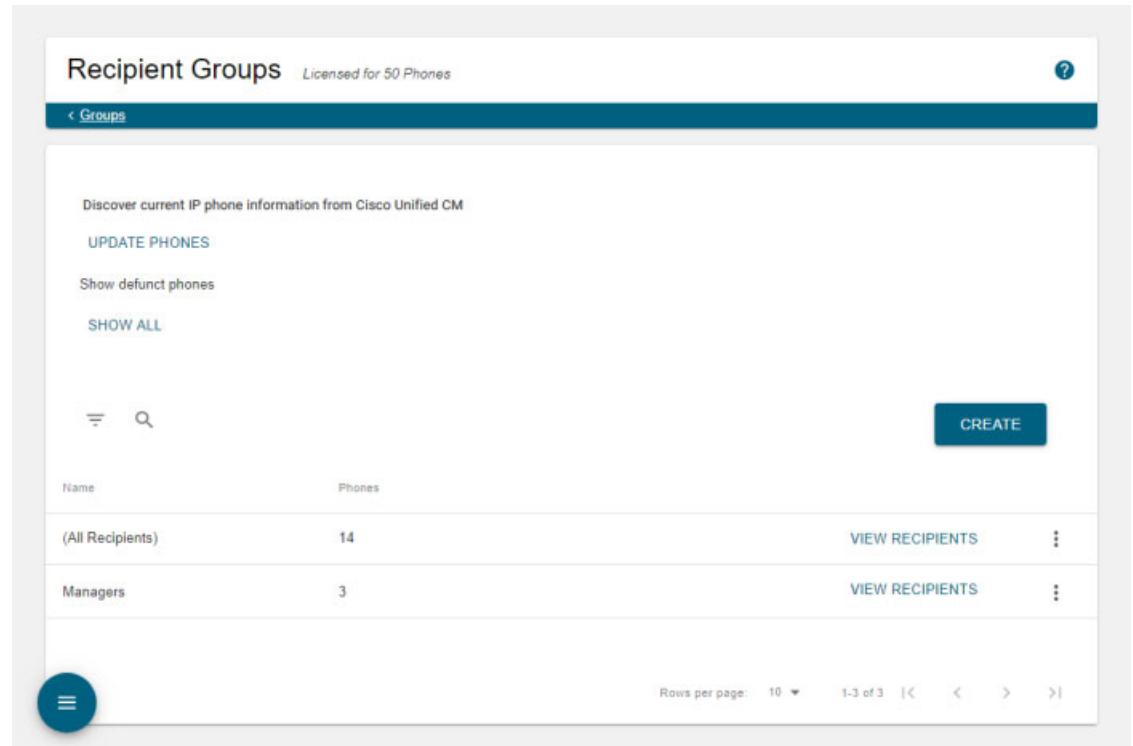
**Step 3** Make your desired changes.

**Step 4** Click the **Save** button. Your recipient group is saved.

## 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 group and make small changes from there.

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



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

**Copy Recipient Group**

< Groups < Recipient\_Groups

1 Details and Additions — 2 Add Rules (Optional) — 3 Select Exceptions (Optional) You must have filtered recipient groups or rules for exceptions — 4 Review Final Group

**General Details**

Name\*  
Managers (Copy)

Create as an exclusionary recipient group

Dial Code

Tags

**Select Individual Recipients**

Available Recipients

<input type="checkbox"/>	Cisco IP Phone: Auto 105021. DNs: 105021. 163668	i
<input type="checkbox"/>	Cisco IP Phone: Auto 105054. DNs: 105054. D3D0E	i
<input type="checkbox"/>	Cisco IP Phone: Auto 105122. DNs: 105122. 072FE6	i
<input type="checkbox"/>	Cisco IP Phone: Auto 105141. DNs: 105141. 1C2AC	i
<input type="checkbox"/>	Cisco IP Phone: Auto 105522. DNs: 105522. E63EE	i
<input type="checkbox"/>	Cisco IP Phone: Auto 105537. DNs: 105537. 05AC5	i
<input type="checkbox"/>	Cisco IP Phone: Auto 105543. DNs: 105543. B51E3	i
<input type="checkbox"/>	Cisco IP Phone: Auto 105021. DNs: 105021. 163668	i
<input type="checkbox"/>	Cisco IP Phone: Auto 105054. DNs: 105054. D3D0E	i
<input type="checkbox"/>	Cisco IP Phone: Auto 105122. DNs: 105122. 072FE6	i

Rows per page: 10 1-10 of 15 |< < > >|

**Filter with Recipient Groups**

Available Groups

(All Recipients)

Rows per page: 10 1-1 of 1 |< < > >|

CANCEL ADD RULES



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

The Copy Recipient Group page will walk you through stages of configuring your recipient group. Immediately, you can select new individual recipients, remove old ones or add/remove existing recipient groups to/from the recipient group you're editing.

Clicking the **Add Rules** button advances the Copy Recipient Group page, and you can add new rules and modify or delete existing ones.

**Copy Recipient Group** ?

< Groups < Recipient Groups

1 Details and Additions — 2 **Add Rules** Optional — 3 Select Exceptions Optional You must have filtered recipient groups or rules for exceptions — 4 Review Final Group

**Filter with Rules**

Logic Type  
Logical...

Logical Expression  
1 OR 2

1	InformaCast Device Type	Does	Equal	Cisco IP Phone	Ignor...	
2	Can Record	Does	Equal	Yes	Ignor...	

**ADD CONDITION**

☰
CANCEL
PREVIOUS
**SELECT EXCEPTIONS**

If your recipient group either uses rules and/or has added existing recipient groups, clicking the **Select Exceptions** button allows you to exclude recipients that had been added to your group through rule or existing group additions. Clicking the **Review Final Group** button will advance the Copy Recipient Group page again.

**Copy Recipient Group**

< Groups < Recipient Groups

1 Details and Additions — 2 Add Rules Optional — 3 Select Exceptions You must have filtered recipient groups or rules for exceptions — 4 Review Final Group Optional

Select Recipient Exceptions

Available Recipients

<input type="checkbox"/>	Cisco IP Phone: Auto 105021; DN: 105021; 163668	(i)
<input type="checkbox"/>	Cisco IP Phone: Auto 105141; DN: 105141; 71C2AC	(i)
<input type="checkbox"/>	Cisco IP Phone: Auto 105522; DN: 105522; 43E63EE	(i)
<input type="checkbox"/>	Cisco IP Phone: Auto 105537; DN: 105537; F05AC5	(i)
<input type="checkbox"/>	Cisco IP Phone: Auto 105543; DN: 105543; FB51E3	(i)
<input type="checkbox"/>	Cisco IP Phone: Auto 105553; DN: 105553; FA3EA6	(i)
<input type="checkbox"/>	Cisco IP Phone: phone 105201 [aide.parker, ljw]; DN: 105201; 2AECA3	(i)

Rows per page: 10 1-8 of 8 |< < > >|

CANCEL PREVIOUS REVIEW FINAL GROUP

If your recipient group doesn't use rules or existing recipient groups, clicking the **Review Final Group** button will advance the Copy Recipient Group page again.

This last area of the Copy Recipient Group page allows you to view the recipients included in your recipient group.

**Copy Recipient Group** ?

< Groups < Recipient Groups

1 Details and Additions — 2 Add Rules Optional — 3 Select Exceptions Optional You must have filtered recipient groups or rules for exceptions — 4 Review Final Group Optional

Review Included Devices

Q

Available Recipients

Cisco IP Phone: Auto 105522; DNs: 105522; [redacted] E63EE	(i)
Cisco IP Phone: Auto 105537; DNs: 105537; [redacted] F05AC5	(i)
Cisco IP Phone: Auto 105543; DNs: 105543; [redacted] B51E3	(i)
Cisco IP Phone: Auto 105553; DNs: 105553; [redacted] A3EA6	(i)
Cisco IP Phone: phone 105201 [aide.parker, ljw]; DNs: 105201; [redacted] AECA3	(i)

Rows per page: 10 1-6 of 6 |< < > >|

☰ CANCEL PREVIOUS SAVE

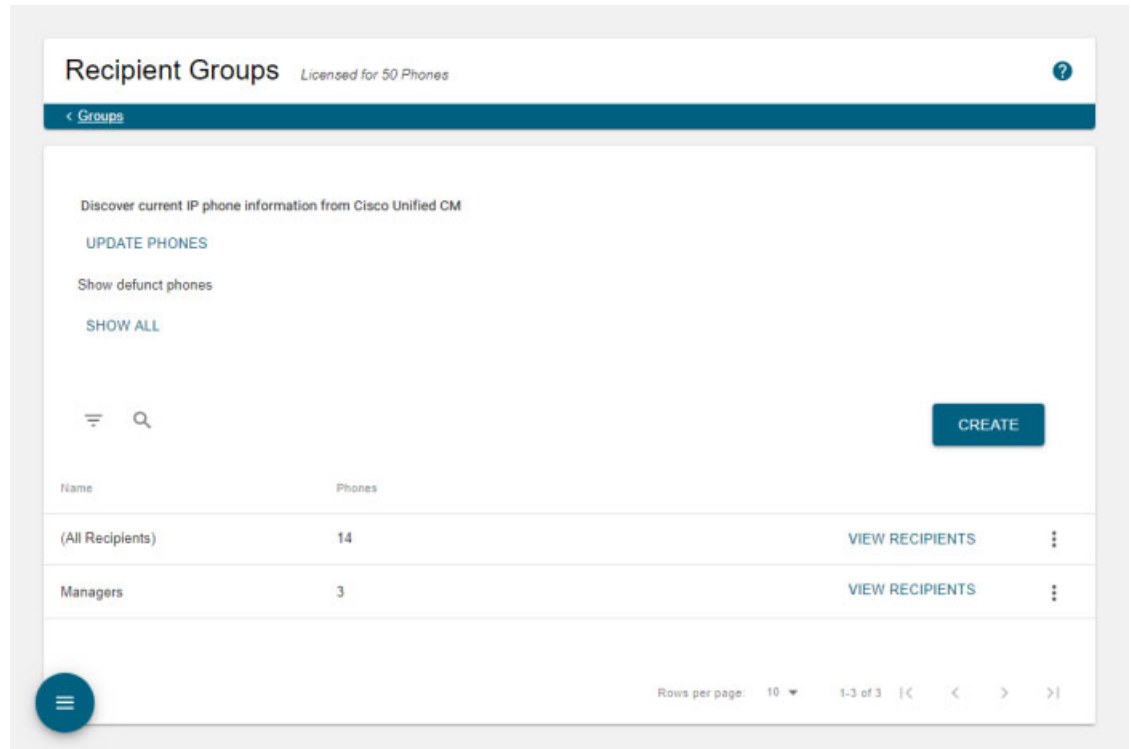
**Step 3** Make your desired changes.

**Step 4** Click the **Save** button. Your recipient group is saved.

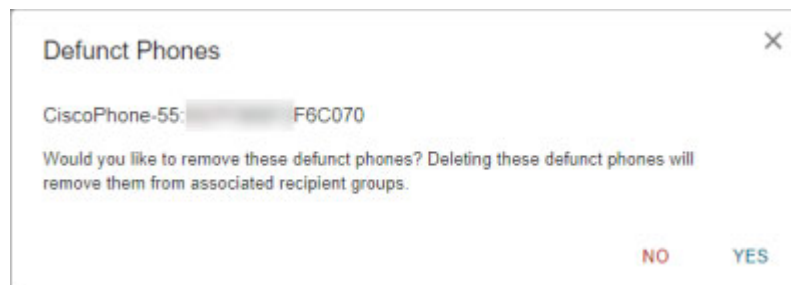
## Remove Defunct Phones from Recipient Groups

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

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



**Step 2** Click the **Show All** button under Show defunct phones. The Defunct Phones pop-up window appears with a listing of your defunct Cisco IP phones for Unified CM.



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





**Note** Recipient groups' rules will not recognize defunct Cisco IP phones as viable recipients for inclusion, nor will the (All Recipients) recipient group.

## Delete a Recipient Group

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

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

**Step 2** Click the **More | Delete** icon of the recipient group you'd like to delete. The Delete Recipient Group pop-up window appears.

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

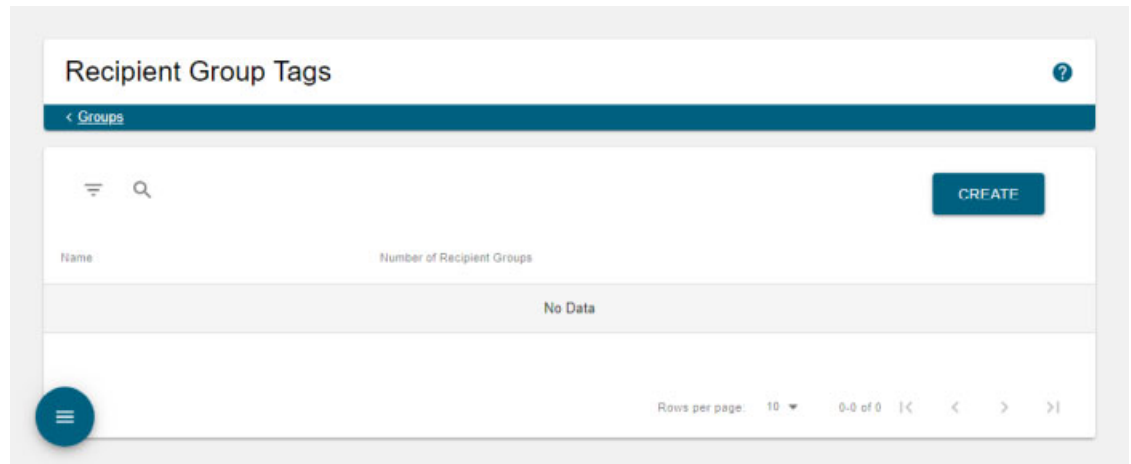
## Configure Recipient Group Tags

Recipient group tags allow you finer control over the display results for recipient groups throughout InformaCast's recipient-specific features. For example, enter a tag's name in the **Recipient Groups** dropdown menu of a dialing configuration to only see the recipient groups assigned that tag.

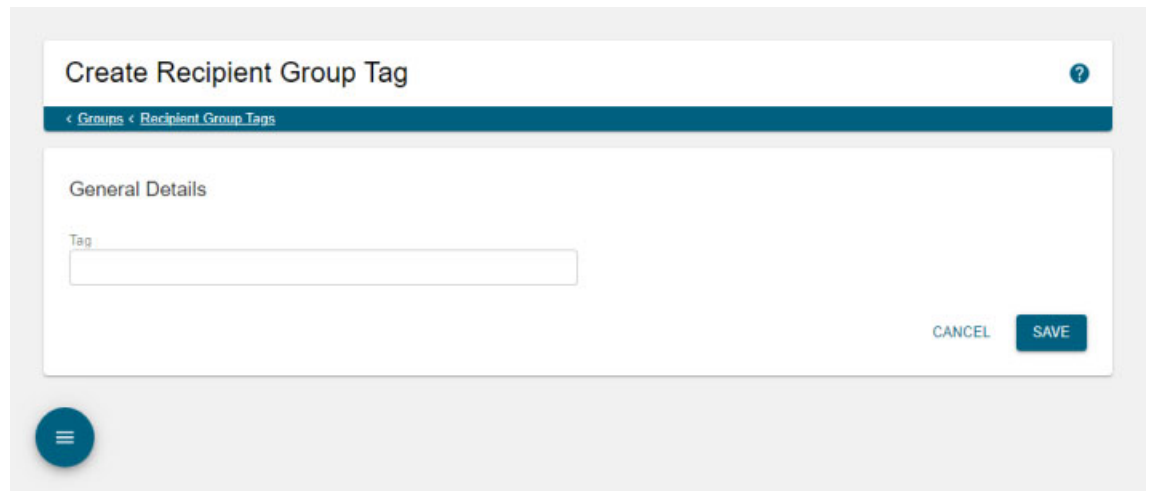
### Add a Recipient Group Tag

Use the following steps to add recipient group tags to InformaCast.

- Step 1** Go to **Recipients | Groups | Tags**. The Recipient Group Tags page appears.

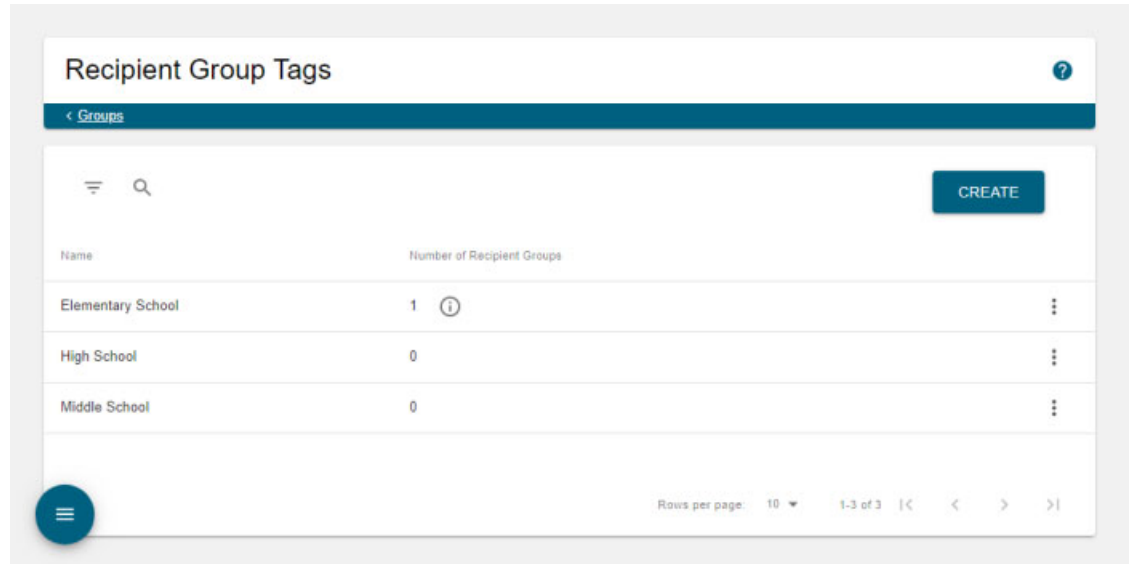


- Step 2** Click the **Create** button. The Create Recipient Group Tag page appears.



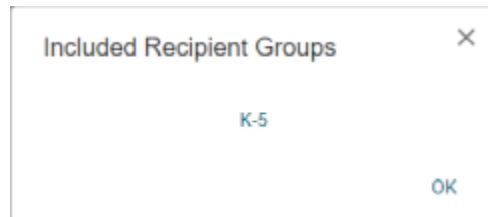
- Step 3** Enter a name for your tag in the **Tag** field, e.g. Elementary School.

**Step 4** Click the **Save** button. The Recipient Group Tags page appears and you can see your added tag.



When you assign your tags to recipient groups, the number of recipient groups assigned to that tag will appear in the table.

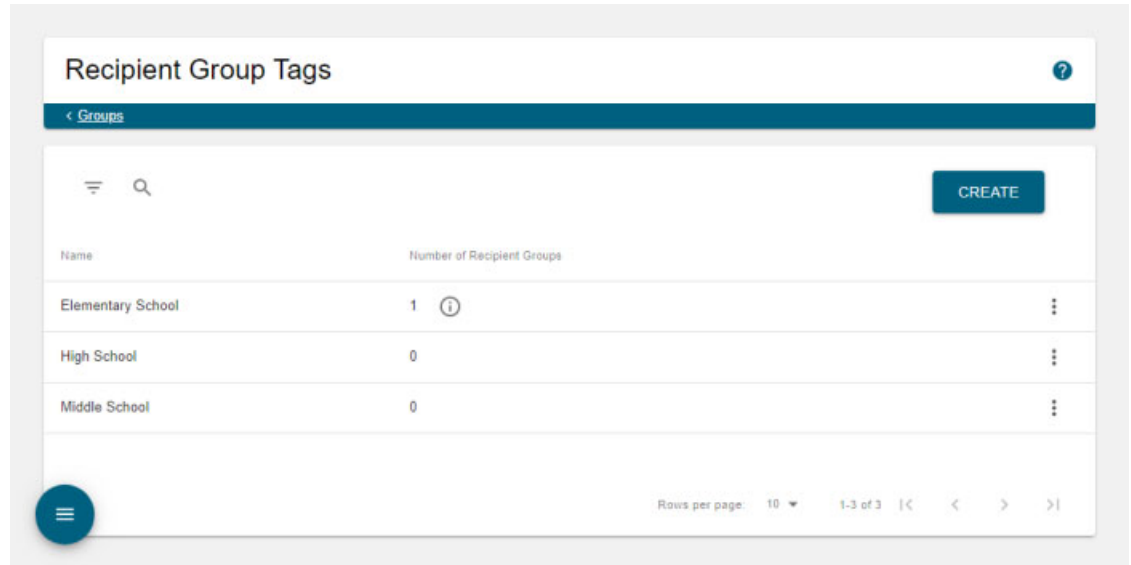
Click a tag's **Info** icon to see the recipient groups that are assigned to tag. The Included Recipient Groups pop-up window appears.



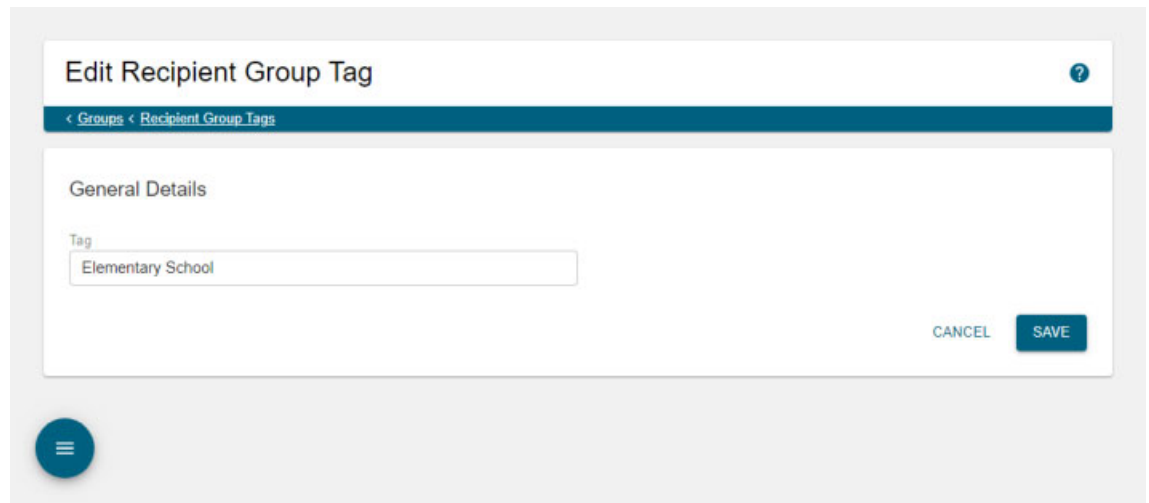
### Edit a Recipient Group Tag

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

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



**Step 2** Click the table row or **More | Edit** icon of the tag you'd like to change. The Edit Recipient Group Tag page appears.



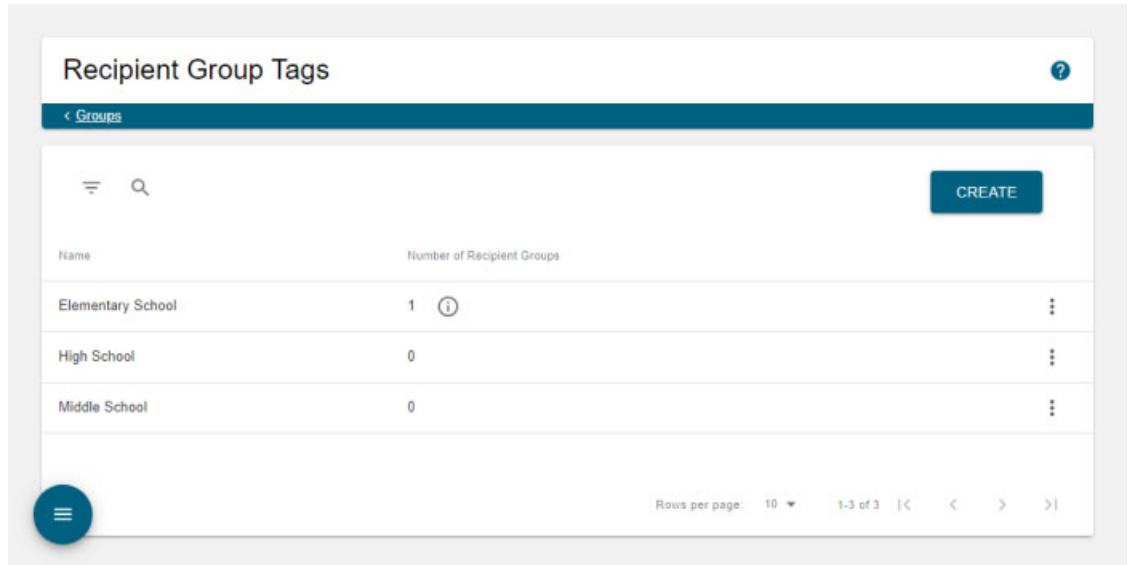
**Step 3** Change your tag's name in the **Tag** field.

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

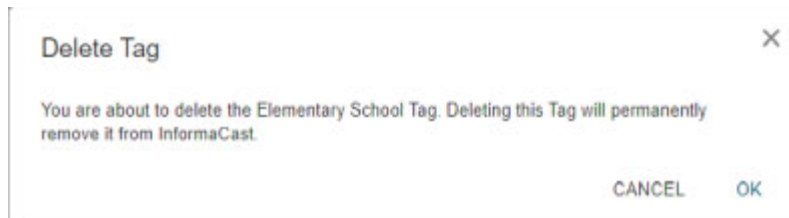
### Delete a Recipient Group Tag

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

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



**Step 2** Click the **More | Delete** icon of the tag you want to delete. The Delete Tag pop-up window appears.



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

## Manage Recipient Administration

Recipient administration covers a number of topics that pertain the administration of your Cisco IP phones for Unified CM:

- “Configure Advanced Matching for Recipient Groups” on page 9-48 discusses using subnets or regular expressions to include or exclude recipients in a recipient group
- “View Calling Terminal Diagnostics” on page 9-50 discusses the health of InformaCast’s CTI connection to Cisco Unified CM and the status of active calls/broadcasts

## 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.** Match all recipients on a particular network based on the IP address range assigned to that network.
- **Regular expressions.** Select devices based on the value of a particular device parameter, 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.

### Subnet Matching

When you are setting up a recipient group rule based on recipients' IP addresses, you will see a **Belong to Host Bitmask** choice in addition to the normal matching constraints. 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 the amount of variance allowed for that address. 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.

In InformaCast, you will 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 **All** from the **Logic Type** dropdown menu, then **IP Address** from the first dropdown menu in the *Filter with Rules* area, **Does** from the second dropdown menu, **Belong to Host Bitmask** 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 it 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 use subnet masks, 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”. To convert from a network bitmask to host bitmask, you must subtract the network bitmask 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 when choosing to include/exclude recipients in a recipient group.

To use this feature, you need to have a solid understanding of the syntax and use of regular expressions, and in particular, the variety used in the Perl programming language. This topic does not attempt to provide this background information. If you need a reference for Perl regular expressions, try this [tutorial](#). If you want to start at a more basic level, try [these tutorials](#).

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 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 the descriptions of all your recipients contain the name of the corporate division in parentheses. To select everyone in Marketing, you 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). On the Create/Edit Recipient Group page, select **Logical Expression** from the **Logic Type** dropdown menu in the *Filter with Rules* area and enter **1** in the **Logical Expression** field. Then, select **Description** from the first dropdown menu and **Does Match Expression** from the two following dropdown menus. Next, enter the following expression in the matching criteria field:

```
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.

In something a bit trickier, suppose you want to have a group containing all Cisco IP phones for Unified CM whose extensions are 27xx. In other words, four digits long, starting with “27.” Set up a rule with **Directory Numbers** from the first dropdown menu, **Does** and **Match Expression** from the following two dropdown menus, and set it to match this expression:

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

This rule will match any Cisco IP phone for Unified CM 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 Create/Edit Recipient Group page, set the rule to **InformaCast Device Type Does Contain**, make sure there is nothing in the last field, and click the **Select Exceptions** button. In the *Select Recipient Exceptions* area, you can see all of the recipients about which InformaCast knows. Clicking the **Info** icon next to any recipient causes the Device Details pop-up window to appear, showing you all the parameters available for the recipient and their values. Once you’ve figured out how to proceed, set the rule back to the parameter you want to use, select **Logical Expression** from the **Logic Type** dropdown menu in the *Filter with Rules* area, and start setting it up.

## View Calling Terminal Diagnostics

The *CTI* area of the Overview page shows the health of InformaCast’s CTI connection to Cisco Unified CM.

Under normal circumstances, the *CTI* area of the Overview page shows you the status of your CTI ports, as shown in the following picture.

CTI						
Port						
Name	DN	State	Registered Address	Active Calls	Marked for Deletion	User Description
CTI1	123149	IN_SERVICE		-	No	-
CTI2	1231499	IN_SERVICE		-	No	-
Route Point						
Name	DN	State	Active Calls			
RP	1231400	IN_SERVICE	-			



The *CTI* area of the Overview page can also show you the status of active calls/broadcasts, as shown in the following picture.

CTI						
Port						
Name	DN	State	Registered Address	Active Calls	Marked for Deletion	User Description
CTI1	123149	IN_SERVICE	[REDACTED]	Call ID: 200062/1 Calling: 123149 Called: 105151	No	com.berbee.lpt.broadcastsystem.cti.outboundcall.d@12/11/2019 09:53:43 AM
CTI2	1231499	IN_SERVICE	[REDACTED]	-	No	-
Route Point						
Name	DN	State	Active Calls			
RP	1231400	IN_SERVICE	-			

Because InformaCast uses CTI for call control, having errors with JTAPI, or CTIManager would affect the ability to source audio for DialCasts from a Cisco IP phone for Unified CM. Use the *CTI* area of the Overview page to verify that your CTI devices in Cisco Unified CM are registered with InformaCast. It is also recommended that you have your Network Monitoring Solution (NMS) view this page to ensure all items are “In Service,” and send you an alert in case of server failures (see “Manage SNMP Monitoring” on page 13-23).



## Broadcast Management

InformaCast allows you to send a live audio broadcast through its DialCast functionality combined with proper Session Initiation Protocol (SIP) configuration (see “Manage SIP Functionality” on page 8-56 for more information). Once you've sent broadcasts, InformaCast records their data (see “Manage Call Detail Records” on page 10-7 for more information).

### Manage Messages

With Basic InformaCast functionality, you only have access to Live Audio broadcasts. In these messages, the audio is streamed to recipient groups in real time when the message is broadcast. These broadcasts will skip any Cisco IP phones for Unified CM 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 Cisco IP phone is set when the broadcast occurs, and if there are simultaneous broadcasts occurring, the first broadcast will play in full, and depending on how long the second broadcast is, it may be skipped entirely.

In order to use your live-audio broadcasts, you need to configure DialCasts (see “Manage DialCasts” on page 10-1).

Once messages are sent, they become broadcasts. Ongoing broadcasts appear on the Active and Queued Broadcasts page and you can cancel them.

### Manage DialCasts

DialCasts allow 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.

Several important points of note exist for DialCasts:

- In order to use DialCasts, you must first configure Session Initiation Protocol (SIP) functionality (see “Manage SIP Functionality” on page 8-56). SIP provides InformaCast with the capability to receive SIP calls, allowing other SIP devices to locate and call InformaCast.
- In the past, Cisco Unified CM CTI route points were recommended for use with DialCast functionality. For easier troubleshooting, it is now recommended that you use a SIP trunk connection instead (see “Configure a SIP Trunk Connection” on page 8-57). If you're still using CTI route points, you should update your DialCast configurations.

- If you want calls to and from InformaCast to use encrypted media, you must configure SRTP support (see “Enable SIP Call Security” on page 8-88).

If your installation of InformaCast is integrated with Cisco Unified CM, you'll also need to ensure your Cisco Unified CM is running in mixed mode and optionally also configure CTI security (see “Manage CTI Security” on page 8-49).

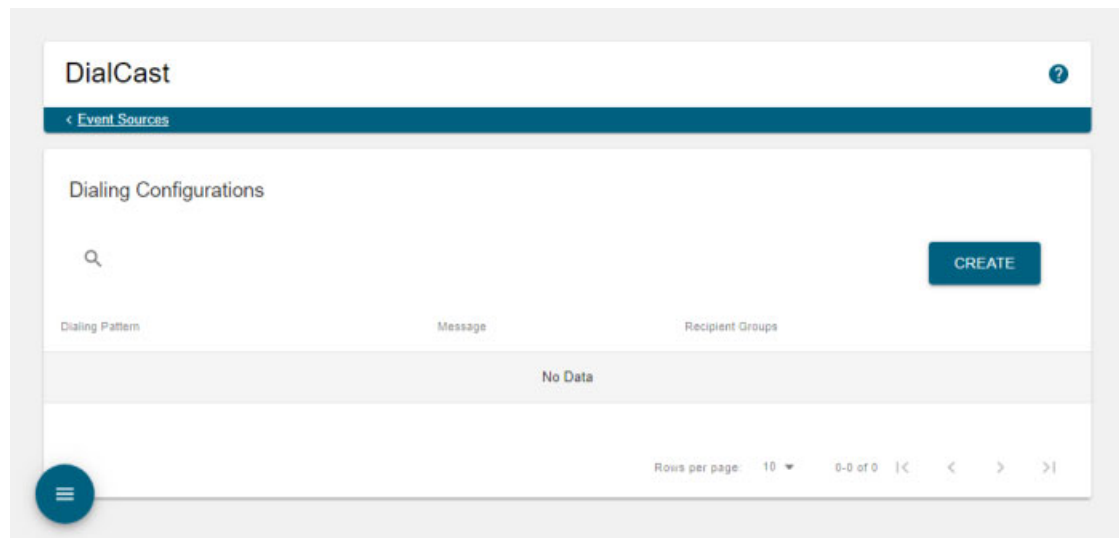
## Manage Dialing Configurations

Once you've finished configuring SIP (see “Manage SIP Functionality” on page 8-56), you can add dialing configurations, which determine the recipient group to receive the broadcast based on the number that is dialed.

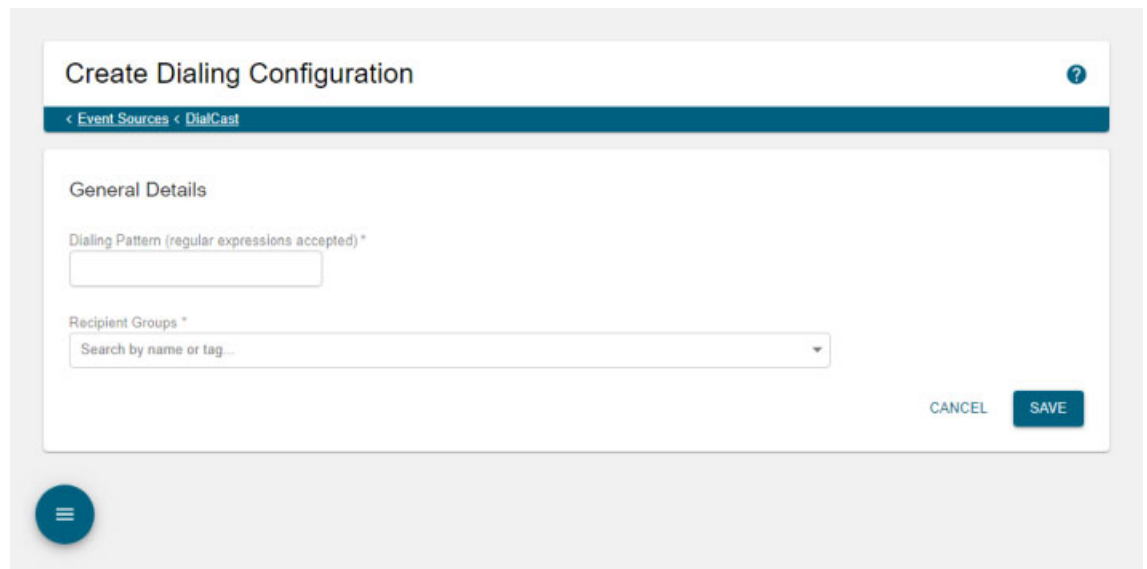
### *Add a Dialing Configuration*

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

- Step 1** Go to **Broadcast Triggers** | **Event Sources** | **DialCast**. The DialCast page appears.



- Step 2** Click the **Create** button in the *Dialing Configurations* area. The Create Dialing Configuration page appears.



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



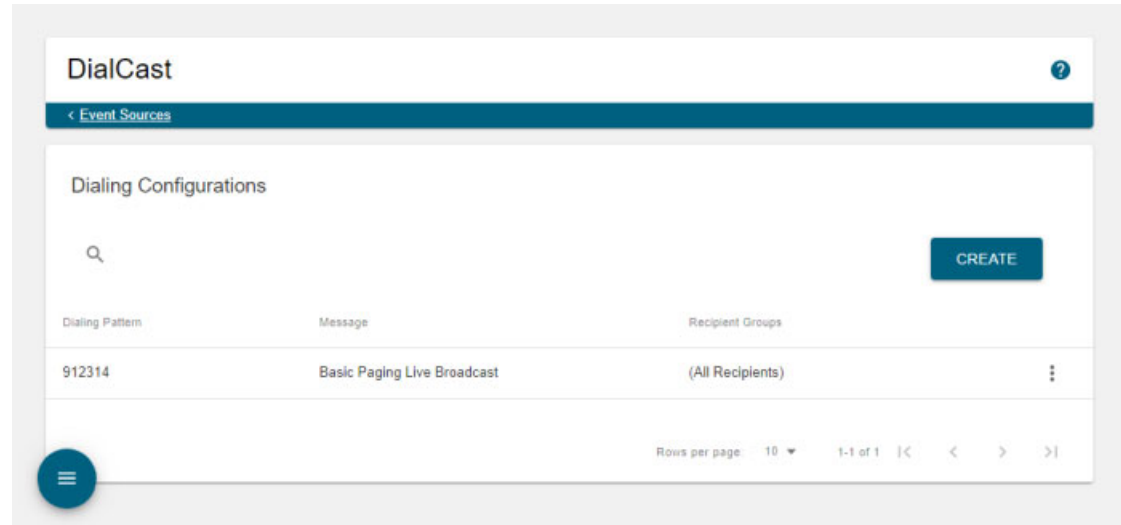
**Tip** It is possible to use \* or #, when setting up a dialing pattern, but you must add \ before the character so that InformaCast doesn't treat it as a wildcard. For example, \*\*1 would have a dialing pattern of \`*\*1`.

- Step 4** Select a recipient group or groups from the **Recipient Groups** field.
- Step 5** Click the **Save** button. Your dialing pattern configuration is saved.

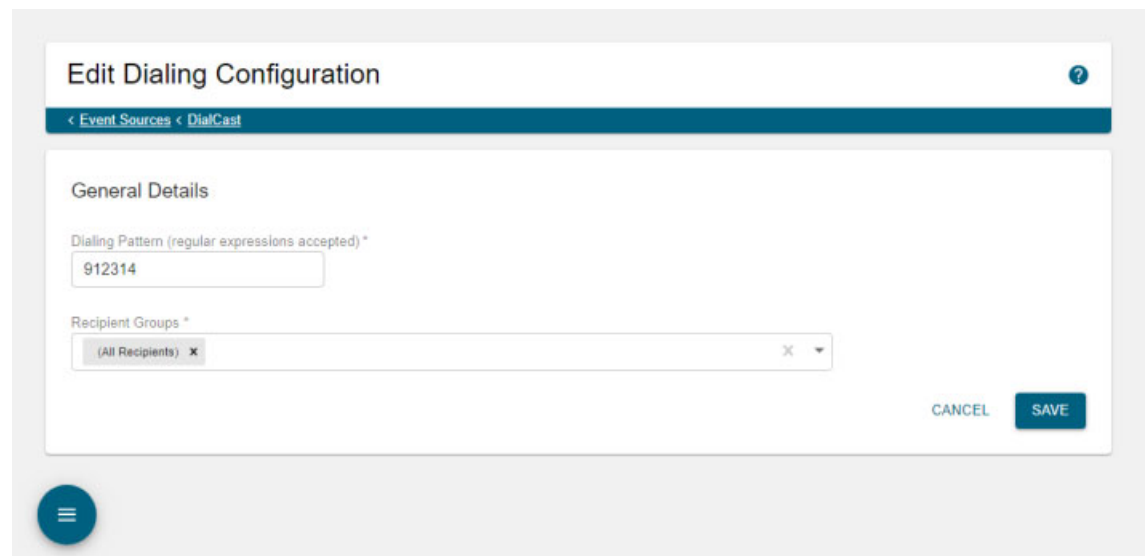
### Edit a Dialing Configuration

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

**Step 1** Go to **Broadcast Triggers | Event Sources | DialCast**. The DialCast page appears.



**Step 2** Click the table row or **More | Edit** icon of the dialing configuration you want to change. The Edit Dialing Configuration page appears.



On the Edit Dialing Configuration page, you can alter the dialing pattern you're using and change the recipient groups to receive your DialCast.

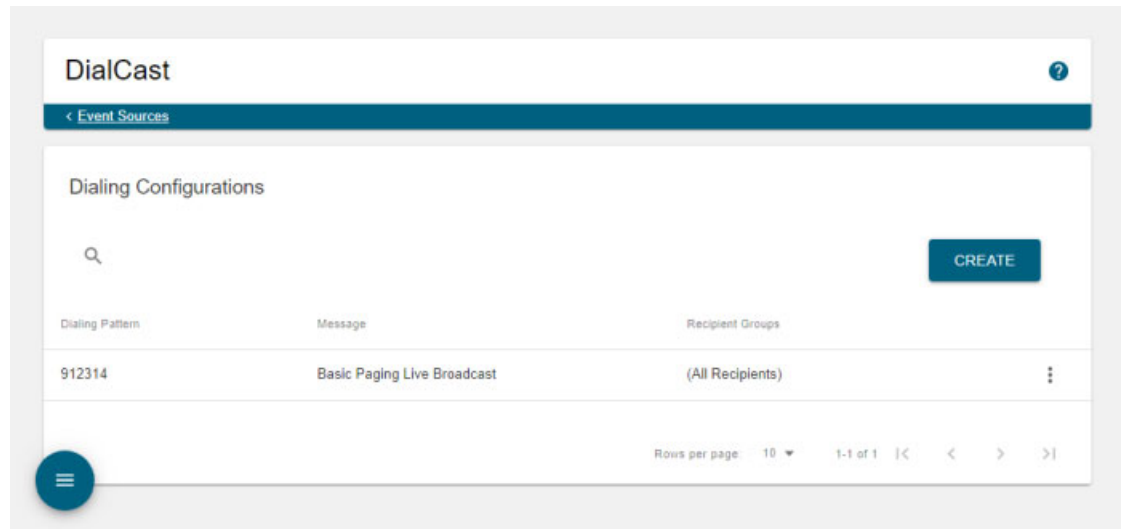
**Step 3** Make your changes.

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

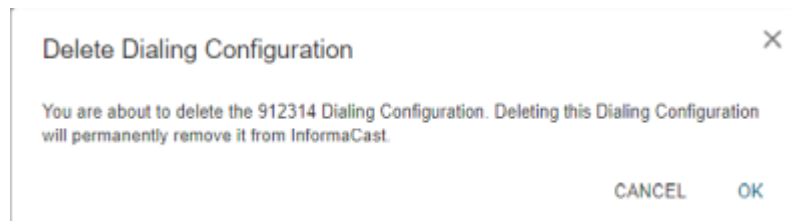
### Delete a Dialing Configuration

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

**Step 1** Go to **Broadcast Triggers | Event Sources | DialCast**. The DialCast page appears.



**Step 2** Click the **More | Delete** icon of the dialing configuration you want to delete. The Delete Dialing Configuration pop-up window appears.



**Step 3** Click the **OK** button. Your 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 the InformaCast message to be sent and the recipient groups who should receive it.



### Tip

Before you can send a broadcast, you must have a SIP trunk connection configured as well as DialCasts (see “Configure a SIP Trunk Connection” on page 8-57 and “Manage DialCasts” on page 10-1, respectively, for more information).

To send a Live Audio broadcast, dial a directory number on your Cisco IP phone that corresponds to a dialing configuration, which is tied to a SIP trunk in Cisco Unified CM. The call will be processed, and as soon as all the recipients specified in your dialing configuration have been activated (minus the phones already in use), you will be broadcasting live.

When you're finished speaking, hang up or press the # button to end your broadcast. Pressing the # button will often result in a better-sounding broadcast that is free of the noise of hanging up the receiver.



### 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 **Broadcasts | History | Active and Queued Broadcasts**. The Active and Queued Broadcasts page appears, offering you the ability to end any active broadcasts.

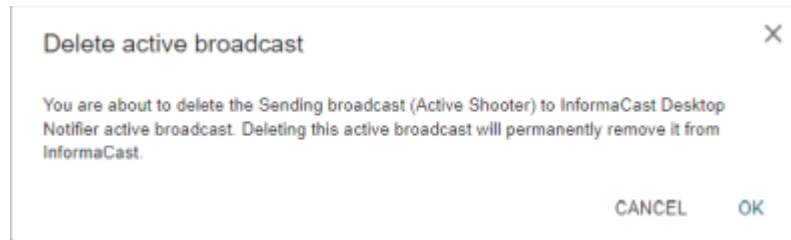
Description	Started	By User
Sending broadcast (Active Shooter) to InformaCast Desktop Notifier	Sun Nov 17 15:50:36 CST 2019	Application Administrator (admin)

Rows per page: 10 | 1-1 of 1

An active broadcast is one that's currently in progress.

A queued broadcast, which is only available for Advanced InformaCast, is one that's waiting for enough recipients to activate before it becomes an active broadcast itself.

- Step 2** Click the **Delete** icon of the broadcast you'd like to cancel. The Delete Active Broadcast pop-up window appears.



- Step 3** Click the **OK** button. InformaCast will stop sending the broadcast.

If the message ends on its own or is canceled 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 Cisco Unified CM. When the call ends, the collected data is written to an InformaCast directory accessible through **System Administration | Reports | Call Detail Records**.

### Collect Call Detail Records

Enable InformaCast to 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 **System Administration | Reports | Call Detail Records**. The Call Detail Records page appears.

By default, InformaCast does not collect call detail records and this page will be empty.

- Step 2** Expand the *Call Detail Record Configuration* area, if it's not already visible.

- Step 3** Select the **Write Call Detail Records** checkbox.

- Step 4** Enter a numeric value in the **Call Detail 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 5** Click the **Save** button to save your changes.

## View Call Detail Records

When InformaCast is configured to collect call detail records, those records are written to a directory accessible through **System Administration | Reports | Call Detail Records**. InformaCast collects two types of call details records: SIP and CTI.

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

The screenshot displays the 'Call Detail Records' interface. At the top, there is a search bar and a table with the following data:

Name	Size (KB)	Last Modified	Download
cti-201911251822.json	4.0 kB	11/25/2019 12:23:00	↓
sip-201911251821.json	837 B	11/25/2019 12:22:00	↓

Below the table, there is a 'Call Detail Record Configuration' section with the following settings:

- Write Call Detail Records
- Call Detail Retention Period\*:

A 'SAVE' button is located at the bottom right of the configuration section.

Call detail records are organized by date and time, e.g. sip-201911251821.json is a call detail record written on November 25, 2019 at 18:21 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 2** Click the **Download** icon of a call detail record to download a JSON file of that record's information.

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

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

Each file has the following call detail record structure:

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

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>} }, ... ]
```



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 and Legacy Paging Interface	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 Cisco Unified CM	105002
fromHost	The host sending the request	xxx.xx.xxx.xxx:5061
to	The destination user in the SIP request; this will be a DN when interacting with Cisco Unified CM	#782
toHost	The host receiving the request	xxx.xx.xxx.xxx:5061

Field	Definition	Example
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 Cisco Unified CM, 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 Cisco Unified CM; 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 Cisco Unified CM, 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 Cisco Unified CM, 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 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 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

Field	Definition	Example
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 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 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
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



Field	Definition	Example
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 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 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 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 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 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:

<b>Field</b>	<b>Definition</b>	<b>Example</b>
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

---



## Administration

Beyond simply using InformaCast to send broadcasts, you can manage its internal settings to customize InformaCast to better fit your environment:

- The Application Administrator is your preset InformaCast superuser, i.e. it holds all possible roles for InformaCast. Because of its elevated status, you may find it helpful to change this user's password periodically (see “Change the Application Administrator's Password”)
- A session timeout is the amount of time InformaCast allows its website users to be inactive before logging them out (see “Configure Session Timeouts” on page 11-3)
- Login banners 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 (see “Manage Login Banners” on page 11-4)
- InformaCast backups ensure you don't lose InformaCast's data in case of an outage by allowing you to backup up its configuration to an external server using Secure File Transfer Protocol (SFTP) and configure the timing of that backup through a scheduled job (see “Manage InformaCast Backups” on page 11-11)

### 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 “Set the Initial Configuration” on page 2-31. Because of its elevated status, you may find it helpful to change this user's password periodically.



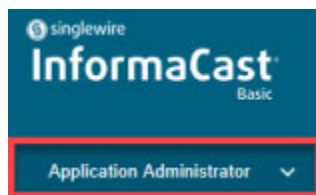
**Warning**

---

**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** Log into InformaCast as the admin user. You should see the name of your application administrator user in the **User** dropdown menu at the top of the left navigational menu.



**Note**

If you are using an older version of InformaCast, “Temporary Administrator” will appear in the **User** dropdown menu.

**Step 2** Click the **User** dropdown menu and select **Help**. The Help Resources page appears.

**Help Resources** ?

- Change Password**  
Change the password of the currently logged-in user.
- Technical Support**  
Access technical support for InformaCast Basic Paging.
- End-User License Agreement**  
View your End-User License Agreement.
- Log Directory**  
View a list of InformaCast's logs and download them, as needed.
- InformaCast User Guide** ↗  
Read step-by-step instructions for the installation, configuration, and management of InformaCast.
- API Quick Start Guide** ↗  
Jump right in and learn the basic tenets of the InformaCast API. The InformaCast API allows you to add users to its system and assign them permissions, create recipient groups, and send messages to recipient groups.
- API Documentation** ↗  
Learn how to combine your existing technology with InformaCast's powerful representational state transfer (REST) application programming interface (API).

**Step 3** Select the **Change Password** card. The Change Password page appears.

**Step 4** Enter your current Application Administrator password in the **Current Password** field.

**Step 5** Enter a new password in the **Password** and **Confirm Password** fields. Choose a password that you will be able to remember (or record it in a secure location).



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

**Step 6** Click the **Save** button. Your password is saved and you're logged out of InformaCast. Log in again with your new password.



**Note** If the passwords you entered in the **Password** and **Confirm Password** fields do not match or if you entered the wrong password, 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 InformaCast Appliance’s Password” on page 13-98).

## Configure Session Timeouts

A general session timeout is the amount of time InformaCast allows its website users to be inactive before logging them out.

If you would like general sessions to remain valid longer, it is possible to change this value.



**Note**

These fields are system-wide; they control the session timeouts of all users.

- Step 1** Go to **System Administration | User Management | Session Timeout**. The Session Timeout page appears.

- Step 2** Enter a numerical value in the **General Session Timeout (seconds)** field. This field controls when users will be logged out of InformaCast's website after a certain amount of inactivity. By default, this field is set to 300 seconds, i.e. five minutes.



**Warning**

**Setting this value to something very small value, e.g. less than 10, will greatly reduce the usability of InformaCast.**

- Step 3** Click the **Save** button to save your changes.

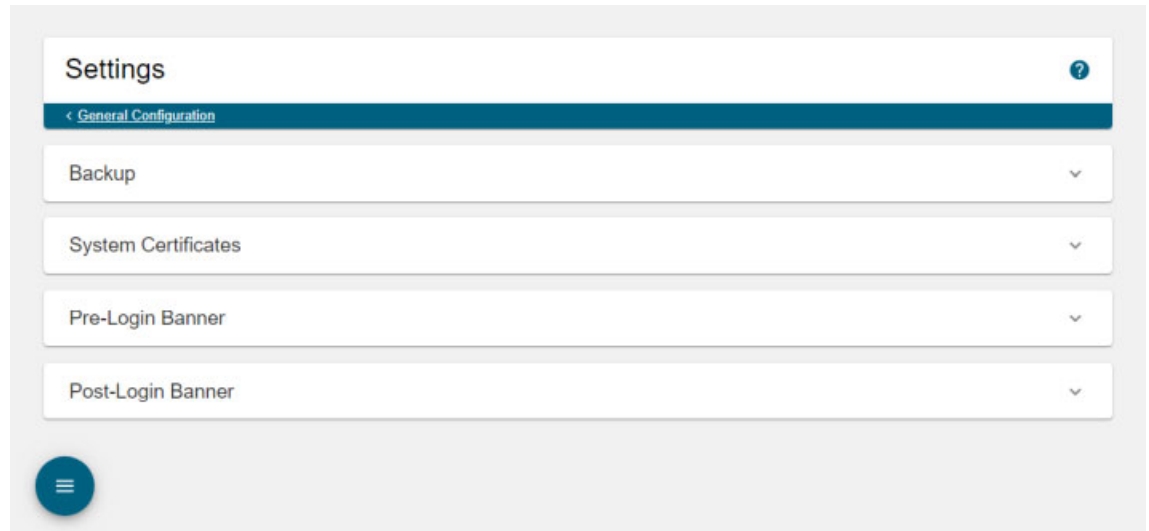
## Manage Login Banners

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** Go to **System Administration | General Configuration | System Settings**. The Settings page appears.



- Step 2** Expand the *Pre-Login Banner* and/or *Post-Login Banner* areas. This topic will use the *Pre-Login Banner* area as an example.

- Step 3** Enter the text you want to appear for your users before they log into InformaCast in the **Pre-Login Text** field.

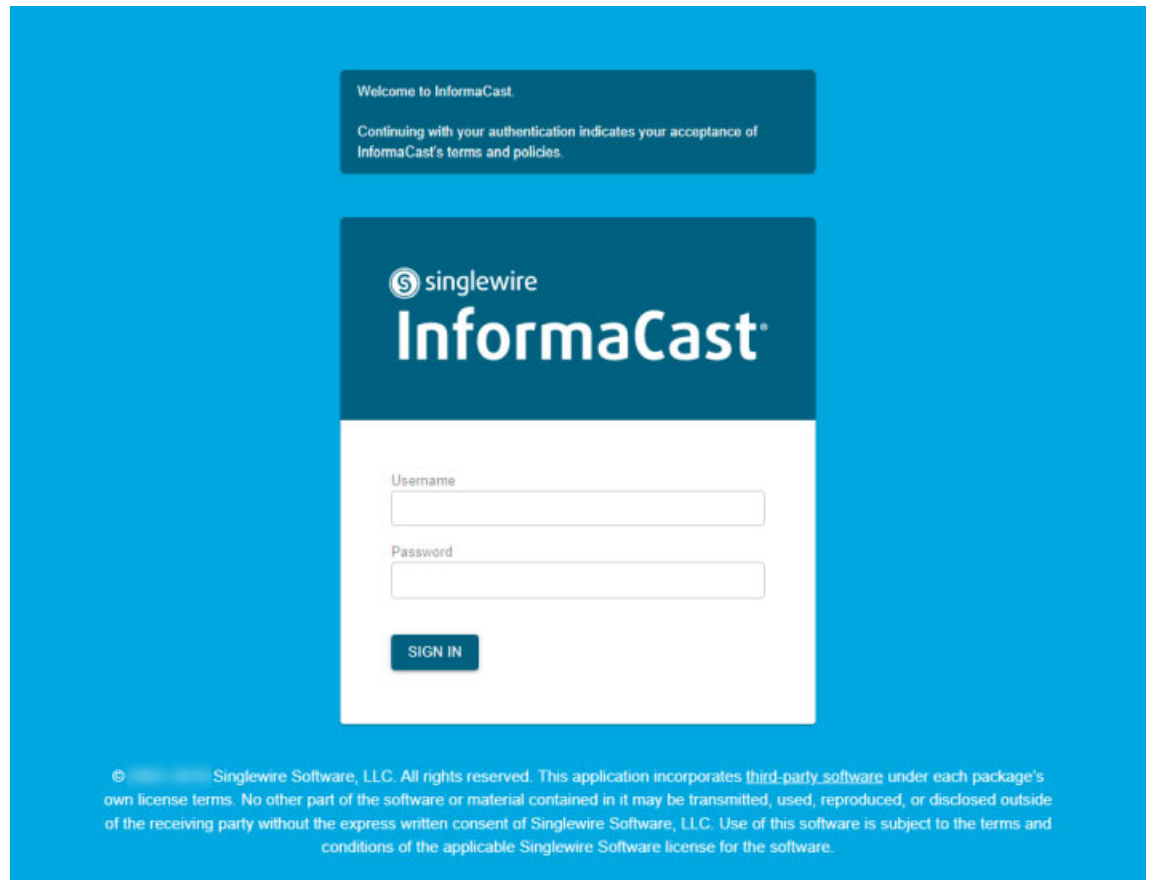


**Note** There is a limit of 1,600 characters, and text must be plain text only, i.e. no HTML or code. Also, you control the line breaks in your banner text. If your pre-login text is longer than your desired screen size, add carriage returns to your **Pre-Login Text** field. They will be replicated on InformaCast's pages.

- Step 4** Click the **Save** button. Your pre-login banner text is saved.



- Step 5** Enter text in the **Post-Login Text** field (optional) and click the **Save** button. Post-login banner text will appear to your users after they log into InformaCast.
- Step 6** Log out of InformaCast. The Sign In page appears and (if you uploaded pre-login text) you should see your new banner text.



**Step 7** Log into InformaCast. One of two things will happen:

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

Dashboard

Welcome to InformaCast.  
Your login indicates compliance with the InformaCast End User License Agreement.

## Welcome to InformaCast Basic Paging (Cisco Paging Server)

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
- Create unlimited recipient groups of 50 phones or less

[Contact Cisco TAC for Support](#)

[User Guide](#)

## Reach More People and Devices

Upgrade to InformaCast Advanced and enjoy a full-featured emergency notification solution that allows you to reach an unlimited number of phones as well as a variety of other endpoints, send text and live or pre-recorded audio as messages, add broadcast confirmations, and much more.

Click the Buy button to begin the process of obtaining an InformaCast Advanced license. You can also click the Try button to start your free 60-day InformaCast Advanced trial. If you would like more information, click the Demo button to request a demo.

**InformaCast Advanced**

[BUY](#) [TRY](#) [DEMO](#)

### Features Include:

- Live audio paging between Cisco IP Phones, with no limit on the number of phones per group
- Integration to existing overhead paging systems
- Text and audio (live or pre-recorded) to Cisco IP Phones and other endpoints
- Audio broadcasts to IP Speakers
- 911/emergency call monitoring/alerting/recording
- Automated weather notifications
- Dynamically-triggered emergency conference calls
- Pre-recorded/scheduled broadcasts(school bells/shift changes)
- Notification to computer desktops (Windows and MacOS) via [InformaCast Desktop Notifier](#)
- Integrate with digital signage solutions and 3rd-party mass notification providers
- Notification and confirmation to mobile devices (Apple, Android, and SMS) with [InformaCast Fusion](#)
- Trigger notification to/from other systems (panic/duress buttons, door locks, lights, etc.)
- And More

### Learn More

- [InformaCast Details](#)

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

**Dashboard**

**Welcome to InformaCast Basic Paging (Cisco Paging Server)**

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
- Create unlimited recipient groups of 50 phones or less

[Technical Support](#)  
[User Guide](#)

**Reach More People and Devices**

Upgrade to InformaCast Advanced and enjoy a full-featured emergency notification solution that allows you to reach an unlimited number of phones as well as a variety of other endpoints, send text and live or pre-recorded audio as messages, add broadcast confirmations, and much more.

Click the Buy button to begin the process of obtaining an InformaCast Advanced license. You can also click the Try button to start your free 60-day InformaCast Advanced trial. If you would like more information, click the Demo button to request a demo.

**InformaCast Advanced**

[BUY](#) [TRY](#) [DEMO](#)

**Features Include:**

- Live audio paging between Cisco IP Phones, with no limit on the number of phones per group
- Integration to existing overhead paging systems
- Text and audio (live or pre-recorded) to Cisco IP Phones and other endpoints
- Audio broadcasts to IP Speakers
- 911/emergency call monitoring/alerting/recording
- Automated weather notifications
- Dynamically-triggered emergency conference calls
- Pre-recorded/scheduled broadcasts(school bells/shift changes)
- Notification to computer desktops (Windows and MacOS) via [InformaCast Desktop Notifier](#)
- Integrate with digital signage solutions and 3rd-party mass notification providers
- Notification and confirmation to mobile devices (Apple, Android, and SMS) with [InformaCast Fusion](#)
- Trigger notification to/from other systems (panic/duress buttons, door locks, lights, etc.)
- And More

**Learn More**

- [InformaCast Details](#)

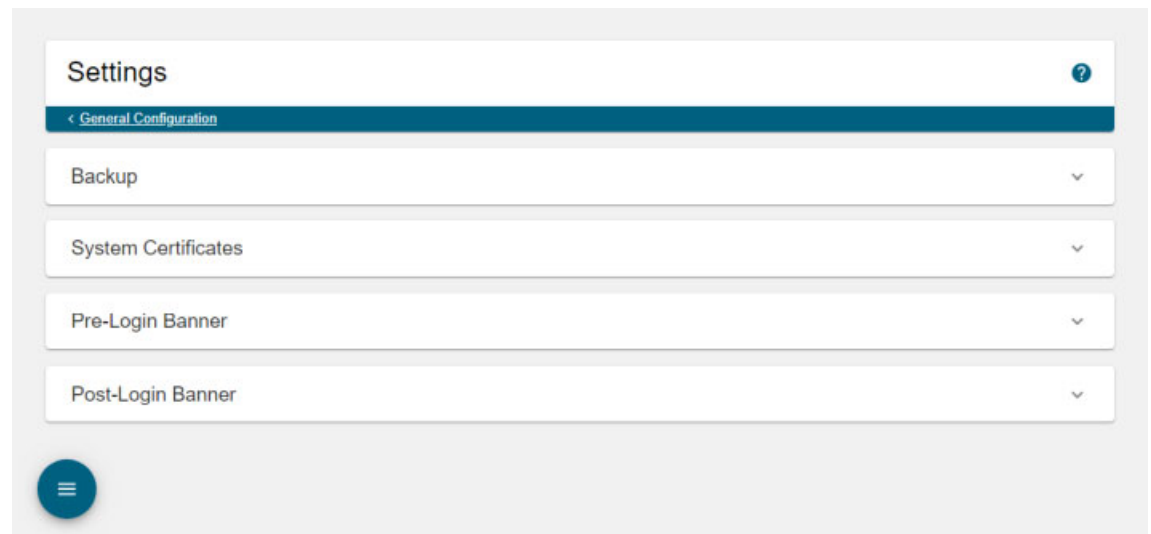
**Note**

Login banner text will only appear for Webmin and the command-line interface after you reboot the InformaCast Appliance (see “Reboot the InformaCast Appliance” on page 13-12).

## Edit a Login Banner

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

- Step 1** Go to **System Administration | General Configuration | System Settings**. The Settings page appears.



- Step 2** Expand the *Pre-Login Banner* and/or *Post-Login Banner* areas. This topic will use the *Pre-Login Banner* area as an example.

- Step 3** Enter the text you want to appear for your users before they log into InformaCast in the **Pre-Login Text** field.



**Note** There is a limit of 1,600 characters, and text must be 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 **Pre-Login Text** field. They will be replicated on InformaCast's pages.

- Step 4** Click the **Save** button. Your pre-login banner text is saved.

- Step 5** Enter text in the **Post-Login Text** field (optional) and click the **Save** button. Post-login banner text will appear to your users after they log into InformaCast.
- Step 6** Log out and back into InformaCast to ensure the appropriate text appears.

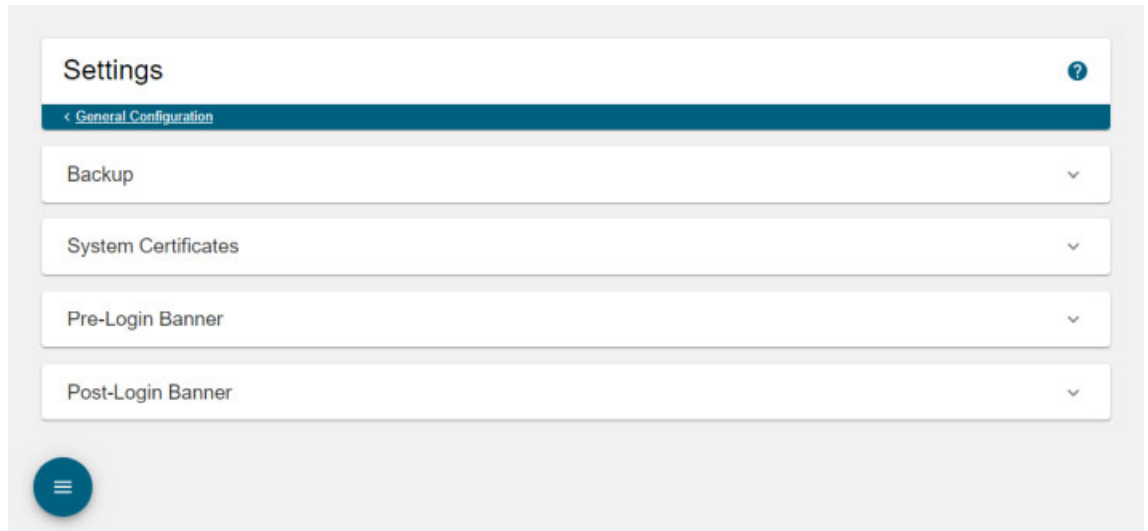


**Note** Login banner text will only appear for Webmin and the command-line interface after you reboot the InformaCast Appliance (see “Reboot the InformaCast Appliance” on page 13-12).

## Delete a Login Banner

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

- Step 1** Go to **System Administration | General Configuration | System Settings**. The Settings page appears.



- Step 2** Expand the *Pre-Login Banner* and/or *Post-Login Banner* areas. This topic will use the *Pre-Login Banner* area as an example.

**Pre-Login Banner** ^

Define the text that should be displayed on the login screen.

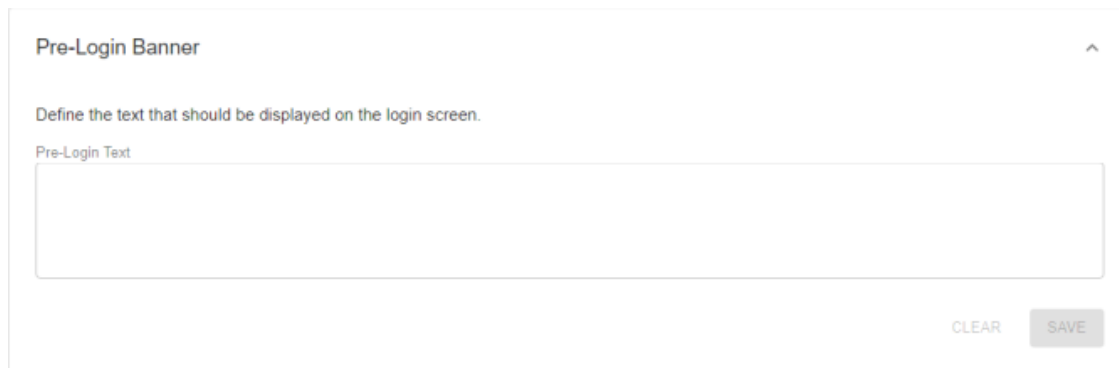
Pre-Login Text

Welcome to InformaCast.

Continuing with your authentication indicates your acceptance of InformaCast's terms and policies.

CLEAR
SAVE

**Step 3** Click the **Clear** button of the login banner you want to delete. InformaCast deletes your text.



## 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, all certificates, and all SSH server keys are preserved during this process.

If you are already backing up your InformaCast Virtual Appliance 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

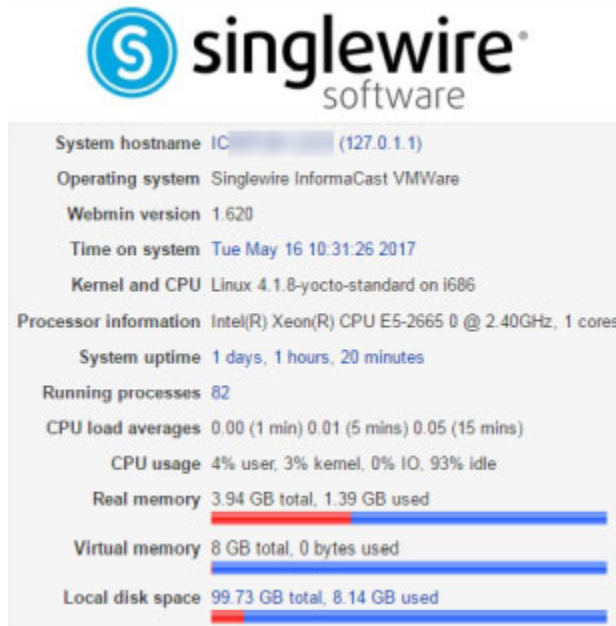
You must configure a connection to an SFTP server in order for InformaCast to properly back up its configuration. InformaCast's backups are fully encrypted using the security passphrase you set up when you installed InformaCast (see "Set the Initial Configuration" on page 2-31).

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 3-14 for specific steps). The Webmin homepage appears.



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

Module Config

### Configure SFTP, Backup or Restore Appliance

This process administers backup and restore to/from an external server running the secure FTP (SFTP) protocol. SFTP information is not configured or the SFTP server is not available.

[Jobs](#) [Configure](#) [Backup](#) [Restore](#)

When a backup or restore job happens, its logs will appear here.

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

Module Config

### Configure SFTP, Backup or Restore Appliance

This process administers backup and restore to/from an external server running the secure FTP (SFTP) protocol.  
SFTP information is not configured or the SFTP server is not available.

- Step 4** Enter the IP address or hostname of your SFTP server in the **SFTP 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.

After the value you specify in the **Number of backups to keep on SFTP server** field is met, InformaCast will delete the oldest backup file to make room for the newest. This only applies to backups of the current major/minor version, e.g. if you enter **2** in the **Number of backups to keep on SFTP server** field and you have a backup file from 12.17.1 and 12.17.2, a backup from 12.19.1 will coexist with your old backup files; however, if you then add backup files from 12.19.2 and 12.19.3, your 12.19.1 backup file will be removed automatically from InformaCast.

In addition, you may want to delete backups from previous versions as only backups from your major/minor version of InformaCast are considered compatible, e.g. you can backup on 12.19.1 and restore on 12.19.2, but not 14.4.2.



- 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.

Module Config

### Configure SFTP, Backup or Restore Appliance

Configuration saved successfully

- Step 10** Continue with “Backup InformaCast’s Configuration” on page 11-14.
- 

## 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: through InformaCast’s user interface or Webmin’s.

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 11-11.



### 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 **System Administration | General Configuration | System Settings**. The Settings page appears.



**Step 2** Expand the *Backup* area, if it's not already visible.

**Step 3** Select the **Activate Backup Schedule** checkbox.

**Step 4** Enter numeric values for when your scheduled backup should occur in the **Hour**, **Minute**, and **Second** fields.



**Note** The time for scheduled backups is calculated in military time, e.g. 18:30:00 is 6:30 p.m.

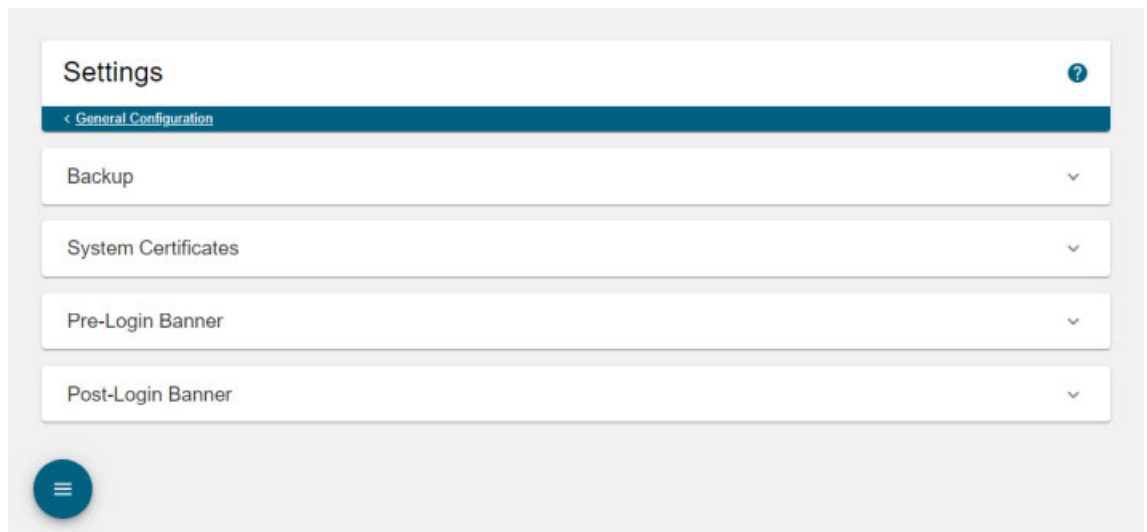
- Step 5** Click the **Save** button. Your backup scheduled job is saved. On the Overview page, you can see your changes reflected in the *InformaCast Server* area.

InformaCast Server	
Version:	Purchased license
Application Mode:	Stand-alone
Maintenance Contract:	
Backup Activated:	Yes
Next Scheduled Backup	2019-12-05T18:30:00.000-0600

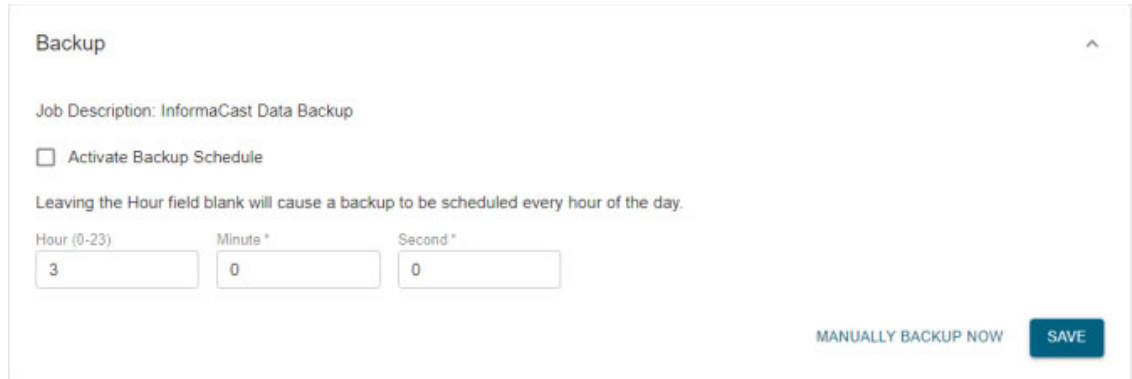
### Manually Back Up InformaCast Through Its User Interface

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

- Step 1** Go to **System Administration | General Configuration | System Settings**. The Settings page appears.



**Step 2** Expand the *Backup* area, if it's not already visible.



**Step 3** Click the **Manually Backup Now** button. InformaCast will begin backing itself up to the location you specified on your SFTP Server. This may take a few moments.

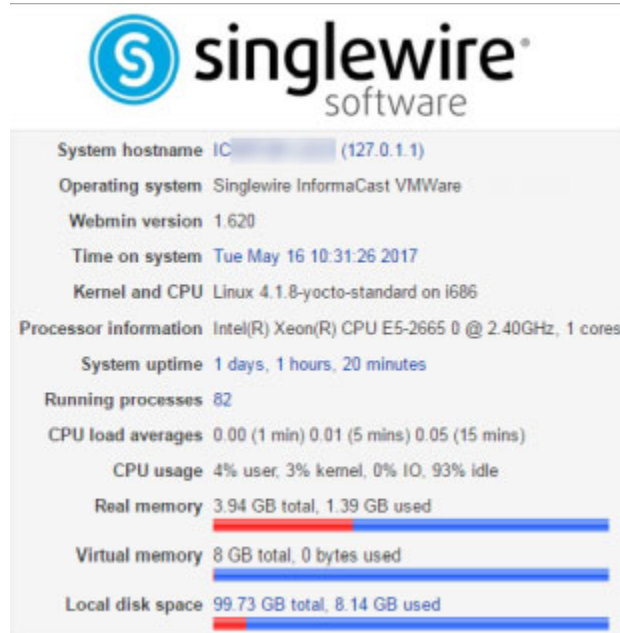


**Note** New backups will overwrite previous backup files once the value specified in the **Number of backups to keep on SFTP server** field is met.

## 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 3-14 for specific steps). The Webmin homepage appears.



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

Module Config

### Configure SFTP, Backup or Restore Appliance

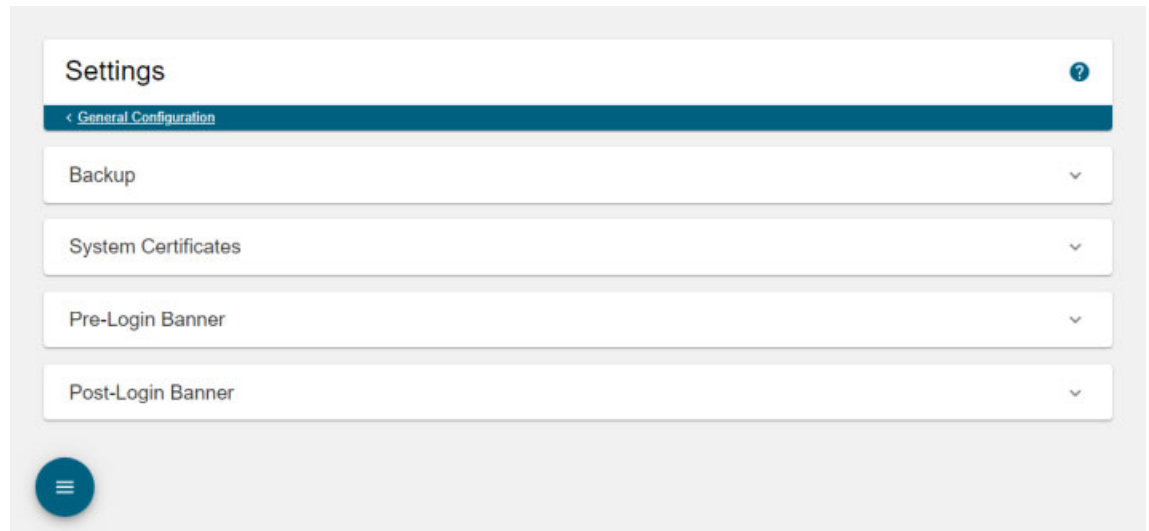
This process administers backup and restore to/from an external server running the secure FTP (SFTP) protocol. SFTP information is not configured or the SFTP server is not available.

[Jobs](#) [Configure](#) [Backup](#) [Restore](#)

When a backup or restore job happens, its logs will appear here.

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

**Step 4** Go to **System Administration | General Configuration | System Settings**. The Settings page appears.



**Step 5** Expand the *Backup* area, if it's not already visible.

**Step 6** Click the **Manually Backup Now** button. InformaCast will begin backing itself up to the location you specified on your SFTP Server. This may take a few moments.

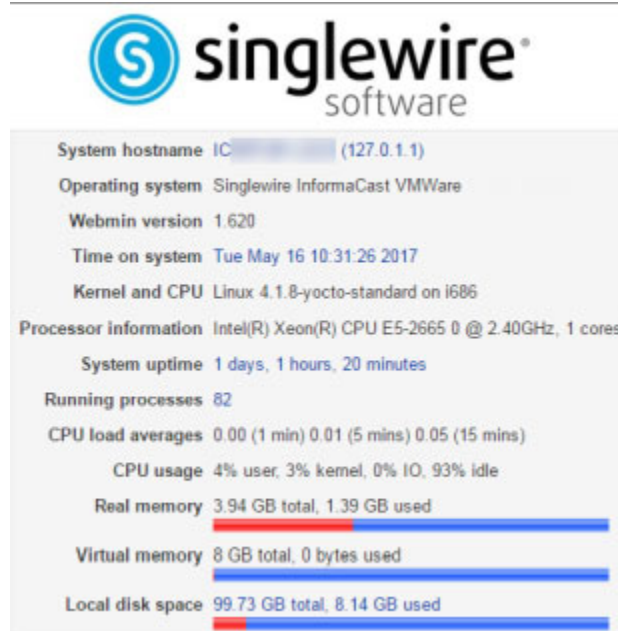


**Note** New backups will overwrite previous backup files once the value specified in the **Number of backups to keep on SFTP server** field is met.

## 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 3-14 for specific steps). The Webmin homepage appears.



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

Module Config

### Configure SFTP, Backup or Restore Appliance

This process administers backup and restore to/from an external server running the secure FTP (SFTP) protocol.

Jobs Configure Backup Restore

#### Job Log

These steps were executed as part of the last backup or restore job. If you do not see Job Successful below, the backup or restore did not finish.

```

2017-05-22 14:47:04-05:00 Starting Backup
2017-05-22 14:47:04-05:00 Removing code from the backup
2017-05-22 14:47:05-05:00 Removing unreferenced files from backup
2017-05-22 14:47:05-05:00 Saving the version
2017-05-22 14:47:05-05:00 Create system package backup
2017-05-22 14:47:05-05:00 InformaCast preflight check
2017-05-22 14:47:09-05:00 Cleaning the platform backup
2017-05-22 14:47:09-05:00 Creating backup set
2017-05-22 14:47:18-05:00 Removing system package
2017-05-22 14:47:18-05:00 Job Successful

```

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.

Module Config

### Configure SFTP, Backup or Restore Appliance

This process administers backup and restore to/from an external server running the secure FTP (SFTP) protocol.

Jobs Configure Backup Restore

Restore a Backup on this Appliance

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

Module Config

### Configure SFTP, Backup or Restore Appliance

Choose which dataset to restore. Once you choose the dataset, the restore will begin. If the restore succeeds, the system will switch versions automatically.

Choose a dataset to restore onto this server ▾

Begin restore using backup set above



- 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.




**Note** You will only be able to select backup files from the **Choose a dataset to restore onto this server** dropdown menu that are compatible with your major/minor version of InformaCast, e.g. you can backup on 12.19.1 and restore on 12.19.2, but not 14.4.2.

InformaCast begins restoring itself to the backup you selected.

[Module Config](#)

### Configure SFTP, Backup or Restore Appliance

Backup or restore job is in progress. Please wait for it to complete. Closing this page does not affect the job. 

```

2017-06-13 14:37:45-05:00 Step 0: restore-system begins
2017-06-13 14:37:45-05:00 Step 1: Select partitions based on location of app partition
2017-06-13 14:37:46-05:00 Step 2: Stop services
2017-06-13 14:38:12-05:00 Step 3: Create the app and data partitions
2017-06-13 14:38:19-05:00 Step 4: Copy rescue partition
2017-06-13 14:38:22-05:00 Step 5: Verify rescue partition
2017-06-13 14:38:25-05:00 Step 6: Copy app partition

```

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 3-9 for specific steps). InformaCast's Dashboard appears.

**Dashboard**

**Welcome to InformaCast**  
**Basic Paging (Cisco Paging Server)**

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
- Create unlimited recipient groups of 50 phones or less

[Technical Support](#)  
[User Guide](#)

**Reach More People and Devices**

Upgrade to InformaCast Advanced and enjoy a full-featured emergency notification solution that allows you to reach an unlimited number of phones as well as a variety of other endpoints, send text and live or pre-recorded audio as messages, add broadcast confirmations, and much more.

Click the Buy button to begin the process of obtaining an InformaCast Advanced license. You can also click the Try button to start your free 60-day InformaCast Advanced trial. If you would like more information, click the Demo button to request a demo.

**InformaCast Advanced**

[BUY](#) [TRY](#) [DEMO](#)

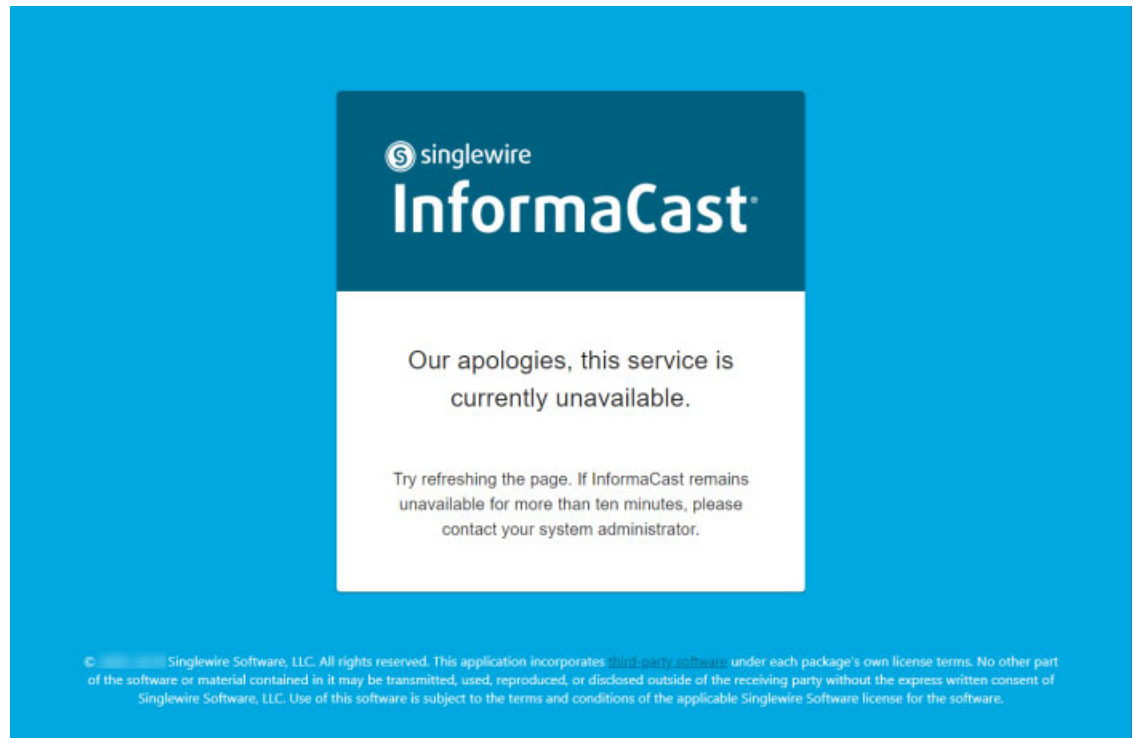
**Features Include:**

- Live audio paging between Cisco IP Phones, with no limit on the number of phones per group
- Integration to existing overhead paging systems
- Text and audio (live or pre-recorded) to Cisco IP Phones and other endpoints
- Audio broadcasts to IP Speakers
- 911/emergency call monitoring/alerting/recording
- Automated weather notifications
- Dynamically-triggered emergency conference calls
- Pre-recorded/scheduled broadcasts(school bells/shift changes)
- Notification to computer desktops (Windows and MacOS) via [InformaCast Desktop Notifier](#)
- Integrate with digital signage solutions and 3rd-party mass notification providers
- Notification and confirmation to mobile devices (Apple, Android, and SMS) with [InformaCast Fusion](#)
- Trigger notification to/from other systems (panic/duress buttons, door locks, lights, etc.)
- And More

**Learn More**

- [InformaCast Details](#)

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



Once InformaCast is done initializing, you may sign in.

**Step 7** Test your InformaCast functionality to ensure its behavior is as expected.

---



## Advanced InformaCast Access



### Note

InformaCast is part of the larger InformaCast Appliance suite of products. If you are looking to upgrade your version of InformaCast Appliance, e.g. 8.3 to 8.5.1, see “Upgrade InformaCast Appliance” on page 13-139.

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. 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 phones for Unified CM. 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
- Send broadcasts to a wide variety of recipients, e.g. Cisco IP phones, IP speakers, InformaCast Desktop Notifier instances, email addresses, Twitter and WordPress references, etc.
- Customize scripts that can be attached to broadcasts
- Receive confirmation when broadcasts are sent
- Configure resiliency

If you're using Basic InformaCast, you can upgrade to Advanced InformaCast using the **Try** or **Buy** buttons on InformaCast's Dashboard or by [contacting Singlewire](#) to obtain a license for a switch in functionality.

If problems with your upgrade arise, you may find answers with Singlewire's [Support Community](#).



### Tip

If you want to learn more about InformaCast Advanced Notification, click the **Demo** button on InformaCast's Dashboard to request a demonstration of InformaCast's functionality or visit [Singlewire's website](#) for more information.

## 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—broadcast 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, which should have been provided to you by your Singlewire salesperson. [Contact sales@singlewire.com](mailto:sales@singlewire.com) if you didn't receive one. If you are using Advanced InformaCast as a trial, your license key is already included.
- 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. Ensure you are [using the right one](#).
- InformaCast's functionality changes dramatically with your move from Basic to InformaCast. Depending on your access level, you'll have access to:
  - **Richer message functionality.** Create, edit, and send more than just live audio, e.g. pre-recorded audio, ad-hoc audio, and you can send text, include confirmations, add scripts to run when the message is sent, etc.
  - **Expanded recipients.** Send broadcasts to more than just Cisco IP phones, e.g. IP speakers, InformaCast Desktop Notifier instances, monitored phone numbers, e.g. 911, that trigger a broadcast when that number is dialed, a liaison between your existing paging system and InformaCast, mobile devices, etc.
  - **Finer scheduling.** Send patterns of scheduled messages (usually brief tones) to IP phones and IP speakers to announce shift changes or changing classes.
  - **Full administration.** View scheduled updates and backups; manage the license key, voice menus, and users; and set up the system, network, and broadcast parameters.
- 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 “Installation” on page 2-1).
- If you fail to configure Cisco Unified CM in Basic InformaCast, upgrading to Advanced InformaCast and then configuring Cisco Unified CM before downgrading to Basic InformaCast will require you to perform all the steps in “Integrate Cisco Unified CM” on page 8-3 again.
- If you have questions about your upgrade, Singlewire's [Support Community](#) may provide answers. Otherwise, you can contact Singlewire Support through the online support request form. Please include:
  - Your name
  - Your email address
  - Your phone number
  - The subject of your query
  - A short description of your issue
  - The product with which you have an issue

- Its version number
- Your telephony environment
- Your Cisco Unified CM version
- The models of Cisco IP phone for Unified CM you're using
- Your Cisco firmware version

## Upgrade InformaCast

If you're using Basic InformaCast, you can upgrade to Advanced InformaCast using the **Try** or **Buy** buttons on InformaCast's Dashboard or by [contacting Singlewire](#) to obtain a license for a switch in functionality.

**Note**

---

InformaCast is part of the larger InformaCast Appliance suite of products. If you are looking to upgrade your version of InformaCast Appliance, e.g. 12.5.1 to 12.19.1, see “Upgrade InformaCast Appliance” on page 13-139.

---

### Try Advanced Notification

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

- 
- Step 1** Click the **Try** button any time while using Basic InformaCast (internet access is required).

If you have internet access, you will see a form. Fill out the required information and click the **Start Trial** button.

The screenshot shows a web form titled "Try InformaCast Advanced" with a help icon in the top right. The main heading is "Start a 60-day InformaCast Trial". The form contains the following fields:

- First Name \* (text input)
- Last Name \* (text input)
- Job Title \* (text input)
- Company Name \* (text input)
- Industry \* (dropdown menu)
- Email Address \* (text input)
- Phone Number \* (text input)
- What best describes your role? \* (text input)
- Street Address \* (text input)
- City \* (text input)
- State/Region \* (text input)
- Postal Code \* (text input)
- Country \* (text input)

At the bottom right, there are two buttons: "CANCEL" and "START TRIAL". A hamburger menu icon is located in the bottom left corner of the form area.

If you don't have internet access, [contact Singlewire](#) and request your 60-day free trial of Advanced InformaCast.

**Step 2** Go to **System Administration | General Configuration | License Key**. The License Key page appears.

InformaCast License Key	
Licensing Mode	Advanced Notification Trial
Application	InformaCast
Licensee	Contact Singlewire at sales@singlewire.com or +1.608.661.1140, option 1 to upgrade to a permanent advanced notification license.
Server IP Address	Not restricted
Feature Codes	Audio, MessageConfirmation
License Expiration Date	Aug 9, 2020
Application Parameters	
Maximum Bell Schedules	10
Maximum IP Speakers	5
Maximum Phones	500
Maximum InformaCast Version	
Maintenance Contract	-

UPLOAD NEW KEY WITH LICENSE MANAGER

On the License Key page, you can see that your license mode is Advanced Notification Trial. Further down the page, you can see the date when your trial will expire.

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.



**Note** Downgrade from Advanced InformaCast back to Basic by clicking the **End Advanced Trial** button in InformaCast’s left navigational menu. This will cause InformaCast to reboot, as will any future change in InformaCast functionality or license type. If you downgrade to Basic InformaCast before your trial period ends, you forfeit the rest of your trial period.

### Buy Advanced Notification

By clicking the **Buy** button, you start the process of obtaining InformaCast Advanced Notification through either a demonstration, subscription, or perpetual license. For more information on InformaCast licenses, see “Licensing Information” on page 1-7.



**Note**

If you are operating InformaCast on a Communications Manager Business Edition 6000 with an IP address within the range of 172.27.199.1/254 and you decide to buy InformaCast, you will need to either change the IP address used by InformaCast or be prepared to accept a succession of one-year subscription licenses (see “Change the InformaCast Appliance’s IP Address” on page 13-37 for more information).

**Step 1** Click the **Buy** button any time while using Basic InformaCast (internet access is required).

If you have internet access, you will be redirected to a Singlewire Software website. Follow the prompts to obtain a new license.

**CONTACT US**

Our team is always eager to help with your [emergency notification system](#) needs. We are available from 7 a.m. to 6 p.m. CDT, Monday through Friday (excluding US Holidays). Reach out to us below to have your questions answered.

At Singlewire, we respect the confidentiality of everyone's personal and business information. Learn more about our [Privacy Policy](#)

**PHONE:**  
+1 608.661.1140

**OFFICE ADDRESS:**  
Singlewire Software  
1002 Deming Way  
Madison, WI 53717  
[Driving Directions](#)

**MAILING ADDRESS:**  
Singlewire Software  
PO Box 46218  
Madison, WI 53744-6218

**SALES & QUOTES**  
[sales@singlewire.com](mailto:sales@singlewire.com)  
+1 608.661.1140 Option 1

**TERRITORY MANAGERS**  
[United States](#) [International](#)

**TECHNICAL SUPPORT**  
[Open a Support Case](#)

**LICENSE KEY HELP**  
[licensing@singlewire.com](mailto:licensing@singlewire.com)

**ORDER HELP**  
[orders@singlewire.com](mailto:orders@singlewire.com)

**BILLING HELP**  
[invoicing@singlewire.com](mailto:invoicing@singlewire.com)

**First Name\***

**Last Name\***

**Email\***

**Company Name\***

**Phone Number\***

**Street Address\***

**City\***

**State/Region\***

**Country**

**Do You Have a Cisco Phone System?\***  
- Please Select -

**Do You Have a Notification System\***  
- Please Select -

**What are you interested in learning more about?**

[Contact Us](#)

If you don't have internet access, [contact Singlewire](#) and request Advanced InformaCast.

**Step 2** Continue with “Upload a New License” on page 4-2.

---



## System Management

While InformaCast allows you to perform many of its necessary functions through its web interface, some of them can only be accomplished through the administrative interface of the InformaCast Appliance (Webmin) or the InformaCast Appliance's command-line interface (CLI). The following table provides you with a list of administrative functions organized by category; notes whether they're available in Webmin, the CLI, or both; provides the corresponding CLI command (if applicable); and gives a short description of the functionality.

Category	Name	Webmin	CLI	Command	Description
<b>Service Control</b>					
	“Start a Service on the InformaCast Appliance” on page 13-9	X	X	<service_name>-service enable	Enable services running on the InformaCast Appliance, e.g. informacast
	“Stop a Service on the InformaCast Appliance” on page 13-7	X	X	<service_name>-service disable	Disable services running on the InformaCast Appliance, e.g. informacast
	“Restart a Service on the InformaCast Appliance” on page 13-10	X	X	<service_name>-service restart	Restart services running on the InformaCast Appliance, e.g. informacast
<b>System State</b>					
	“Shut Down the InformaCast Appliance” on page 13-14	X	X	halt-appliance	Shut down the InformaCast Appliance
	“Reboot the InformaCast Appliance” on page 13-19	X	X	restart-appliance	Restart the InformaCast Appliance
<b>Network Commands</b>					
	“Test the InformaCast Appliance's Connectivity” on page 13-21		X	test-network-connectivity	Verify connectivity between the InformaCast Appliance and its default gateway, several servers, and a variety of services

Category	Name	Webmin	CLI	Command	Description
	“Show Multicast Statistics” on page 13-22		X	show-multicast-statistics	Display information about the current multicast groups joined on each interface and the IGMP version in use
	“Configure SNMP Monitoring” on page 13-26		X	configure-snmp	Pair the InformaCast Appliance’s embedded SNMP agent with your own Network Management Software to monitor certain aspects of InformaCast Appliance
	“Display Current SNMP Monitoring Configuration” on page 13-32		X	show-snmp-configuration	Display your current SNMP configuration
	“Restart SNMP Monitoring Service” on page 13-34		X	snmp-service disable snmp-service enable	Stop and start the InformaCast Appliance’s SNMP monitoring service
	“Remove Current SNMP Monitoring Configuration” on page 13-35		X	remove-snmp-configuration	Reset your SNMP monitoring configuration to its default values
	“Show the InformaCast Appliance's Network Configuration” on page 13-36		X	show-network-configuration	Display the current network configuration for the on-premises server
	“Change the InformaCast Appliance’s IP Address” on page 13-37		X	configure-network	Change the InformaCast Appliance's IP address
	“Change the InformaCast Appliance’s Hostname” on page 13-41	X			Change the InformaCast Appliance's hostname
	“Restart the Network” on page 13-43		X	restart-network	Load and apply the IP configuration from your InformaCast Appliance's disk
	“List Current NTP Servers” on page 13-44		X	show-time-configuration	Display the configured NTP server(s)
	“Change NTP Servers” on page 13-45		X	configure-time	Change your NTP server(s)

Category	Name	Webmin	CLI	Command	Description
	“Display ntpd State and InformaCast's Sync Status” on page 13-47		X	show-time-status	Display the current state of the NTP daemon and whether the InformaCast Appliance is in sync with it
	“Set the IGMP Version” on page 13-49		X	set-ipv4-igmp-version 2 set-ipv4-igmp-version 3	Force the kernel to use either IGMPv2 or IGMPv3 on interface eth0 for IPv
Problem Reporting and Troubleshooting					
	“Display the Current State of Your Firewall” on page 13-51		X	show-firewall	Display the current state of your firewall
	“Capture InformaCast Appliance Network Traffic” on page 13-53	X			Capture network traffic to/from the InformaCast Appliance
	“Display System Health Information” on page 13-54		X	show-system-health	Display the status of several metrics in the InformaCast Appliance Fusion, e.g. disk utilization, network connection, system services, etc.
	“Access the InformaCast Appliance’s Logs” on page 13-62	X	X	follow-log-<log_name>	View the different logs available to you
	“Collect the InformaCast Appliance’s Logs” on page 13-67	X	X	collect-logs	Collect the InformaCast Appliance’s logs and send them to Singlewire Support
	“Redact IP Addresses in Logs” on page 13-72		X	redact-last-log-bundle	Replace IP addresses in the last-collected log bundle with placeholders, e.g. IPADDRESS_1
	“Display InformaCast's Phone Cache” on page 13-74		X	show-phone-caches	Display InformaCast's encrypted phone cache in a human-readable format
	Send logs to a local server		X	configure-logging	Send various InformaCast logs to your local syslog server

Category	Name	Webmin	CLI	Command	Description
	Display InformaCast's logging configuration		X	show-logging	Display InformaCast's logging configuration, such as whether you've enabled the sending of InformaCast's logs to a local server or live logging
	“Show Technical Support Information” on page 13-82		X	show-tech-support	Display the information that Singlewire Support will need to aid you in troubleshooting
	“Enable the Singlewire Support Account” on page 13-84		X	enable-support disable-support	Allow Singlewire Support to access your InformaCast Appliance through its built-in account, and after they've finished helping you, disable Singlewire Support's access your InformaCast Appliance through its built-in account
	“Display Your Consent Token” on page 13-88		X	show-latest-consent-token	Display a consent token to use in securing your communication to Cisco TAC
	“Display a List of Processes Running on the InformaCast Appliance” on page 13-90	X			Display a list of processes running on the InformaCast Appliance
	“Show Monit Status” on page 13-92		X	show-monit-status	Show the status of monit, a service controller
	“Show the InformaCast Appliance's Version” on page 13-94		X	show-version	Display the InformaCast Appliance's version
	“Show the Appliance Type” on page 13-95		X	show-appliance-type	Display the hardware or virtualization hypervisor on which your InformaCast Appliance is running
	“Show the BIOS Version” on page 13-96		X	show-bios-version	Display the BIOS version your InformaCast Appliance is running

Security and Passwords

Category	Name	Webmin	CLI	Command	Description
	“Change the InformaCast Appliance’s Password” on page 13-98	X	X	passwd	Change the InformaCast Appliance's password
	“Recover Your OS and Application Passwords” on page 13-101		X	recovery	Recover your OS and Application passwords
	“Disable/Enable Password Recovery” on page 13-110		X	configure-recovery	Disable/enable the ability to recover your OS and Application passwords
	“Change the Security Passphrase” on page 13-114		X	change-security-passphrase	Change the passphrase you set during your initial configuration
	“Set Allowed SSL Protocols” on page 13-117		X	configure-ssl-parameters	Set your cryptographic protocols to provide authentication and data encryption between network servers, machines, and applications
	“Display Remote SSL Certificates” on page 13-121		X	show-certificate-from-network	Obtain copies of SSL certificates from remote-network-connected servers
	“Import a Signed SSL Certificate to InformaCast's SIP Certificate Store” on page 13-122		X	import-ssl-cert-to-sip-store	Import a signed SSL certificate into InformaCast's SIP certificate store to use SIP over TLS
	“Create and Install a Signed Certificate” on page 13-125		X	create-certificate-signing-request import-signed-certificate	Create a public key and certificate to protect yourself against Man-in-the-Middle (MITM) attacks, and then import a certificate (or a chain of certificates) signed and provided by your Certificate Authority
	“Display Your Trusted Certificates” on page 13-131		X	show-trusted-certificates	Display the certificates that your InformaCast Appliance trusts, either signed or self-signed

Category	Name	Webmin	CLI	Command	Description
	“Display Your Local Trust” on page 13-133		X	show-local-trust	Display the state of trust between the InformaCast Appliance and the currently installed certificate and trusted certificates
	“Remove Added Trust Certificates” on page 13-134		X	remove-all-user-added-trust-ed-certificates	Remove any Certificate Authority root and intermediate certificates that you've added
	Revert to a self-signed certificate		X	regenerate-ssl-certificates	Revert to a self-signed certificate, remove your previous signed certificate, and keep the Certificate Authority root and intermediate certificates
Upgrade, Backup, Restore, and Reset					
	“Upgrade InformaCast Appliance” on page 13-139	X			Upgrade your InformaCast Appliance to the latest version
	“Switch Virtual Appliance Versions” on page 13-179		X	switch-version	Switch between versions of the InformaCast Appliance
	“Return the InformaCast Appliance to its Original System State” on page 13-180		X	factory-reset	Return your InformaCast Appliance to its original system state

## Manage the InformaCast Appliance's Actions

Stopping, starting, and restarting services and rebooting or shutting down the InformaCast Appliance are management actions you can perform through Webmin or the command-line interface.

### Webmin

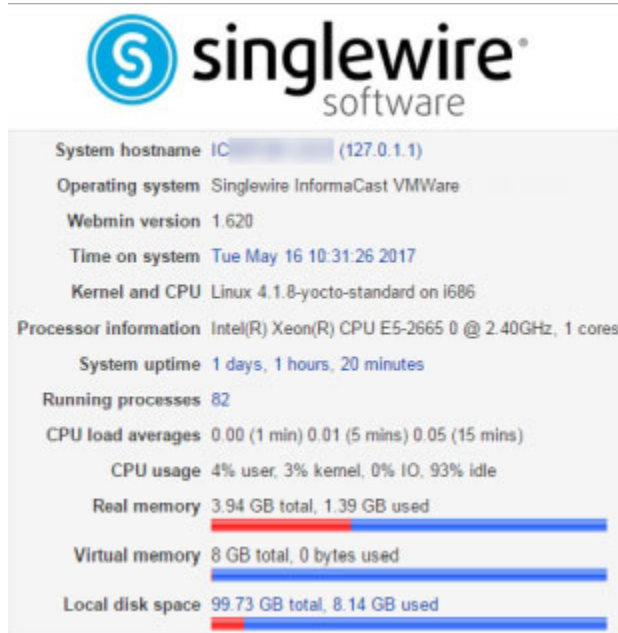
Through Webmin, you can stop/start/restart services running on the InformaCast Appliance and reboot or shut down the server itself.



## Stop a Service on the InformaCast Appliance

Follow these steps to stop individual services on the InformaCast Appliance.

- Step 1** Log into Webmin (see “Log into Webmin” on page 3-14 for specific steps). The Webmin homepage appears.



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

### Bootup and Shutdown

Boot system : SysV init

Action	At boot?	Description
<input type="checkbox"/> apache2	Yes	Apache web server and request router
<input type="checkbox"/> ntpd	Yes	Network Time Protocol (NTP) server and client
<input type="checkbox"/> shibd	Yes	Single Sign On Service
<input type="checkbox"/> singlewireInformaCast	Yes	InformaCast service from Singlewire
<input type="checkbox"/> singlewirePTT	Yes	PushToTalk service from Singlewire
<input type="checkbox"/> singlewireSyncer	No	Syncer service from Singlewire
<input type="checkbox"/> singlewireToolbox	Yes	Toolbox service from Singlewire
<input type="checkbox"/> slpspeaker	Yes	Singlewire SIP Speaker Service, powered by Asterisk
<input type="checkbox"/> vmttoolsd	Yes	Manages services needed to run Open VM Tools

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

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

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

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

The screenshot shows the 'Edit Action' page for the service 'singlewireInformaCast'. The page has a blue header with 'Module Index' on the left and 'Edit Action' in the center. Below the header is a blue bar labeled 'Action Details'. Under this bar, the 'Name' field contains 'singlewireInformaCast'. The 'Action Script' field contains the following text:

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

# Author: [REDACTED]
#

# Do NOT "set -e"

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

Below the script, there is a 'Start at boot time?' section with two radio buttons: 'Yes' and 'No'. The 'No' button is selected. At the bottom of the form are five buttons: 'Save', 'Start Now', 'Show Status', 'Stop Now', and 'Delete'. Below the buttons is a blue arrow pointing left with the text 'Return to bootup and shutdown actions'.

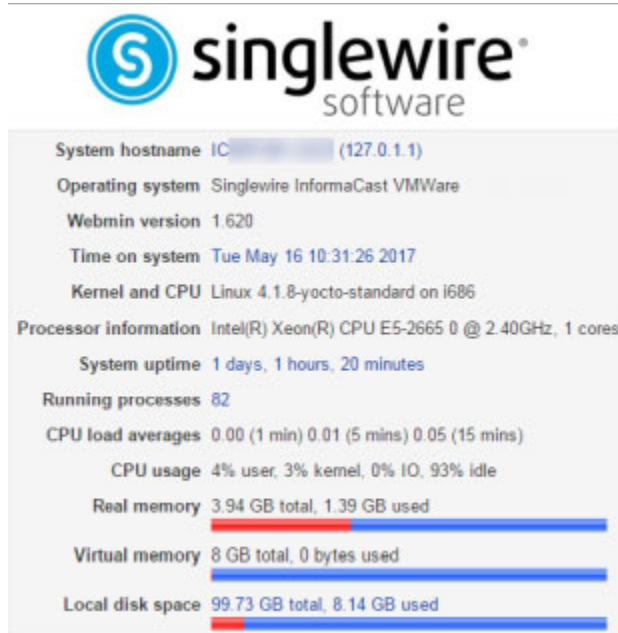
- Step 4** Click the **Stop Now** button. It will take a minute or so for the service to stop.

The screenshot shows the 'Stop Action' page. It has a blue header with 'Module Index' on the left and 'Stop Action' in the center. Below the header, the text 'Executing /etc/init.d/singlewireInformaCast stop ..' is displayed.

### Start a Service on the InformaCast Appliance

Follow these steps to start individual services on the InformaCast Appliance.

- Step 1** Log into Webmin (see “Log into Webmin” on page 3-14 for specific steps). The Webmin homepage appears.



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

### Bootup and Shutdown

Boot system : SysV init

Action	At boot?	Description
<input type="checkbox"/> apache2	Yes	Apache web server and request router
<input type="checkbox"/> ntpd	Yes	Network Time Protocol (NTP) server and client
<input type="checkbox"/> shibd	Yes	Single Sign On Service
<input type="checkbox"/> singlewireInformaCast	Yes	InformaCast service from Singlewire
<input type="checkbox"/> singlewirePTT	Yes	PushToTalk service from Singlewire
<input type="checkbox"/> singlewireSyncer	No	Syncer service from Singlewire
<input type="checkbox"/> singlewireToolbox	Yes	Toolbox service from Singlewire
<input type="checkbox"/> slpspeaker	Yes	Singlewire SIP Speaker Service, powered by Asterisk
<input type="checkbox"/> vmttoolsd	Yes	Manages services needed to run Open VM Tools

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

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

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

Module Index Edit Action

---

**Action Details**

Name:

Action Script

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

# Author: © 2007 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
#

# Do NOT "set -e"

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

Start at boot time?  Yes  No

Save Start Now Show Status Stop Now Delete

[Return to bootup and shutdown actions](#)

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

Module Index Start Action

---

Executing /etc/init.d/singlewireInformaCast start ..

[Return to action](#)

### *Restart a Service on the InformaCast Appliance*

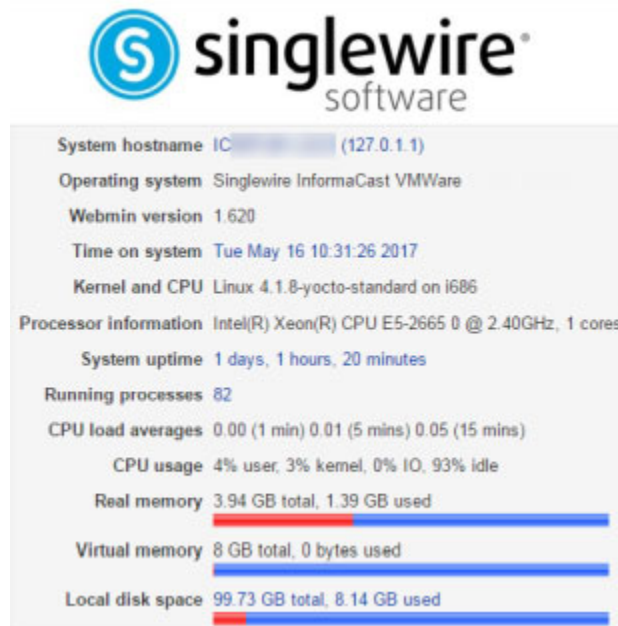
Changing the InformaCast Appliance's IP address or hostname all require you to restart the singlewireInformaCast service. The singlewireInformaCast service is a Linux service that manages recipients, e.g. Cisco IP phones for Unified CM. Linux services are a set of processes running in the background 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 3-14 for specific steps). The Webmin homepage appears.



The screenshot shows the Singlewire software Webmin homepage. At the top is the Singlewire logo. Below it, a box displays system information:

- System hostname: IC (127.0.1.1)
- Operating system: Singlewire InformaCast VMWare
- Webmin version: 1.620
- Time on system: Tue May 16 10:31:26 2017
- Kernel and CPU: Linux 4.1.8-yocto-standard on i686
- Processor information: Intel(R) Xeon(R) CPU E5-2665 0 @ 2.40GHz, 1 cores
- System uptime: 1 days, 1 hours, 20 minutes
- Running processes: 82
- CPU load averages: 0.00 (1 min) 0.01 (5 mins) 0.05 (15 mins)
- CPU usage: 4% user, 3% kernel, 0% IO, 93% idle
- Real memory: 3.94 GB total, 1.39 GB used (with a red progress bar)
- Virtual memory: 8 GB total, 0 bytes used (with a blue progress bar)
- Local disk space: 99.73 GB total, 8.14 GB used (with a red progress bar)

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

### Bootup and Shutdown

Boot system : SysV init

Action	At boot?	Description
<input type="checkbox"/> apache2	Yes	Apache web server and request router
<input type="checkbox"/> ntpd	Yes	Network Time Protocol (NTP) server and client
<input type="checkbox"/> shibd	Yes	Single Sign On Service
<input type="checkbox"/> singlewireInformaCast	Yes	InformaCast service from Singlewire
<input type="checkbox"/> singlewirePTT	Yes	PushToTalk service from Singlewire
<input type="checkbox"/> singlewireSyncer	No	Syncer service from Singlewire
<input type="checkbox"/> singlewireToolbox	Yes	Toolbox service from Singlewire
<input type="checkbox"/> sipspeaker	Yes	Singlewire SIP Speaker Service, powered by Asterisk
<input type="checkbox"/> vmttoolsd	Yes	Manages services needed to run Open VM Tools

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

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

- Step 3** Scroll down the list of actions until you come to your service'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.

[Module Index](#)    **Restarting Actions**

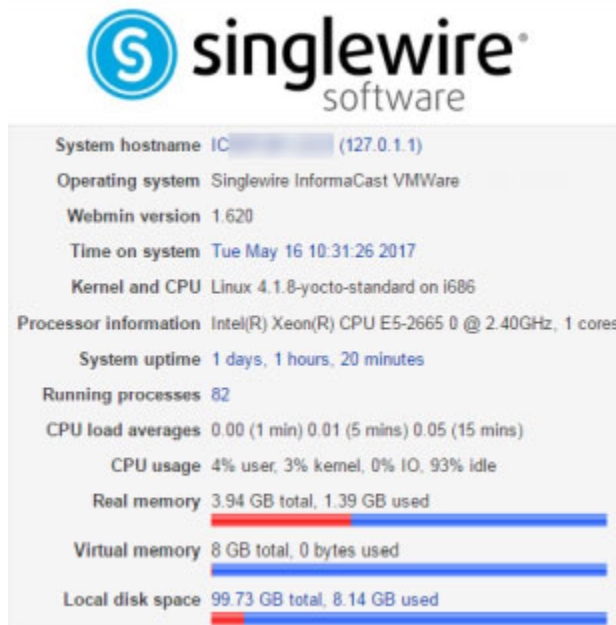
```
Executing /etc/init.d/singlewireInformaCast restart ..
Restarting InformaCast: singlewireInformaCast
```

It will take a minute for your service to restart.

### *Reboot the InformaCast Appliance*

Follow these steps to reboot the InformaCast Appliance.

- Step 1** Log into Webmin (see “Log into Webmin” on page 3-14 for specific steps). The Webmin homepage appears.



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

### Bootup and Shutdown

Boot system : SysV init

Action	At boot?	Description
<input type="checkbox"/> apache2	Yes	Apache web server and request router
<input type="checkbox"/> ntpd	Yes	Network Time Protocol (NTP) server and client
<input type="checkbox"/> shibd	Yes	Single Sign On Service
<input type="checkbox"/> singlewireInformaCast	Yes	InformaCast service from Singlewire
<input type="checkbox"/> singlewirePTT	Yes	PushToTalk service from Singlewire
<input type="checkbox"/> singlewireSyncer	No	Syncer service from Singlewire
<input type="checkbox"/> singlewireToolbox	Yes	Toolbox service from Singlewire
<input type="checkbox"/> sipspeaker	Yes	Singlewire SIP Speaker Service, powered by Asterisk
<input type="checkbox"/> vmttoolsd	Yes	Manages services needed to run Open VM Tools

---

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

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

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

[Module Index](#)

## Reboot

Are you sure you want to reboot the system with the command `reboot` ?

[Return to bootup and shutdown actions](#)

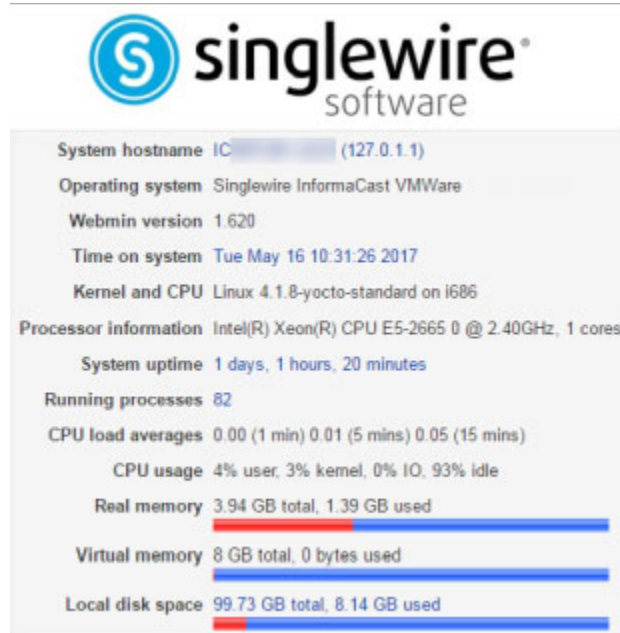
**Step 4** Click the **Reboot System** button. The server will shutdown, then restart.



## Shut Down the InformaCast Appliance

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

- Step 1** Log into Webmin (see “Log into Webmin” on page 3-14 for specific steps). The Webmin homepage appears.



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

### Bootup and Shutdown

Boot system : SysV init

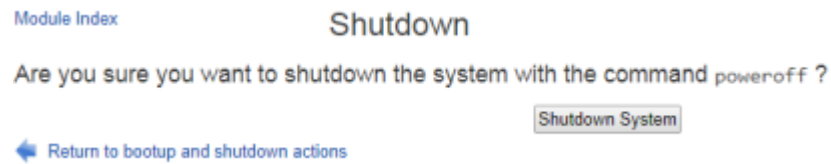
Action	At boot?	Description
<input type="checkbox"/> apache2	Yes	Apache web server and request router
<input type="checkbox"/> ntpd	Yes	Network Time Protocol (NTP) server and client
<input type="checkbox"/> shibd	Yes	Single Sign On Service
<input type="checkbox"/> singlewireInformaCast	Yes	InformaCast service from Singlewire
<input type="checkbox"/> singlewirePTT	Yes	PushToTalk service from Singlewire
<input type="checkbox"/> singlewireSyncer	No	Syncer service from Singlewire
<input type="checkbox"/> singlewireToolbox	Yes	Toolbox service from Singlewire
<input type="checkbox"/> slpspeaker	Yes	Singlewire SIP Speaker Service, powered by Asterisk
<input type="checkbox"/> vmttoolsd	Yes	Manages services needed to run Open VM Tools

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

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

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





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

### Command-line Interface

Through the command-line interface, you can stop/start/restart services running on the InformaCast Appliance and reboot or restart the InformaCast Appliance itself. The services you can stop/start/restart include:

- `apache-service`
- `controlcenter-service`
- `informacast-service`
- `lighttpd-service`
- `ntp-service`
- `pushtotalk-service`
- `sipspeaker-service`
- `snmp-service`
- `ssh-service`
- `vmtools-service` (for InformaCast Virtual Appliances only)
- `webmin-service`

## Stop a Service

Follow these steps to stop individual services on the InformaCast Appliance.

- Step 1** Log into the command-line interface (see “Log into the Command-line Interface” on page 3-16). The command-line interface appears, showing you that you’re logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$
```

- Step 2** Enter the name of the service you want to stop, e.g. **informacast-service disable** at the prompt and press the **Enter** key. The command-line interface refreshes and the singlewireInformaCast service stops.

```
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:~$ informacast-service disable
Stopping InformaCast: singlewireInformaCast ... requesting that InformaCast stop
...
InformaCast has stopped
Success
InformaCast will not start at boot
admin@singlewire:~$
```

*Start a Service*

Follow these steps to start individual services on the InformaCast Appliance.

- Step 1** Log into the command-line interface (see “Log into the Command-line Interface” on page 3-16). The command-line interface appears, showing you that you’re logged in.

```

login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$

```

- Step 2** Enter name of the service you want to start, e.g. **informacast-service enable** at the prompt and press the **Enter** key. The command-line interface refreshes and the singlewireInformaCast service starts.

```

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:~$ informacast-service enable
InformaCast will start at boot, starting
Starting InformaCast: singlewireInformaCast ... InformaCast has been started.
Success
admin@singlewire:~$

```

*Restart a Service***Note**

JTAPI automatically updates every time the singlewireInformaCast service is restarted.

- Step 1** Log into the command-line interface (see “Log into the Command-line Interface” on page 3-16). The command-line interface appears, showing you that you’re logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun 2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$
```

- Step 2** Enter name of the service you want to restart, e.g. **informacast-service restart** at the prompt and press the **Enter** key. The command-line interface refreshes and the singlewireInformaCast service restarts.

```
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:~$ informacast-service restart
Restarting InformaCast: singlewireInformaCast ... requesting that InformaCast st
op...
InformaCast has stopped
InformaCast has been started.
Success
admin@singlewire:~$
```

## Reboot the InformaCast Appliance

Follow these steps to reboot the InformaCast Appliance.

- Step 1** Log into the command-line interface (see “Log into the Command-line Interface” on page 3-16). The command-line interface appears, showing you that you’re logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun 2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$
```

- Step 2** Enter **restart-appliance** at the prompt and press the **Enter** key. The command-line interface refreshes and your InformaCast Appliance reboots.

```
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:~$ restart-appliance
Rebooting appliance immediately

Broadcast message from root@singlewire (pts/0) (Wed Aug 30 13:34:49 2017):
The system is going down for reboot NOW!
admin@singlewire:~$
```

### Shut Down the InformaCast Appliance

Follow these steps to shut down the InformaCast Appliance.

- Step 1** Log into the command-line interface (see “Log into the Command-line Interface” on page 3-16). The command-line interface appears, showing you that you’re logged in.

```

login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$

```

- Step 2** Enter `halt-appliance` at the prompt and press the **Enter** key. The command-line interface refreshes.

```

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:~$ halt-appliance
Halting appliance immediately
admin@singlewire:~$
Broadcast message from root@singlewire (pts/0) (Wed Aug 30 13:45:50 2017):
The system is going down for system halt NOW!

```



#### Tip

Once shut down, to start an InformaCast Virtual Appliance, you'll need to log into vSphere, right click your server, and select **Power** | **Power On**. For an InformaCast Physical Appliance, you'll need to unplug it, plug it in again, and press the **Power** button.

## Test the InformaCast Appliance's Connectivity

Testing the InformaCast Appliance's connectivity allows you to verify connectivity between the InformaCast Appliance and:

- The default gateway through Address Resolution Protocol (ARP)
- The default gateway via ICMP ping

**Step 1** Log into the command-line interface (see “Log into the Command-line Interface” on page 3-16). The command-line interface appears, showing you that you're logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$
```

**Step 2** Enter **test-network-connectivity** at the prompt and press the **Enter** key. The command-line interface refreshes with the results of its test.

```
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:~$ test-network-connectivity
Pinging the default gateway... OK
admin@singlewire:~$
```

When a test fails, the detailed test logs are printed, which aid the troubleshooting process.

## Show Multicast Statistics

Available only in the command-line interface, `show-multicast-statistics` displays kernel-level information about the current multicast groups joined on each interface and the IGMP version in use. Verifying your multicast traffic can aid in troubleshooting network issues.

- Step 1** Log into the command-line interface (see “Log into the Command-line Interface” on page 3-16). The command-line interface appears, showing you that you’re logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$
```



- Step 2** Enter `show-multicast-statistics` at the prompt and press the **Enter** key. The command-line interface refreshes with details on your multicast traffic.

```
login as: admin
admin's password:
Last login: Thu Feb 21 18:42:37 2019

Welcome to Singlewire Paging Gateway Vltware

admin@PagingGateway:~$ show-multicast-statistics
IGMP statistics:
Idx   Device   : Count Querier      Group   Users Timer      Reporter
1     lo       :    1    V3          010000E0  1 0:00000000  0
2     eth0    :    2    V2          FDFFFFFF  1 0:00000000  1
                010000E0  1 0:00000000  0

Group statistics:
IPv6/IPv4 Group Memberships
Interface  RefCnt Group
-----
lo         1     224.0.0.1
eth0      1     239.255.255.253
eth0      1     224.0.0.1
lo         1     ff02::1
lo         1     ff01::1
eth0      1     ff02::1
eth0      1     ff01::1
sit0      1     ff02::1
sit0      1     ff01::1

IPv4 IGMP version currently in use for eth0:
2
IPv4 IGMP version set at boot for eth0:
net.ipv4.conf.eth0.force_igmp_version = 2
0 = highest available IGMP version
2 = IGMPv2
3 = IGMPv3
admin@PagingGateway:~$
```

## 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 rebuild of Cisco IP phones for Unified CM succeeded, the count of registered IP speakers, 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. 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 rebuild of Cisco IP phones for Unified CM started	20180805071459, yyyy-mm-dd hh:mm:ss
1.3.6.1.4.1.3137.1.1.1.2.4.2.0	Last time the rebuild of Cisco IP phones for Unified CM succeeded	19691231180000, yyyy-mm-dd hh:mm:ss
1.3.6.1.4.1.3137.1.1.1.2.4.3.0	Next time an update of Cisco IP phones for Unified CM is scheduled	20180805081000, yyyy-mm-dd hh:mm:ss
1.3.6.1.4.1.3137.1.1.1.2.4.4.0	Cisco IP phones 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

OID	Data	Example
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 InformaCast Appliance.

InformaCast MIBs can be found in three locations:

- /usr/local/singlewire/InformaCast/web/resources/mib/ on the InformaCast Appliance
- As a downloadable ZIP on Singlewire's website
- Through a link to the InformaCast Appliance:
  - <https://<InformaCast Appliance IP Address>:8444/InformaCast/resources/mib/BERBEE-APPLICATIONS-IPT-INFORMACAST.html>
  - <https://<InformaCast Appliance IP Address>:8444/InformaCast/resources/mib/BERBEE-APPLICATIONS-IPT-INFORMACAST.pdf>
  - <https://<InformaCast 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 InformaCast Appliance
- SNMP over D/TLS; 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 13-26
- “Display Current SNMP Monitoring Configuration” on page 13-32
- “Restart SNMP Monitoring Service” on page 13-34
- “Remove Current SNMP Monitoring Configuration” on page 13-35

### 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 rebuild of Cisco IP phones for Unified CM 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 3-16). The command-line interface appears, showing you that you’re logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun 2 10:15:02 2020

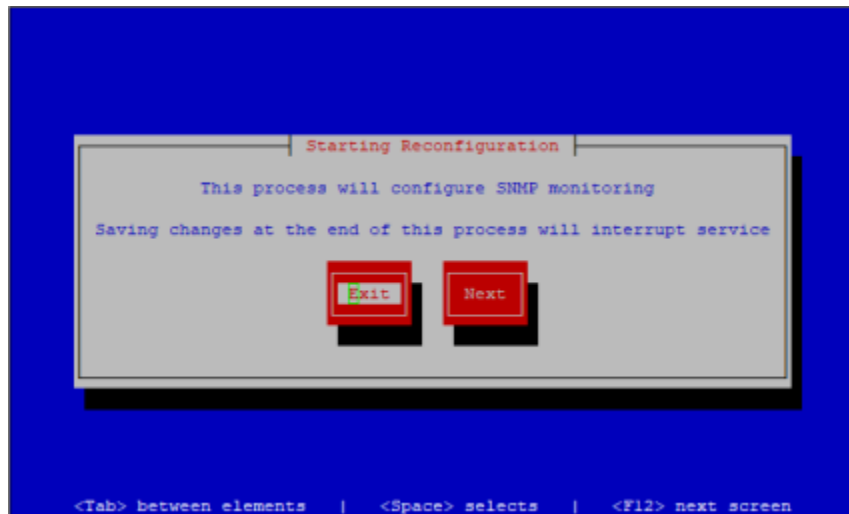
Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

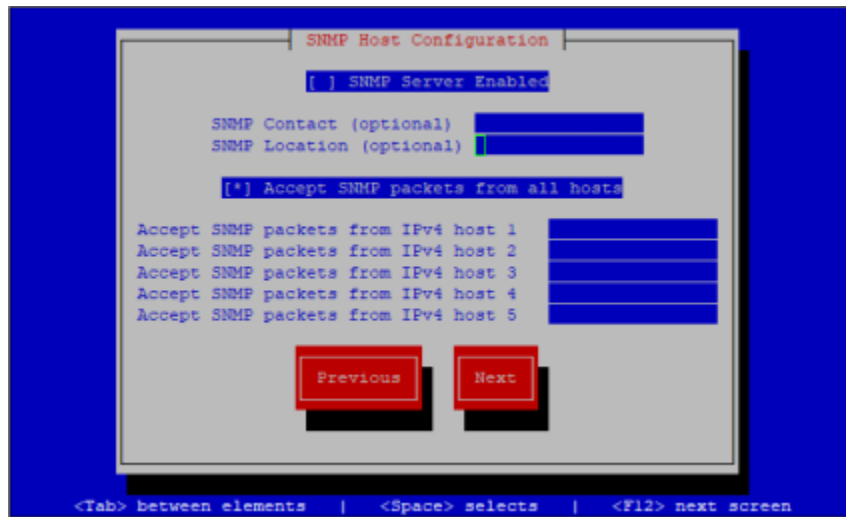
This build is 0 days old

admin@singlewire:~$
```

- 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.

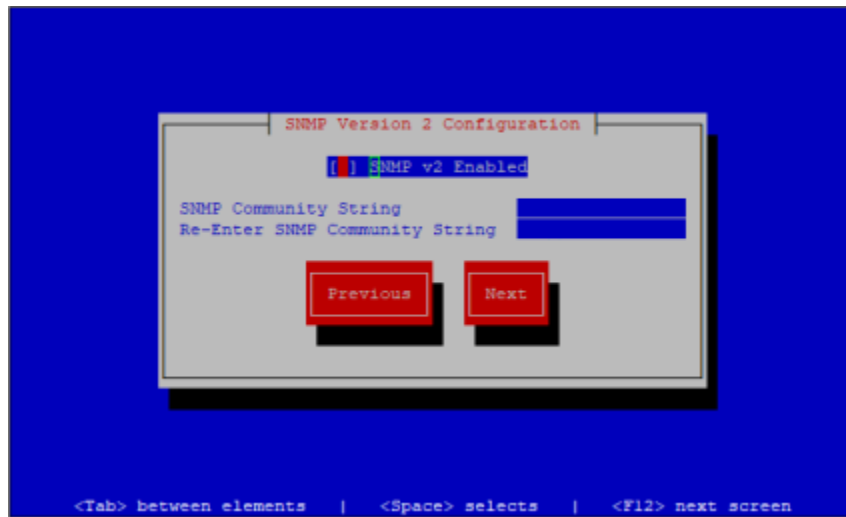
- Step 5** Press the **Tab** key to enter the **SNMP Contact** field and enter your SNMP contact's information, e.g. John Lennon, SNMP Admin (optional).
- Step 6** Press the **Tab** key to enter the **SNMP Location** field and enter your SNMP contact's location, e.g. Madison (optional).
- Step 7** Press 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.



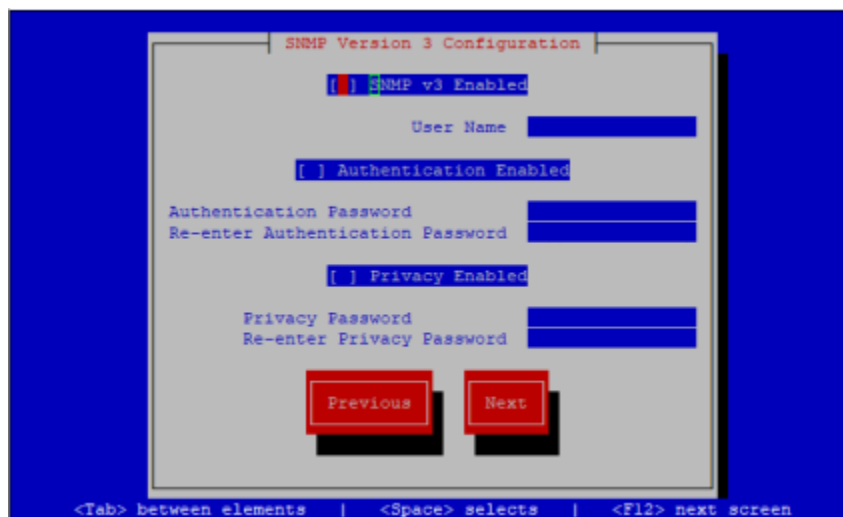
**Note** While you are allowed to add up to five SNMP hosts, if you are using SNMPv2, they must all use the same community string.

- 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.

```
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:~$ configure-snmp
Stopping network management services: snmpd.
SNMP daemon will start at boot, starting
Starting network management services: snmpd.
Restarting network management services:Stopping network management services: snm
pd.

admin@singlewire:~$
```

## 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 3-16). The command-line interface appears, showing you that you’re logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun 2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$
```

- 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 -- * * .4 0.0.0.0/0
udp dpt:161 /* SNMP traffic from 172.30.222.4 */
0 0 ACCEPT udp -- * * .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: .4
Accept SNMP host address 2: .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 3-16). The command-line interface appears, showing you that you're logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$
```

- 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.

```
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 disable
Stopping network management services: snmpd.
SNMP daemon will not start at boot

admin@singlewire:~$
```

- 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 3-16). The command-line interface appears, showing you that you’re logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

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:~$
```

---

## Show the InformaCast Appliance's Network Configuration

The **show-network-configuration** command displays the current configuration of your InformaCast Appliance's on-premises server's Paging Gateway's network.

- Step 1** Log into the command-line interface (see “Log into the Command-line Interface” on page 3-16). The command-line interface appears, showing you that you’re logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun 2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$
```

- Step 2** Enter `show-network-configuration` at the prompt and press the Enter key. The command-line interface refreshes with your current network configuration, e.g. your InformaCast Appliance's IP address, subnet mask, hardware address, 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-network-configuration
eth0      Link encap:Ethernet  HWaddr 00:50:
          inet addr:          Bcast:0.0.0.0  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3002218 errors:0 dropped:94 overruns:0 frame:0
          TX packets:1042530 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:38117058430 (35.4 GiB)  TX bytes:139912409 (133.4 MiB)

admin@singlewire:~$
```

## Change the InformaCast Appliance's IP Address

You set the static IP address for your InformaCast Appliance when you installed InformaCast (see “Deploy InformaCast” on page 2-17), but you may need to change it.



### Note

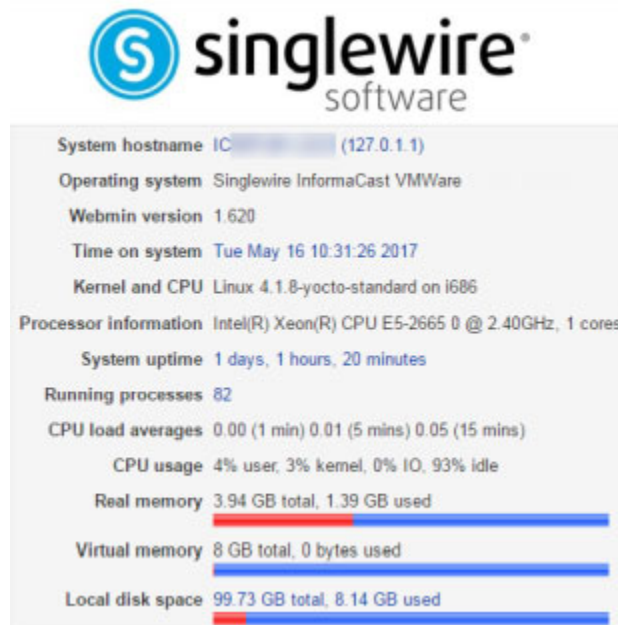
Complete the steps in this topic before making any changes to your network, e.g. changing the virtual network assigned to the VMware virtual NIC or the upstream network configuration for the assigned virtual network.



### 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 2-17).**

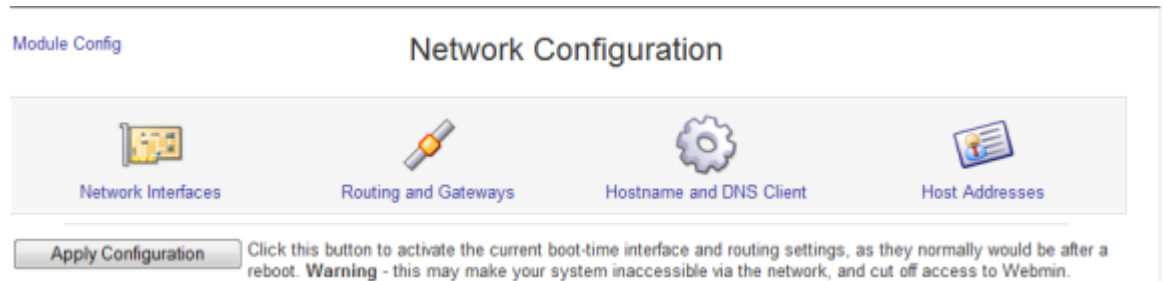
- Step 1** Log into Webmin (see “Log into Webmin” on page 3-14 for specific steps). The Webmin homepage appears.



The screenshot shows the Singlewire software Webmin homepage. At the top is the Singlewire logo. Below it, a grey box displays system information:

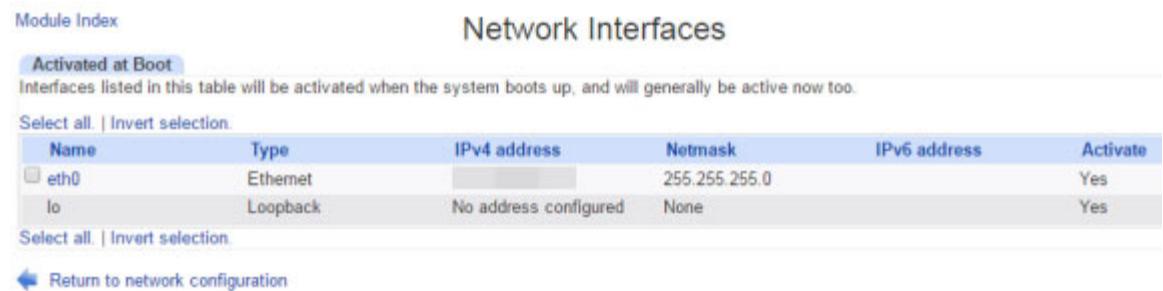
- System hostname: IC (127.0.1.1)
- Operating system: Singlewire InformaCast VMWare
- Webmin version: 1.620
- Time on system: Tue May 16 10:31:26 2017
- Kernel and CPU: Linux 4.1.8-yccto-standard on i686
- Processor information: Intel(R) Xeon(R) CPU E5-2665 0 @ 2.40GHz, 1 cores
- System uptime: 1 days, 1 hours, 20 minutes
- Running processes: 82
- CPU load averages: 0.00 (1 min) 0.01 (5 mins) 0.05 (15 mins)
- CPU usage: 4% user, 3% kernel, 0% IO, 93% idle
- Real memory: 3.94 GB total, 1.39 GB used (with a red progress bar)
- Virtual memory: 8 GB total, 0 bytes used (with a blue progress bar)
- Local disk space: 99.73 GB total, 8.14 GB used (with a red progress bar)

- Step 2** Go to **Networking | Network Configuration**. The Network Configuration page appears.



The screenshot shows the Network Configuration page in Webmin. The page title is "Network Configuration". Below the title are four icons representing different network settings: Network Interfaces, Routing and Gateways, Hostname and DNS Client, and Host Addresses. At the bottom of the page is an "Apply Configuration" button with a warning message: "Click this button to activate the current boot-time interface and routing settings, as they normally would be after a reboot. Warning - this may make your system inaccessible via the network, and cut off access to Webmin."

- Step 3** Click the **Network Interfaces** icon. The Network Interfaces page refreshes.



The screenshot shows the Network Interfaces page in Webmin. The page title is "Network Interfaces". Below the title is a section titled "Activated at Boot" with a sub-header "Interfaces listed in this table will be activated when the system boots up, and will generally be active now too." Below this is a table with columns: Name, Type, IPv4 address, Netmask, IPv6 address, and Activate. The table contains two rows: eth0 (Ethernet, 255.255.255.0) and lo (Loopback, No address configured). Below the table are links for "Select all." and "Invert selection." and a "Return to network configuration" button.

Name	Type	IPv4 address	Netmask	IPv6 address	Activate
<input type="checkbox"/> eth0	Ethernet		255.255.255.0		Yes
lo	Loopback	No address configured	None		Yes



**Step 4** Click the **eth0** link. The Edit Bootup Interface page appears.

Module Index **Edit Bootup Interface**

**Boot Time Interface Parameters**

Name eth0

Activate at boot? Yes

Static configuration

IPv4 address

Netmask 255.255.255.0

Broadcast  Automatic

IPv6 addresses  IPv6 disabled

MTU  Default

Hardware address  Default

[Return to network interfaces](#)

**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.

Module Index **Routing and Gateways**

**Boot time configuration**

This section allows you to configure the routes that are activated when the system boots up, or when network settings are fully re-applied.

**Routing configuration activated at boot time**

Default router  Gateway 172.30.228.1 eth0

Static routes	Interface	Network	Netmask	Gateway
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Local routes	Interface	Network	Netmask
	<input type="text"/>	<input type="text"/>	<input type="text"/>

[Return to network configuration](#)

**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 InformaCast Appliance (see “Reboot the InformaCast Appliance” on page 13-12).

**Step 14** Log into Cisco Unified CM, 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 Cisco IP phones for Unified CM 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 Cisco Unified CMs in your InformaCast environment (see “Install the InformaCast SIP Certificate on Cisco Unified CM” on page 8-64).



---

**Note** If you are using SIP over TLS, you will need to install InformaCast's SIP certificate on all SIP system servers in your InformaCast environment.

---

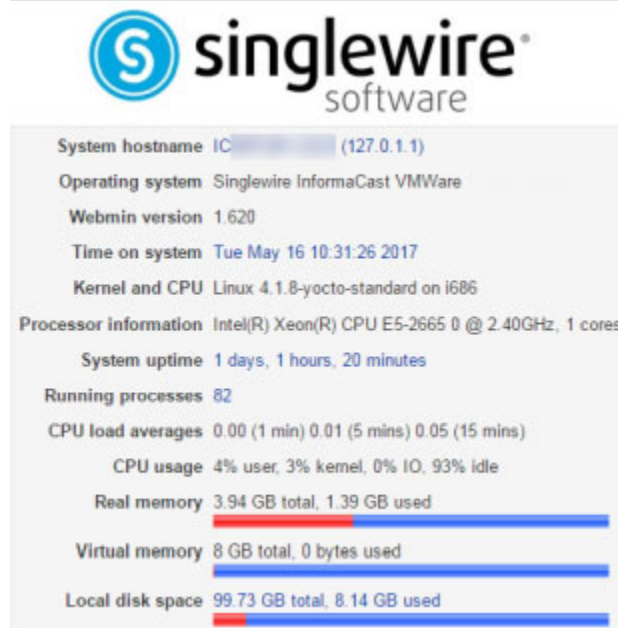
**Step 15** Reset all of your Cisco IP phones for Unified CM.

---

## Change the InformaCast Appliance's Hostname

You set your InformaCast Appliance's hostname when you installed InformaCast (see “Deploy InformaCast” on page 2-17), but you may need to change it.

- Step 1** Log into Webmin (see “Log into Webmin” on page 3-14 for specific steps). The Webmin homepage appears.



- Step 2** Go to **Networking | Network Configuration**. The Network Configuration page appears.

The screenshot shows the Network Configuration page in Webmin. The page title is "Network Configuration" under the "Module Config" section. Below the title are four main configuration options, each with an icon and a label:

- Network Interfaces (with a network card icon)
- Routing and Gateways (with a fiber optic cable icon)
- Hostname and DNS Client (with a gear icon)
- Host Addresses (with a document icon)

At the bottom of the page, there is an "Apply Configuration" button and a warning message: "Click this button to activate the current boot-time interface and routing settings, as they normally would be after a reboot. **Warning** - this may make your system inaccessible via the network, and cut off access to Webmin."

**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 InformaCast 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 InformaCast Appliance will restart. This may take some time. Until the restart has completed, some of InformaCast's features may be inoperable.

## Restart the Network

The **restart-network** command will load and apply the IP configuration from your InformaCast Appliance's disk. Restarting your network stack is used to make a network change take effect or as a step in troubleshooting.

- Step 1** Log into the command-line interface (see “Log into the Command-line Interface” on page 3-16). The command-line interface appears, showing you that you’re logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$
```

- Step 2** Enter **restart-network** at the prompt and press the **Enter** key. Your network stack will be restarted and your IP configuration from your InformaCast Appliance's disk will be loaded and applied.

## 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 2-31). 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 3-16). The command-line interface appears, showing you that you’re logged in.

```

login as: admin
admin@singlewire's password:
Last login: Tue Jun 2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$

```

- 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:          ntpl.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 3-16). The command-line interface appears, showing you that you’re logged in.

```

login as: admin
admin@singlewire's password:
Last login: Tue Jun 2 10:15:02 2020

Welcome to Singlewire InformaCast

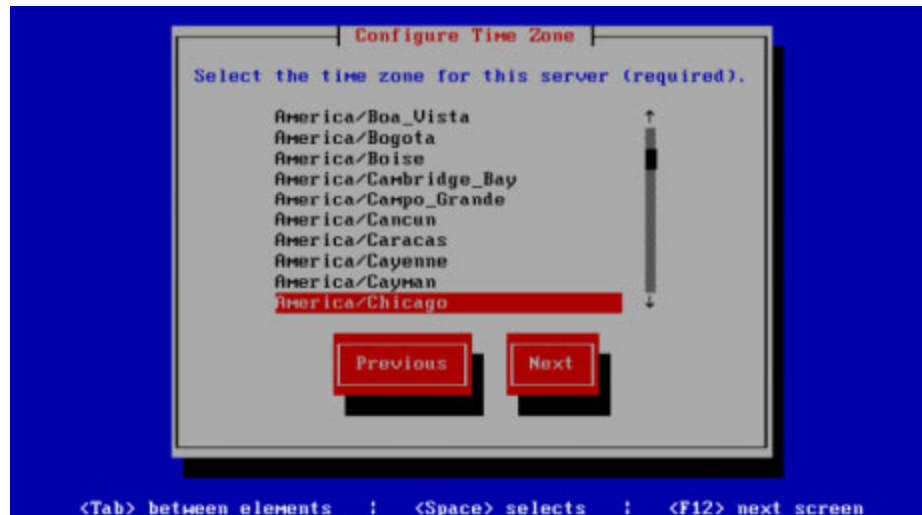
Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$

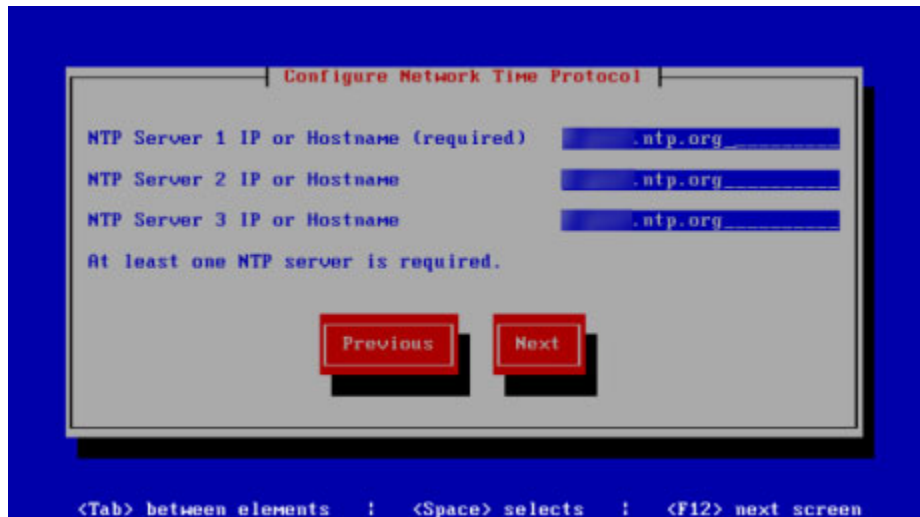
```

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

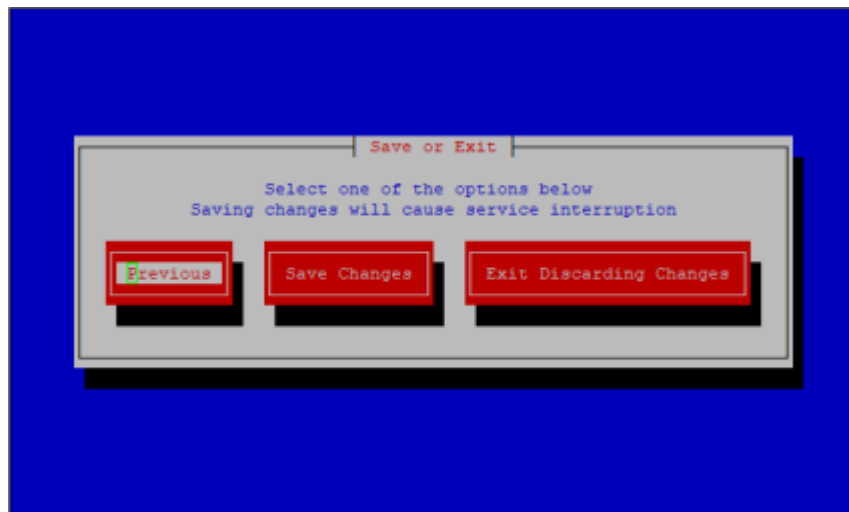


- Step 3** Use the arrow keys to select a time zone for your InformaCast Appliance server.

- 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 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 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 3-16). The command-line interface appears, showing you that you’re logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun 2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$
```

- 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 at t when poll reach delay offset jitter
-----
ntp1.singlewire.lan
.POOL. 46666 16 p - 64 0 0.000 0.000 0.000
*fit-sw1-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 0811 yes none none reject mobilize 1
2 46667 163a no yes none sys_peer sys_peer 3

admin@singlewire: ~$

```

## Set the IGMP Version

If you have network routing restrictions that require you to use one version or the other, you can use the command, **set-ipv4-igmp-version**, to force the kernel to use either IGMPv2 or IGMPv3 on interface eth0 for IPv4.

- Step 1** Log into the command-line interface (see “Log into the Command-line Interface” on page 3-16). The command-line interface appears, showing you that you’re logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$
```

- Step 2** Enter `set-ipv4-igmp-version 2` or `set-ipv4-igmp-version 3` at the prompt and press the **Enter** key. **2** forces the kernel to use IGMPv2 and **3** forces the kernel to use IGMPv3 on interface eth0 for ipv4. The command-line interface refreshes with your new network information.

```
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:~$ set-ipv4-igmp-version 3
Forced IGMP IPv4 on eth0 to version 3
net.ipv4.conf.eth0.force_igmp_version = 3

IGMP statistics:
Idx   Device   : Count Querier      Group   Users Timer      Reporter
1     lo       :    2      V3             4B4B00E0  1 0:00000000  0
                               010000E0  1 0:00000000  0
2     eth0    :    3      V3             FDFFFFFF  1 0:00000000  0
                               4B4B00E0  1 0:00000000  0
                               010000E0  1 0:00000000  0

Group statistics:
IPv6/IPv4 Group Memberships
Interface  RefCnt Group
-----
lo         1     224.0.75.75
lo         1     224.0.0.1
eth0      1     239.255.255.253
eth0      1     224.0.75.75
eth0      1     224.0.0.1
lo         1     ff02::1
lo         1     ff01::1
eth0      1     ff02::1
eth0      1     ff01::1
sit0      1     ff02::1
sit0      1     ff01::1

IPv4 IGMP version currently in use for eth0:
3
IPv4 IGMP version set at boot for eth0:
net.ipv4.conf.eth0.force_igmp_version = 3
0 = highest available IGMP version
2 = IGMPv2
3 = IGMPv3
admin@singlewire:~$
```

## Display the Current State of Your Firewall

Viewing the current state of your firewall can aid in troubleshooting, but is also useful when verifying the security of your network.

- Step 1** Log into the command-line interface (see “Log into the Command-line Interface” on page 3-16). The command-line interface appears, showing you that you’re logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$
```

- Step 2** Enter **show-firewall** at the prompt and press the **Enter** key. The command-line interface refreshes with your firewall's data.

```

login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Wed Aug 30 15:01:24 2017

Welcome to Singlewire InformaCast

Running on VMware
Licensed as Purchased

admin@singlewire:~$ show-firewall

Filter filter:

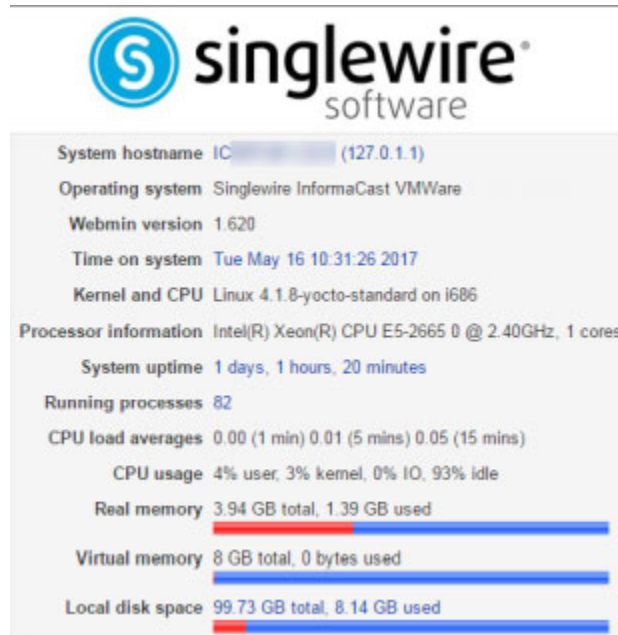
Chain INPUT (policy DROP 714 packets, 83538 bytes)
pkts bytes target      prot opt in      out     source      destination
545K 2321M ACCEPT    all  --  *      *       0.0.0.0/0    0.0.0.0/0
    ctstate RELATED,ESTABLISHED
    0 ACCEPT    tcp  --  *      *       0.0.0.0/0    0.0.0.0/0
    tcp dpts:16384:16634 /* LPI plugin pseudo-speaker connections */
    0 ACCEPT    udp  --  *      *       0.0.0.0/0    0.0.0.0/0
    udp dpts:32568:32768 /* CallAware plugin RTP for call recording */
    0 ACCEPT    tcp  --  *      *       0.0.0.0/0    0.0.0.0/0
    tcp dpt:8201 /* ICAP inbound https interface */
    0 ACCEPT    udp  --  *      *       0.0.0.0/0    0.0.0.0/0
    state ESTABLISHED /* M2M plugin SNMP responses */
    0 ACCEPT    udp  --  *      *       0.0.0.0/0    0.0.0.0/0
    udp dpt:1162 /* M2M plugin SNMP traps */
    0 ACCEPT    tcp  --  *      *       0.0.0.0/0    0.0.0.0/0
    tcp dpt:5060 /* InformaCast SIP non-secure */
    0 ACCEPT    udp  --  *      *       0.0.0.0/0    0.0.0.0/0
    udp dpt:5060 /* InformaCast SIP non-secure */
    0 ACCEPT    tcp  --  *      *       0.0.0.0/0    0.0.0.0/0
    tcp dpt:5061 /* InformaCast SIP secure */
    0 ACCEPT    udp  --  *      *       0.0.0.0/0    0.0.0.0/0
    udp dpt:1161 /* InformaCast SNMP responses */
    0 ACCEPT    tcp  --  *      *       127.0.0.1    0.0.0.0/0
    tcp dpt:8005 /* InformaCast Tomcat communication, localhost only */
201 12060 ACCEPT    tcp  --  *      *       0.0.0.0/0    0.0.0.0/0
    tcp dpt:8081 /* InformaCast http interface */
    0 ACCEPT    tcp  --  *      *       0.0.0.0/0    0.0.0.0/0
    tcp dpt:8444 flags:0x02/0x02 limit: up to 25/sec burst 1500 mode srcip-
dstport /* Allow in https sessions under limit */
    0 LOG      tcp  --  *      *       0.0.0.0/0    0.0.0.0/0
    tcp dpt:8444 flags:0x02/0x02 limit: avg 1/min burst 1 /* Log deny https
TCP requests over limit */ LOG flags 0 level 4 prefix " Exceeded InformaCast ht
tps h"
    0 DROP     tcp  --  *      *       0.0.0.0/0    0.0.0.0/0
    tcp dpt:8444 flags:0x02/0x02 /* Deny https TCP requests over limit */
    0 ACCEPT    tcp  --  *      *       0.0.0.0/0    0.0.0.0/0
    tcp dpt:8444 /* InformaCast https interface */
22588 1788K ACCEPT    udp  --  *      *       0.0.0.0/0    0.0.0.0/0
    udp dpt:427 /* SLP inbound */

```

## Capture InformaCast 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 InformaCast Appliance.

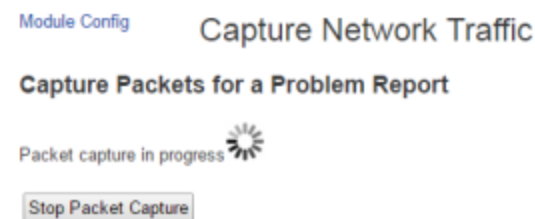
- Step 1** Log into Webmin (see “Log into Webmin” on page 3-14 for specific steps). The Webmin homepage appears.



- 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 InformaCast Appliance’s Logs” on page 13-67. The collection of logs will include the packet capture you just performed as well as the InformaCast Appliance’s other logs.

---

## Display System Health Information

Available only through the command-line interface, `show-system-health` displays the status of several metrics in the InformaCast:

- **Clock.** Whether the InformaCast is synchronized with specified NTP network servers (see “Set the Initial Configuration” on page 2-31 for more information).
- **Disk Utilization.** Whether the InformaCast is approaching full disk utilization, i.e. running out of the disk space required to perform InformaCast actions such as sending.
- **Network.** Whether the InformaCast is connected to the network.
- **System Services.** Whether the InformaCast's collection of services is running, e.g. Apache, SSH daemon, `singlewireInformaCast`.
- **System Resources.** Whether OS resources, such as memory or data structures, are too heavily utilized (or nearly too heavily utilized) and should be resolved.
- **Overall.** An amalgam of all previous metrics.

Each metric is paired with a measurement of its health, e.g. GREEN, YELLOW, or RED. If a metric is GREEN, everything is running as expected; the system is healthy. If a metric is YELLOW, the system is impacted, but will still be delivered. You should investigate this metric when you have the time. If a metric is RED, delivery is impacted. You should investigate and remediate this metric immediately.

Checking your system health can aid in troubleshooting network issues.



- Step 1** Log into the command-line interface (see “Log into the Command-line Interface” on page 3-16 for more information). The command-line interface appears, showing you that you’re logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$
```

- Step 2** Enter **show-system-health** at the prompt and press the **Enter** key. The command-line interface refreshes with details on your system health.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$ show-system-health
This command displays aggregate system health information

Clock           GREEN
Disk Utilization GREEN
Network         GREEN
Services        GREEN
System Resources GREEN
Overall         GREEN

admin@singlewire:~$
```

In this example, all metrics measured by InformaCast Fusion are GREEN, i.e. healthy.

This command displays aggregate system health information

Clock	GREEN
Disk Utilization	GREEN
Network	GREEN
System Services	GREEN
System Resources	GREEN
Overall	GREEN

In cases where a metric is RED, i.e. unhealthy, your results may look like the following example.

This command displays aggregate system health information

```
Clock                RED
Disk Utilization     GREEN
Network              GREEN
System Services      RED
System Resources     GREEN
Overall              RED
```

```
Red alarm(s) present. Administrator should take immediate action. Message
delivery is impacted.
```

```
RED alarms cause:
```

```
AL-NTPS Clock is unsynchronized with NTP server
```

```
AL-NTPSV Network time service is stopped
```

```
Each cause is preceded by a cause tag. You can find information in the
documentation on how to address each cause by searching the documentation
for a cause tag.
```

Note that when any metric is RED (or YELLOW), the Overall metric is also RED (or YELLOW).

When a metric is either RED or YELLOW, a cause tag and failure reason appear below the metrics' statuses. The following table details these cause tags and failure reasons along with whose responsibility it is to remediate the failure and the manner in which remediation can occur.

Cause Tag	Failure Reason	Who can address the situation?	What should be done?
AL-ACTS	The Activation service is stopped	You	Reboot the InformaCast Appliance (see “Reboot the InformaCast Appliance” on page 13-12 for more information). Contact Cisco TAC for assistance if rebooting is unsuccessful.
AL-APAS	The Apache web service is stopped	You	Enter <b>apache-service start</b> or <b>reboot</b> in the CLI. Contact Cisco TAC for assistance if restarting the Apache service is unsuccessful.
AL-APPRO	The app partition is not mounted as read-only	You	Reboot the InformaCast Appliance (see “Reboot the InformaCast Appliance” on page 13-12 for more information). Contact Cisco TAC for assistance if rebooting is unsuccessful.
AL-CONSH	The console shell is stopped	You	Reboot the InformaCast Appliance (see “Reboot the InformaCast Appliance” on page 13-12 for more information). Contact Cisco TAC for assistance if rebooting is unsuccessful.

<b>Cause Tag</b>	<b>Failure Reason</b>	<b>Who can address the situation?</b>	<b>What should be done?</b>
AL-CONSM	The console message service is stopped	You	Reboot the InformaCast Appliance (see “Reboot the InformaCast Appliance” on page 13-12 for more information). Contact Cisco TAC for assistance if rebooting is unsuccessful.
AL-CONSV	The Console service is stopped	You	Reboot the InformaCast Appliance (see “Reboot the InformaCast Appliance” on page 13-12 for more information). Contact Cisco TAC for assistance if rebooting is unsuccessful.
AL-CRONS	The system scheduler is stopped	You	Reboot the InformaCast Appliance (see “Reboot the InformaCast Appliance” on page 13-12 for more information). Contact Cisco TAC for assistance if rebooting is unsuccessful.
AL-DAFULL	Your data partition is more than 95% in use	You	Reduce your data retention period (see “Broadcast Parameters Management” on page 7-1 for more information) or contact Cisco TAC for assistance.
AL-DARO	Your data partition is not mounted read-write	You	Reboot the InformaCast Appliance (see “Reboot the InformaCast Appliance” on page 13-12 for more information). Contact Cisco TAC for assistance if rebooting is unsuccessful.
AL-ETHDIS	Ethernet is disconnected from the InformaCast	You	Connect the virtual machine or physical to the network.
AL-F2BS	The security monitoring service is stopped	You	Reboot the InformaCast Appliance (see “Reboot the InformaCast Appliance” on page 13-12 for more information). Contact Cisco TAC for assistance if rebooting is unsuccessful.
AL-FWS	The firewall monitoring service is stopped	You	Reboot the InformaCast Appliance (see “Reboot the InformaCast Appliance” on page 13-12 for more information). Contact Cisco TAC for assistance if rebooting is unsuccessful.
AL-HEAP	Heap dumps are present	Cisco TAC	Contact Cisco TAC for assistance and collect logs (see “Collect the InformaCast Appliance’s Logs” on page 13-67 for more information).

Cause Tag	Failure Reason	Who can address the situation?	What should be done?
AL-ICBA	The size of InformaCast's backups directory is too large	Cisco TAC	Contact Cisco TAC for assistance and collect logs (see “Collect the InformaCast Appliance’s Logs” on page 13-67 for more information).
AL-ICCTIPAUT H	The InformaCast CTI provider could not authenticate to Cisco Unified CM	You	Change the application user credentials used by InformaCast to match those configured in Cisco Unified CM or reconfigure both to use new credentials. Contact Cisco TAC for assistance if reconfiguration is unsuccessful.
AL-ICCTIPOOS	The InformaCast CTI connection is out of service	You	Enter <b>test-network-connectivity</b> in the CLI and investigate why InformaCast cannot connect to Cisco Unified CM over the network: <ul style="list-style-type: none"> <li>• Is the communication path between InformaCast and Cisco Unified CM available?</li> <li>• Can you ping Cisco Unified CM from InformaCast?</li> <li>• Is there a WAN or VPN connection or firewall that could be down that might account for this lack of connectivity?</li> </ul> Contact Cisco TAC for assistance if your investigation is unsuccessful.
AL-ICDB	The size of InformaCast's database is too large	You	Reduce your data retention period (see “Broadcast Parameters Management” on page 7-1 for more information) and check the metric's status after 4:00 a.m. the morning after your change or contact Cisco TAC for assistance.
AL-ICFD	InformaCast's file descriptor consumption is too high	You	Enter <b>informacast-service restart</b> in the CLI. Contact Cisco TAC for assistance if restarting the singlewireInformaCast service is unsuccessful.
AL-ICLOG	The size of InformaCast's logs are too large	Cisco TAC	Contact Cisco TAC for assistance and collect logs (see “Collect the InformaCast Appliance’s Logs” on page 13-67 for more information).
AL-ICMSPACE	The Java Virtual Machine Metaspace is nearly exhausted	Cisco TAC	Contact Cisco TAC for assistance and collect logs (see “Collect the InformaCast Appliance’s Logs” on page 13-67 for more information).

<b>Cause Tag</b>	<b>Failure Reason</b>	<b>Who can address the situation?</b>	<b>What should be done?</b>
AL-ICS	The InformaCast service is stopped	You	Enter <b>informacast-service restart</b> in the CLI. Contact Cisco TAC for assistance if restarting the singlewireInformaCast service is unsuccessful.
AL-ICTHR	InformaCast's thread consumption is too high	You	Contact Cisco TAC for assistance.
AL-ICUPL	The size of InformaCast's uploads directory is too large	Cisco TAC	Contact Cisco TAC for assistance and collect logs (see “Collect the InformaCast Appliance’s Logs” on page 13-67 for more information).
AL-LICM	The license mode monitor is stopped	You	Reboot the InformaCast Appliance (see “Reboot the InformaCast Appliance” on page 13-12 for more information). Contact Cisco TAC for assistance if rebooting is unsuccessful.
AL-MONS	The service supervisor service is stopped	You	Reboot the InformaCast Appliance (see “Reboot the InformaCast Appliance” on page 13-12 for more information). Contact Cisco TAC for assistance if rebooting is unsuccessful.
AL-NTPS	InformaCast's clock isn't synchronized with its assigned NTP server	You	Enter <b>ntp-service restart</b> in the CLI. Contact Cisco TAC for assistance if restarting the NTP service is unsuccessful.
AL-NTPSV	The network time service is stopped	You	Enter <b>ntp-service restart</b> in the CLI. Contact Cisco TAC for assistance if restarting the NTP service is unsuccessful.
AL-PCPC	The PCP collector daemon is stopped	You	Reboot the InformaCast Appliance (see “Reboot the InformaCast Appliance” on page 13-12 for more information). Contact Cisco TAC for assistance if rebooting is unsuccessful.
AL-PCPD	The size of the PCP data directory is too large	Cisco TAC	Contact Cisco TAC for assistance and collect logs (see “Collect the InformaCast Appliance’s Logs” on page 13-67 for more information).
AL-PCPL	The PCP logger is stopped	You	Reboot the InformaCast Appliance (see “Reboot the InformaCast Appliance” on page 13-12 for more information). Contact Cisco TAC for assistance if rebooting is unsuccessful.

Cause Tag	Failure Reason	Who can address the situation?	What should be done?
AL-PMIE	The PCP inference engine is stopped	You	Reboot the InformaCast Appliance (see “Reboot the InformaCast Appliance” on page 13-12 for more information). Contact Cisco TAC for assistance if rebooting is unsuccessful.
AL-RANS	The random number seeding service is stopped	You	Reboot the InformaCast Appliance (see “Reboot the InformaCast Appliance” on page 13-12 for more information). Contact Cisco TAC for assistance if rebooting is unsuccessful.
AL-ROTLS	The rotate logs service is stopped	You	Reboot the InformaCast Appliance (see “Reboot the InformaCast Appliance” on page 13-12 for more information). Contact Cisco TAC for assistance if rebooting is unsuccessful.
AL-SLOGS	The remote syslog service is stopped	You	Reboot the InformaCast Appliance (see “Reboot the InformaCast Appliance” on page 13-12 for more information). Contact Cisco TAC for assistance if rebooting is unsuccessful.
AL-SLOGS	The remote syslog service is stopped	You	Reboot the InformaCast Appliance (see “Reboot the InformaCast Appliance” on page 13-12 for more information). Contact Cisco TAC for assistance if rebooting is unsuccessful.
AL-SSH	The secure shell service is stopped	You	Enter <b>ssh-service restart</b> in the CLI. Contact Cisco TAC for assistance if restarting the SSH service is unsuccessful.
AL-STATS	The Status screen service is stopped	You	Reboot the InformaCast Appliance (see “Reboot the InformaCast Appliance” on page 13-12 for more information). Contact Cisco TAC for assistance if rebooting is unsuccessful.
AL-SWAPF	The swap partition is not available or is full	You	Reboot the InformaCast Appliance (see “Reboot the InformaCast Appliance” on page 13-12 for more information). Contact Cisco TAC for assistance if rebooting is unsuccessful.

Cause Tag	Failure Reason	Who can address the situation?	What should be done?
AL-SYNCLOG	The size of the Syncer log's directory is too large	Cisco TAC	Contact Cisco TAC for assistance and collect logs (see “Collect the InformaCast Appliance’s Logs” on page 13-67 for more information).
AL-SYSLOG	The size of the System log's directory is too large	Cisco TAC	Contact Cisco TAC for assistance and collect logs (see “Collect the InformaCast Appliance’s Logs” on page 13-67 for more information).
AL-TBXS	Control Center is stopped	You	Enter <b>controlcenter-service restart</b> in the CLI.  Contact Cisco TAC for assistance if restarting the Control Center service is unsuccessful.
AL-UDEV	The device daemon is stopped	You	Reboot the InformaCast Appliance (see “Reboot the InformaCast Appliance” on page 13-12 for more information).  Contact Cisco TAC for assistance if rebooting is unsuccessful.
AL-UPDMON	The resource update monitor daemon is stopped	You	Reboot the InformaCast Appliance (see “Reboot the InformaCast Appliance” on page 13-12 for more information).  Contact Cisco TAC for assistance if rebooting is unsuccessful.
AL-UPGRW	The upgrade partition is not mounted as read-write	You	Reboot the InformaCast Appliance (see “Reboot the InformaCast Appliance” on page 13-12 for more information).  Contact Cisco TAC for assistance if rebooting is unsuccessful.
AL-VMT	The VMware tools service is stopped	You	Reboot the InformaCast Appliance (see “Reboot the InformaCast Appliance” on page 13-12 for more information).  Contact Cisco TAC for assistance if rebooting is unsuccessful.

**Note**

System health is calculated every 60 seconds, and the **show-system-health** command displays the last calculated system health, which means your metric results could be up to 60 seconds old. If you also configure system alarms for your system health metrics, those occur every two minutes, which means there could be up to a two-minute lag between when an event occurs and when an action tied to a system alarm about that event happens.

**Tip**

System health is logged to InformaCast's syslog (see "Access the InformaCast Appliance's Logs" on page 13-62 for more information). It cannot be disabled and it is not configurable.

## Access the InformaCast Appliance's Logs

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

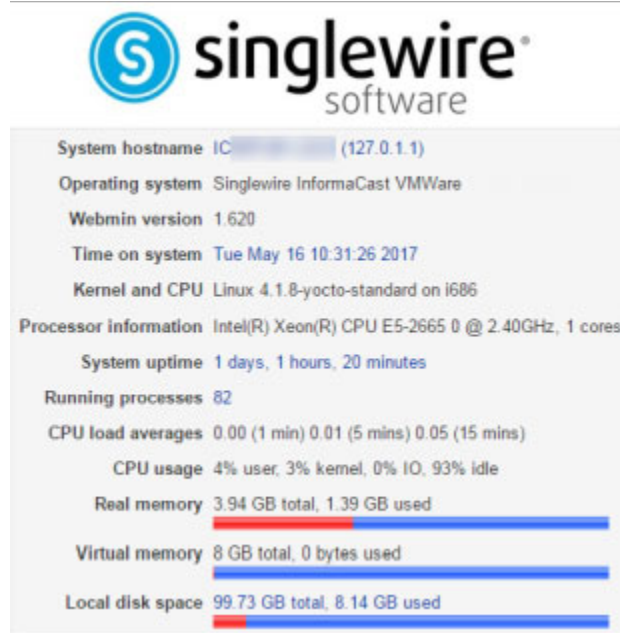
- Various OS logs:
  - File /var/log/auth.log
  - File /var/log/syslog
  - File /var/log/cron.log
  - File /var/log/daemon.log
  - File /var/log/kern.log
  - File /var/log/lpr.log
  - File /var/log/mail.log
  - File /var/log/user.log
  - File /var/log/mail.info
  - File /var/log/mail.warn
  - File /var/log/mail.err
  - 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)



## Webmin

Use Webmin to access InformaCast’s logs.

- Step 1** Log into Webmin (see “Log into Webmin” on page 3-14 for specific steps). The Webmin homepage appears.



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

**System Logs**

Log destination	Active?	Messages selected	
Output from dmesg	Yes	Kernel messages	<a href="#">View..</a>
Output from show-log-paging-gateway	Yes	Paging Gateway Log	<a href="#">View..</a>
File /var/webmin/miniserv.error	Yes	Webmin error log	<a href="#">View..</a>

**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.

```

Module Index
View Logfile
show-log-performance

Last 20 lines of Only show lines with text Refresh
2017-04-04T15:18:19.493-0500 [Thread-46] INFO bd [] - advertising config service: http://172.30.228.21
2017-04-04T15:18:19.493-0500 [Thread-46] INFO UA [] - trying to send a message to any DA, via mcast
2017-04-04T15:18:19.493-0500 [Thread-46] INFO bd [] - advertising SOAP service: http://172.30.228.212:
2017-04-04T15:18:19.493-0500 [Thread-46] INFO UA [] - trying to send a message to any DA, via mcast
2017-04-04T15:18:21.529-0500 [pool-42-thread-1] INFO EventSubscriptionCenter [] - Submitted 1 tasks fo
2017-04-04T15:18:22.525-0500 [pool-41-thread-1] INFO EventSubscriptionCenter [] - Submitted 1 tasks fo
2017-04-04T15:18:22.752-0500 [0000003B9DD3-registration-cycle--at-15:18:22] INFO ag [] - Starting regi
2017-04-04T15:18:22.752-0500 [0000003B9DD3-registration-cycle--at-15:18:22] INFO U [] - Endpoint is be
2017-04-04T15:18:22.752-0500 [000000D65F8A-registration-cycle--at-15:18:22] INFO ag [] - Starting regi
2017-04-04T15:18:22.752-0500 [000000D65F8A-registration-cycle--at-15:18:22] INFO U [] - Endpoint is be
2017-04-04T15:18:22.775-0500 [0000003B9DD3-registration-task-http://172.30.228.212:8081/InformaCast/adm
2017-04-04T15:18:22.776-0500 [000000D65F8A-registration-task-http://172.30.228.212:8081/InformaCast/adm
2017-04-04T15:18:22.782-0500 [000000D65F8A-registration-task-http://172.30.228.212:8081/InformaCast/adm
2017-04-04T15:18:22.783-0500 [0000003B9DD3-registration-task-http://172.30.228.212:8081/InformaCast/adm
2017-04-04T15:18:23.769-0500 [pool-41-thread-1] INFO EventSubscriptionCenter [] - Submitted 1 tasks fo
2017-04-04T15:19:08.600-0500 [pool-41-thread-1] INFO EventSubscriptionCenter [] - Submitted 1 tasks fo
2017-04-04T15:19:21.531-0500 [pool-42-thread-1] INFO EventSubscriptionCenter [] - Submitted 1 tasks fo
2017-04-04T15:20:21.529-0500 [pool-42-thread-1] INFO EventSubscriptionCenter [] - Submitted 1 tasks fo
2017-04-04T15:21:21.528-0500 [pool-42-thread-1] INFO EventSubscriptionCenter [] - Submitted 1 tasks fo
2017-04-04T15:22:21.531-0500 [pool-42-thread-1] INFO EventSubscriptionCenter [] - Submitted 1 tasks fo

Last 20 lines of Only show lines with text Refresh
Return to system logs

```

## Command-line Interface

Use the command-line interface to access InformaCast's logs.

**Step 1** Log into the command-line interface. The command-line interface appears, showing you that you're logged in.

```

admin@singlewire:~$ login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$

```

**Step 2** Enter one of the following log commands at the prompt and press the **Enter** key:

- follow-log-apache
- follow-log-audit

- follow-log-performance
- follow-log-restore
- follow-log-summary
- follow-log-syslog
- follow-log-backup
- follow-log-restapi
- follow-log-sipstack

In the following example, you're viewing the contents generated by entering **follow-log-performance**.

```

login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Thu Aug 31 13:47:55 2017

Welcome to Singlewire InformaCast

Running on VMware
Licensed as Purchased

admin@singlewire:~$ follow-log-performance
plugins/com.singlewire.plugin.prayertimes/data
2017-08-31T15:21:49.314-0500 [pool-21-thread-1] INFO c [] - getting files to re
plicate from PI extension: com.singlewire.plugin.im.IMStartupExtension@7c29b6, u
sing directory /usr/local/singlewire/InformaCast/web/WEB-INF/plugins/com.singlew
ire.plugins.IM/data
2017-08-31T15:21:49.314-0500 [pool-21-thread-1] INFO c [] - getting files to re
plicate from PI extension: com.singlewire.plugin.legacypaging.LPIStartupExtensio
n@9987bb, using directory /usr/local/singlewire/InformaCast/web/WEB-INF/plugins/
com.singlewire.plugin.legacypaging/data
2017-08-31T15:21:49.314-0500 [pool-21-thread-1] INFO c [] - getting files to re
plicate from PI extension: com.singlewire.plugin.lync.LyncStartupExtension@1e2a1
1, using directory /usr/local/singlewire/InformaCast/web/WEB-INF/plugins/com.siw
glewire.plugin.Lync/data
2017-08-31T15:21:49.314-0500 [pool-21-thread-1] INFO c [] - getting files to re
plicate from PI extension: com.singlewire.plugin.m2m.ContactClosureStartupExtens
ion@68d2f6, using directory /usr/local/singlewire/InformaCast/web/WEB-INF/plugin
s/com.singlewire.plugin.m2m/data
2017-08-31T15:21:49.315-0500 [pool-21-thread-1] INFO c [] - getting files to re
plicate from PI extension: com.singlewire.plugin.nightbell.NightBellStartupExten
sion@117701c, using directory /usr/local/singlewire/InformaCast/web/WEB-INF/plug
ins/com.singlewire.plugin.nightbell/data
2017-08-31T15:21:49.315-0500 [pool-21-thread-1] INFO c [] - getting files to re
plicate from PI extension: com.singlewire.plugin.oep.OEPStartupExtension@1948157
, using directory /usr/local/singlewire/InformaCast/web/WEB-INF/plugins/com.sing
lewire.plugin.oep/data
2017-08-31T15:21:49.315-0500 [pool-21-thread-1] INFO c [] - getting files to re
plicate from PI extension: com.singlewire.plugin.paginggateway.PagingGatewayLife
cycleExtension@1938129, using directory /usr/local/singlewire/InformaCast/web/WE
B-INF/plugins/com.singlewire.informacast.plugins.PagingGateway/data
2017-08-31T15:21:49.315-0500 [pool-21-thread-1] INFO c [] - getting files to re
plicate from PI extension: com.singlewire.plugin.parkandpage.ParkAndPageStartupE
xtension@e47352, using directory /usr/local/singlewire/InformaCast/web/WEB-INF/p
lugins/com.singlewire.plugin.parkandpage/data
2017-08-31T15:21:49.316-0500 [pool-21-thread-1] INFO c [] - getting files to re
plicate from PI extension: com.singlewire.plugin.quickurl.UrlStartupExtension@17
1caad, using directory /usr/local/singlewire/InformaCast/web/WEB-INF/plugins/com
.singlewire.plugin.quickurl/data
2017-08-31T15:21:49.316-0500 [pool-21-thread-1] INFO c [] - getting files to re
plicate from PI extension: com.singlewire.plugin.schoolmessenger.SchoolMessenger
StartupExtension@de4d32, using directory /usr/local/singlewire/InformaCast/web/W
EB-INF/plugins/com.singlewire.plugin.SchoolMessenger/data
2017-08-31T15:21:49.316-0500 [pool-21-thread-1] INFO c [] - getting files to re
plicate from PI extension: com.singlewire.plugin.script.ScriptStartupExtension@f

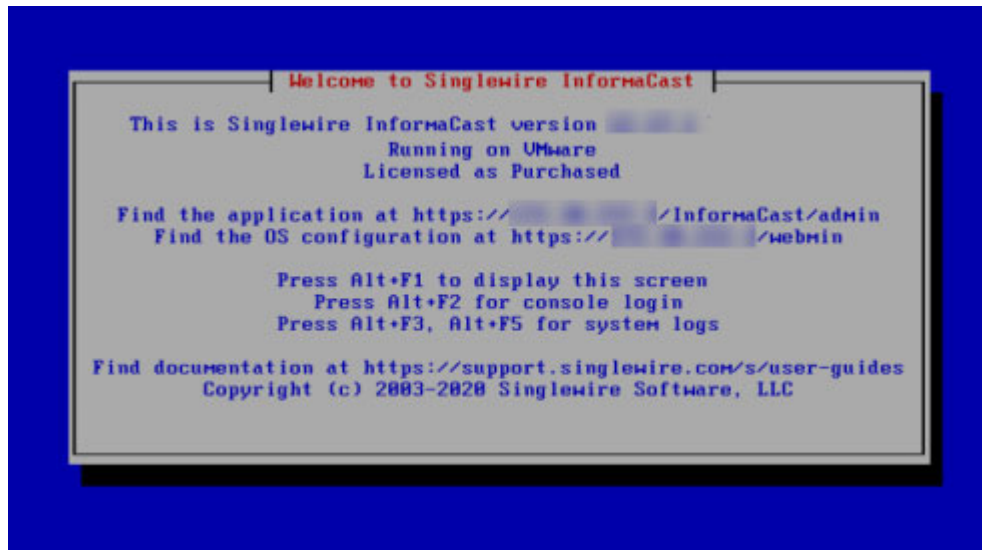
```

## vSphere Interface

Several logs are available on the vSphere console through the function keys:

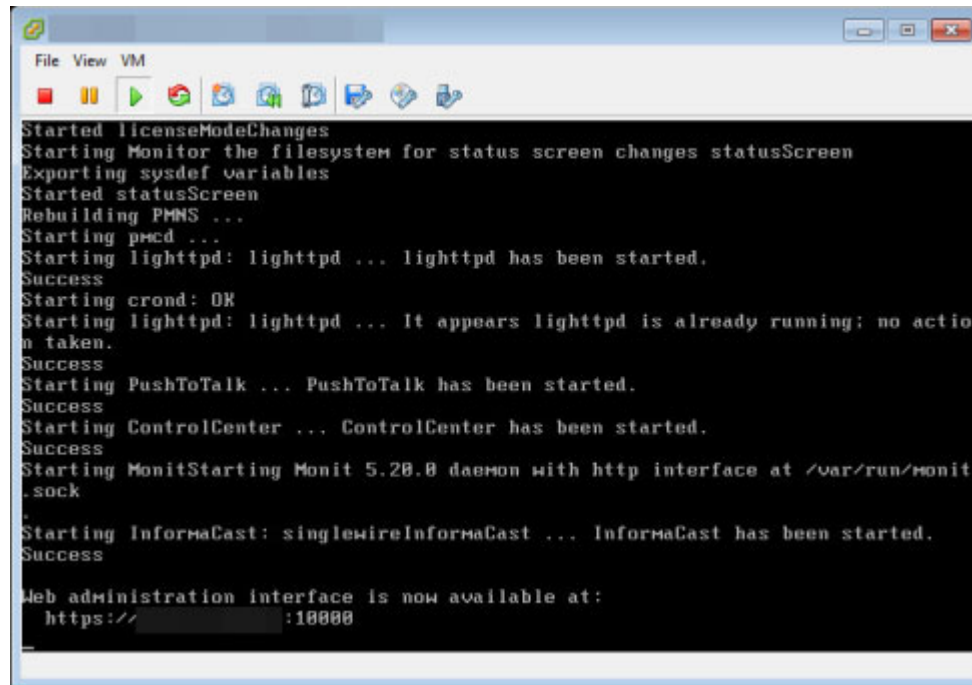
- `/var/log/boot` (viewable by pressing the Alt + F3 keys), which contains service initialization and shutdown information
- `var/log/messages` (viewable on by pressing the Alt + F5 keys), which contains global system messages from kernel and running services

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



**Step 2** Press the **Alt + F3** or **F5** keys to view either the `/var/log/boot` or `/var/log/messages` log, respectively.

In the following example, you're viewing the contents of the `/var/log/boot` log (**Alt + F3**).



```

Started licenseModeChanges
Starting Monitor the filesystem for status screen changes statusScreen
Exporting sysdef variables
Started statusScreen
Rebuilding PMNS ...
Starting pmed ...
Starting lighttpd: lighttpd ... lighttpd has been started.
Success
Starting crond: OK
Starting lighttpd: lighttpd ... It appears lighttpd is already running; no action taken.
Success
Starting PushToTalk ... PushToTalk has been started.
Success
Starting ControlCenter ... ControlCenter has been started.
Success
Starting MonitStarting Monit 5.28.8 daemon with http interface at /var/run/monit.sock
Starting InformaCast: singlewireInformaCast ... InformaCast has been started.
Success
Web administration interface is now available at:
https://[redacted]:18888

```

## Collect the InformaCast Appliance's Logs

If you are having an issue with InformaCast that you cannot resolve without help, it is likely that Cisco TAC will ask for a collection of your logs in order to analyze your problem. The Webmin and the command-line interface offer a way to create a log archive that can be downloaded and emailed to Cisco TAC.

By default, all logs collected and sent to Cisco TAC or downloaded from InformaCast are not encrypted; however, an administrator using the command-line interface can encrypt the logs by appending `--encrypt` to the `collect-logs` command, e.g. **collect-logs --encrypt**.



### Tip

Within unencrypted log bundles are IP addresses that you may not want to expose to anyone outside of your organization. If you're in this situation, you can use the **redact-last-log-bundle** command to replace all IP addresses in your most recent log bundle with placeholders, such as "IPADDRESS\_1" and "IPADDRESS\_2," etc.



### Note

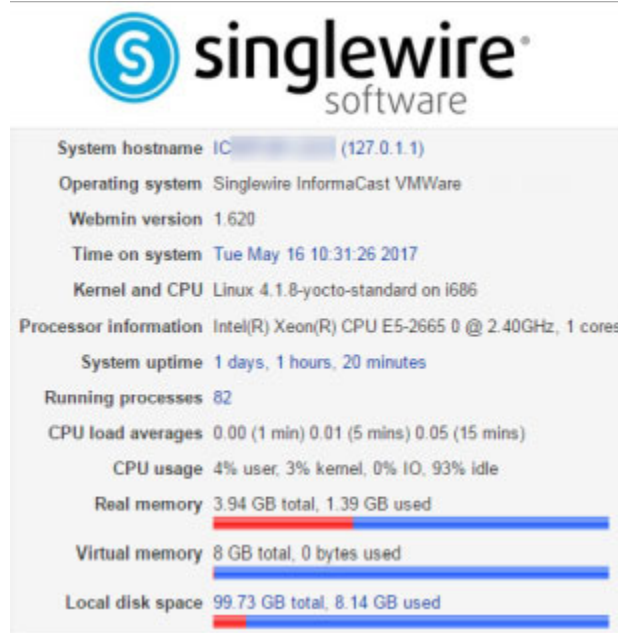
Unencrypted log bundles will not include InformaCast's phone cache data.



## Webmin

Use the following steps to collect the InformaCast Appliance's logs through Webmin.

- Step 1** Log into Webmin (see “Log into Webmin” on page 3-14 for specific steps). The Webmin homepage appears.



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

The screenshot shows the 'Collect Logs' page in the Webmin interface. The page title is 'Collect Logs' and the sub-header is 'Collect a New Set of Logs for a Problem Report'. Below the sub-header, there is a brief instruction: 'This process will produce a package of logs for use by technical support'. The main content area is titled 'Collect New Log Set' and contains the following form fields:

- Problem description to include in report:** A text input field.
- Singlewire support contract number, if known:** A text input field.
- Do not automatically send the log collection to Singlewire Support:** A checkbox that is currently unchecked.
- Collect a new set of logs:** A button to submit the form.

- 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.

Module Config Collect Logs

**Collect a New Set of Logs for a Problem Report**

This process will produce a package of logs for use by technical support

**Collect New Log Set**

Problem description to include in report

Singlewire support contract number, if known

Do not automatically send the log collection to Singlewire Support

**Log Actions**

The log collection from 2016-04-08 14:33:45 was uploaded successfully to Singlewire Support

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.

Module Config Collect Logs

**Collect a New Set of Logs for a Problem Report**

This process will produce a package of logs for use by technical support

**Collect New Log Set**

Problem description to include in report

Singlewire support contract number, if known

Do not automatically send the log collection to Singlewire Support

**Log Actions**

The log collection from 2016-04-08 21:10:03 must be downloaded and sent to Singlewire Support

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

## Command-line Interface

Use the following steps to collect the InformaCast Appliance's logs through the command-line interface.

- Step 1** Log into the command-line interface (see “Log into the Command-line Interface” on page 3-16). The command-line interface appears, showing you that you're logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun 2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$
```

- Step 2** Enter `collect-logs` at the prompt and press the **Enter** key. The command-line interface refreshes.

```
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Thu Aug 31 15:19:40 2017

Welcome to Singlewire InformaCast

Running on VMware
Licensed as Purchased

admin@singlewire:~$ collect-logs
Enter a one line description of your issue:

```



- Step 3** Enter a short description of the problem you're having at the prompt and press the **Enter** key. The command-line interface refreshes.

```
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Thu Aug 31 15:19:40 2017

Welcome to Singlewire InformaCast

Running on VMware
Licensed as Purchased

admin@singlewire:~$ collect-logs
Enter a one line description of your issue:
I can't hear my broadcasts.
Enter your Singlewire support contract number
(leave blank if you don't know):
```

- Step 4** Enter your Singlewire maintenance contract number (if you know it) at the prompt and press the **Enter** key. The command-line interface refreshes and InformaCast begins collecting its logs. When it's finished, the command-line interface refreshes, and if there is no HTTPS proxy server prohibiting its internet access, InformaCast will send the logs to Singlewire.

```
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Thu Aug 31 15:19:40 2017

Welcome to Singlewire InformaCast

Running on VMware
Licensed as Purchased

admin@singlewire:~$ collect-logs
Enter a one line description of your issue:
I can't hear my broadcasts.
Enter your Singlewire support contract number
(leave blank if you don't know):
Collecting logs, please wait

Saving SHA512 of unencrypted log archive to /var/log/lct/LogCollection_PG_20160408-143345_80e3e62b.tgz.sha512

The encrypted logs in /var/log/lct/LogCollection_PG_20160408-143345_80e3e62b.tgz
have been successfully uploaded to Singlewire support

admin@singlewire:~$
```



**Tip**

If sending the logs to Singlewire fails, you can enter the **send-logs-to-singlewire** command to re-run the send portion of the collect-logs command without running the entirety of the command.

If InformaCast can't send the logs to Singlewire Support, the command-line interface will refresh with a location of your compiled logs and suggest that you send them to Singlewire.

```
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Thu Aug 31 15:19:40 2017

Welcome to Singlewire InformaCast

Running on VMware
Licensed as Purchased

admin@singlewire:~$ collect-logs
Enter a one line description of your issue:
I can't hear my broadcasts.
Enter your Singlewire support contract number
(leave blank if you don't know):
Collecting logs, please wait

Saving SH0512 of unencrypted log archive to /var/log/ict/LogCollection_PG_281604
00-163000_61c91273.tgz.sha512

Send the following file to Singlewire support: /var/log/ict/LogCollection_PG_281
60400-163000_61c91273.tgz

admin@singlewire:~$
```

To do this, you'll need to transfer your log file to your computer.

- Step a.** Start a secure file transfer application, such as WinSCP or WinSFTP.
- Step b.** Browse to the directory in which your compiled logs are located.
- Step c.** Copy them to a directory on your computer.
- Step d.** [Email Singlewire Support](#) and attach the log file.

## Redact IP Addresses in Logs

If you are having an issue with InformaCast that you cannot resolve without help, it is likely that Cisco TAC will ask for a collection of your logs in order to analyze your problem. Within these logs are IP addresses that you may not want to expose to anyone outside of your organization. If you're in this situation, you can use the **redact-last-log-bundle** command to replace all IP addresses in your most recent log bundle with placeholders, such as "IPADDRESS\_1" and "IPADDRESS\_2," etc.



### Note

Before running the **redact-last-log-bundle** command, you must have first collected an unencrypted log bundle.

- Step 1** Log into the command-line interface (see “Log into the Command-line Interface” on page 3-16). The command-line interface appears, showing you that you’re logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$
```

- Step 2** Enter **redact-last-log-bundle** at the prompt and press the **Enter** key. The command-line interface refreshes, and you can see the location of the file that has your log bundle with its IP addresses redacted.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$ redact-last-log-bundle
See /home/admin/LogCollection Fusion 20211026-111403 2d867142.redacted.tgz
admin@singlewire:~$
```

- Step 3** Examine the log file and determine whether its redactions meet your needs.
- Step 4** Contact Cisco TAC and ask them to assist you in analyzing your redacted logs. They will provide further direction as to the preferred method of transferring your log bundle.

## Display InformaCast's Phone Cache

InformaCast's cache of Cisco IP phones for Unified CM contains Personally Identifiable Information (PII). As such, it is encrypted while at rest to protect its information. When troubleshooting phone issues, you may find it helpful to read InformaCast's phone cache. Since it's encrypted, you'll need to run the **show-phone-caches** command to obtain an unencrypted file of information.

- Step 1** Log into the command-line interface (see “Log into the Command-line Interface” on page 3-16). The command-line interface appears, showing you that you’re logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun 2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$
```

- Step 2** Enter `show-phone-caches` at the prompt and press the **Enter** key. The command-line interface refreshes with InformaCast's phone cache details.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$ show-phone-caches

<phoneCache>
  <phoneDescription deviceName="          482" deviceType="303">
    <address>          </address>
    <authenticationUrl>http://          :8081/InformaCast/phone/auth</aut
henticationUrl>
    <callingSearchSpace>internal</callingSearchSpace>
    <description>Bulk Phone 840482</description>
    <devicePool>          </devicePool>
    <dns>          482</dns>
    <endUserIdentifier></endUserIdentifier>
    <location>Hub_None</location>
    <partitionNames>On Cluster</partitionNames>
    <pbxAxiDescription>          AxiDescription>
    <pbxDescription>Default configuration</pbxDescription>
  </phoneDescription>
</phoneCache>
This build is 1 days old

admin@singlewire:~$
```

## Send Logs to a Local Server

If you're using your own infrastructure to collect and store log information from syslog clients, you may want to include various InformaCast logs in that infrastructure:

- `/var/log/syslog`
- `/var/log/messages`
- `/var/log/dmesg`
- `Performance.log`

Once configured, InformaCast will send syslog messages over UDP to port 514, which is the standard syslog port, to one or more syslog servers. Syslog over TCP or TLS is not supported, nor is syslog over UDP ports other than 514.

- Step 1** Log into the command-line interface (see “Log into the Command-line Interface” on page 3-16). The command-line interface appears, showing you that you’re logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

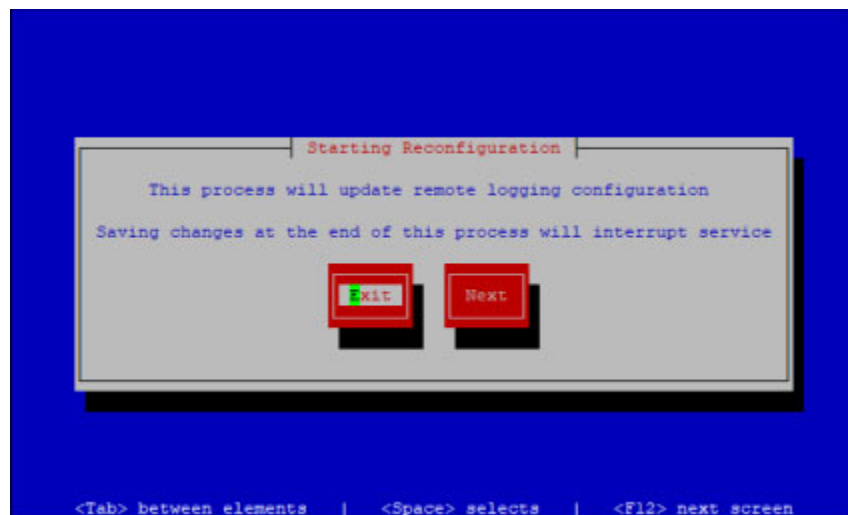
Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

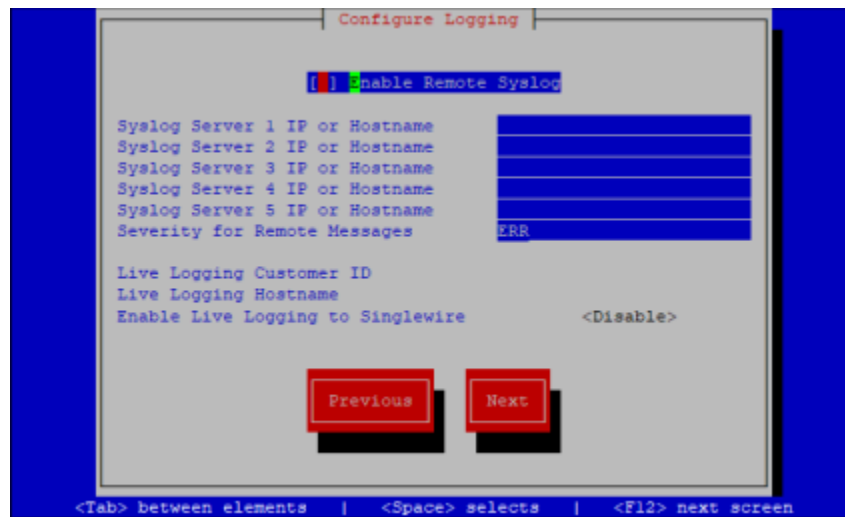
This build is 0 days old

admin@singlewire:~$
```

- Step 2** Enter **configure-logging** 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 Logging window appears.



**Step 4** Press the **Spacebar** while in the **Enable Remote Syslog** field to enable sending logs to a local server. Your **Enable Remote Syslog** field should look like **[\*]**.

**Step 5** Press the **Tab** key to enter the **Syslog Server 1 IP or Hostname** field and enter up to five IP addresses or hostnames where InformaCast should send its logs. Press the **Tab** key to move between fields.



**Note** InformaCast does not validate the IP address(es)/hostname(s) you enter in these fields; however, you can use the **show-logging** command after saving your logging configuration to check that the information you entered is correct (see “Display InformaCast’s Logging Configuration” on page 13-80).

**Step 6** Press the **Tab** key to enter the **Severity for Remote Messages** field and enter the severity level of log messages you’d like InformaCast to send to your local server:

- emerg
- alert
- crit
- err
- warning
- notice
- info
- debug

These severities are listed in order from most severe (emerg) to least severe (debug). Specifying a severity includes messages of that severity and higher, e.g. debug includes all messages that the system generates. Setting a higher severity level lowers the amount of logs sent to your syslog server.

**Tip**

The assignment of logs to severity levels differs based on your logging infrastructure. Trial and error is the best method to determine your severity needs. If you're getting too many logs, increase your severity level.

- Step 7** Press the **Tab** key to highlight the **Next** button, then the **Spacebar** to select it. The Save or Exit window appears.



Your changes aren't saved until you select the **Save Changes** button.

**Note**

Saving your logging configuration causes InformaCast to restart and there will be a service disruption for your users and broadcasts.



- Step 8** Press the **Tab** key to highlight the **Save Changes** button, then the **Spacebar** to select it. Your logging configuration changes are saved. You're returned to the command-line interface and InformaCast's logging agents along with InformaCast itself are restarted to accept your changes. At this point, logs will be sent to the local server(s) you specified.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun 2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$ configure-logging
Restarting logging agents
Restarting InformaCast
Restarting InformaCast: singlewireInformaCast ... requesting that InformaCast st
op...
InformaCast has stopped
Setting authentication mode to native
Apache2 web server is enabled
Testing configuration on Apache web server: apache2 ... Success
Restarting apache with new auth config...
Restarting Apache web server: apache2 ... requesting that apache2 stop...
apache2 has stopped
apache2 has been started.
Success
InformaCast authentication mode changed successfully
InformaCast has been started.
Success
stopping rsyslogd ... done
starting rsyslogd ... done
Restarting Send logs to Singlewire Logger filebeat
Exporting sysdef variables
Exporting buildinfo variables
LiveLogging is enabled (dev build)
filebeat restarted successfully
Logging agents restarted

This build is 0 days old

admin@singlewire:~$
```

## Display InformaCast's Logging Configuration

Available only through the command-line interface, the **show-logging** command displays InformaCast's logging configuration, which may be useful when validating that the logging information you entered is correct or when troubleshooting the reason you're receiving too many logs or not enough.

- Step 1** Log into the command-line interface (see “Log into the Command-line Interface” on page 3-16). The command-line interface appears, showing you that you’re logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun 2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$
```

- Step 2** Enter **show-logging** at the prompt and press the **Enter** key. The command-line interface refreshes with the details of your current logging configuration.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$ show-logging
Remote syslog enabled:                True
Syslog server 1:
Syslog server 2:
Syslog server 3:
Syslog server 4:
Syslog server 5:
Syslog severity for remote messages: ERR
Syslog service status:
status rsyslogd ... running

Live logging customer ID: SampleCust
Live logging hostname:                .com
filebeat (pid 30915) is running...

This build is 0 days old

admin@singlewire:~$
```

In your logging details, you can see whether you've enabled the sending of InformaCast's logs to a local server and that server's address along with the severity level of the logs being sent and the status of the syslog service, e.g. running.

## Show Technical Support Information

When you are talking with Cisco TAC or opening up a support case with them, they will ask you for certain information to aid you in the troubleshooting process. The show-tech-support command provides you with the relevant information Cisco TAC will need.

- Step 1** Log into the command-line interface (see “Log into the Command-line Interface” on page 3-16). The command-line interface appears, showing you that you’re logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$
```

- Step 2** Enter **show-tech-support** at the prompt and press the **Enter** key. The command-line interface refreshes and displays version and phone count information.

```
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-tech-support
show-tech-support begins

InformaCast Version
=====
Version specific data can be found in the Compatibility Matrix
https://www.singlewire.com/compatibility-matrix.html

1
2 This is Singlewire InformaCast version
3 Running on VMware
4 Licensed as Purchased
5
6

Phone Models & Count
=====
Below is a count of the supported phone models that InformaCast found.
For a list of supported phone models, please visit the Compatibility Matrix:
https://www.singlewire.com/compatibility-matrix.html

Cisco 6921 : 0
Cisco 6941 : 1
Cisco 6945 : 1
Cisco 6961 : 0
Cisco 7811 : 0
Cisco 7821 : 0
Cisco 7841 : 0
Cisco 7861 : 0
Cisco 7905 : 0
Cisco 7906 : 0
Cisco 7911 : 0
Cisco 7912 : 0
Cisco 7920 : 0
Cisco 7921 : 0
Cisco 7925 : 0
Cisco 7926 : 0
Cisco 7931 : 0
Cisco 7937 : 0
Cisco 7940 : 0
Cisco 7941 : 0
Cisco 7942 : 0
Cisco 7945 : 0
Cisco 7960 : 0
Cisco 7961 : 0
Cisco 7962 : 0
Cisco 7965 : 2
Cisco 7970 : 0
Cisco 7971 : 0
Cisco 7975 : 1
Cisco 8811 : 2
```

## Enable the Singlewire Support Account

Sometimes, when troubleshooting an issue, it is helpful to “turn on” access to your InformaCast 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 InformaCast 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 3-16). The command-line interface appears, showing you that you're logged in.

```

login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

Welcome to Singlewire InformaCast

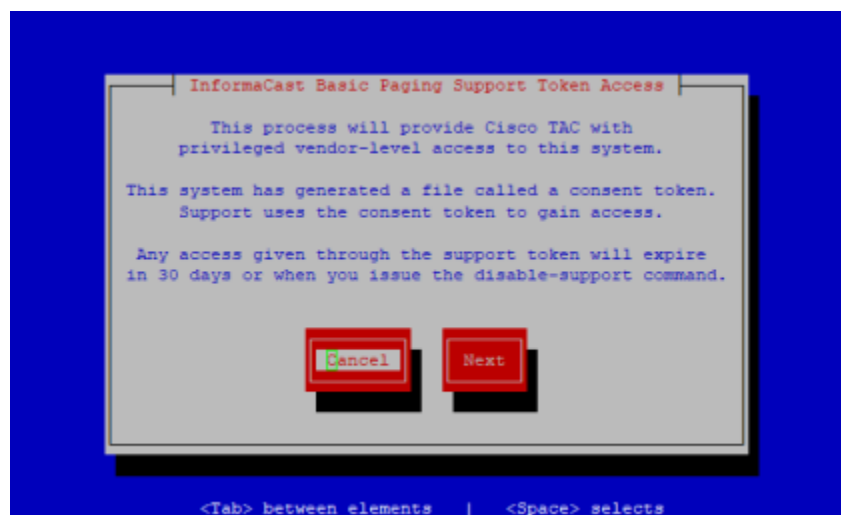
Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$

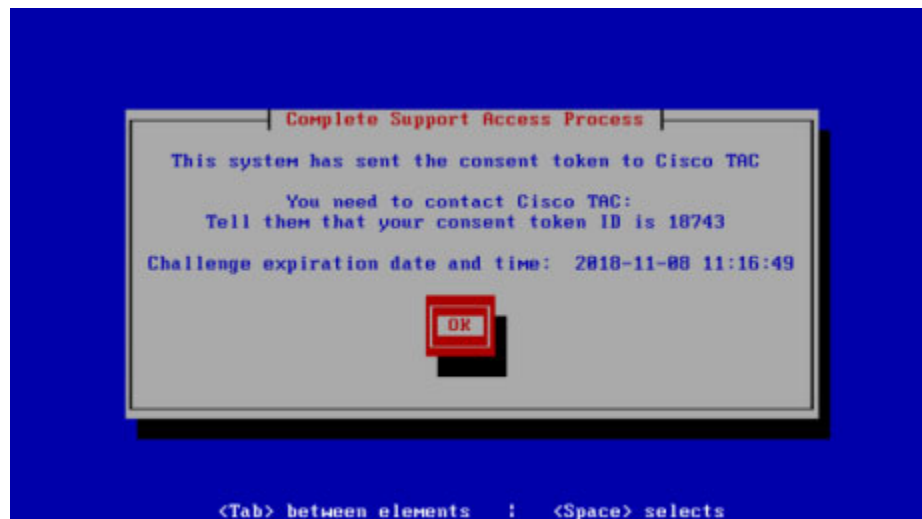
```

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

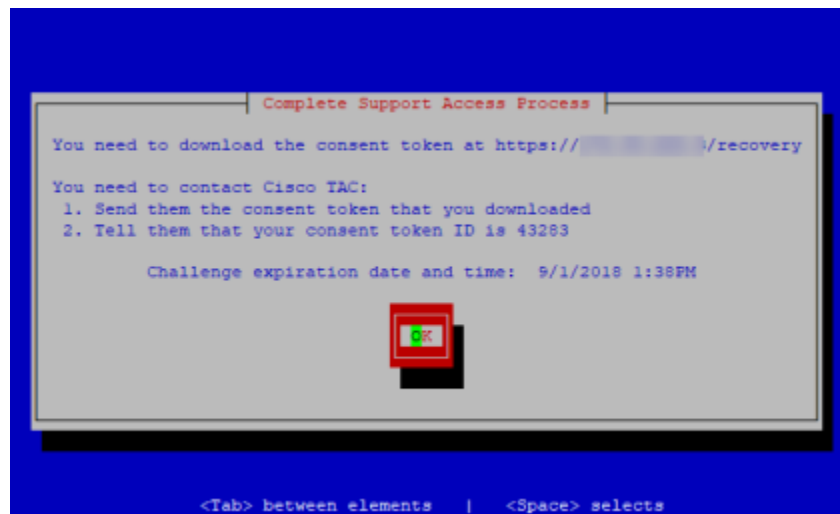


- Step 3** Use the **Tab** or **Right Arrow** key to highlight the **Next** button, then press the **Spacebar** to select it.

If your InformaCast Appliance has internet access, a consent token will be sent to Cisco TAC and this console window appears.



If your InformaCast Appliance doesn't have internet access, this console window appears.



Depending on your internet access, you will now follow different steps:

- “Internet Access” on page 13-85
- “No Internet Access” on page 13-86

## Internet Access

Use the following steps if your InformaCast Appliance has internet access.

- Step 1** Make note of your token ID number, e.g. 01867. This ID lets Cisco TAC know you are who you say you are.

- Step 2** Contact Cisco TAC and tell them you want to enable the Support account.
- Step 3** 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.

---

## No Internet Access

Use the following steps if your InformaCast Appliance doesn't have internet access.

- 
- Step 1** Make note of your token ID number, e.g. 01867. This ID lets Cisco TAC know you are who you say you are.
- Step 2** Leave your vSphere console window open. You will come back to it.



**Step 3** Access your consent token in one of two ways:

- Use an SSH client to log into the command-line interface of your InformaCast Appliance. Enter **show-latest-consent-token** at the prompt and press the **Enter** key. The command-line interface refreshes with the contents of your consent token.

```
Running on VMware
Licensed as Purchased

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old
admin@singlewire:~$ show-latest-consent-token
=== BEGIN CONSENT_TOKEN password_recovery 98dcf317c9c20d8e044f5d5d65e4d701ca29fe
d07512f0e96f792cf2d9ddd497 1 ===
==== BEGIN KEY ====
U1kSg2AW2GObApFzpVa/WtSNpzLmhijMG7
t0b8DEu5Ryh+YNvr15YHDd3DABb6BbAFNN
pc7u7RHqCoOqFqrcI7bxoSeZlvh7UA1k5H
aSyR+w0jaYzFE/HTHhSG-JsZoawQyRQBm7p
tVdbnaqf1g/WhFINcm9m+n1QJvNjwF3xaf
AhmNAJFyFYNBjIv/ZEdeB8nFos4nHUr5Gd
hbtSmzK/Eoz3Jofn2E12skpQWkxzW1klW+
B7AmAlInf5EojlrZho/lh/kDNnC9v1GgZi
qEMg89MYODQGqPdXVehRXeGXG3bnqjUEvQ
zMQydfTaw7Ev4KYe9kIyeDv/HsdUUFb7AJ
+0CaIs3E4FURk=
==== END KEY ====
==== BEGIN PAYLOAD ====
HEPIvwNWLcNcb7WLK+NoCqYS/CznA
061Q/ld0bd/BSjj8K0Ab1SGtiGh0Dm
cuddKIQD1BBbVr3INuqP/hEjTzwnHM
8CQn7mAlfcubIFxXyjrqI4qzrv4WnX
5MmuwYZTeHASP/0jXnKOCx0agRFQMG
vzGW45aCZsFZqZoD/AnbpJd6sN0hHf
3B11LPhE4hFTEQ1eZIrXLPYdD8neAf
thNIuH0bz1bQA6v2tqG7HERw6RdOFv
9T8B1wFvg7P4dqx66W06X+bqjrrq4Q5
9125Dv1UjsBExjUVy/hJFXZOE6xBOv
bLb9GWBKI=
==== END PAYLOAD ====
=== END CONSENT_TOKEN ===
This build is 0 days old
admin@singlewire:~$
```

Copy everything from `===BEGIN CONSENT_TOKEN` through `END CONSENT_TOKEN===` and paste it into a TXT file. Name it `token.txt`. Continue with Step 4.

- Start a secure file transfer application, such as WinSCP or WinSFTP, and browse to the directory where your consent token is located, i.e. `/home/admin/recovery`. Copy the `token.txt` file to a directory on your computer. Continue with Step 4.

**Step 4** Return to your vSphere console window.

**Step 5** Contact Cisco TAC and tell them you want to enable the Support account.

**Step 6** Send them your `token.txt` file 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 Your Consent Token

When talking with Cisco TAC about issues you may be having with InformaCast, it's important to secure your communication so that Cisco TAC knows you are who you say you are and vice versa. This security comes through a token ID number and a consent token you send to Cisco TAC when enabling the Singlewire Support account or recovering your OS and application passwords (see “Enable the Singlewire Support Account” on page 13-84 or “Manage Password Recovery for the InformaCast Appliance” on page 13-101 for more information).

Your token ID number is displayed in your vSphere or SSH console window when performing either action and, if your InformaCast Appliance has internet access, your consent token will be automatically sent to Cisco TAC; however if your InformaCast Appliance doesn't have internet access, you'll need a way to access your consent token, so you can send it to Cisco TAC.

- Step 1** Use an SSH client to log into the command-line interface (see “Log into the Command-line Interface” on page 3-16). The command-line interface appears, showing you that you're logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$
```

- Step 2** Enter `show-latest-consent-token` at the prompt and press the **Enter** key. The command-line interface refreshes with the contents of your consent token.

```
Running on VMware
Licensed as Purchased

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old
admin@singlewire:~$ show-latest-consent-token
==== BEGIN CONSENT_TOKEN password_recovery 98dcf317c9c20d8e044f5d5d65e4d701ca29f6
d07512f0e96f792cf2d9ddd497 1 ====
==== BEGIN KEY ====
U1kSg2AW2GObApFzpVa/WtSNpzLmhiJMG7
t0b9DEuSRyh+YNvr15YHDD3DABb6BhAFNN
pc7u7RMqCoOqFqrcI7bxoSeZlVh7UAik5M
aSyH+w0jaYzFE/HTHh5GJsZoswQyHGBM7p
tVdbnaqf1g/WhFINcm9m+n1QJvNjwF3xaf
AhmNAJFyFYNBjIv/ZEdEB8nFos4nHUz5Gd
hbtzmzK/Eoz3Jofn2Ei2skpQWkzW1klW+
B7AmAlInf5Eoj1rZho/lh/kDNnC9v1GgZi
qEMg89MYODQGqPdXVehRXeGXG3bnqjUEvQ
zMQydfTaw7Ev4XYo9kiYeDv/Hsd0Uf7AJ
+0CaIs3E4FURk=
==== END KEY ====
==== BEGIN PAYLOAD ====
HEPIwMwLcNcb7WLK+NoCqYS/CznA
061Q/ld0bd/BSjj8K0Ab1SGt1Gh0Dm
cuddK1QD1BBbVr3INUqP/hEjTzwnHM
8CQn7mAlfcuhIFxXyjrql4qzrv4WnX
5MnuwYZTeHASP/OjXnKOCx0agRfPOM0
vzGW45aCZsFZqZoD/AnbpJd6sNOhHf
3B11LPHe4hFTEQleZIrXLPYdD8neAf
thNIuH0bz1bQA6v2tqG7HEHw6RdOFv
9T8B1wFvg7P4dgx66W06X+bqjrq4QS
9125Dv1UjsBEXjUVy/hJFXZOE6xBOv
bLb9GWbKI=
==== END PAYLOAD ====
==== END CONSENT_TOKEN ====
This build is 0 days old
admin@singlewire:~$
```

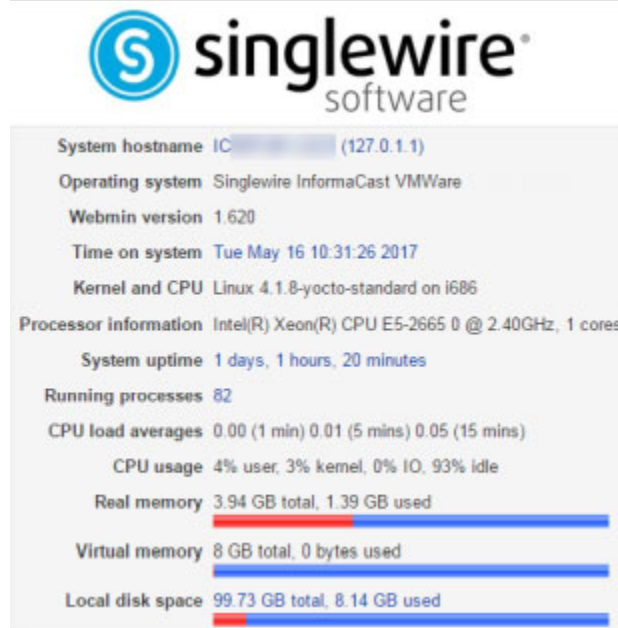
- Step 3** Copy everything from `====BEGIN CONSENT_TOKEN` through `END CONSENT_TOKEN====` and paste it into a TXT file.
- Step 4** Name it `token.txt`.
- Step 5** Contact Cisco TAC and tell them what you'd like to do, e.g. enable the Singlewire Support account or reset your OS and application passwords.
- Step 6** Send them your `token.txt` file and tell them your token ID number. They will either enable the Singlewire Support account or provide you with a challenge response.

“Enable the Singlewire Support Account” on page 13-84 and “Manage Password Recovery for the InformaCast Appliance” on page 13-101 have more information on each of these processes.

## Display a List of Processes Running on the InformaCast 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 3-14 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/udev -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	ptl	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 Monit Status

Monit is a service controller for services on the InformaCast Appliance that are not under administrator control. The **show-monit-status** command displays the status of these automatic services.

- Step 1** Log into the command-line interface (see “Log into the Command-line Interface” on page 3-16). The command-line interface appears, showing you that you’re logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$
```

- Step 2** Enter `show-monit-status` at the prompt and press the **Enter** key. The command-line interface refreshes and displays the status of the automatic services running on the InformaCast Appliance.

```

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-monit-status
Monit 5.20.0 uptime: 16h 47m

Process 'status-screen'
  status           Running
  monitoring status Monitored
  monitoring mode   active
  on reboot         start
  pid               3917
  parent pid        1
  uid               0
  effective uid     0
  gid               0
  uptime            16h 48m
  threads           1
  children           1
  cpu                0.0%
  cpu total         0.0%
  memory            0.1% [2.7 MB]
  memory total      0.1% [3.0 MB]
  data collected    Thu, 07 Mar 2019 09:26:15

Process 'sipspeaker'
  status           Execution failed | Does not exist
  monitoring status Monitored
  monitoring mode   active
  on reboot         start
  data collected    Thu, 07 Mar 2019 09:26:45

Program 'vmtoolsd-check'
  status           Status ok
  monitoring status Monitored
  monitoring mode   active
  on reboot         start
  last exit value   0
  last output       -
  data collected    Thu, 07 Mar 2019 09:26:45

Program 'check-pmic'
  status           Status ok
  monitoring status Monitored
  monitoring mode   active
  on reboot         start
  last exit value   0
  last output       -
  data collected    Thu, 07 Mar 2019 09:26:45

System 'singlewire'
  status           Running
  monitoring status Monitored
  monitoring mode   active
  on reboot         start
  load average      [0.05] [0.09] [0.05]
  cpu                5.0%us 1.5%sy 0.1%wa
  memory usage      1.3 GB [33.7%]
  swap usage        32.6 MB [0.4%]
  uptime            16h 49m
  boot time         Wed, 06 Mar 2019 16:37:49
  data collected    Thu, 07 Mar 2019 09:26:45

This build is 1 days old
admin@singlewire:~$ █

```

## Show the InformaCast Appliance's Version

The **show-version** command displays the InformaCast 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 3-16). The command-line interface appears, showing you that you’re logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun 2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

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:~$
```



## Show the Appliance Type

The **show-appliance-type** command displays the hardware or virtualization hypervisor on which your InformaCast Appliance is running.

- Step 1** Log into the command-line interface (see “Log into the Command-line Interface” on page 3-16). The command-line interface appears, showing you that you’re logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$
```

- Step 2** Enter **show-appliance-type** at the prompt and press the **Enter** key. The command-line interface refreshes with your Virtual Appliance's machine type.

```
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-appliance-type
VMware

admin@singlewire:~$
```

Depending on whether your appliance is virtual or physical, you may see VMware or IPTA-IAS.



**Note** InformaCast Basic Paging does not support the InformaCast Physical Appliance, so you will always see VMware returned by the **show-appliance-type** command.

## Show the BIOS Version

Occasionally, Singlewire will require upgrades to InformaCast's BIOS to facilitate new features or bug fixes. Running the **show-bios-version** command will return to you whether your BIOS is up to date or requires an upgrade.

- Step 1** Log into the command-line interface (see “Log into the Command-line Interface” on page 3-16). The command-line interface appears, showing you that you’re logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$
```

**Step 2** Enter **show-bios-version** at the prompt and press the **Enter** key. The command-line interface refreshes with whether your InformaCast Appliance's on-premises server's BIOS is up to date or needs updating.

An up-to-date BIOS will return the following:

```
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-bios-version
VMware: BIOS is up to date
admin@singlewire:~$
```

An out-of-date BIOS will return the following:

```
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-bios-version
IPTA-IAS: BIOS requires an update
admin@singlewire:~$
```

An out-of-date BIOS will also display its out-of-date status on the Status screen.

If your BIOS is out of date, Singlewire will contact you with materials and instructions to assist you in your upgrades along with a date before which you should complete your upgrades.

## Change the InformaCast Appliance's Password

Your OS credentials are used to enter Webmin and Control Center and when using SSH to access the InformaCast Appliance, and you initially set the OS Administrator's password in Step 21 on page 2-37. 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.

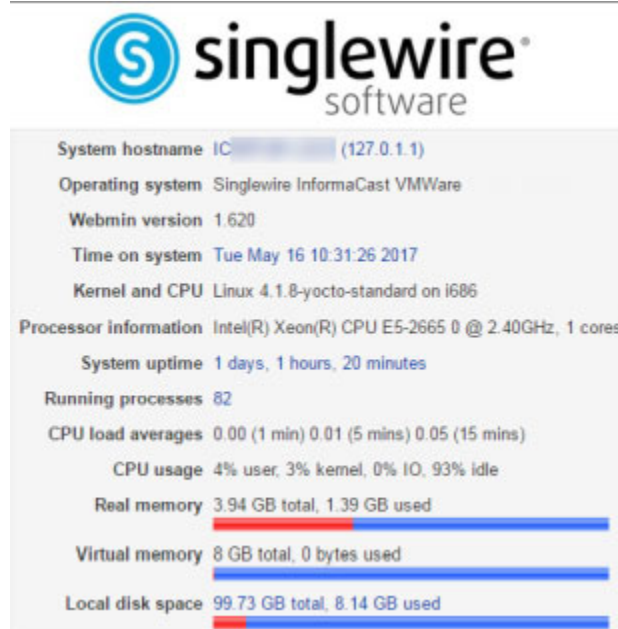
Symbol	Description
!	Exclamation mark
"	Double quotes (or speech marks)
#	Number
\$	Dollar
%	Percent
&	Ampersand
'	Single quote
(	Open parenthesis (or open bracket)
)	Close parenthesis (or close bracket)
*	Asterisk
+	Plus
,	Comma
-	Hyphen
.	Period, dot or full stop
/	Slash or divide
0	Zero
1	One
2	Two
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)

<b>Symbol</b>	<b>Description</b>
?	Question mark
@	At symbol
A/a	Upper- or lowercase A
B/b	Upper- or lowercase B
C/c	Upper- or lowercase C
D/d	Upper- or lowercase D
E/e	Upper- or lowercase E
F/f	Upper- or lowercase F
G/g	Upper- or lowercase G
H/h	Upper- or lowercase H
I/i	Upper- or lowercase I
J/j	Upper- or lowercase J
K/k	Upper- or lowercase K
L/l	Upper- or lowercase L
M/m	Upper- or lowercase M
N/n	Upper- or lowercase N
O/o	Upper- or lowercase O
P/p	Upper- or lowercase P
Q/q	Upper- or lowercase Q
R/r	Upper- or lowercase R
S/s	Upper- or lowercase S
T/t	Upper- or lowercase T
U/u	Upper- or lowercase U
V/v	Upper- or lowercase V
W/w	Upper- or lowercase W
X/x	Upper- or lowercase X
Y/y	Upper- or lowercase Y
Z/z	Upper- or lowercase Z
[	Opening bracket
\	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 3-14 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 11-1).

## Manage Password Recovery for the InformaCast Appliance

Your InformaCast Appliance allows for password recovery management:

- If you lose your InformaCast 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 InformaCast Appliance's password is enabled, but you may need to turn off/on this functionality depending on your environment's needs.

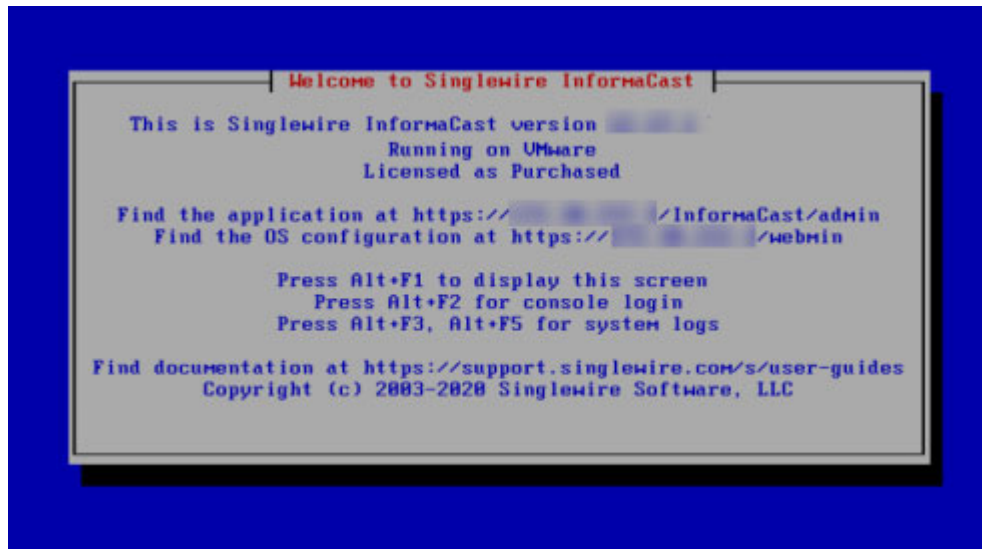
### Recover Your OS and Application Passwords

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

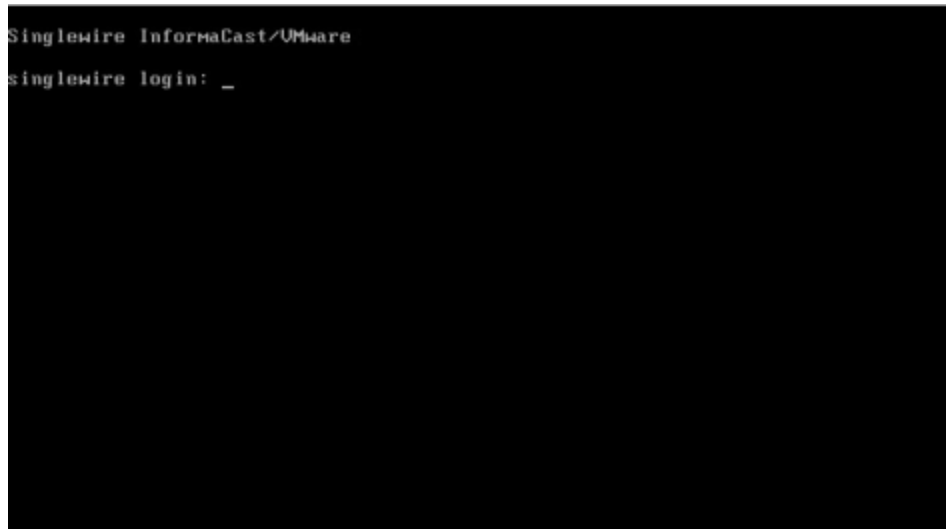


**Note** Completing this process will cause your InformaCast Appliance to reboot.

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



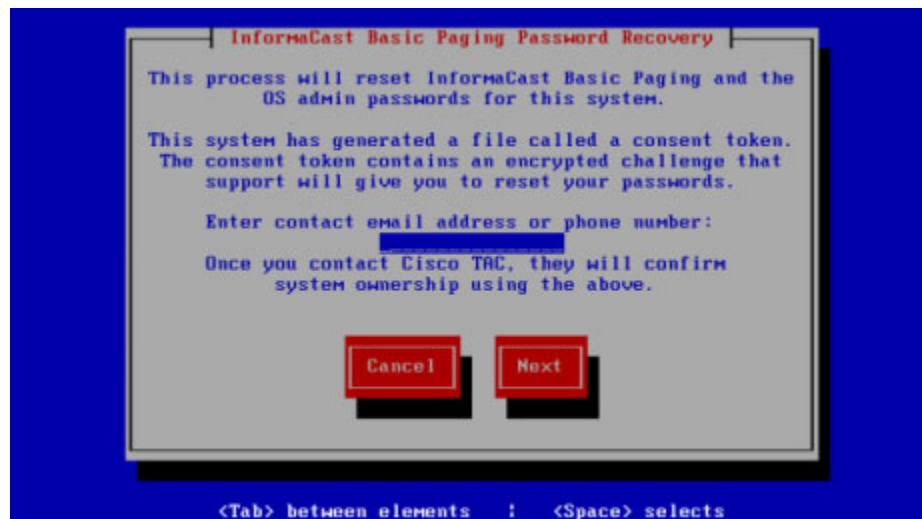
- Step 2** Press the **Alt + F2** keys to switch to the console screen where you can enter commands.



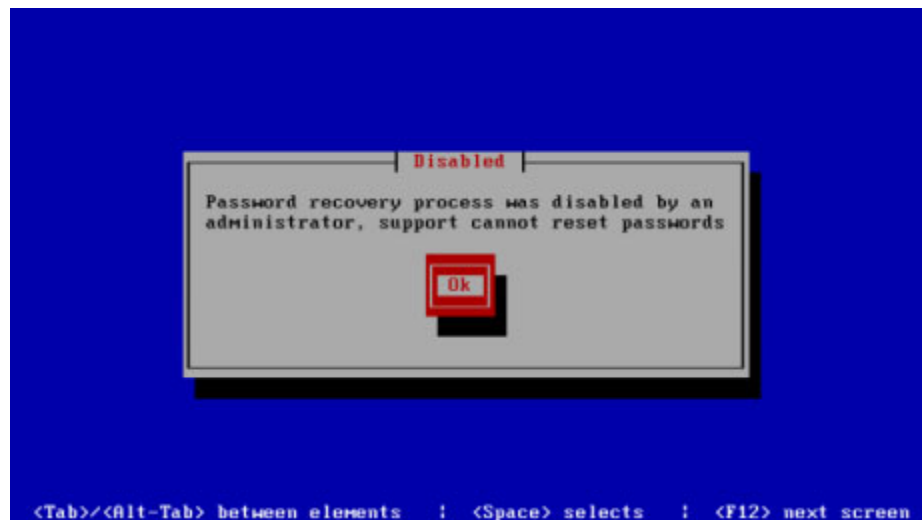
- Step 3** Enter **recovery** at the prompt and press the **Enter** key.



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

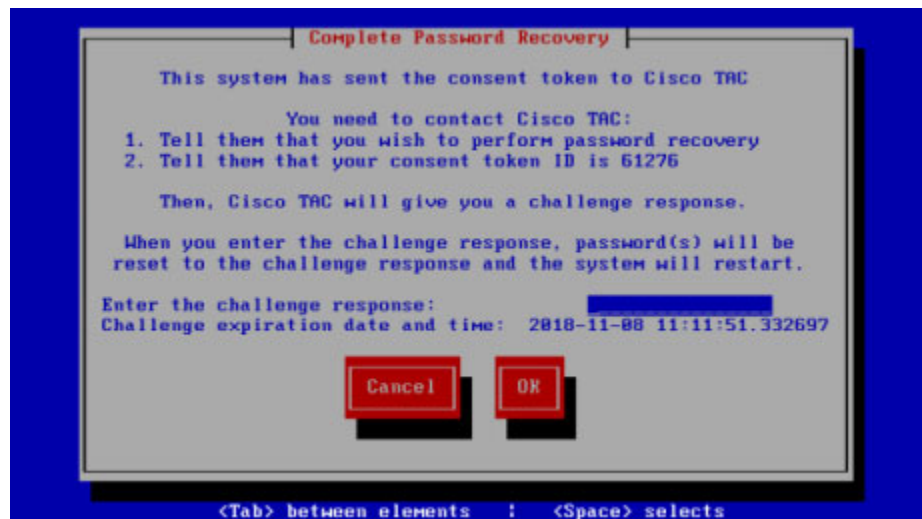


If you don't have password recovery enabled, this console window appears, and you cannot continue with these steps until you enable password recovery.

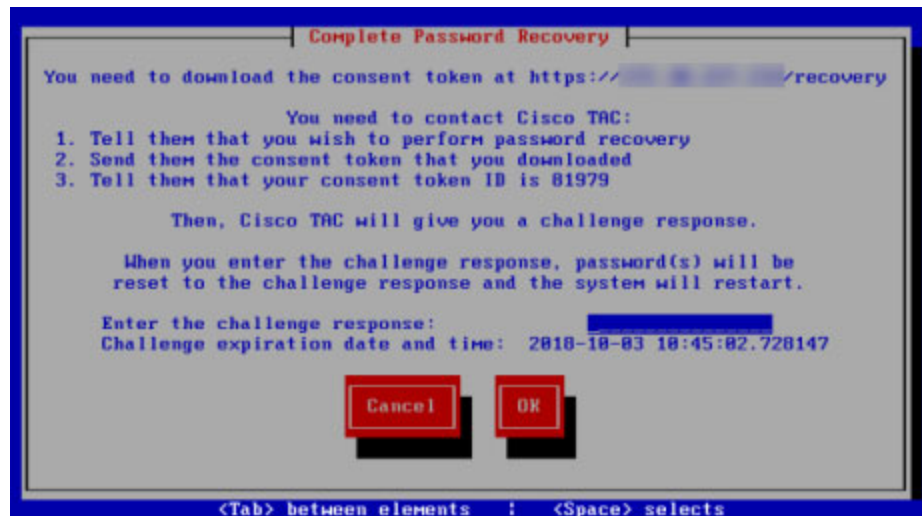


- Step 4** Enter your email address or phone number, press the **Tab** or **Right Arrow** key to highlight the **Next** button, and press the **Spacebar** to select it.

If your InformaCast 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 2.



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



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

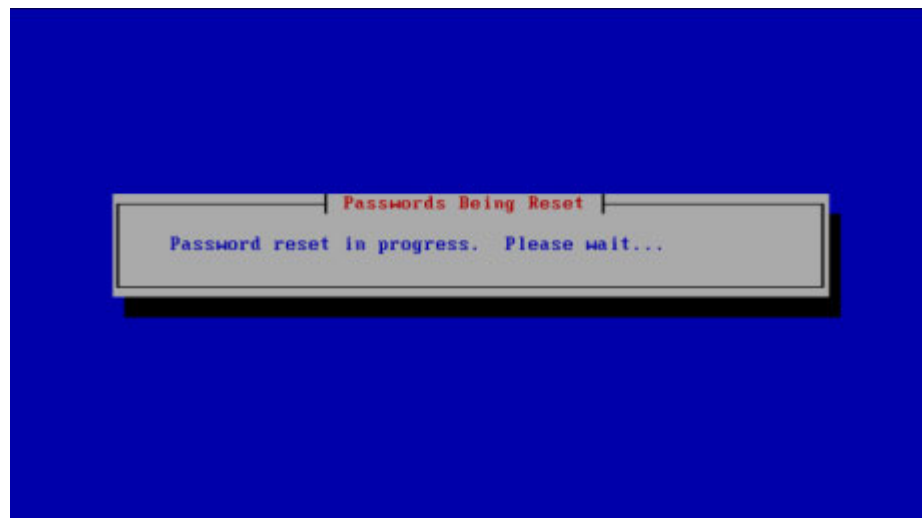
Depending on your internet access, you will now follow different steps:

- “Internet Access” on page 13-105
- “No Internet Access” on page 13-106

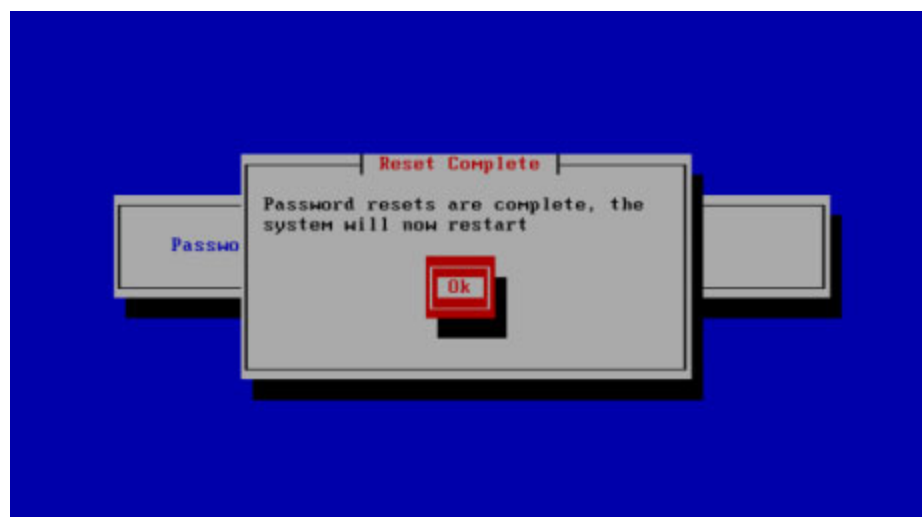
*Internet Access*

Use the following steps if your InformaCast Appliance has internet access.

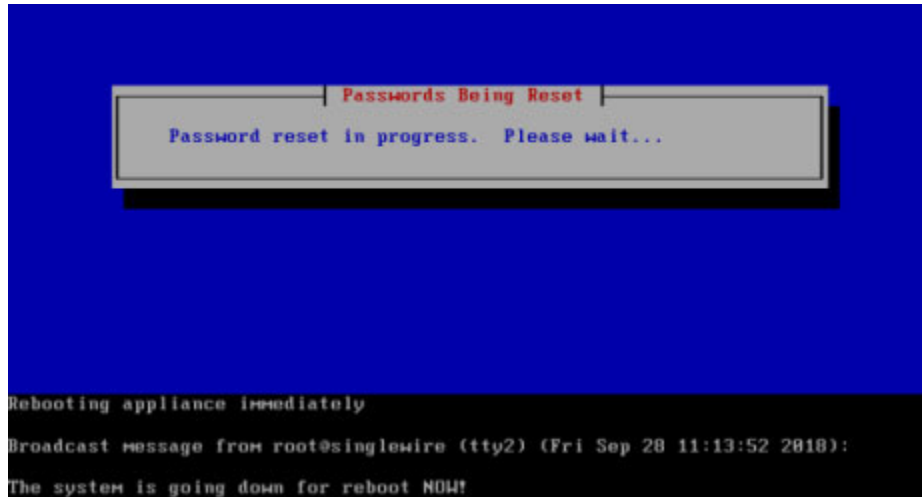
- Step 1** Make note of your token ID number, e.g. 01867. This ID lets Cisco TAC know you are who you say you are.
- Step 2** Contact Cisco TAC and tell them you want to reset your OS and application passwords.
- Step 3** Tell them your token ID number. They will provide you with a challenge response. This is your new password.
- Step 4** 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 InformaCast Appliance will need to reboot.



**Step 5** Press the **Spacebar** to select the **Ok** button. Your InformaCast Appliance will reboot.



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

- “Change the InformaCast Appliance’s Password” on page 13-98
- “Change the Application Administrator’s Password” on page 11-1

---

### *No Internet Access*

Use the following steps if your InformaCast Appliance doesn’t have internet access.

- 
- Step 1** Make note of your token ID number, e.g. 01867. This ID lets Cisco TAC know you are who you say you are.
- Step 2** Leave your vSphere console window open. You will come back to it.

**Step 3** Access your consent token in one of two ways:

- Use an SSH client to log into the command-line interface of your InformaCast Appliance. Enter **show-latest-consent-token** at the prompt and press the **Enter** key. The command-line interface refreshes with the contents of your consent token.

```
Running on VMware
Licensed as Purchased

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old
admin@singlewire:~$ show-latest-consent-token
=== BEGIN CONSENT_TOKEN password_recovery 98dcf317c9c20d8e044f5d5d65e4d701ca29fe
d07512f0e96f792cf2d9ddd497 1 ===
==== BEGIN KEY ====
U1kSg2AW2GObApFzpVa/WtSNpzLmhijMG7
t0b8DEu5Ryh+YNvr15YHDD3DABb6BbAFNN
pc7u7RHqCo0qFqrcI7bxoSe2Ivh7UA1k5H
aSyR+w0jaYzfE/HTHhSG-JsZoawQyHGBM7p
tVdbnaqf1g/WhFINcm9m+n1QJvNjwF3xaf
AhmNAJFyFYNBjIv/ZEdeB8nFos4nHUr5Gd
hbtSmzK/Eoz3Jofn2EI2skpQWkxzW1klW+
B7AmAlInf5EojlrZho/lh/kDNnC9v1GgZi
qEMg89MYODQGqPdXVehRXeGXG3bnqjUEvQ
zMQydfTaw7Ev4KYe9kIyeDv/HsdUUFb7AJ
+0CaIs3E4FURk=
==== END KEY ====
==== BEGIN PAYLOAD ====
HEPIvwNWLcNcb7WLK+NoCqYS/CznA
061Q/ld0bd/BSjj8K0Ab1SGtiGh0Dm
cuddK1QD1BBbVr3INUqP/hEjTzwnHM
8CQn7mAlfcuhIFxXyjrqI4qzrv4WnX
5MmuwYZTeHASP/0jXnKOCx0agRFQMO
vzGW45aCZsFZqZoD/AnbpJd6sN0hHf
3B11LPHe4hFTEQ1eZIrXLPYdD8neAf
thNIuH0bz1bQA6v2tqG7HERw6RdOPv
9T8BiwFvg7P4dqx66W06X+bqjrrq4Q5
9125Dv1UjsBExjUVy/hJFXZOE6xB0v
bLb9GWBKI=
==== END PAYLOAD ====
=== END CONSENT_TOKEN ===
This build is 0 days old
admin@singlewire:~$
```

Copy everything from `===BEGIN CONSENT_TOKEN` through `END CONSENT_TOKEN===` and paste it into a TXT file. Name it `token.txt`. Continue with Step 4.

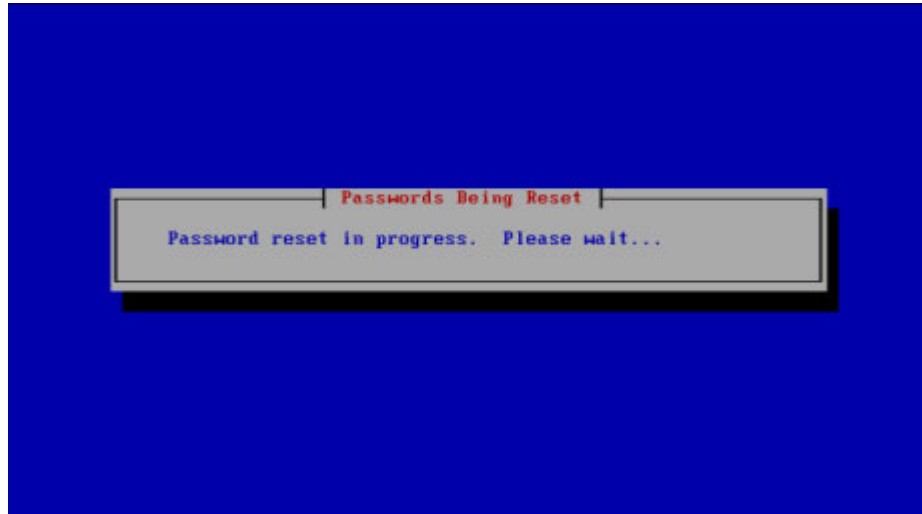
- Start a secure file transfer application, such as WinSCP or WinSFTP, and browse to the directory where your consent token is located, i.e. `/home/admin/recovery`. Copy the `token.txt` file to a directory on your computer. Continue with Step 4.

**Step 4** Contact Cisco TAC and tell them you want to reset your OS and application passwords.

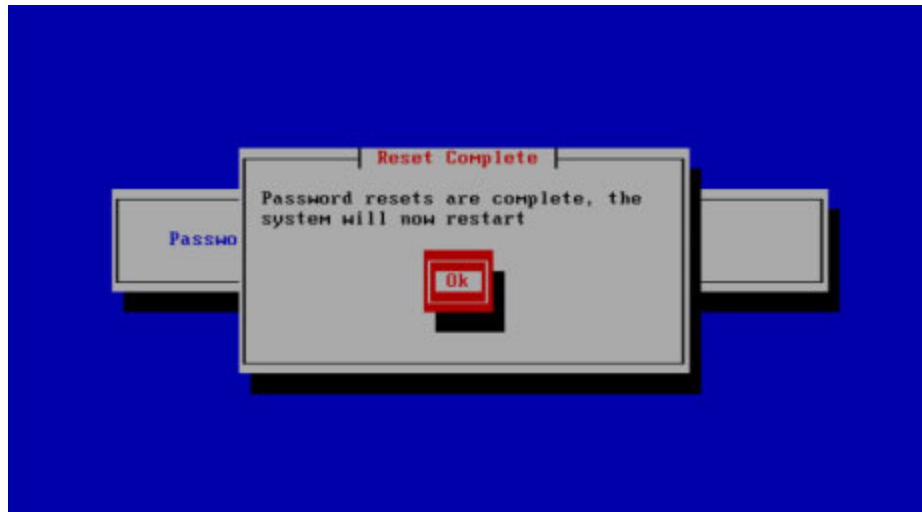
**Step 5** Send them your `token.txt` file and tell them your token ID number. They will provide you with a challenge response. This is your new password.

**Step 6** Return to your vSphere console window.

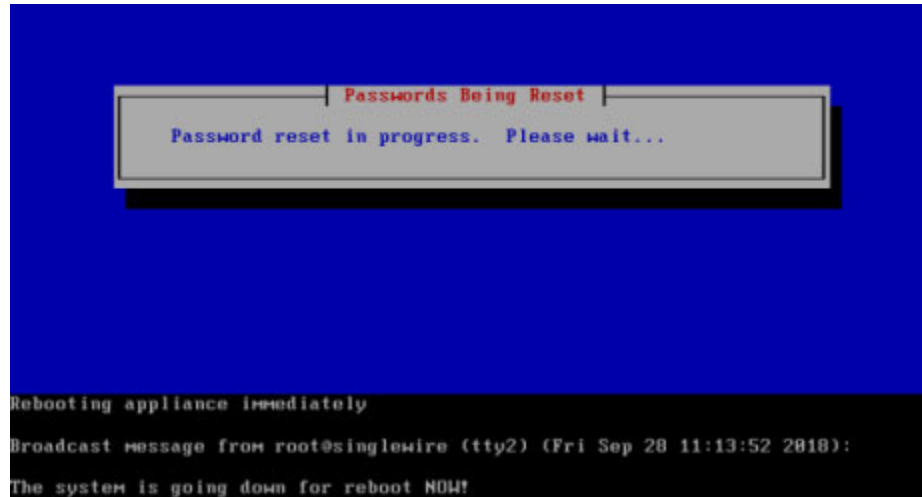
- Step 7** Enter the challenge response (three sets of four alpha-numeric characters including the dashes), press the **Tab** or **Right Arrow** key to highlight the **Next** button, and press the **Spacebar** to select it. The command-line interface refreshes.



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



**Step 8** Press the **Spacebar** to select the **Ok** button. Your InformaCast Appliance will reboot.



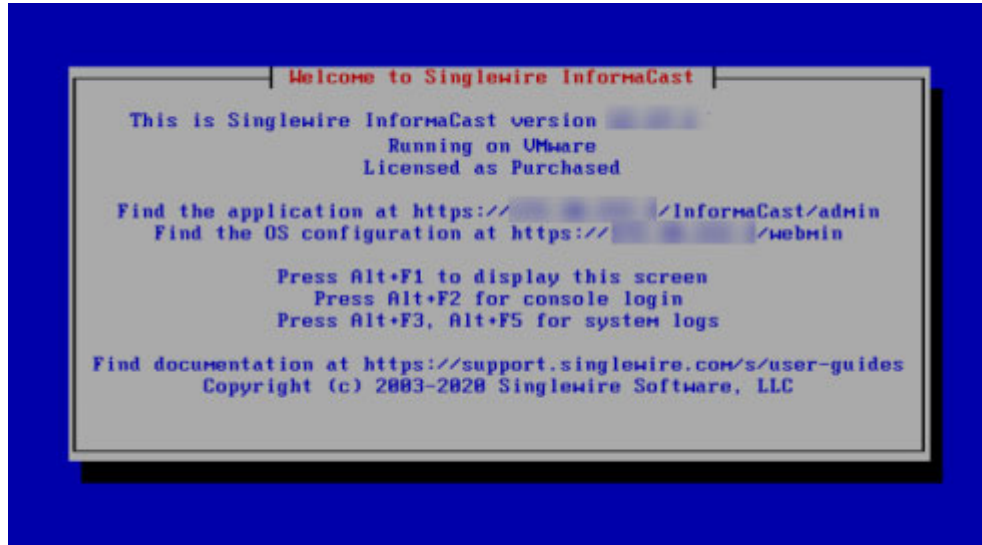
Once your InformaCast Appliance reboots, log in with your new password. Depending on your policy, you may need to change it again:

- “Change the InformaCast Appliance’s Password” on page 13-98
- “Change the Application Administrator’s Password” on page 11-1

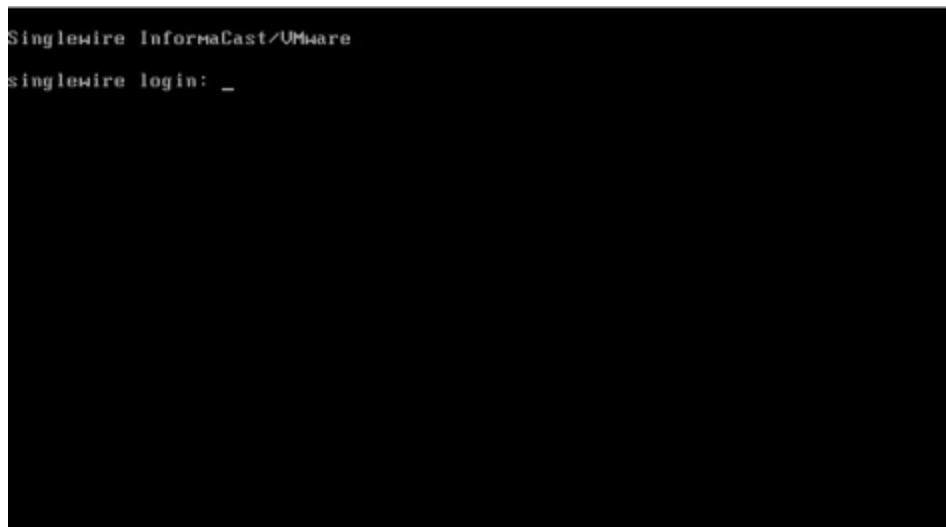
## Disable/Enable Password Recovery

This process will turn off/on your ability to recover your InformaCast 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 InformaCast Appliance. A console window to your InformaCast Appliance appears.



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



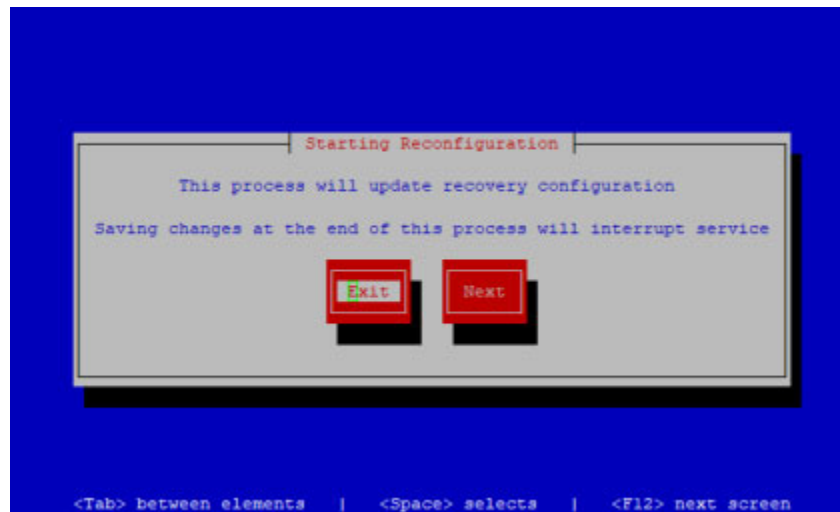


**Step 3** Log in. The console window refreshes, showing you that you're logged in.

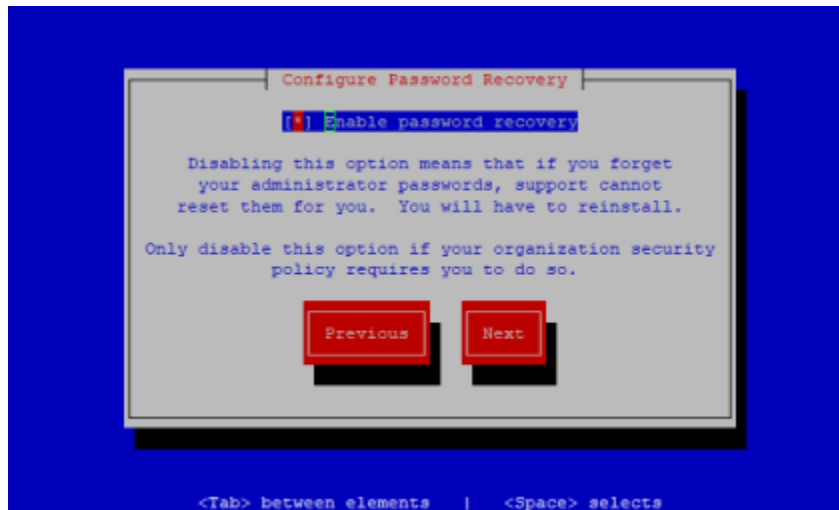
```
Singlewire InformaCast/UMware
singlewire login: admin
Password:

Welcome to Singlewire InformaCast version
Running on UMware
Licensed as Subscription
admin@singlewire:~$ _
```

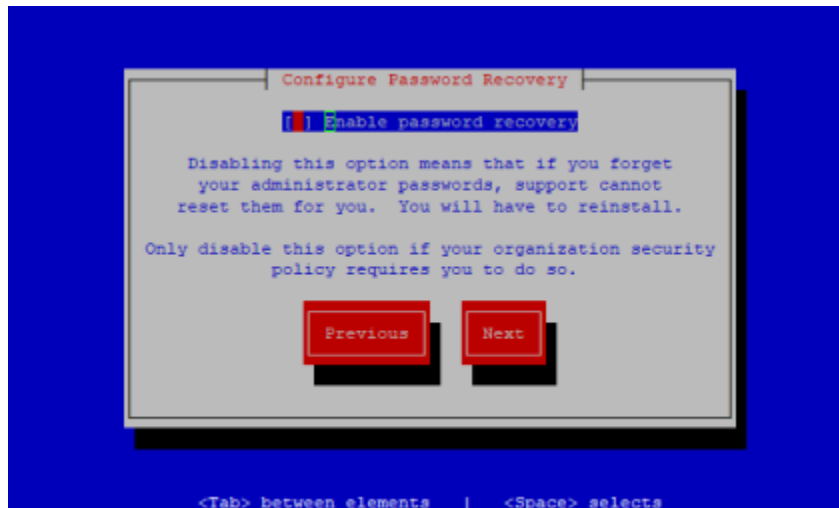
**Step 4** Enter `configure-recovery` at the prompt and press the **Enter** key. The Starting Reconfiguration window appears.



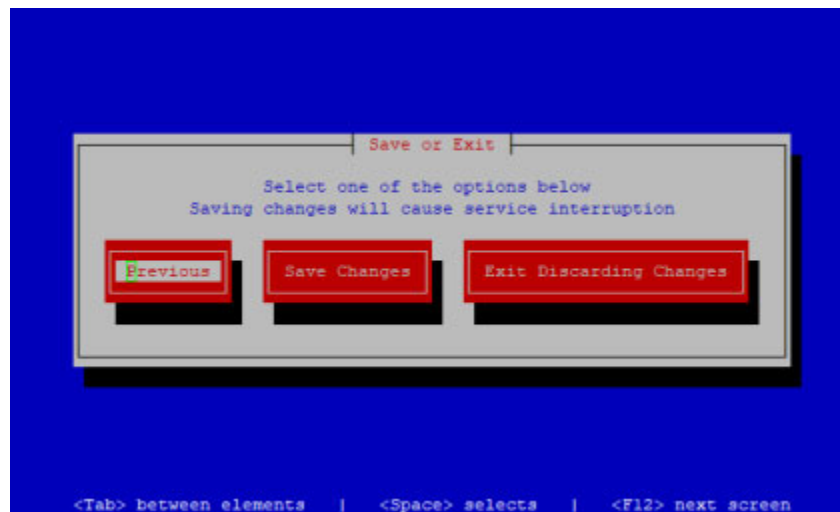
- Step 5** Use the **Tab** or **Right Arrow** key to highlight the **Next** button, then press the **Spacebar** to select it. The Configure Password window appears.



- 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.

## Change the Security Passphrase

The **change-security-passphrase** command allows you to change the passphrase you set during your initial configuration (see “Set the Initial Configuration” on page 2-31). This passphrase is used to secure your backups of the InformaCast Appliance. You must remember this passphrase. Singlewire Support personnel cannot recover it for you if it's lost.


**Note**

Completing this process will cause your InformaCast Appliance to reboot.

- Step 1** Log into the command-line interface (see “Log into the Command-line Interface” on page 3-16). The command-line interface appears, showing you that you’re logged in.

```

login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

Welcome to Singlewire InformaCast

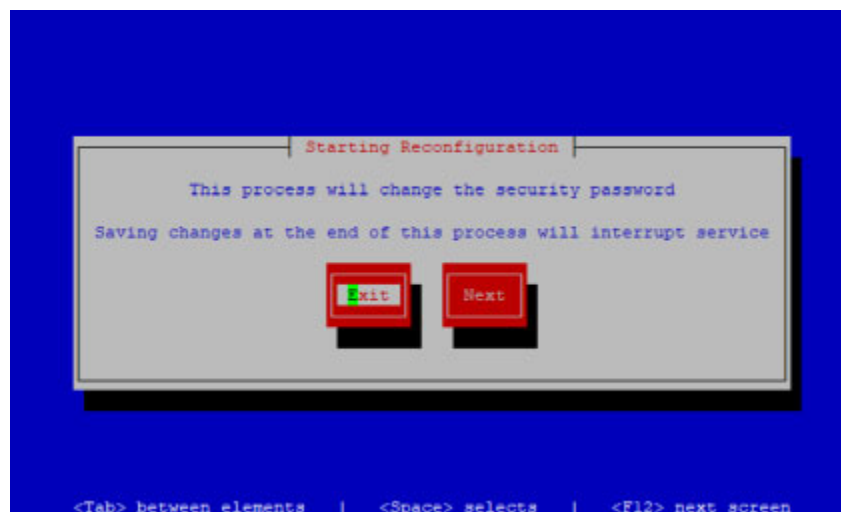
Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

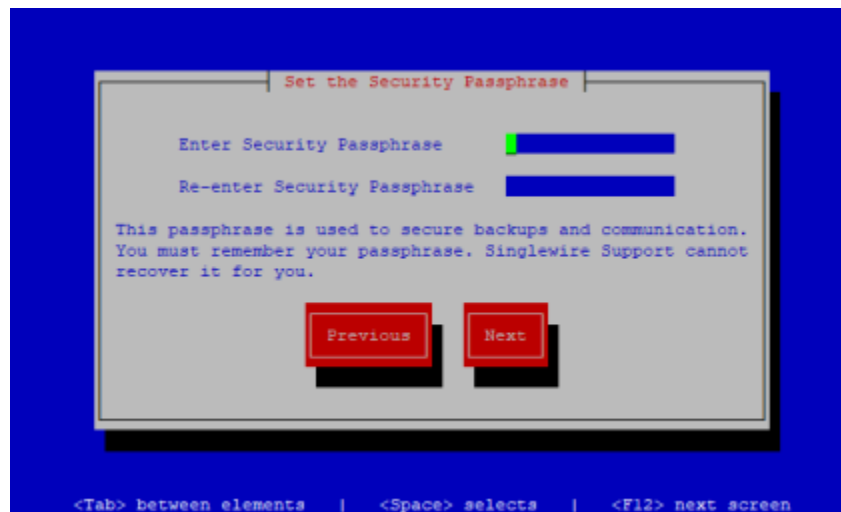
admin@singlewire:~$

```

- Step 2** Enter **change-security-passphrase** at the prompt and press the **Enter** key. The Starting Reconfiguration window appears.



- Step 3** Use the **Tab** or **Right Arrow** key to highlight the **Next** button, then press the **Spacebar** to select it. The Set Security Passphrase window appears.

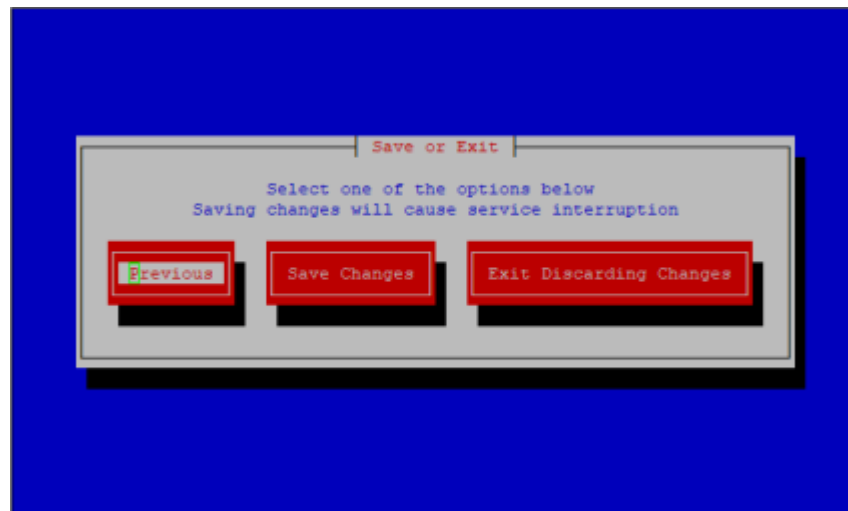


- Step 4** Enter a new security passphrase in the **Enter Security Passphrase** field, press the **Tab** key, and enter the passphrase again in the **Re-enter Security Passphrase** field.



**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 5** 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 6** Use the **Tab** or **Right Arrow** key to highlight the **Save Changes** button, then press the **Spacebar** to select it. The command-line interface appears

```
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:~$ change-security-passphrase
/usr/bin/pbkdf2: line 4: warning: command substitution: ignored null byte in input
Security passphrase changed
**Action required**: existing backups are now invalid.
Remove them from the SFTP path. Backups will fail
until this is done.
Press enter to acknowledge this
█
```

- Step 7** Press the **Enter** key. The command-line interface refreshes and the InformaCast Appliance reboots.

```
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:~$ change-security-passphrase
/usr/bin/pbkdf2: line 4: warning: command substitution: ignored null byte in input
Security passphrase changed
**Action required**: existing backups are now invalid.
Remove them from the SFTP path. Backups will fail
until this is done.
Press enter to acknowledge this

The system will now reboot
Rebooting appliance immediately

The system is going down for reboot NOW!2223 (pts/0) (Fri Mar 8 10:59:41 201
admin@singlewire:~$ █
```

Once your InformaCast Appliance is finished rebooting, your new security passphrase will take effect.



**Note** Remember to remove your old backups from the SFTP path because they will no longer work. You set this path in “Configure InformaCast's Connection to an SFTP Server” on page 11-11.

## 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 3-16). The command-line interface appears, showing you that you're logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

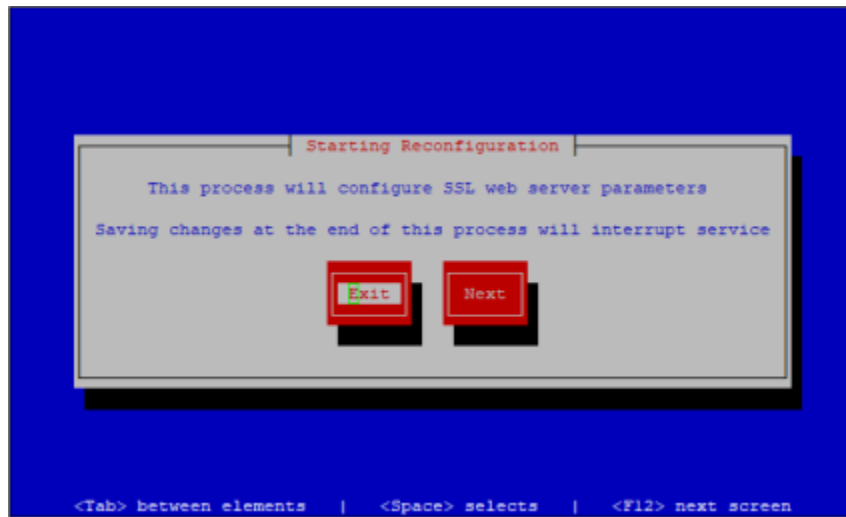
Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$
```

- 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, TLSv1.2 is enabled and all other versions of are disabled.

- 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 Appliance landing page. With HTTP disabled, HTTPS will be used when accessing the InformaCast Appliance landing page.

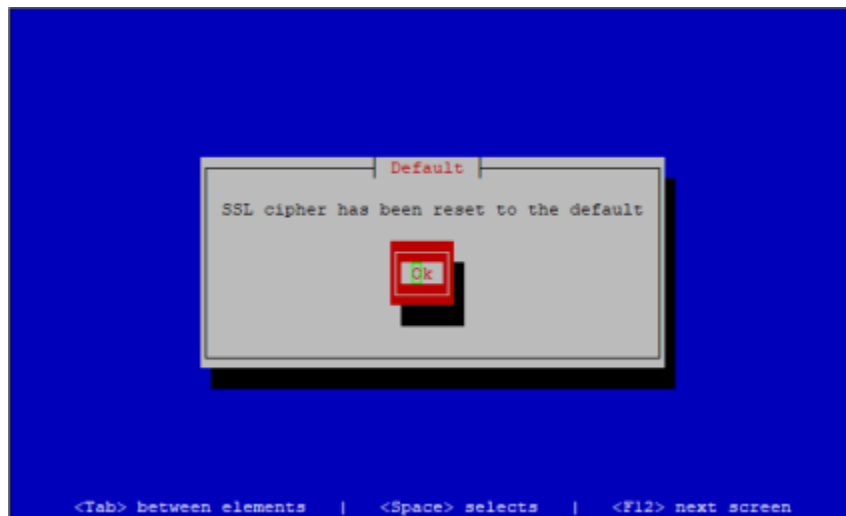


- Step 6** Press the **Tab** key to enter the **SSL Cipher String** field and either accept the cipher string provided or enter your cipher string of choice.

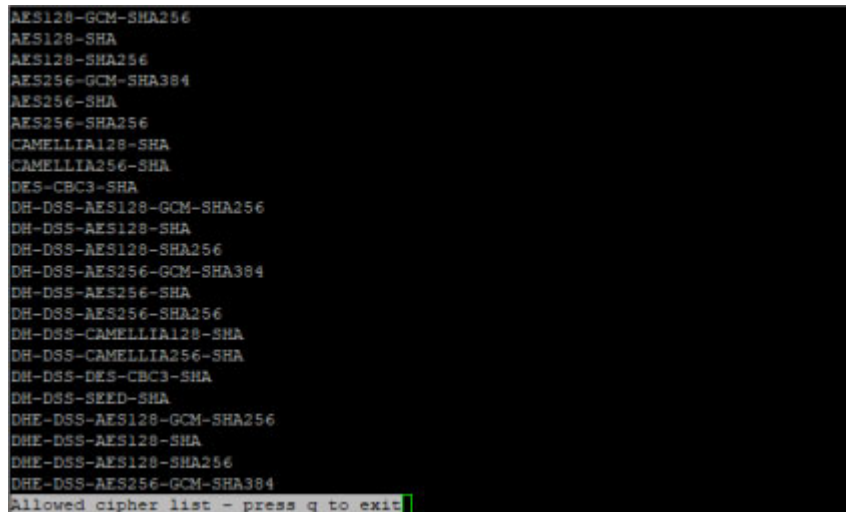
A cipher suite is a set of algorithms that help secure a network connection that uses SSL or TLS. The set of algorithms that cipher suites usually contain include: a key exchange algorithm, a bulk encryption algorithm, and a message authentication code (MAC) algorithm. There are hundreds of different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

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

Welcome to Singlewire InformaCast Software

admin@singlewire:~$ configure-ssl-parameters
Restarting Apache web server: apache2 ... requesting that apache2 stop...
apache2 has stopped
apache2 has been started.
Success
admin@singlewire:~$ █
```

## Display Remote SSL Certificates

Obtain copies of SSL certificates from remote-network-connected servers with the `show-certificate-from-network` command.

- Step 1** Log into the command-line interface (see “Log into the Command-line Interface” on page 3-16). The command-line interface appears, showing you that you’re logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$
```

**Step 2** Enter `show-certificate-from-network <Server IP Address> <Server Port>` at the prompt and press the **Enter** key, e.g. `show-certificate-from-network 127.0.0.1 636`, where 127.0.0.1 is the IP address of an LDAP server and 636 is its port number.

The command-line interface refreshes with a fragment that begins with `BEGIN CERTIFICATE` and ends with `END CERTIFICATE`. You can save this fragment, including the `BEGIN CERTIFICATE` and `END CERTIFICATE` lines, to a text file for import it into InformaCast's trust store.

```
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-certificate-from-network [redacted] 636

Retrieving certificate from [redacted] on 636
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number:
    21:5d:1e:b4:00:00:00:00:05
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: DC=lan, DC=singlewire, DC=windowsldap, CN=windowsldap-
64-CA
  Validity
    Not Before: May 11 16:02:36 2019 GMT
    Not After : May 10 16:02:36 2020 GMT
  Subject: CN=[redacted].windowsldap.singlewire.lan
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (1024 bit)
    Modulus:
      [redacted] 0f:ad:c4:07:32:8c:e4:
      [redacted] e3:ee:b7:00:91:51:50:
      [redacted] 4b:b6:45:5b:3f:17:2a:
      [redacted] f7:93:92:7e:b3:96:c0:
      [redacted] 51:b1:db:27:69:fd:f3:
      [redacted] 7c:4c:22:02:84:99:ee:
      [redacted] 8e:17:f5:b4:8d:2e:95:
      [redacted] 79:c2:45:ca:49:87:73:
      [redacted] 45
    Exponent: 65537 (0x10001)

admin@singlewire:~$
```

## Import a Signed SSL Certificate to InformaCast's SIP Certificate Store

To use secure SIP, i.e. Session Initiation Protocol (SIP) over Transport Level Security (TLS), you must have a certificate for the SIP service in InformaCast's SIP certificate store. This certificate is used to encrypt the traffic between InformaCast and Cisco Unified CM, e.g. traffic for DialCasts, and by default, it's a self-signed certificate.

Due to self-signed certificates' inherent security vulnerabilities, you may want to install a signed certificate instead. 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). Signed certificates are more secure, and allow you to establish a hierarchy of trust.

You may already have installed your root and intermediate Certificate Authority (CA) certificates that you used to sign the InformaCast certificate on Cisco Unified CM, which means you won't have to upload the InformaCast certificate directly. Cisco Unified CM will see that the InformaCast certificate was signed by the intermediate CA, which was signed by the root CA, and because Cisco Unified CM trusts the root CA, it will trust anything signed by the root CA.

Once created, this signed certificate will need to be copied into InformaCast's SIP certificate store.

- 
- Step 1** Create and install a signed certificate (see “Create and Install a Signed Certificate” on page 13-125).
  - Step 2** Use an SSH client to log into the command-line interface (see “Log into the Command-line Interface” on page 3-16). The command-line interface appears, showing you that you’re logged in.

```

login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$

```

- Step 3** Stop the InformaCast service (see “Stop a Service on the InformaCast Appliance” on page 13-7).
- Step 4** Enter **import-ssl-cert-to-sip-store** at the prompt and press the **Enter** key. InformaCast imports into its SIP certificate store the certificate you created in “Create and Install a Signed Certificate” on page 13-125.




---

**Note** The **import-ssl-cert-to-sip-store** command clears anything that had previously been in InformaCast's SIP trust store. If you previously uploaded other certificates, those are now gone. You must complete the following steps or InformaCast will be unable to communicate using SIP over TLS.

---

- Step 5** Start the InformaCast service (see “Start a Service on the InformaCast Appliance” on page 13-9).
  - Step 6** Go to **System Administration | Telephony | SIP** on your InformaCast, and expand the *Certificates* area, if it's not already visible
  - Step 7** Upload all CA certificates in the CA chain for InformaCast's SSL server certificate. “Install Cisco Unified CM Certificates on InformaCast” on page 8-77 walks you through the upload process.
  - Step 8** Restart SIP (see “Restart SIP” on page 8-101).
-

## Manage Trust Certificates

**Note**

This topic and its related topics are optional.

The InformaCast 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 InformaCast 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 13-125
- “Display Your Trusted Certificates” on page 13-131
- “Display Your Local Trust” on page 13-133
- “Remove Added Trust Certificates” on page 13-134
- “Regenerate Trust Certificates” on page 13-136

## 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 3-16). The command-line interface appears, showing you that you’re logged in.

```

login as: admin
admin@singlewire's password:
Last login: Tue Jun 2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

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-----
MIIC4zCCAacsCAQAwTElMakGAlUEBhMCdXMxCzAJBgNVBAGMAndpMQowCAyDVQQH
DAFhMQowCAyDVQQKDAFhMQowCAyDVQQLEDAFhMScwJQYDVQQDDDB5JmZvcmlhQ2Fz
...abridged...
GN3irc+2FfVMZIVBOgkrZZqF0UNzkkkAwTGo5FvJ4Uuaety2ng4j95tZU+TmAsyf
aRMmQ8jeorsO5oimC7CblxwJ9lu7202UIjLQprD/EQ9016xekVc/UPsTIUORNiBS
ucQv8JWsm1S/vYfn5D0Y7eSulB0eHIk=
-----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
kAzsSQBSKGHKeXTU92wuH0aVfg5kVC4a1L4CP03dhHICafbJaLRyDOTwPnZy0+n+
rRa8XH0AtP4fVYPJn/qyOf+Qp2cgT1oroCbeCcAHY5VGEMpoM/w9WB9RuwwCwgCL
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 InformaCast 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 InformaCast 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.

```

Aa0CAUkwggFFMBMGAlUdJQcMMAoGCCsGAQUFBwMBMB0GAlUdDgQWBBS6tTCvBLIT
0d6Vq3                                IfSkVOSUM5
MFBVQj                                BF67JxWe77
9dqlyl                                Npbmds2Wl3
cmUubG                                E4LVFBLmNy
bDA+Bg                                iC5086hsWi
T4EKkK                                EFBQcDATAN
Bgkqhk                                G906WW10BW
PzySpD                                y36q2pYVOL
IlnlT6                                mI9EPHh4+j
UYdpQT5484RkSLfzvQjInTR3PpMY6327WAjtdEh50les9SayVBu6ShOb2nM0jx6w
Mfhq40bTP+IQkGZVqTVdQzuZ4gpVekTO0JfgxOrUFU+UDb7xfI5RIqLyBK/bTyvF
X6vh2pvAgjnlKsGY6oUI6n0ghkacGBmHIFWcCIXJbodiA==
-----END CERTIFICATE-----

Certificate subject and fingerprints:
subject= /C=us/ST=wi/L=wi/O=Singlewire/OU=qa/CN=
emailAddress=qa-internal@singlewire.com
MD5:    49:16:86:42:FA:35:                :AF
SHA1:   78:27:F5:8A:4A:E2:                :C0:1D:6F:F8:27
SHA256: 34:1F:7F:96:A8:65:                :44:C2:C9: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.

```

CltKrhYIpkHhrM8+nm=8?%/(3eR3K+48K+6fF0keCmm=8-YO,lv7D0eQKtXaRltKmg
95I69Lapq4d+mpuC                                LryNlj9ikLG
W89lj1LzZqWUwS=C                                zEvDgYDVR0P
AQH/BAQDAggGMA8G                                f5rvMyBQwk3
+KJtWpRXoQKjMBAG                                vUAA4IBAQBf
8BQXm0Z1OT6//GRt                                kqokFEfEqyX
j9Gps6orSSv0iIbe                                aqXhVZZ13GF
cTgik8KQVYQzqOrI                                3Lh/4m+ntz8
aQBefWfaK7zJp8URARuyk75ZmKP8L00BVYalN3oyyqMR1GRZwKGFW5kQSH9uZq6v
yKZqetDSDJKE9E7JQgNLE7MH5NBwO3AVv330zU6f+SuiY77uhn4MVSpuqG3GQabb
1GDy8VuyFaiRX5qVRBc
-----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:                :84
SHA1:   16:7B:B6:23:D6:78:                :DA:BB:8C:36:05
SHA256: 9E:1E:8D:9D:D1:5B:                :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/MeTi2NJStw44dcOR9fwnuPCHUxjDyFsjXRrO+Ocr886ffRd5ml.
gqxTqufxs6zmpKjleWuRbqRlBFqPNzjwLlncROIIqsQOrVwZolSgja0Y5mE+aY5I
lOzdSrQbHlXhN821qGBTXNbelEvnVQqrt8qxln6Siz+9MlKGVacZEZH9Qw72zQ==
-----END CERTIFICATE-----

Analyzing certificate, please wait...

Trusted certificate subject and fingerprints:
subject= /DC=lan/DC=singlewire/CN=SinglewireIssuingCA-2018-0A
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 InformaCast Appliance, apply your signed certificate, and start the InformaCast 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:A0:72:7F: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 InformaCast Appliance trusts, either signed or self-signed.

- Step 1** Log into the command-line interface (see “Log into the Command-line Interface” on page 3-16). The command-line interface appears, showing you that you're logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$
```

- 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 3-16). The command-line interface appears, showing you that you’re logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

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 InformaCast Appliance, 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 3-16). The command-line interface appears, showing you that you're logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$
```



- 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 InformaCast Appliance (see “Reboot the InformaCast Appliance” on page 13-12). 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 3-16). The command-line interface appears, showing you that you’re logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

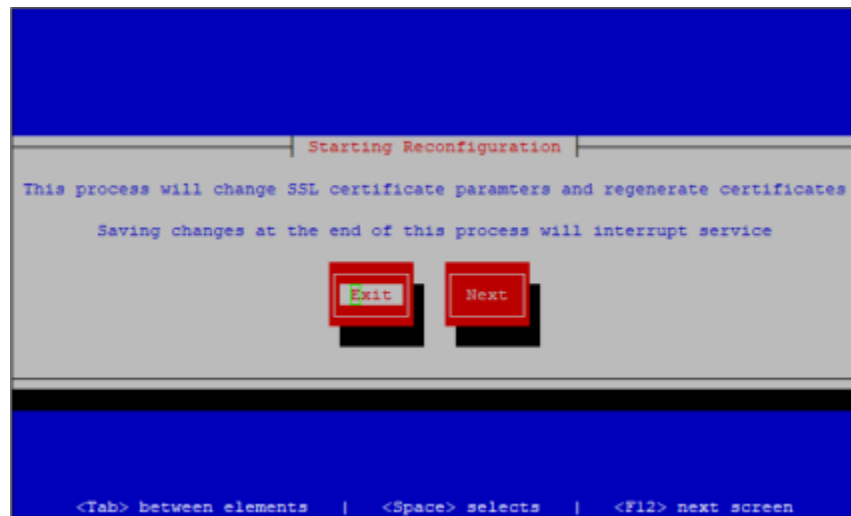
Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$
```

- 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.

```
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:~$ regenerate-ssl-certificates

Saving changes, please wait. Services are being restarted.
Updating the system certificate trust store and restarting applications, please
wait...
Changes saved, applications restarted

admin@singlewire:~$ █
```

## Upgrade InformaCast Appliance

Stay current with the latest InformaCast features by upgrading the InformaCast Appliance, which includes the InformaCast application and the platform on which InformaCast runs. Curious about your new features? Review “Release Notes” on page 14-1 for a list of everything that has improved with your new version.

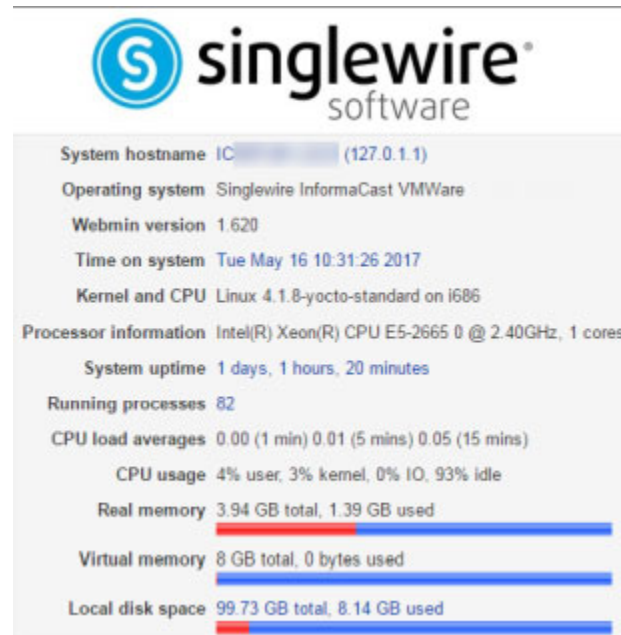
### Note the Differences

If you are upgrading from an earlier version of InformaCast Appliance, please review “Release Notes” on page 14-1 for a list of new features.

### Determine Your Current Version

Depending on the version of InformaCast 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 3-9 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 13-140. 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 3-14 for specific steps). The Webmin homepage appears.



- Step 4** Look at the top line of the Webmin homepage, e.g. InformaCast 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 13-140 or “Upgrade InformaCast 12.0.1 and Later” on page 13-168.
- 

### **Upgrade InformaCast Pre-12.0.1**

You can download the latest version of InformaCast Appliance from the Cisco website. Contact Cisco if you need help.

Depending on the version of InformaCast Appliance from which you are starting, you will follow different steps.

#### ***8.3 or 8.4***

Your download should include three package files and two ISO files 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-12.17.1.iso
- CiscoPagingServer\_UpgradeFrom1217To-14.4.2.iso

#### ***8.5.1, 9.0.1, or 9.0.2***

Your download will include two package files and two ISO files that must be uploaded/attached in the following order:

- CiscoPagingServer\_9.1.1.deb
- CiscoPagingServer\_11.5.2.deb
- CiscoPagingServer\_UpgradeFrom115To-12.17.1.iso
- CiscoPagingServer\_UpgradeFrom1217To-14.4.2.iso

#### ***9.1.1, 11.0.1, 11.0.2, 11.0.5***

Your download will include one package file and two ISO files that must be uploaded/attached in the following order:

- CiscoPagingServer\_11.5.2.deb
- CiscoPagingServer\_UpgradeFrom115To-12.17.1.iso
- CiscoPagingServer\_UpgradeFrom1217To-14.4.2.iso

#### ***11.5.1 or 11.5.2***

Your download will include two ISO files that must be uploaded/attached in the following order:

- CiscoPagingServer\_UpgradeFrom115To-12.17.1.iso
- CiscoPagingServer\_UpgradeFrom1217To-14.4.2.iso

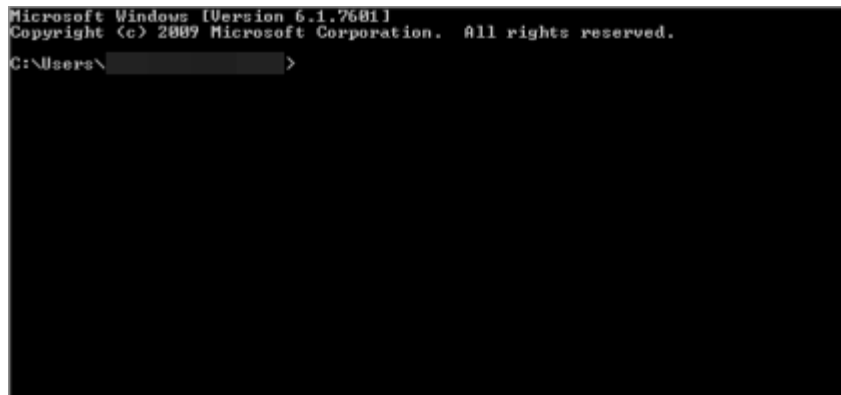
Once you've obtained your package file(s) and ISO file, you can install them and update your version of InformaCast Virtual Appliance. Depending on your starting version of InformaCast, you will follow different steps:

- 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 13-141 first and finish with “Upgrade from 11.5.1 or 11.5.2” on page 13-146
- 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 13-146

### *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 13-146.

- 
- 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.
- Step a.** Open a command window on the machine on which you've saved your .deb file(s). A command window appears.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\ >
```

**Step b.** Enter `cd <directory>` and press the **Enter** key, where <directory> is the location of your .deb file(s). The command window refreshes to the location of your directory.

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\>cd C:\Users\ \Downloads
C:\Users\ \Downloads>
```

**Step c.** Enter `pscp <file name> admin@<InformaCast 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 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`.

**Step d.** Enter your Virtual Appliance password at the prompt and press the **Enter** key. The file will be transferred.

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\>cd C:\Users\ \Downloads
C:\Users\ \Downloads>pscp singlewireUAPUpgrade-2.1.deb admin@172.
38.222.3:/home/admin
admin@172.38.222.3's password:
singlewireUAPUpgrade-2.1.d | 1213351 kB | 12639.1 kB/s | ETA: 00:00:00 | 100%
C:\Users\ \Downloads>
```

**Step e.** Repeat Steps a through d until you've copied all of your .deb files to the Virtual Appliance.

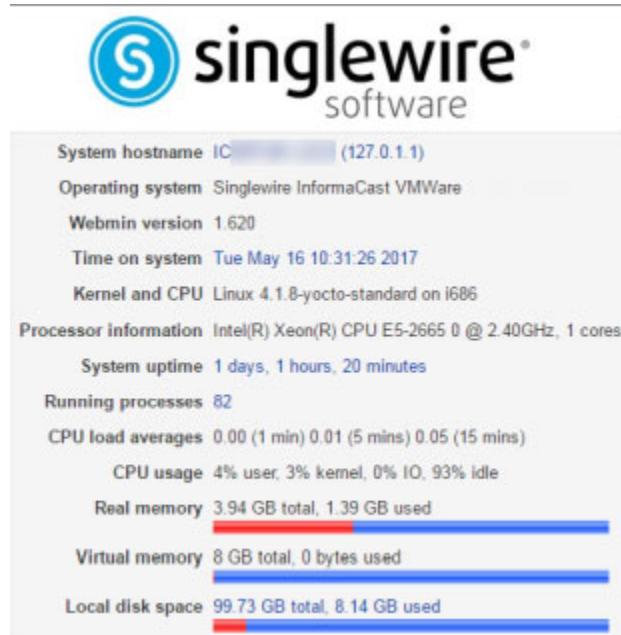
**Step 4** Log into Webmin (see "Log into Webmin" on page 3-14 for specific steps).



**Note** For versions of InformaCast Virtual Appliance prior to 8.4, you will need to go to `https://<InformaCast Appliance IP Address>/webmin`, where <InformaCast Appliance IP Address> is the InformaCast Appliance's statically configured IP address.



The Webmin homepage appears.



**Step 5** Go to **System | Software Packages**. The Software Packages page appears.

Help..  
Module Config

## Software Packages

**Installed Packages**

Search For Package:  Package Tree

---

**Install a New Package**

Select the location to install a new Debian DPKG package from..

From local file    
 From uploaded file    
 From ftp or http URL   
 Package from APT

---

**Identify a File**

Enter a command or the pathname of a file to search the Debian DPKG database for.

Search For:

---

**Upgrade All Packages**

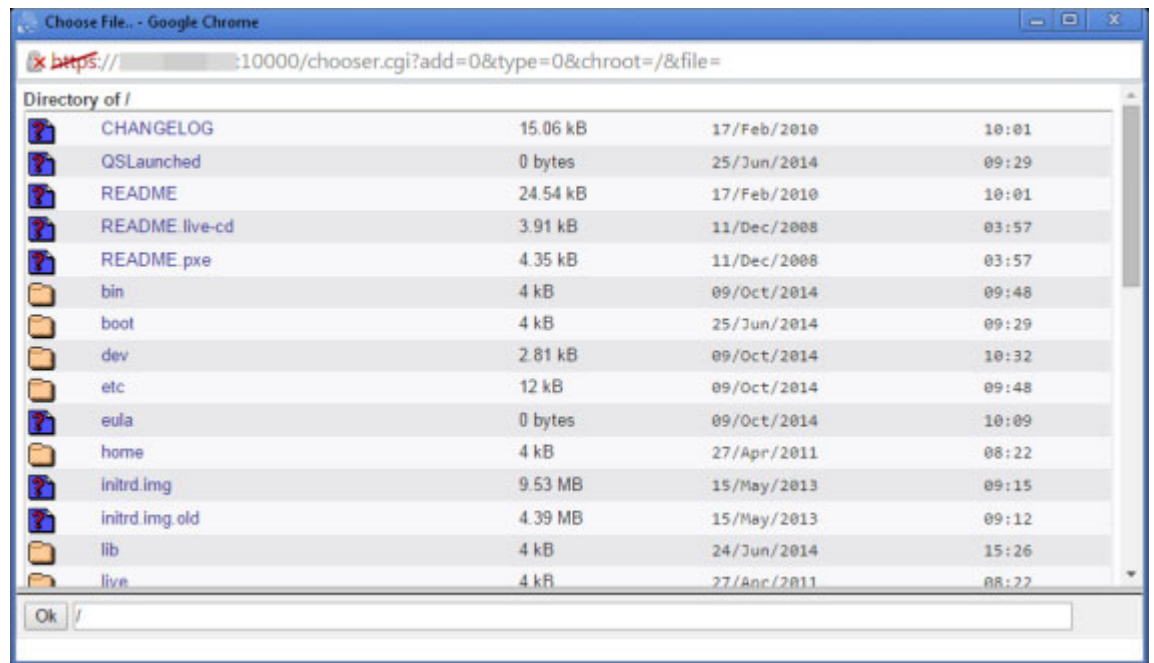
**APT package upgrade options**

Resynchronize package list (update)  Yes  No

Upgrade mode  Distribution upgrade (upgrade-dist)  Normal upgrade  Don't upgrade

Only show which packages would be upgraded  Yes  No

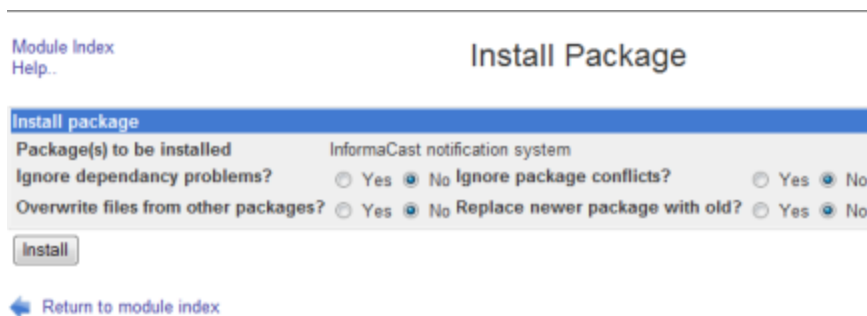
**Step 6** Select the **From local file** radio button in the *Install a New Package* area and click its **Browse** button. The Choose File window appears.



**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 Appliance” on page 13-12)
    - 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 Appliance” on page 13-12)
    - 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 13-146
  - 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 Appliance” on page 13-12)
    - 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 13-146
  - 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 13-146.

### *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.



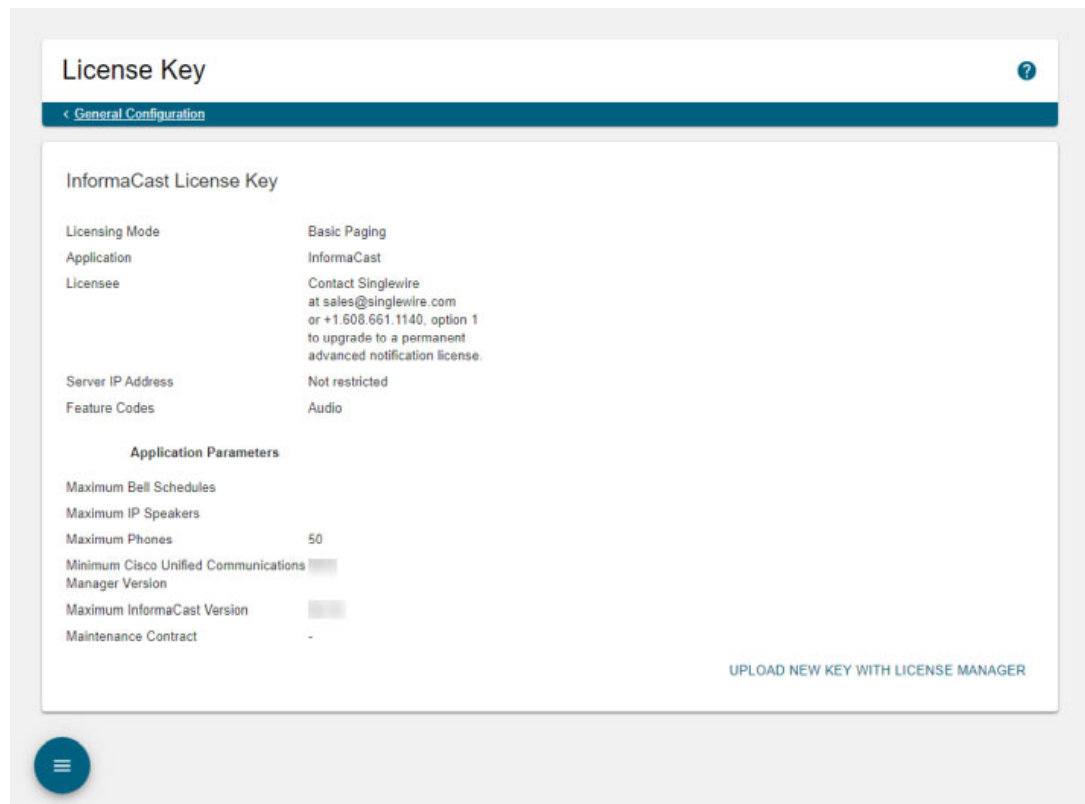
---

**Note** If you're coming here from “Upgrade from 8.3 through 11.0.5” on page 13-141, you can skip Steps 1 and 2.

---

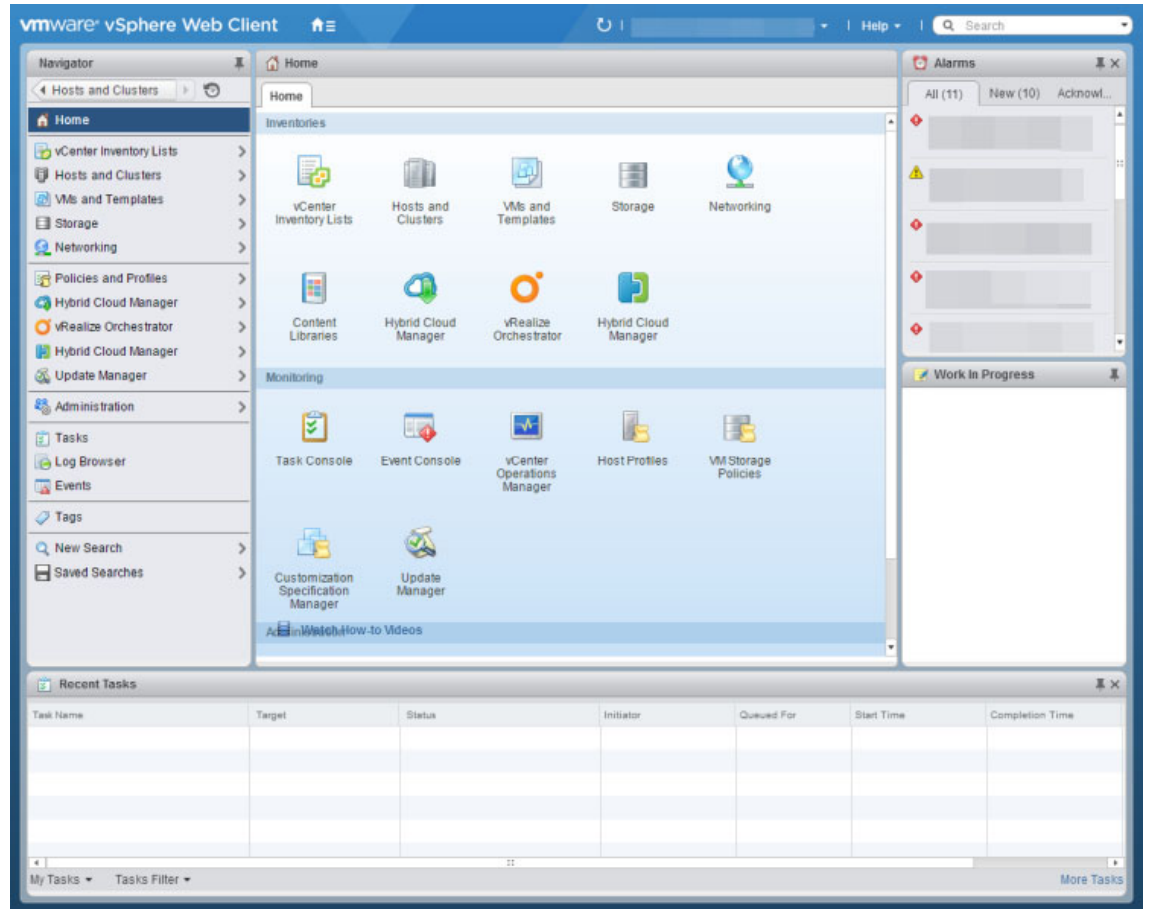
- Step 1** Declare an outage window and ensure that it falls outside of regular business hours.
- Step 2** Create a clone of your current InformaCast Virtual Appliance installation, which allows for a return to the previous version of InformaCast if there are problems with the upgrade. Snapshots are not sufficient.

**Step 3** Go to **System Administration | General Configuration | License Key**. The License Key page appears.

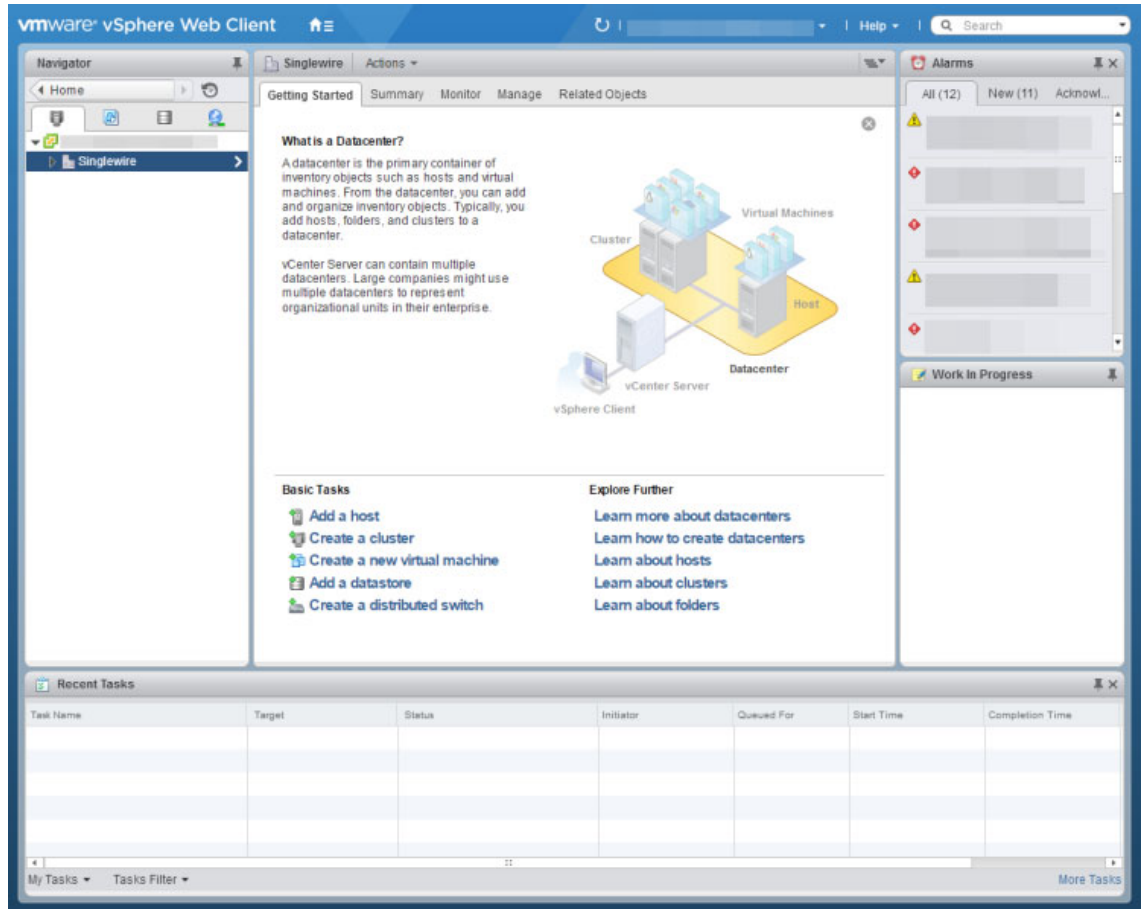


- Step 4** Ensure that the Maximum InformaCast Version parameter is higher than the InformaCast version to which you're upgrading. If it is not, you'll need to contact Singlewire, request a new license, and upload it before continuing.
- Step 5** Shut down the Virtual Appliance (see “Shut Down the InformaCast Appliance” on page 13-14).
- Step 6** Connect the CiscoPagingServer\_UpgradeFrom115To-12.17.1.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](#).

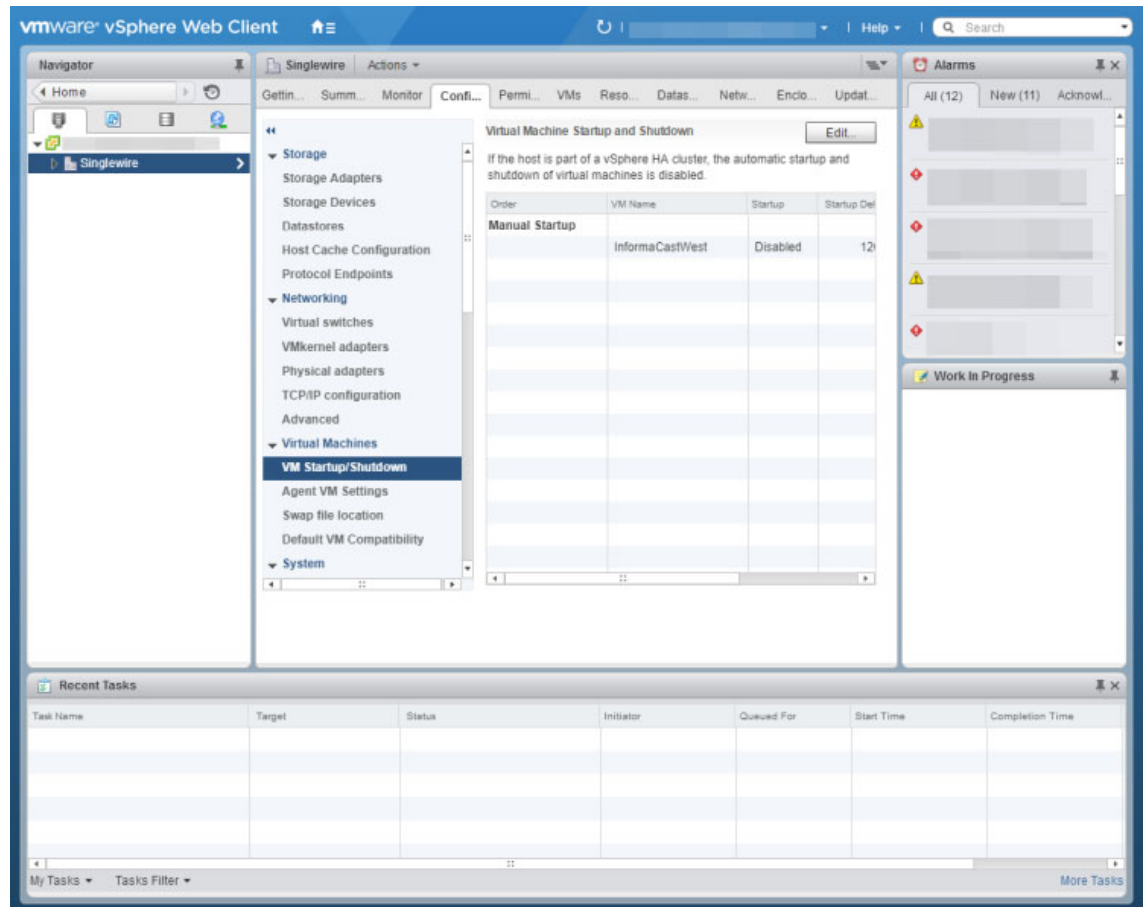
**Step 7** Open a web browser and log into your vSphere web client. The vSphere Web Client page appears.



**Step 8** Click the **Hosts and Clusters** icon. The vSphere Web Client page refreshes.

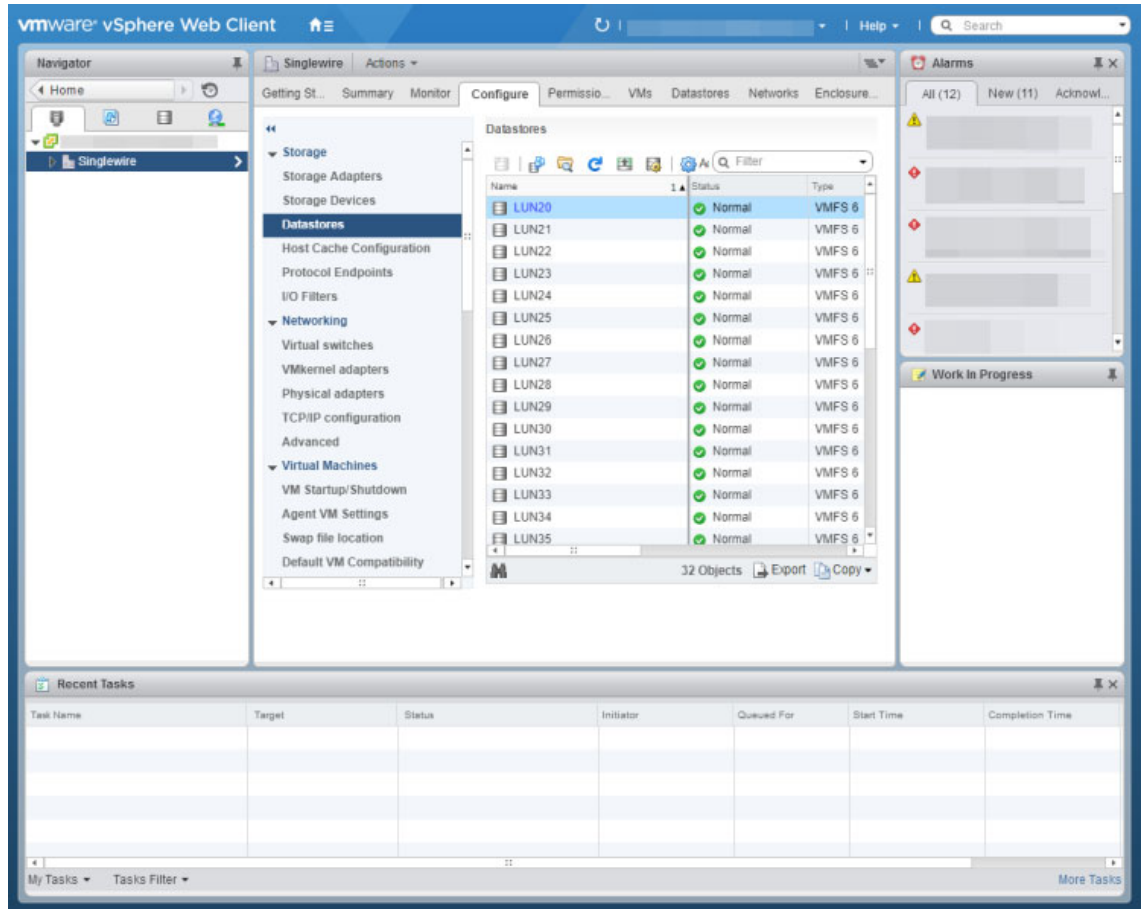


- Step 9** Select the host server on which the InformaCast Virtual Appliance is located and select its **Configure** tab. The vSphere Web Client window's right pane refreshes.

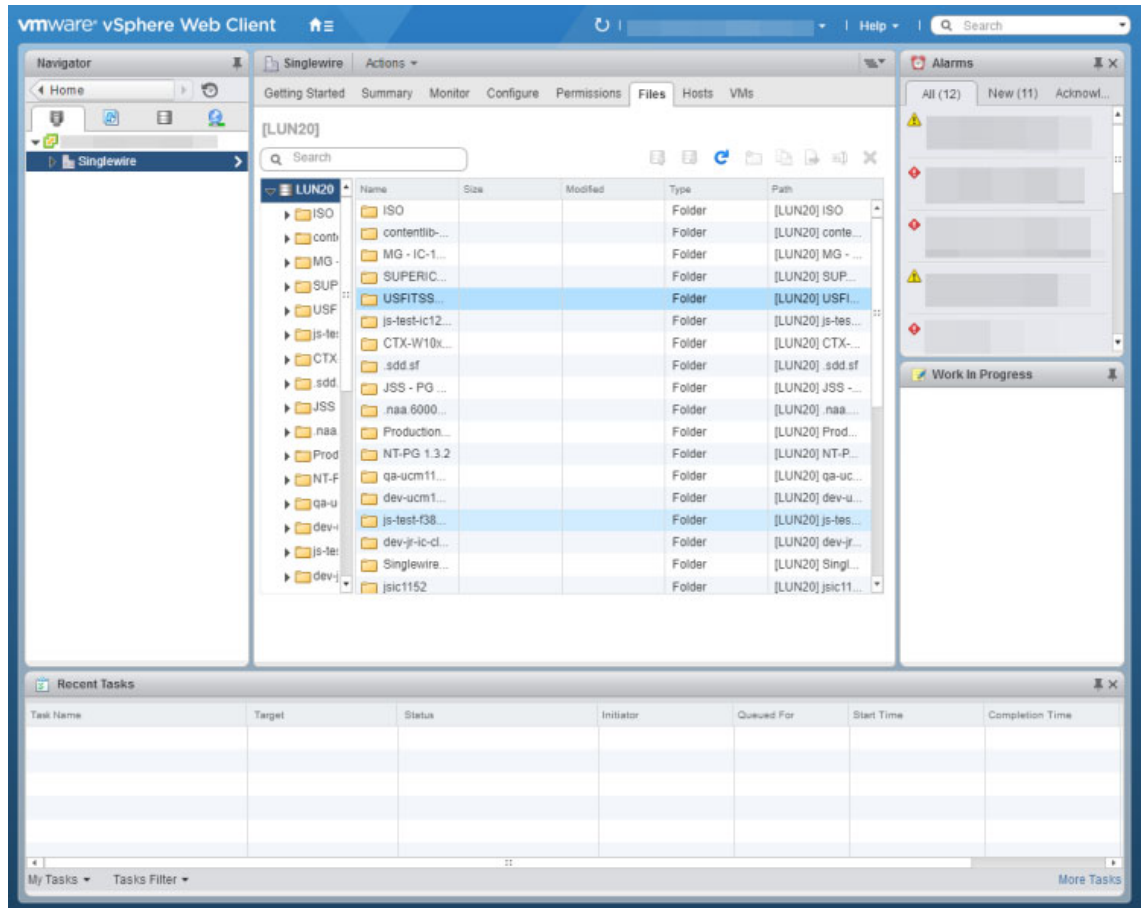




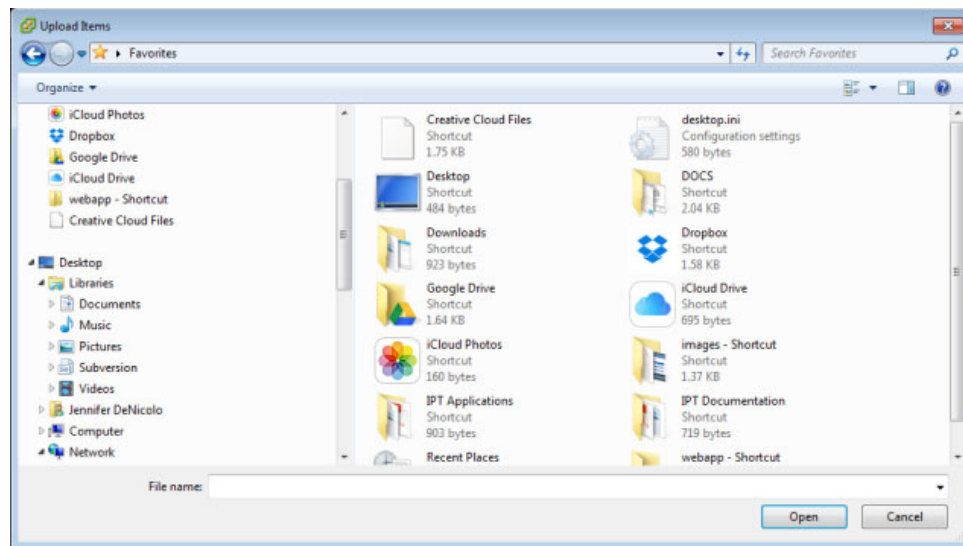
**Step 10** Click the **Datastores** link under **Storage**. The vSphere Web Client window right pane refreshes.



**Step 11** Right click the datastore to which you want to upload the CiscoPagingServer\_UpgradeFrom115To-12.17.1.iso file and select **Browse Files**. The vSphere Web Client window right pane refreshes and you're taken to the **Files** tab.

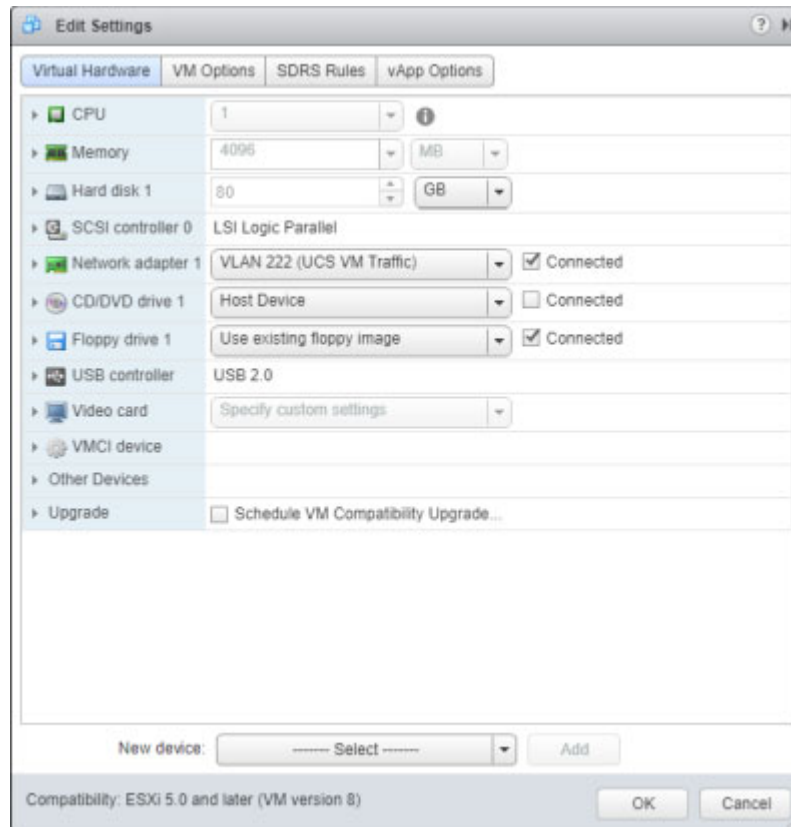


**Step 12** Click the **Upload a file to this datastore** icon and select **Upload File**. The Upload Items dialog box appears.

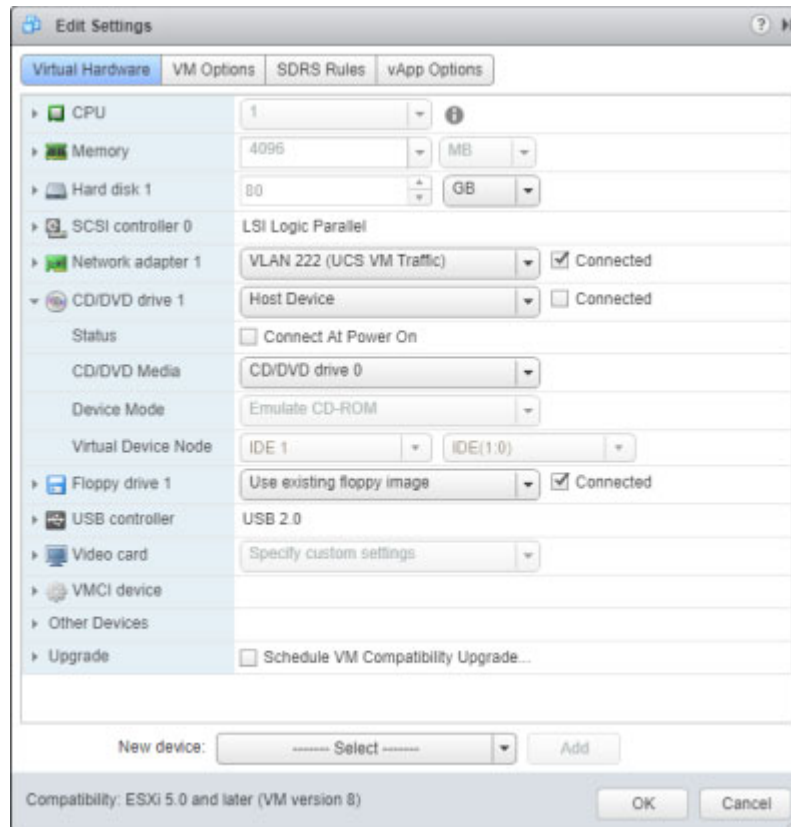


**Step 13** Navigate to the location of the `CiscoPagingServer_UpgradeFrom115To-12.17.1.iso` file, select it, and click the **Open** button. vSphere will upload the ISO file to your host server.

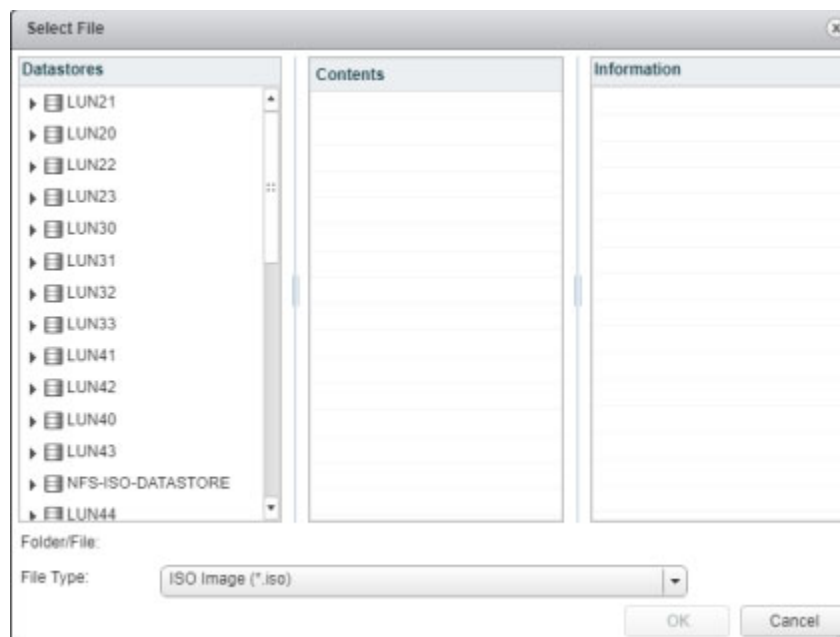
**Step 14** Right click your virtual machine and select **Edit Settings**. The Edit Settings pop-up window appears.



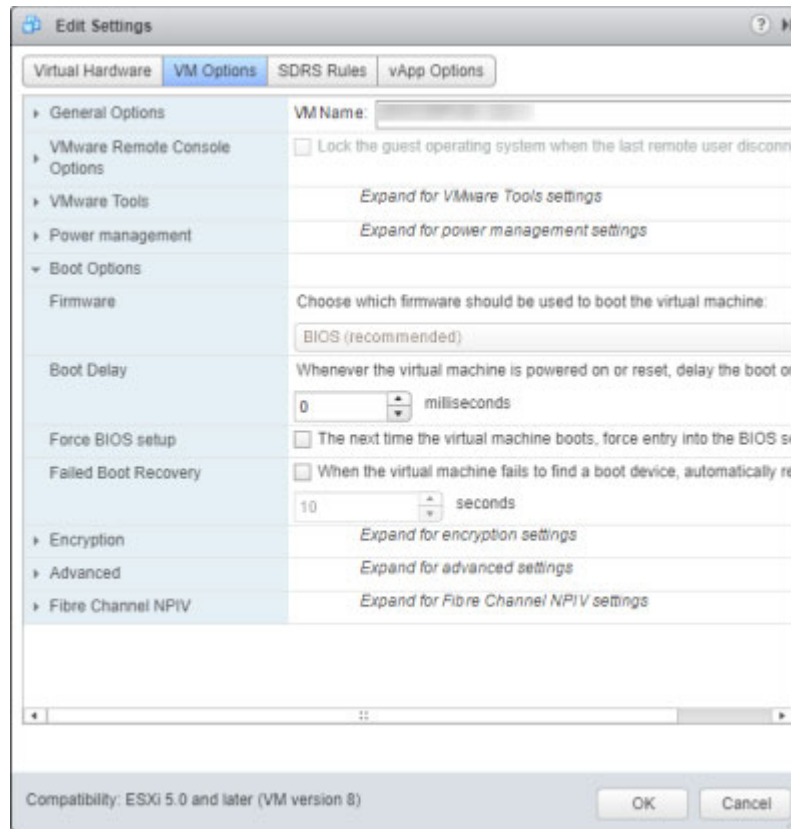
**Step 15** Select the **CD/DVD drive 1** link. The Edit Settings pop-up window refreshes.



**Step 16** Select **Datastore ISO File** from the second dropdown menu. The Select File pop-up window appears.

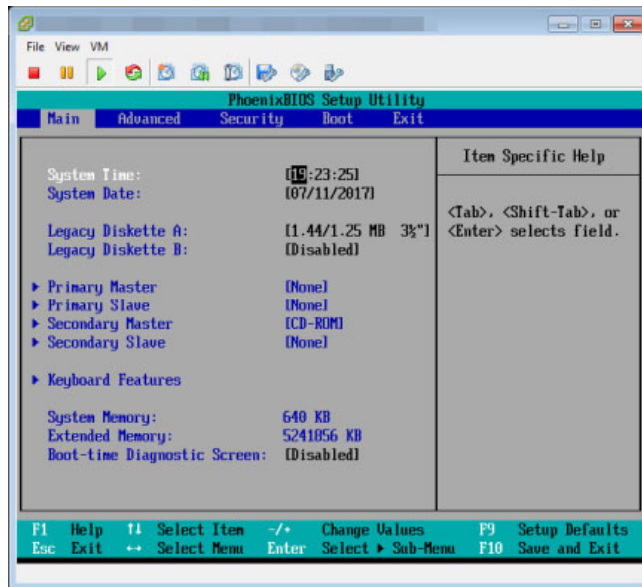


- Step 17** Navigate to the location of the CiscoPagingServer\_UpgradeFrom115To-12.17.1.iso file, select it, and click the **OK** button.
- Step 18** Select the **Connect at Power On** checkbox.
- Step 19** Select the **VM Options** tab and expand **Boot Options**. The Edit Settings pop-up window refreshes.

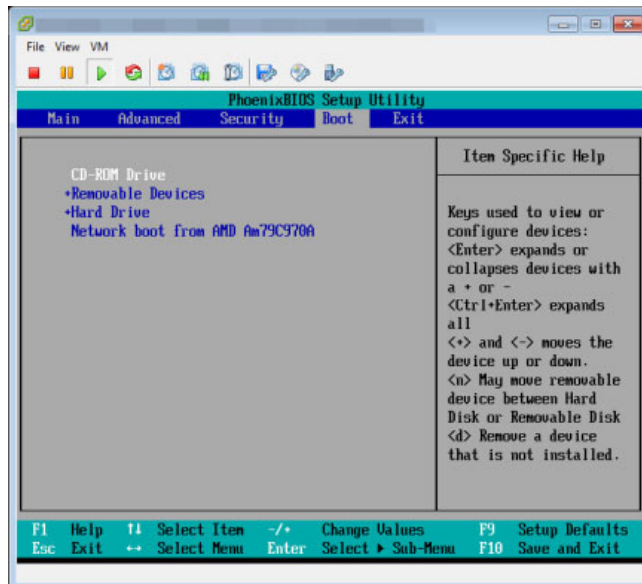


- Step 20** Select the **Force BIOS setup** checkbox and click the **OK** button. The Edit Settings pop-up window closes.
- Step 21** Right click your virtual machine in the vSphere Web Client window and select **Power | Power On**.

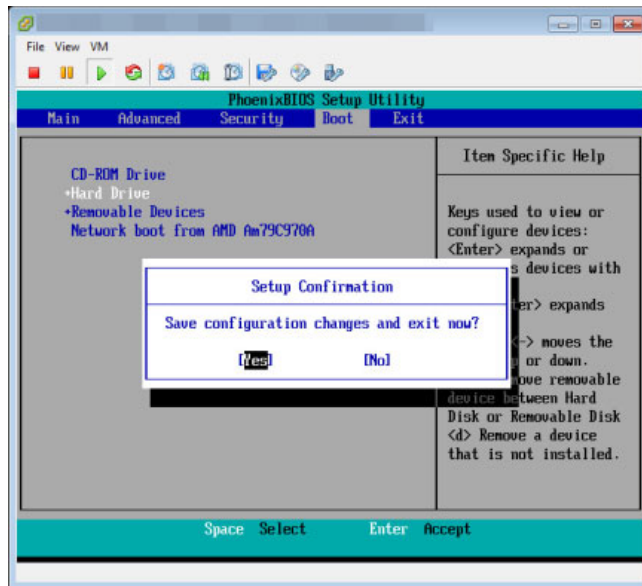
**Step 22** Right click your virtual machine and select and select **Open Console**. The Singlewire InformaCast console window appears.



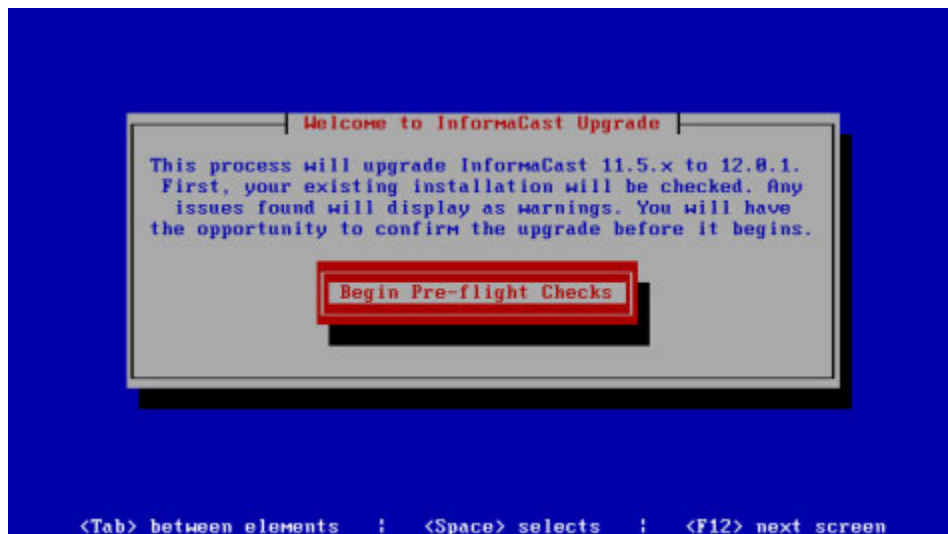
**Step 23** Click inside the Singlewire InformaCast console window and press your right arrow key three times to move to the **Boot** tab. The Singlewire InformaCast console window refreshes.



- Step 24** 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 25** Press the **F10** key. The Singlewire InformaCast console window refreshes.

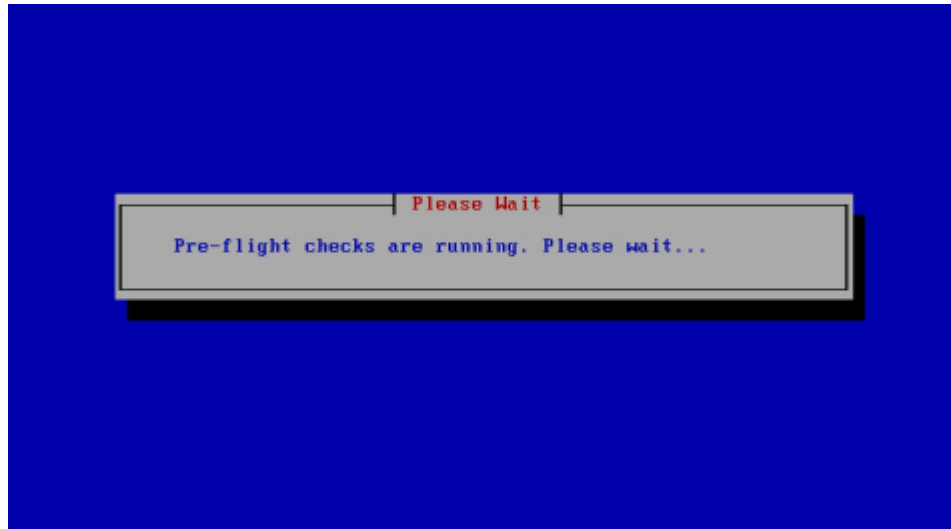


- Step 26** Press the **Enter** key to save your changes. The Virtual Appliance begins booting. This may take a few moments. When the Virtual Appliance is finished booting, the Singlewire InformaCast console window refreshes.



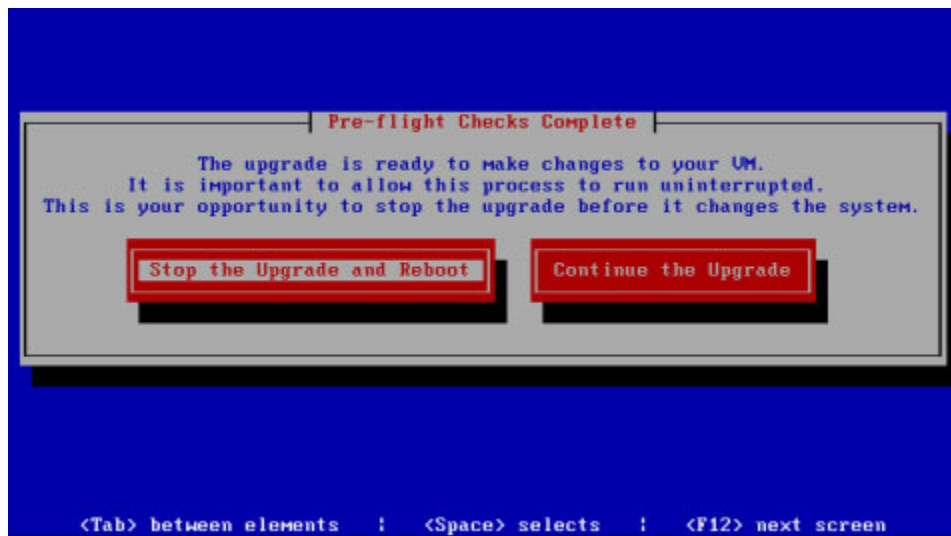


**Step 27** Press the **Enter** key to begin pre-flight checks. The Singlewire InformaCast console window refreshes.



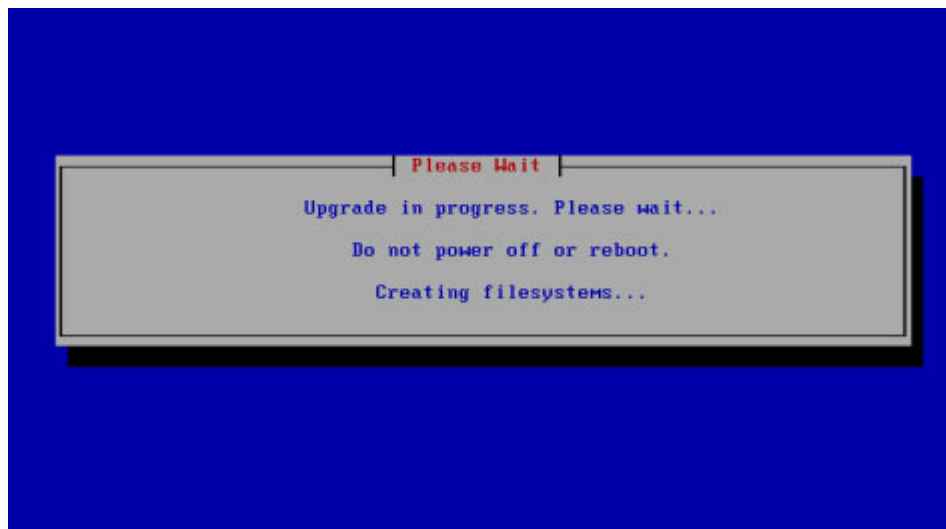
Pre-flight checks do not make any changes to the Virtual Appliance. They merely check that everything is in order for your upgrade and give you a way to back out if anything is not in order. If the pre-flight checks do find anything amiss, you may be prompted to address the issues before continuing with your upgrade.

When pre-flight checks are finished, the Singlewire InformaCast console window refreshes.

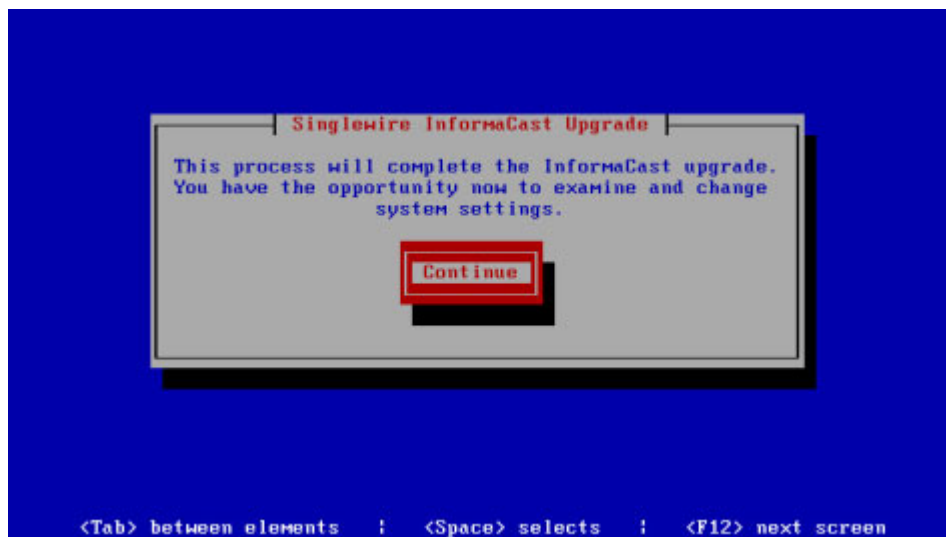


**Note** Continuing with the following steps will make changes to the Virtual Appliance. Once started, you must finish the process to ensure a successful upgrade.

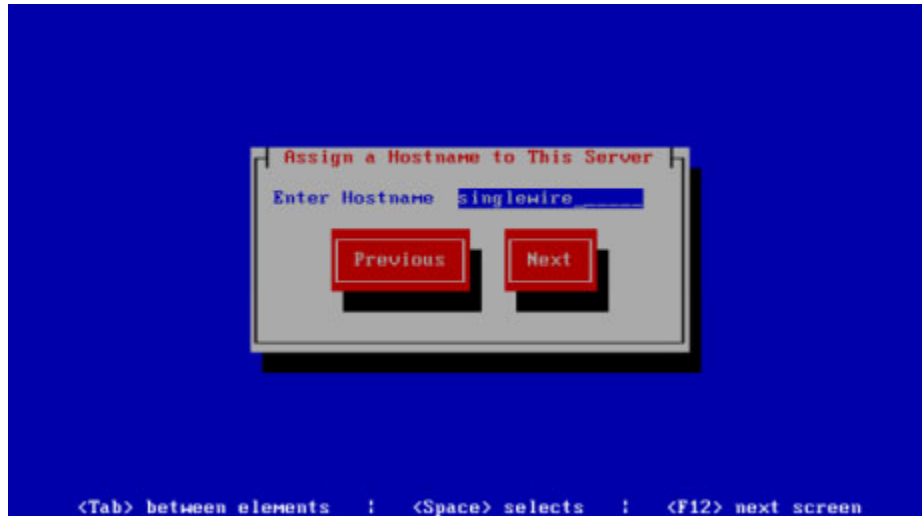
**Step 28** Select the **Continue the Upgrade** button. The Singlewire InformaCast console window refreshes and your upgrade begins. This may take a few moments.



When your upgrade is finished, the Singlewire InformaCast console window refreshes.

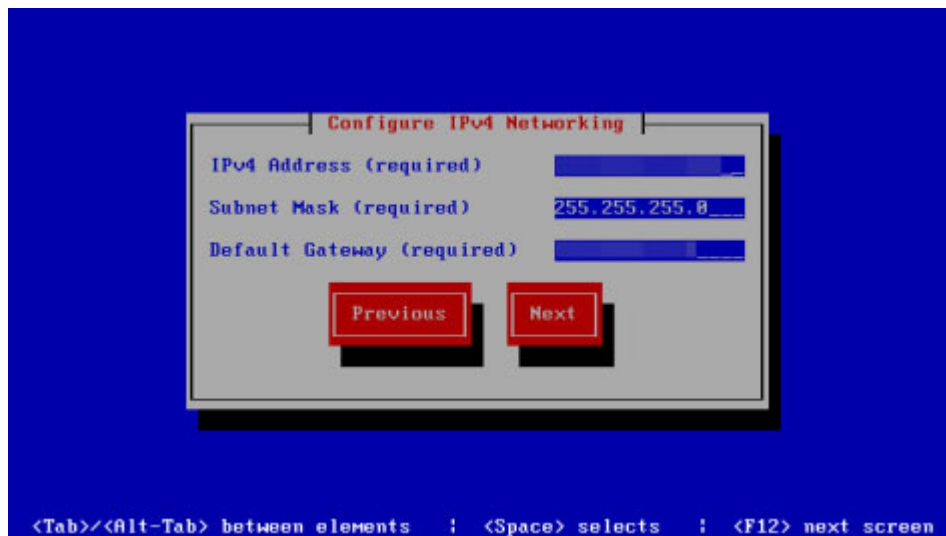


**Step 29** Select the **Continue** button. The Singlewire InformaCast console window refreshes.

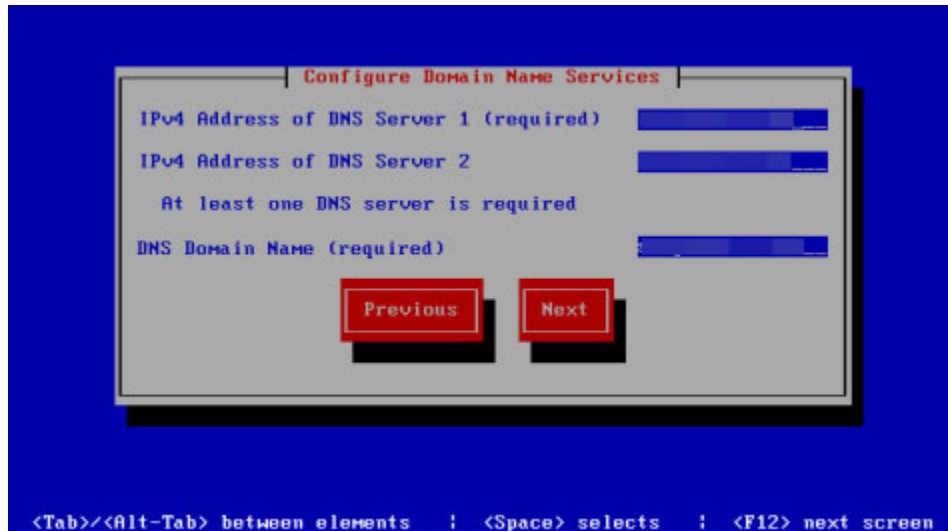


**Step 30** Enter a hostname for your InformaCast Virtual Appliance server in the **Enter Hostname** field, e.g. InformaCastWest. This hostname will appear in Webmin's user interface.

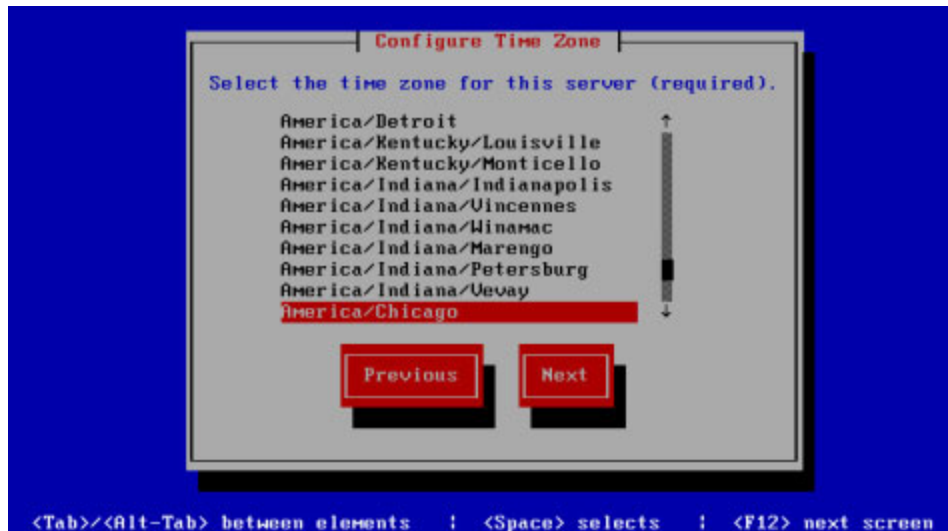
**Step 31** Select the **Next** button. The InformaCast Appliance then attempts to use DHCP to find suitable IP addresses on your network. The Singlewire InformaCast console window refreshes.



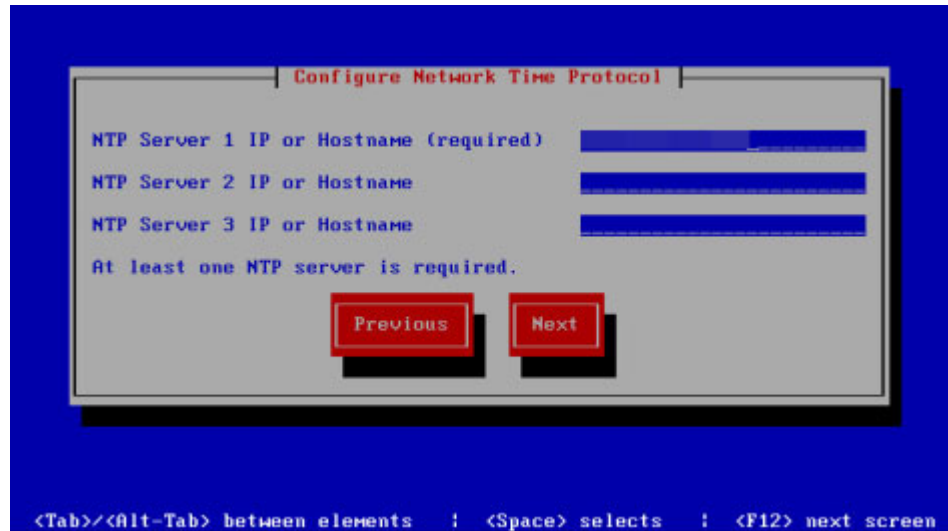
- Step 32** Accept these IP addresses or provide valid ones of your own in the **IPv4 Address**, **Subnet Mask**, and **Default Gateway** fields and select the **Next** button. The Singlewire InformaCast console window refreshes.



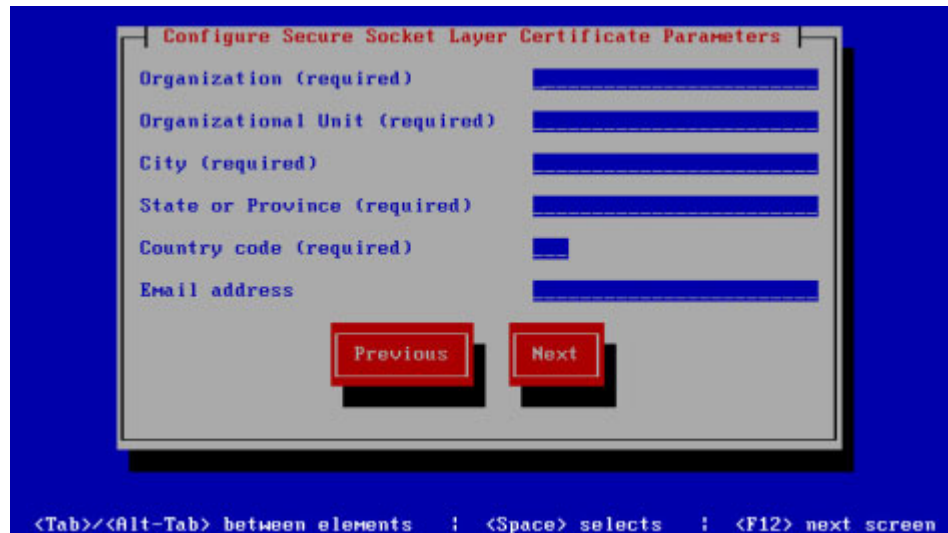
- Step 33** Enter at least one DNS server IP address in the field provided or accept the one provided to you and enter a DNS domain name. Select the **Next** button. The Singlewire InformaCast console window refreshes.



**Step 34** Select a time zone for your InformaCast Appliance and select the **Next** button. The InformaCast Appliance then attempts to find an NTP server on your network. The Singlewire InformaCast console window refreshes.



**Step 35** 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 console window refreshes.



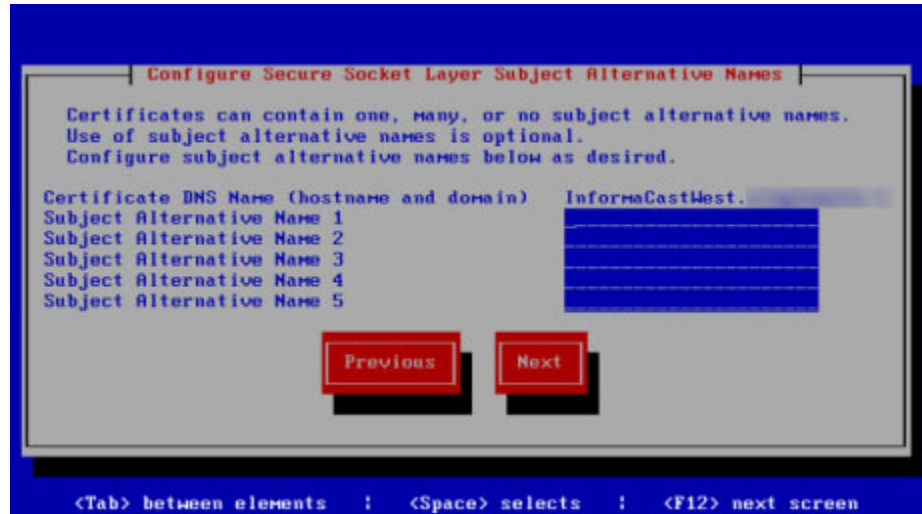
**Step 36** Enter the information necessary for a signed certificate (while the information is required, signing the certificate is not). A signed certificate, which can protect against Man-in-the-Middle (MITM) attacks, is an electronic document that proves ownership of a public key; it includes information 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 37** Select the **Next** button. The Singlewire InformaCast console window refreshes.



**Step 38** 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 39** 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 console window refreshes.





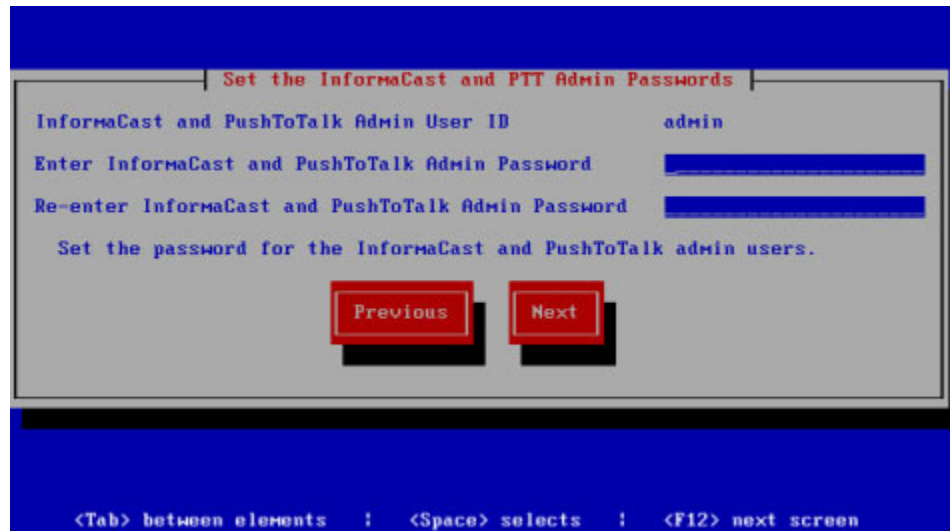
**Note** If you've never changed your password from the default of "changeMe," you will be forced to change your password.

**Step 40** Enter a password in the **Enter 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 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 41** 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 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 42** 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 43** Select the **Next** button. The Singlewire InformaCast console window refreshes.

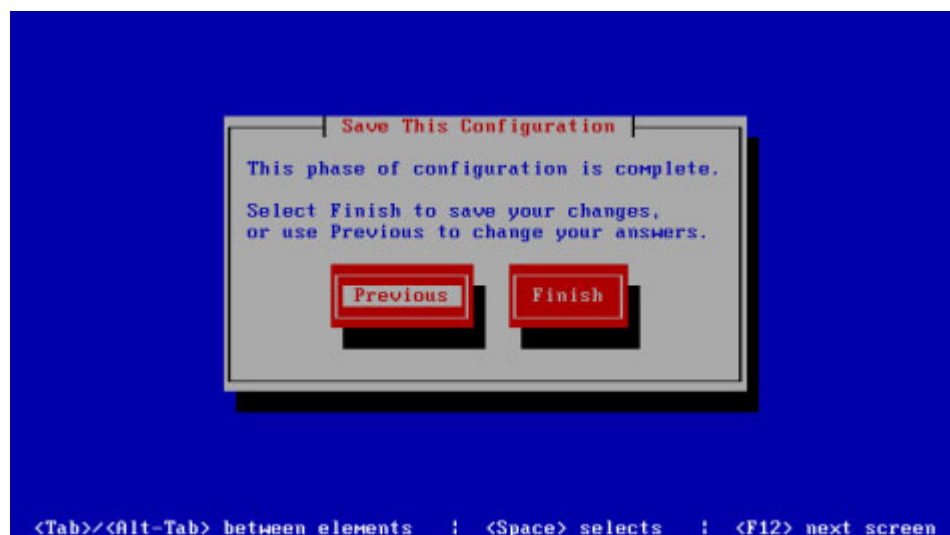


**Step 44** Enter a security passphrase in the **Enter Security Passphrase** and **Re-enter Security Passphrase** fields. This passphrase is used to secure your backups of the InformaCast Appliance. You must remember this passphrase. Singlewire Support personnel cannot recover it for you if it's lost.



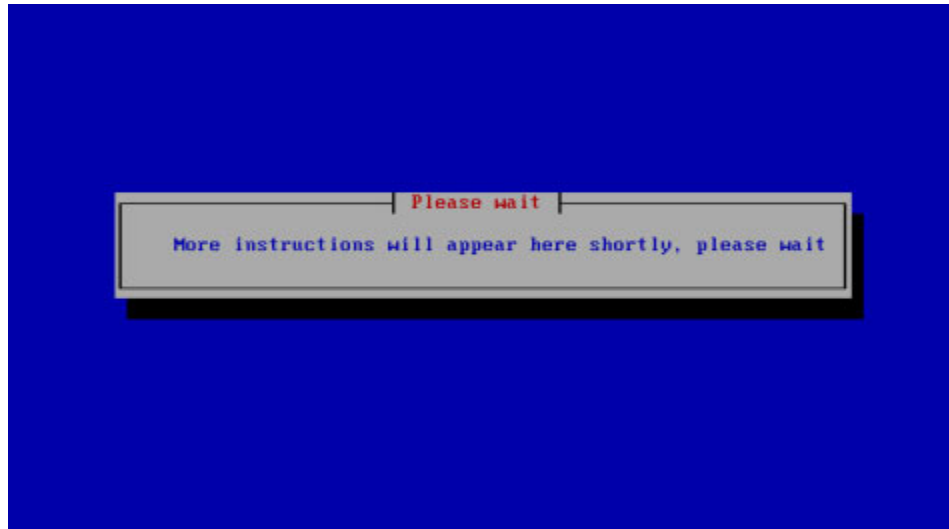
**Note** Your passphrase must follow the same character requirements as your OS admin password.

**Step 45** Select the **Next** button. The Singlewire InformaCast console window refreshes.



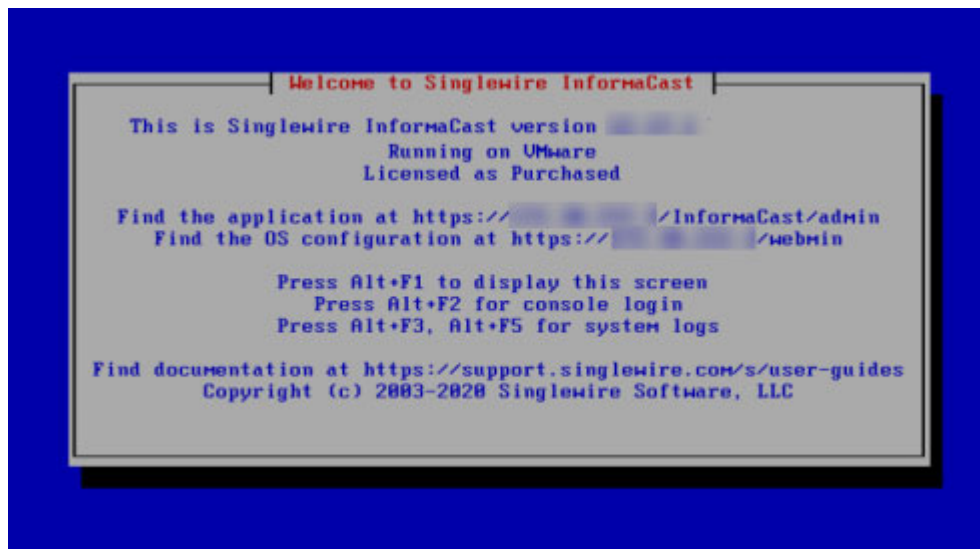


**Step 46** Select the **Finish** button to save your changes. The Singlewire InformaCast console window refreshes.



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

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



**Step 47** Make a note of the displayed IP address. This is the IP address of the InformaCast Appliance's landing page, which you will use to access the InformaCast Appliance, Control Center, and Webmin web user interfaces.

**Step 48** Close your open console window.

**Step 49** Take a snapshot of the powered off virtual machine (optional).

**Step 50** Clear your web browser's cache.

**Step 51** Log into Webmin (see "Log into Webmin" on page 3-14) to verify your new version.

**Step 52** Continue with “Upgrade InformaCast 12.0.1 and Later” on page 13-168.

## Upgrade InformaCast 12.0.1 and Later

In order to stay current with the latest InformaCast features, you need to upgrade your InformaCast Appliance to the latest version. When upgrading, it's important to understand your InformaCast Appliance's architecture as well as following the steps to upgrade through Webmin or the command-line interface (CLI).



**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 13-140 first.

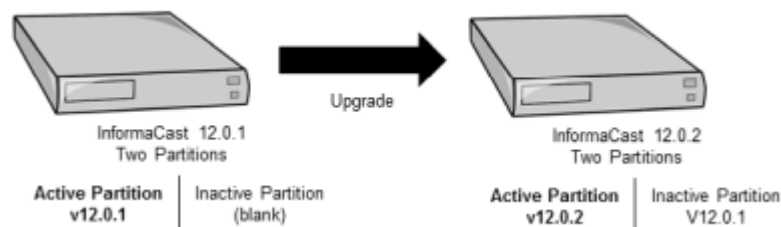


**Note** If you are upgrading from InformaCast 12.0.1, 12.0.2, or 12.1.1, you will need to perform the steps in either “Upgrade Through Webmin” on page 13-169 or “Upgrade Through the Command-line Interface” on page 13-175 twice: once to upgrade to 12.17.1 and a second time to upgrade to the current version.

### *Understand the InformaCast Appliance's Architecture*

The InformaCast Appliance is a dually-partitioned platform that is comprised of one active partition and one inactive partition. Having two partitions means you can move between versions of InformaCast easily while preserving the previous version 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.

When running as a virtual machine, InformaCast should be deployed on hardware supported by VMware ESXi; however, you do not need to worry about upgrading your VMware tools in conjunction with upgrading InformaCast because InformaCast doesn't use them. Instead, it 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.”<sup>1</sup> Open VM Tools offers the same services as VMware Tools, but simplifies your management because its upgrades are completely transparent to you, occurring during InformaCast upgrades. There's nothing for you to manage or upgrade.

### Upgrade Through Webmin

Use the following steps to Upgrade InformaCast 12.0.1 and later through Webmin.



#### Note

If you're coming here from “Upgrade InformaCast Pre-12.0.1” on page 13-140, you can skip Steps 1 and 2.



#### Caution

If you are upgrading from InformaCast 12.1.1, you cannot do so through Webmin. You will have to use InformaCast’s command-line interface (see “Upgrade Through the Command-line Interface” on page 13-175).

- 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 11-14). Optionally, take a VMware snapshot.
- Step 3** Ensure your InformaCast server(s) are in a GREEN state by logging in to the command-line interface and running the **show-system-health** command.

If there are errors, you can learn more information about them by running the less /var/log/health-errors.log command.

Fix any errors and ensure your InformaCast server(s) are in a GREEN state before continuing with your upgrade.



#### Tip

Contact Cisco TAC if you need further assistance in resolving your errors.



#### Note

The **show-system-health** command is only available for InformaCast servers 12.15.1 and newer. If your InformaCast servers are older than 12.15.1, you can skip this step.

1. <https://github.com/vmware/open-vm-tools>

**Step 4** Go to **System Administration | General Configuration | License Key**. The License Key page appears.

InformaCast License Key	
Licensing Mode	Basic Paging
Application	InformaCast
Licensee	Contact Singlewire at sales@singlewire.com or +1.608.661.1140, option 1 to upgrade to a permanent advanced notification license.
Server IP Address	Not restricted
Feature Codes	Audio
Application Parameters	
Maximum Bell Schedules	
Maximum IP Speakers	
Maximum Phones	50
Minimum Cisco Unified Communications Manager Version	<input type="text"/>
Maximum InformaCast Version	<input type="text"/>
Maintenance Contract	-

UPLOAD NEW KEY WITH LICENSE MANAGER

**Step 5** Ensure that the Maximum InformaCast Version parameter is higher than the InformaCast version to which you're upgrading. If it is not, you'll need to contact Cisco TAC, request a new license, and upload it before continuing (see "Upload a New License" on page 4-2).

**Step 6** Download the upgrade file from [cisco.com](http://cisco.com).

**Step 7** 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.

**Step a.** Open a command window on the machine on which you've saved your .upg file. A command window appears.

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\>
```

**Step 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.

**Step c.** Enter `pscp <file name> admin@<InformaCast Appliance IP Address>:/upgrade` at the prompt and press the **Enter** key, where <file name> is the name of your .upg file and <InformaCast Appliance IP Address> is your actual Virtual Appliance's IP address, e.g. `pscp CiscoPagingServer-UpgradeTo14.4.2_XXXX.upg admin@111.22.333.4:/upgrade`.

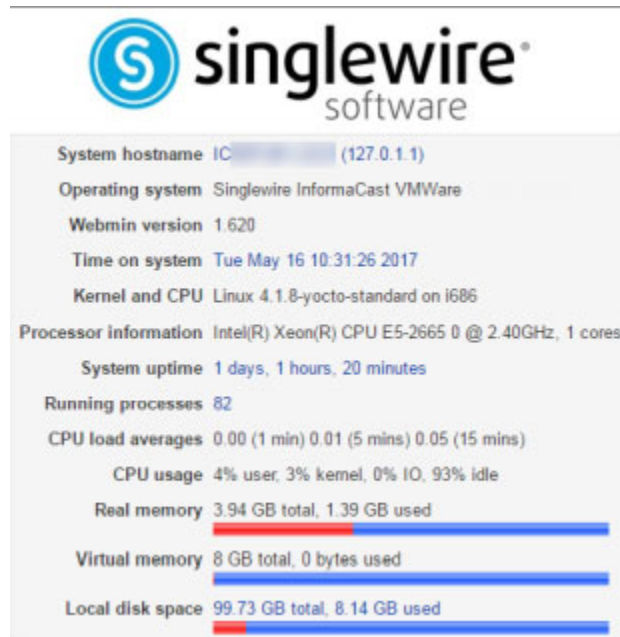


**Note** If you are upgrading from InformaCast 12.0.1, 12.0.2, or 12.1.1, you'll want to enter the `CiscoPagingServer-UpgradeTo12.17.1_XXXX.upg` file name.

**Step d.** Enter your Virtual Appliance password at the prompt and press the **Enter** key. The file will be transferred.

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\>cd C:\Users\ \Downloads
C:\Users\ \Downloads>pscp singlewireUaUpgrade-2.1.deb admin@172.
30.222.3:/home/admin
admin@172.30.222.3's password:
singlewireUaUpgrade-2.1.d | 1213351 kB | 12639.1 kB/s | ETA: 00:00:00 | 100%
C:\Users\ \Downloads>
```

**Step 8** Log into Webmin (see “Log into Webmin” on page 3-14). The Webmin homepage appears.



**Step 9** Go to **System | Upgrade or Switch Versions**. The Upgrade to a New Version or Switch Versions page appears.

[Module Config](#)

### Upgrade to a New Version or Switch Versions

This system has two copies of itself, an active version and an inactive version. The active version is the one you are using now. The inactive version is a holding area for either a new upgrade or an older version. A switch version will swap the inactive version for the active one.

#### Active Version

The currently running version is 12.0.1

An upgrade to version 12.0.2 is available. Avoid using the system until the upgrade has finished.

[Upgrade to version 12.0.2](#)

#### Inactive Version

The inactive version is empty. This is normal if the system has never been upgraded or the previous upgrade did not complete.

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 10** Click the **Upgrade to version** button in the *Active Version* area. The Upgrade to a New Version or Switch Versions page refreshes.

Module Config

### Upgrade to a New Version or Switch Versions


Are you sure you want to upgrade to 12.0.2?

Confirm upgrade to version 12.0.2

- Step 11** Click the **Confirm upgrade to version** button. The Upgrade to a New Version or Switch Versions page refreshes and your upgrade begins.

Module Config

### Upgrade to a New Version or Switch Versions

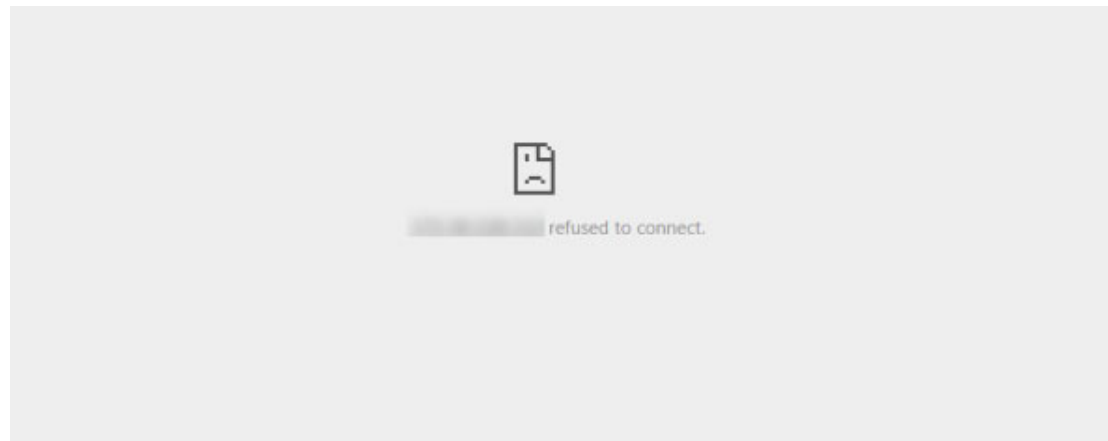
Upgrade is in progress. Please wait for it to complete. Closing this page does not affect the upgrade. When the upgrade succeeds, the system will switch versions automatically. 

Cancel Upgrade

2017-04-04 10:24:46 Preparing for upgrade  
2017-04-04 10:24:46 Extracting manifest

Cancel Upgrade

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 12** Refresh the page and log into Webmin again. Note that the version of InformaCast (visible in the Operating system line) has been upgraded.



**Note** Most upgrades are successful. If yours is not, you will notice it has failed when you log back into Webmin and view InformaCast's version on the Webmin homepage.

**Step 13** Go to **System | Upgrade or Switch Versions**. The Upgrade to a New Version or Switch Versions page appears.

Module Config

### Upgrade to a New Version or Switch Versions

This system has two copies of itself, an active version and an inactive version. The active version is the one you are using now. The inactive version is a holding area for either a new upgrade or an older version. A switch version will swap the inactive version for the active one.

Upgrades are downloaded from the cloud automatically. By default, new upgrades are downloaded between 1:30a and 3:30a daily. Once an upgrade is downloaded, install it using this application.

#### Active Version

The currently running version is 3.0.1  
You are running the latest available version

#### Inactive Version

The inactive version is 3.0.5. To activate it, switch versions.

Switch version to 3.0.5

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.



**Note**

As of InformaCast 12.19.1, the InformaCast operating system and application are 64-bit, and may only run on 64-bit CPUs. As such, if you upgrade from a previous version of InformaCast to 12.19.1, but then use the **Switch version** button to return to your previous version, you cannot use the **Switch version** button again to return to 12.19.1. You will need to re-apply the upgrade, i.e. use the **Upgrade to version** command. This does not apply to upgrades from pre-12.18.1 to 12.18.1 or from 12.19.1 to post-12.19.1.

**Step 14** Perform the steps in this section a second time (only required if you are upgrading from InformaCast 12.0.1, 12.0.2, or 12.1.1). When you get to this step, enter the CiscoPagingServer-UpgradeTo14.4.2\_XXXX.upg file name.

**Step 15** Clear your web browser's cache.

**Step 16** Perform any necessary post-upgrade steps, depending on your environment:

- 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 8-88).
- If your starting version of InformaCast was 11.5.2 and earlier, the backup process changed between the 11.x and 12.x versions of InformaCast. You will need to re-configure your backup of InformaCast (see “Manage InformaCast Backups” on page 11-11).
- If you previously had a signed certificate, new security requirements necessitate regenerating it (see “Create and Install a Signed Certificate” on page 13-125).

### *Upgrade Through the Command-line Interface*

Use the following steps to Upgrade InformaCast 12.0.1 and later through the command-line interface.

**Note**

If you're coming here from “Upgrade InformaCast Pre-12.0.1” on page 13-140, you can skip Steps 1 and 2.

**Caution**

If you are upgrading from InformaCast 12.1.1 to the current version, you must use InformaCast's command-line interface (CLI).

**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 11-14). Optionally, take a VMware snapshot.

**Step 3** Ensure your InformaCast server(s) are in a GREEN state by logging in to the command-line interface and running the **show-system-health** command.

If there are errors, you can learn more information about them by running the less /var/log/health-errors.log command.

Fix any errors and ensure your InformaCast server(s) are in a GREEN state before continuing with your upgrade.



**Tip** Contact Cisco TAC if you need further assistance in resolving your errors.



**Note** The **show-system-health** command is only available for InformaCast servers 12.15.1 and newer. If your InformaCast servers are older than 12.15.1, you can skip this step.

**Step 4** Go to **System Administration | General Configuration | License Key**. The License Key page appears.

**Step 5** Ensure that the Maximum InformaCast Version parameter is higher than the InformaCast version to which you're upgrading. If it is not, you'll need to contact Singlewire, request a new license, and upload it before continuing.

**Step 6** Download the upgrade file from [cisco.com](http://cisco.com).

**Step 7** 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.

**Step a.** Open a command window on the machine on which you've saved your .upg file. A command window appears.

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\>
```

**Step 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.

**Step c.** Enter `pscp <file name> admin@<InformaCast Appliance IP Address>:/upgrade` at the prompt and press the **Enter** key, where <file name> is the name of your .upg file and <InformaCast Appliance IP Address> is your actual Virtual Appliance's IP address, e.g. `pscp CiscoPagingServer-UpgradeTo14.4.2_XXXX.upg admin@111.22.333.4:/upgrade`.



**Note** If you are upgrading from InformaCast 12.0.1, 12.0.2, or 12.1.1, you'll want to enter the `CiscoPagingServer-UpgradeTo12.17.1_XXXX.upg` file name.

**Step d.** Enter your Virtual Appliance password at the prompt and press the **Enter** key. The file will be transferred.

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\>cd C:\Users\ \Downloads
C:\Users\ \Downloads>pscp singlewireUaUpgrade-2.1.deb admin@172.
30.222.3:/home/admin
admin@172.30.222.3's password:
singlewireUaUpgrade-2.1.d | 1213351 kB | 12639.1 kB/s | ETA: 00:00:00 | 100%
C:\Users\ \Downloads>
```

- Step 8** Log into the command-line interface (see “Log into the Command-line Interface” on page 3-16). The command-line interface appears, showing you that you’re logged in.

```

login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$

```

- Step 9** Enter **ls upgrade** at the prompt and press the **Enter** key. The command-line interface refreshes.

```

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:~$ ls upgrade
UpgradeTo.....upg
admin@singlewire:~$

```

- Step 10** Ensure that only one upgrade file exists in the upgrade directory.



**Tip** If there's more than one file, delete it by entering **rm upgrade/<name of file>** at the prompt and pressing the **Enter** key. Enter **y** at the prompt to confirm the deletion and press the **Enter** key. The file is removed.

- Step 11** Enter **apply-upgrade** at the prompt and press the **Enter** key. The system will begin the upgrade. When complete, InformaCast will automatically restart and boot to the new version.



**Note** Most upgrades are successful. If yours is not, you will notice it has failed when you log back into the command-line interface and view InformaCast's version in the console window.

- Step 12** Perform the steps in this section a second time (only required if you are upgrading from InformaCast 12.0.1, 12.0.2, or 12.1.1). When you get to this step, enter the CiscoPagingServer-UpgradeTo14.4.2\_XXXX.upg file name.
- Step 13** Perform any necessary post-upgrade steps, depending on your environment:
- 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 8-88).
  - If your starting version of InformaCast was 11.5.2 and earlier, the backup process changed between the 11.x and 12.x versions of InformaCast. You will need to re-configure your backup of InformaCast (see “Manage InformaCast Backups” on page 11-11).
  - If you previously had a signed certificate, new security requirements necessitate regenerating it (see “Create and Install a Signed Certificate” on page 13-125).

## Switch Virtual Appliance Versions

Virtual Appliance's dually-partitioned platform (comprised of one active partition and one inactive partition) means that you can upgrade to a new version of InformaCast while preserving the one in case of conflict. The switch-version command allows you to switch your inactive partition with your active one, restoring your older version of InformaCast.

- Step 1** Log into the command-line interface (see “Log into the Command-line Interface” on page 3-16). The command-line interface appears, showing you that you’re logged in.

```

login as: admin
admin@singlewire's password:
Last login: Tue Jun  2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$
```

- Step 2** Enter **switch-version** at the prompt and press the **Enter** key. The command-line interface refreshes and begins the process of switching your active and inactive partitions.

```

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:~$ switch-version
Switch version begins. Please wait...
#!/bin/sh
exec tail -n +3 $0
# Custom menu entry for Singlewire's rescue image. Be careful not to change
# the 'exec tail' line above.

# Boot directly into default kernel
#set timeout=5

set timeout_style=hidden

echo ''
# This is in the rescue partition
cat /etc/swlogo.txt

```




---

**Note** This process will reboot the Virtual Appliance.

---




---

**Note** As of InformaCast 12.19.1, the InformaCast operating system and application are 64-bit, and may only run on 64-bit CPUs. As such, if you upgrade from a previous version of InformaCast to 12.19.1, but then use the **switch-version** command to return to your previous version, you cannot use the **switch-version** command again to return to 12.19.1. You will need to re-apply the upgrade, i.e. use the **apply-upgrade** command. This does not apply to upgrades from pre-12.18.1 to 12.18.1 or from 12.19.1 to post-12.19.1.

---

## Return the InformaCast Appliance to its Original System State

The **factory-reset** command will return your InformaCast Appliance to its original system state, i.e. erase all of the information stored on your InformaCast Appliance in an attempt to restore it to its original manufacturer settings.

- Step 1** Log into the command-line interface (see “Log into the Command-line Interface” on page 3-16). The command-line interface appears, showing you that you’re logged in.

```
login as: admin
admin@singlewire's password:
Last login: Tue Jun 2 10:15:02 2020

Welcome to Singlewire InformaCast

Overall system health is GREEN
Use show-system-health for more information

This build is 0 days old

admin@singlewire:~$
```

- Step 2** Enter **factory-reset** at the prompt and press the **Enter** key. Your InformaCast Appliance will go through several steps of resetting its partitions back to their original state before rebooting itself.

```
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:~$ factory-reset

admin@singlewire [1.4.0_p26949]:~$ factory-reset
2019-03-04 19:52:27+00:00 Step 0: factory-reset begins
2019-03-04 19:52:27+00:00 Step 1: Select partitions based on location of app par
partition
2019-03-04 19:52:27+00:00 Step 2: Stop services
2019-03-04 19:52:39+00:00 Step 3: Create the app and data partitions
2019-03-04 19:52:42+00:00 Step 4: Copy rescue partition
2019-03-04 19:52:47+00:00 Step 5: Verify rescue partition
2019-03-04 19:52:53+00:00 Step 6: Copy app partition
2019-03-04 19:53:25+00:00 Step 7: Verify app partition
2019-03-04 19:54:26+00:00 Step 8: Expand default data partition
2019-03-04 19:54:27+00:00 Step 9: Verify data partition
2019-03-04 19:54:27+00:00 Step 10: Cleaning up
2019-03-04 19:54:28+00:00 Step 11: Renaming partitions before switch-version
factory-reset complete and successful, beginning switch version
2019-03-04 19:54:29+00:00 Step 12: Switch versions

Broadcast message from root@singlewire (pts/0) (Mon Mar 4 19:54:36 2019):
The system is going down for reboot NOW!
```



## Release Notes

The following sections contain the release notes for InformaCast from version 8.3 (Basic Paging's inception) through the current version.

### InformaCast 14.4.2

#### Compatibility

InformaCast is compatible with the following versions of Cisco Unified Communications Manager server (including Business Edition 6000): 11.5.1, 12.0.1, 12.5.1, and 14.0.1.

#### New Features

**New Upgrade File for pre-12.0.1 Versions of InformaCast.** Two new files (CiscoPagingServer\_UpgradeFrom115To-12.17.1.iso and CiscoPagingServer\_UpgradeFrom1217To-14.4.2.iso) have 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 two ISO files (CiscoPagingServer\_8.5.1.deb, CiscoPagingServer\_9.1.1.deb, CiscoPagingServer\_11.5.2.deb, CiscoPagingServer\_UpgradeFrom115To-12.17.1.iso, and CiscoPagingServer\_UpgradeFrom1217To-14.4.2.iso)
- For 8.5.1, 9.0.1, or 9.0.2 to the current version, you will install two package files and two ISO files (CiscoPagingServer\_9.1.1.deb, CiscoPagingServer\_11.5.2.deb, CiscoPagingServer\_UpgradeFrom115To-12.17.1.iso, and CiscoPagingServer\_UpgradeFrom1217To-14.4.2.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 two ISO files (CiscoPagingServer\_11.5.2.deb, CiscoPagingServer\_UpgradeFrom115To-12.17.1.iso, and CiscoPagingServer\_UpgradeFrom1217To-14.4.2.iso)
- For 11.5.1 or 11.5.2 to the current version, you will attach one ISO file (CiscoPagingServer\_UpgradeFrom115To-14.4.2.iso)

InformaCast Virtual Appliance 8.5.1, 9.1.1, 11.5.x and 12.17.1 are waypoints in the upgrade process. For 8.3 and 8.4 versions of the InformaCast Virtual Appliance, you must upgrade to 8.5.1, reboot the InformaCast Virtual Appliance, upgrade to 9.1.1, reboot the InformaCast Virtual Appliance, upgrade to 11.5.2, upgrade to 12.17.1, and finally upgrade to 14.4.2. For 8.5.1, 9.0.1, and 9.0.2 versions of the InformaCast Virtual Appliance, you must upgrade to 9.1.1, reboot the InformaCast Virtual Appliance, upgrade to 11.5.2, upgrade to 12.17.1, and finally upgrade to 14.4.2. For 9.1.1, 11.0.1, 11.0.2, 11.0.5



versions of the InformaCast Virtual Appliance, you must upgrade to 11.5.2, upgrade to 12.17.1, and finally upgrade to 14.4.2. For 11.5.1, 11.5.2, 12.0.1, 12.0.2 and 12.1.1 versions of the InformaCast Virtual Appliance you must first upgrade to 12.17.1 and then you can upgrade to 14.4.2.

If you're already using InformaCast 12.0.1 or later, ignore this note; [your upgrade process](#) involves fewer steps and files.

## Announcement

**Log4j2 Vulnerabilities Mitigated.** On December 9, 2021, Log4j team disclosed a high-severity vulnerability in multiple versions of Log4j2 (see [CVE-2021-44228](#) for more details). A second vulnerability was discovered on December 14 (see [CVE-2021-45046](#) for more details) Upgrading to InformaCast 14.4.2 includes Log4j2 version 2.16, which resolves both vulnerabilities. Search for CSCwa47395 in Cisco's bug search tool for current details.

## 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 14.4.1

## Compatibility

InformaCast is compatible with the following versions of Cisco Unified Communications Manager server (including Business Edition 6000): 11.5.1, 12.0.1, 12.5.1, and 14.0.1.

## New Features

- **Merged Separate Environment Types.** Past versions of InformaCast had separate environments, e.g. one for users of Cisco Unified Communications Manager and one for Hybrid Runtime Environments (or non-Cisco Unified CM users), and those environments dictated the user interface elements you were able to see. There were even separate user guides. InformaCast 14.4.1 merges these separate environments into one, and makes the following improvements:
  - Organizations can now have Cisco IP phones for Unified CM and IP phones for cloud calling instead of only one or the other.
  - Moving from an installation of InformaCast integrated with Cisco Unified Communications Manager to one without it no longer requires rebuilding InformaCast from scratch.
  - New and upgraded installations of InformaCast integrated with Cisco Unified CM no longer have a default cluster, which lessens code complexity and improves stability. These installations can also delete all Cisco Unified CM clusters, including those set as Primary.
  - Deleting all Cisco Unified CM clusters stops any previous Cisco IP phone for Unified CM activations, and the next scheduled phone cache update job removes all Cisco IP phones from InformaCast's cache.
  - New and upgraded installations of InformaCast integrated with Cisco Unified CM can now take advantage of SIP server groups and SIP registrations when establishing SIP communication between InformaCast and Cisco Unified CM.

- Features’ user interface pages that require the configuration of a Cisco Unified CM cluster now display a banner (if that cluster isn’t configured), alerting users of that prerequisite and directing them to the user interface page where they can configure a cluster.
- **New System Health Alarms.** Three new system health alarms were added. In installations of InformaCast integrated with Cisco Unified CM, two new alarms, AL-ICCTIPAUTH and AL-ICCTIPOOS, alert you if InformaCast’s CTI communication to Cisco Unified CM is misconfigured or missing. For all installations of InformaCast, the new AL-ICMSPACE alarm alerts you if InformaCast is running low on Java Virtual Machine (JVM) Metaspace memory, i.e. less than 1% left. If any of these alarms are RED, the Overall alarm will also show RED. RED alarms indicate that notification delivery is impacted. You should investigate and remediate them immediately. See “Display System Health Information” on page 13-54 for more information.
- **Improved the Format of the InformaCast REST API Log.** The REST API log’s format changed from .log to .json, making it machine-readable and protecting against log injection from user-supplied data in API requests. The show-log-restapi and follow-log-restapi CLI commands remained the same.
- **Redact IP Addresses from Unencrypted Log Bundles.** Within unencrypted log bundles are IP addresses that you may not want to expose to anyone outside of your organization. If you're in this situation, you can use the new redact-last-log-bundle command to replace all IP addresses in your most recent log bundle with placeholders, such as “IPADDRESS\_1” and “IPADDRESS\_2,” etc.
- **New Upgrade File for pre-12.0.1 Versions of InformaCast.** Two new files (CiscoPagingServer\_UpgradeFrom115To-12.17.1.iso and CiscoPagingServer\_UpgradeFrom1217To-14.4.1.iso) have 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 two ISO files (CiscoPagingServer\_8.5.1.deb, CiscoPagingServer\_9.1.1.deb, CiscoPagingServer\_11.5.2.deb, CiscoPagingServer\_UpgradeFrom115To-12.17.1.iso, and CiscoPagingServer\_UpgradeFrom1217To-14.4.1.iso)
  - For 8.5.1, 9.0.1, or 9.0.2 to the current version, you will install two package files and two ISO files (CiscoPagingServer\_9.1.1.deb, CiscoPagingServer\_11.5.2.deb, CiscoPagingServer\_UpgradeFrom115To-12.17.1.iso, and CiscoPagingServer\_UpgradeFrom1217To-14.4.1.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 two ISO files (CiscoPagingServer\_11.5.2.deb, CiscoPagingServer\_UpgradeFrom115To-12.17.1.iso, and CiscoPagingServer\_UpgradeFrom1217To-14.4.1.iso)
  - For 11.5.1 or 11.5.2 to the current version, you will attach one ISO file (CiscoPagingServer\_UpgradeFrom115To-14.4.1.iso)

InformaCast Virtual Appliance 8.5.1, 9.1.1, 11.5.x and 12.17.1 are waypoints in the upgrade process. For 8.3 and 8.4 versions of the InformaCast Virtual Appliance, you must upgrade to 8.5.1, reboot the InformaCast Virtual Appliance, upgrade to 9.1.1, reboot the InformaCast Virtual Appliance, upgrade to 11.5.2, upgrade to 12.17.1, and finally upgrade to 14.4.1. For 8.5.1, 9.0.1, and 9.0.2 versions of the InformaCast Virtual Appliance, you must upgrade to 9.1.1, reboot the InformaCast Virtual Appliance, upgrade to 11.5.2, upgrade to 12.17.1, and finally upgrade to 14.4.1. For 9.1.1, 11.0.1, 11.0.2, 11.0.5 versions of the InformaCast Virtual Appliance, you must

upgrade to 11.5.2, upgrade to 12.17.1, and finally upgrade to 14.4.1. For 11.5.1, 11.5.2, 12.0.1, 12.0.2 and 12.1.1 versions of the InformaCast Virtual Appliance you must first upgrade to 12.17.1 and then you can upgrade to 14.4.1.

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 14.2.1

The following information pertains to InformaCast 14.2.1.

### Compatibility

InformaCast is compatible with the following versions of Cisco Unified Communications Manager server (including Business Edition 6000): 11.5.1, 12.0.1, 12.5.1, and 14.0.1.

### New Features

- **Display Your Consent Token.** The `show-latest-consent-token` command allows you to display your most recent consent token, which was generated during your performance of either the `enable-support` or `recovery` commands. In combination with your token ID number, your consent token secures communication between yourself and Cisco TAC.
- **New Upgrade File for pre-12.0.1 Versions of InformaCast.** Two new files (`CiscoPagingServer_UpgradeFrom115To-12.17.1.iso` and `CiscoPagingServer_UpgradeFrom1217To-14.2.1.iso`) have 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 two ISO files (`CiscoPagingServer_8.5.1.deb`, `CiscoPagingServer_9.1.1.deb`, `CiscoPagingServer_11.5.2.deb`, `CiscoPagingServer_UpgradeFrom115To-12.17.1.iso`, and `CiscoPagingServer_UpgradeFrom1217To-14.2.1.iso`)
  - For 8.5.1, 9.0.1, or 9.0.2 to the current version, you will install two package files and two ISO files (`CiscoPagingServer_9.1.1.deb`, `CiscoPagingServer_11.5.2.deb`, `CiscoPagingServer_UpgradeFrom115To-12.17.1.iso`, and `CiscoPagingServer_UpgradeFrom1217To-14.2.1.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 two ISO files (`CiscoPagingServer_11.5.2.deb`, `CiscoPagingServer_UpgradeFrom115To-12.17.1.iso`, and `CiscoPagingServer_UpgradeFrom1217To-14.2.1.iso`)
  - For 11.5.1 or 11.5.2 to the current version, you will attach one ISO file (`CiscoPagingServer_UpgradeFrom115To-14.2.1.iso`)

InformaCast Virtual Appliance 8.5.1, 9.1.1, 11.5.x and 12.17.1 are waypoints in the upgrade process. For 8.3 and 8.4 versions of the InformaCast Virtual Appliance, you must upgrade to 8.5.1, reboot the InformaCast Virtual Appliance, upgrade to 9.1.1, reboot the InformaCast Virtual Appliance, upgrade to 11.5.2, upgrade to 12.17.1, and finally upgrade to 14.2.1. For 8.5.1, 9.0.1, and 9.0.2 versions of the InformaCast Virtual Appliance, you must upgrade to 9.1.1, reboot the InformaCast Virtual Appliance, upgrade to 11.5.2, upgrade to 12.17.1, and finally upgrade to 14.2.1. For 9.1.1, 11.0.1, 11.0.2, 11.0.5 versions of the InformaCast Virtual Appliance, you must upgrade to 11.5.2, upgrade to 12.17.1, and finally upgrade to 14.2.1. For 11.5.1, 11.5.2, 12.0.1, 12.0.2 and 12.1.1 versions of the InformaCast Virtual Appliance you must first upgrade to 12.17.1 and then you can upgrade to 14.2.1.

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 14.0.1

The following information pertains to InformaCast 14.0.1.

### Compatibility

InformaCast is compatible with the following versions of Cisco Unified Communications Manager server (including Business Edition 6000): 11.5.1, 12.0.1, 12.5.1, and 14.0.1.

### New Features

- **Multiple Package Updates Improved Security.** The software packages InformaCast uses within its build have been updated, improving the security of the system as a whole. Singlewire strongly recommends upgrading to the latest version of InformaCast.
- **New Upgrade File for pre-12.0.1 Versions of InformaCast.** Two new files (CiscoPagingServer\_UpgradeFrom115To-12.17.1.iso and CiscoPagingServer\_UpgradeFrom1217To-14.0.1.iso) have 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 two ISO files (CiscoPagingServer\_8.5.1.deb, CiscoPagingServer\_9.1.1.deb, CiscoPagingServer\_11.5.2.deb, CiscoPagingServer\_UpgradeFrom115To-12.17.1.iso, and CiscoPagingServer\_UpgradeFrom1217To-14.0.1.iso)
  - For 8.5.1, 9.0.1, or 9.0.2 to the current version, you will install two package files and two ISO files (CiscoPagingServer\_9.1.1.deb, CiscoPagingServer\_11.5.2.deb, CiscoPagingServer\_UpgradeFrom115To-12.17.1.iso, and CiscoPagingServer\_UpgradeFrom1217To-14.0.1.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 two ISO files (CiscoPagingServer\_11.5.2.deb, CiscoPagingServer\_UpgradeFrom115To-12.17.1.iso, and CiscoPagingServer\_UpgradeFrom1217To-14.0.1.iso)
- For 11.5.1 or 11.5.2 to the current version, you will attach one ISO file (CiscoPagingServer\_UpgradeFrom115To-14.0.1.iso)

InformaCast Virtual Appliance 8.5.1, 9.1.1, 11.5.x and 12.17.1 are waypoints in the upgrade process. For 8.3 and 8.4 versions of the InformaCast Virtual Appliance, you must upgrade to 8.5.1, reboot the InformaCast Virtual Appliance, upgrade to 9.1.1, reboot the InformaCast Virtual Appliance, upgrade to 11.5.2, upgrade to 12.17.1, and finally upgrade to 14.0.1. For 8.5.1, 9.0.1, and 9.0.2 versions of the InformaCast Virtual Appliance, you must upgrade to 9.1.1, reboot the InformaCast Virtual Appliance, upgrade to 11.5.2, upgrade to 12.17.1, and finally upgrade to 14.0.1. For 9.1.1, 11.0.1, 11.0.2, 11.0.5 versions of the InformaCast Virtual Appliance, you must upgrade to 11.5.2, upgrade to 12.17.1, and finally upgrade to 14.0.1. For 11.5.1, 11.5.2, 12.0.1, 12.0.2 and 12.1.1 versions of the InformaCast Virtual Appliance you must first upgrade to 12.17.1 and then you can upgrade to 14.0.1.

If you're already using InformaCast 12.0.1 or later, ignore this note; [your upgrade process](#) involves fewer steps and files.

## Announcements

- **Newly Supported Communications Manager.** Cisco's Unified Communications Manager 14.0.1 is now supported by InformaCast.
- **Two Certificates Now Required for DialCasts Using Secure SIP over TLS.** Using a secure SIP trunk now requires you to download two certificates from Unified Communications Manager: CallManager.pem and CallManager-ECDSA.pem. Both of these certificates must then be installed on InformaCast in order for DialCasts to succeed.
- **vSphere May Prevent Changes to Virtual Machine Settings.** The latest version of vSphere supported by InformaCast seems to handle the CD/DVD drive differently than previous vSphere versions. By default, vSphere has a CD/DVD drive configured to connect to the host CD/DVD; however, InformaCast doesn't use it. In the past, this was not a problem. In vSphere 7.0, if there is no host CD/DVD in the VMware ESXi server, vSphere will refuse to save the virtual machine, and you won't be able to save changes to InformaCast's vSphere settings. While Singlewire works to resolve this issue with vSphere, if you encounter this issue, edit your virtual machine and either remove the CD/DVD entirely or select the option to connect the CD/DVD to a client drive. Neither option has any effect on InformaCast. New installations of InformaCast are unaffected by this issue.

## 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 12.22.2

The following information pertains to InformaCast 12.22.2.

### Compatibility

InformaCast is compatible with the following versions of Cisco Unified Communications Manager server (including Business Edition 6000): 11.5.1, 12.0.1, and 12.5.1.

### New Features

- **TLS 1.2 is Default Supported Protocol.** For new installations, HTTPS requests to the InformaCast Appliance now require TLS 1.2. This applies to requests from web browsers and API clients. Upgrading customers will retain their current TLS settings, which likely include insecure versions. Customers who wish to adjust their TLS and SSL supported versions can do so using the `configure-ssl-parameters` command; however, Singlewire recommends that all customers configure their systems to use only TLS 1.2.
- **New SIP Log.** A new SIP log, `sipOptions.log`, was created to simplify SIP logging and enhance the readability of the `sipStack.log`, which is one of the more high-traffic InformaCast logs. The `sipOptions.log`—accessible from the Log Directory page and the command-line interface—records the SIP OPTIONS requests sent from InformaCast to other SIP servers, e.g. LPI SIP server groups and SIP speaker telephony providers, and the SIP OPTIONS requests sent to InformaCast by other SIP servers.
- **New Upgrade File for pre-12.0.1 Versions of InformaCast.** Two new files (`CiscoPagingServer_UpgradeFrom115To-12.17.1.iso` and `CiscoPagingServer_UpgradeFrom1217To-12.22.2.iso`) have 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 two ISO files (`CiscoPagingServer_8.5.1.deb`, `CiscoPagingServer_9.1.1.deb`, `CiscoPagingServer_11.5.2.deb`, `CiscoPagingServer_UpgradeFrom115To-12.17.1.iso`, and `CiscoPagingServer_UpgradeFrom1217To-12.22.2.iso`)
  - For 8.5.1, 9.0.1, or 9.0.2 to the current version, you will install two package files and two ISO files (`CiscoPagingServer_9.1.1.deb`, `CiscoPagingServer_11.5.2.deb`, `CiscoPagingServer_UpgradeFrom115To-12.17.1.iso`, and `CiscoPagingServer_UpgradeFrom1217To-12.22.2.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 two ISO files (`CiscoPagingServer_11.5.2.deb`, `CiscoPagingServer_UpgradeFrom115To-12.17.1.iso`, and `CiscoPagingServer_UpgradeFrom1217To-12.22.2.iso`)
  - For 11.5.1 or 11.5.2 to the current version, you will attach one ISO file (`CiscoPagingServer_UpgradeFrom115To-12.22.2.iso`)

InformaCast Virtual Appliance 8.5.1, 9.1.1, 11.5.x and 12.17.1 are waypoints in the upgrade process. For 8.3 and 8.4 versions of the InformaCast Virtual Appliance, you must upgrade to 8.5.1, reboot the InformaCast Virtual Appliance, upgrade to 9.1.1, reboot the InformaCast Virtual Appliance, upgrade to 11.5.2, upgrade to 12.17.1, and finally upgrade to 12.22.2. For 8.5.1, 9.0.1, and 9.0.2 versions of the InformaCast Virtual Appliance, you must upgrade to 9.1.1, reboot the InformaCast Virtual Appliance, upgrade to 11.5.2, upgrade to 12.17.1, and finally upgrade to

12.22.2. For 9.1.1, 11.0.1, 11.0.2, 11.0.5 versions of the InformaCast Virtual Appliance, you must upgrade to 11.5.2, upgrade to 12.17.1, and finally upgrade to 12.22.2. For 11.5.1, 11.5.2, 12.0.1, 12.0.2 and 12.1.1 versions of the InformaCast Virtual Appliance you must first upgrade to 12.17.1 and then you can upgrade to 12.22.2.

If you're already using InformaCast 12.0.1 or later, ignore this note; [your upgrade process](#) involves fewer steps and files.

## Announcement

**Unrelated Issue Triggers .2 Release.** An issue unrelated to Basic InformaCast required a .2 release of InformaCast 12.22. There are no new features for InformaCast 12.22.2, just the new upgrade files for pre-12.0.1 versions of InformaCast.

## 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 12.20.1

The following information pertains to InformaCast 12.20.1.

### Compatibility

InformaCast is compatible with the following versions of Cisco Unified Communications Manager server (including Business Edition 6000): 11.5.1, 12.0.1, and 12.5.1.

### New Features

- **New Upgrade File for pre-12.0.1 Versions of InformaCast.** A new file (CiscoPagingServer\_UpgradeFrom115To-12.20.1.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-12.20.1.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-12.20.1.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-12.20.1.iso)
  - For 11.5.1 or 11.5.2 to the current version, you will attach one ISO file (CiscoPagingServer\_UpgradeFrom115To-12.20.1.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 12.20.1. 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 12.20.1. 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 12.20.1. For 11.5.1 and 11.5.2 versions of the Virtual Appliance, you can upgrade directly to 12.20.1.

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 12.19.2

The following information pertains to InformaCast 12.19.2.

### Compatibility

InformaCast is compatible with the following versions of Cisco Unified Communications Manager server (including Business Edition 6000): 11.5.1, 12.0.1, and 12.5.1.

### New Features

- **New Upgrade File for pre-12.0.1 Versions of InformaCast.** A new file (CiscoPagingServer\_UpgradeFrom115To-12.19.2.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-12.19.2.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-12.19.2.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-12.19.2.iso)
  - For 11.5.1 or 11.5.2 to the current version, you will attach one ISO file (CiscoPagingServer\_UpgradeFrom115To-12.19.2.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 12.19.2. 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 12.19.2. 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 12.19.2. For 11.5.1 and 11.5.2 versions of the Virtual Appliance, you can upgrade directly to 12.19.2.



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 12.19.1

The following information pertains to InformaCast 12.19.1.

### Compatibility

InformaCast is compatible with the following versions of Cisco Unified Communications Manager server (including Business Edition 6000): 11.5.1, 12.0.1, and 12.5.1.

### New Features

- **Improved Phone Activation and Deactivation Times.** InformaCast now adheres to Unified Communications Manager's Maximum Devices Per Provider parameter, which sets the maximum number of devices that can be opened by a CTI application instance, i.e. InformaCast. With this adherence, InformaCast will no longer open more devices on Unified Communications Manager than is allowed by the Maximum Devices Per Provider parameter, improving the speed at which broadcasts can reach your audience.
- **New Location for the Send Commands to Phones by JTAPI and Create Telephony Terminals for All Phones Checkboxes.** The **Send Commands to Phones by JTAPI** and **Create Telephony Terminals for All Phones** checkboxes have moved from the Broadcast Parameters page to the Edit Cisco Unified Communications Manager Cluster page for each cluster you have on your InformaCast server. InformaCast's adherence to Unified Communications Manager's Maximum Devices Per Provider parameter necessitated this move.
- **Moved Broadcast Parameters Menu Option.** The **Broadcast Parameters** menu option has moved from **System Administration | Telephony** to a more intuitive location of **System Administration | General Configuration**.
- **New Major/Minor Release Versions for Backups.** InformaCast's backup files now include the major/minor release versions, e.g. informacast12.19.gpg versus informacast12.17.gpg. Due to this change, when restoring InformaCast from a backup, you are only able to select backup files that are compatible with your major/minor version of InformaCast, e.g. you can backup on 12.19.1 and restore on 12.19.2, but not 12.20.1. In addition, you may want to delete backups from previous versions as they are now incompatible. InformaCast will only automatically delete the oldest version of a backup once the **Number of backups to keep on SFTP server** parameter is met. Any other deletions will need to be done manually.
- **New Supported ESXi Version.** VMware ESXi 7.0 is now supported by virtual InformaCast Appliances/on-premises servers. If you are still running a VMware version prior to 6.0, you are strongly encouraged to upgrade to 7.0, or at least 6.0.

- **Import Your Signed Certificate to InformaCast's SIP Trust Store.** To use secure SIP, i.e. Session Initiation Protocol (SIP) over Transport Level Security (TLS), you must have a certificate for the SIP service in InformaCast's SIP certificate store. By default, it's a self-signed certificate, but you may want to install a signed certificate instead. If you have already installed your root and intermediate Certificate Authority (CA) certificates that you used to sign the InformaCast certificate on Unified Communications Manager, you can use InformaCast's **import-ssl-cert-to-sip-store** command to copy that certificate into InformaCast's SIP trust store. Unified Communications Manager will see that the InformaCast certificate was signed by the intermediate CA, which was signed by the root CA, and because Unified Communications Manager trusts the root CA, it will trust anything signed by the root CA.
- **Phone Cache Security Improvements.** InformaCast's phone cache contains Personally Identifiable Information (PII). As such, it is now encrypted while at rest to protect its information.
- **New Phone Cache Command.** When troubleshooting phone issues, you may find it helpful to read InformaCast's phone cache. Since it's encrypted, you'll need to run the **show-phone-caches** command to obtain an unencrypted file of information.
- **New Upgrade File for pre-12.0.1 Versions of InformaCast.** A new file (CiscoPagingServer\_UpgradeFrom115To-12.19.1.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-12.19.1.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-12.19.1.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-12.19.1.iso)
  - For 11.5.1 or 11.5.2 to the current version, you will attach one ISO file (CiscoPagingServer\_UpgradeFrom115To-12.19.1.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 12.19.1. 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 12.19.1. 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 12.19.1. For 11.5.1 and 11.5.2 versions of the Virtual Appliance, you can upgrade directly to 12.19.1.

If you're already using InformaCast 12.0.1 or later, ignore this note; [your upgrade process](#) involves fewer steps and files.

## Announcements

- **Discontinued Support for Cisco Unified Communications Manager 11.0.x.** InformaCast no longer supports 11.0.x versions of Cisco Unified Communications Manager due to these versions reaching Cisco's end of software maintenance date.

- **Discontinued Support for Certain Phone Models.** InformaCast no longer supports the 7920, 7905, and 7912 models of Cisco IP phones due to these models losing support through Cisco's end of software maintenance date for 11.0.x versions of Cisco Unified Communications Manager.

## 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 12.17.1

The following information pertains to InformaCast 12.17.1.

### Compatibility

InformaCast is compatible with the following versions of Cisco Unified Communications Manager server (including Business Edition 6000): 11.0.1, 11.5.1, 12.0.1, and 12.5.1.

### New Features

- **Improved Display and Behavior for Tables.** The display and behavior of tables within InformaCast's user interface has been improved to remember user preferences for display values across tables, e.g. selecting **25** from the **Rows per page** dropdown menu on the Messages page will carry across to other tables like the table on the Recipient Groups page. Additionally, tables no longer scroll within their contained spaces, e.g. selecting **10** from the **Rows per page** dropdown menu for any table will no longer display seven results and force you to scroll for the last three.
- **New Ability to Easily Find a Phone's Recipient Groups.** You can now enter the complete DN or IP address of a phone and display the recipient groups of which it is a member. Quickly and easily determining a phone's recipient groups can be useful when discovering why a phone is getting a certain broadcast, determining whether removing/moving a phone will affect people's ability to receive broadcasts, or troubleshooting why a phone didn't get a broadcast.
- **New System Health Monitoring.** **show-system-health** is a new command available through the command-line interface that displays the status of several metrics in the InformaCast Appliance: Clock, Disk Utilization, Network, System Services, System Resources, and Overall. Each metric is paired with a measurement of its health, e.g. GREEN, YELLOW, or RED, and each measurement connotes your level of concern. If a metric is GREEN, everything is running as expected. If a metric is YELLOW, the system is impacted, broadcasts will still be delivered, but you should investigate this metric when you have the time. If a metric is RED, broadcast delivery is impacted, and you should investigate and remediate this metric immediately. Checking your system health can aid in troubleshooting network issues, and configuring system alarms based on changes in system health can alert you quickly to situations that need to be resolved.
- **Include InformaCast Logs in your Syslog Infrastructure.** If you're using your own infrastructure to collect and store log information from syslog clients, you can now include various InformaCast logs in that infrastructure with the **configure-logging** command.
- **New Logging Command.** The **show-logging** command displays InformaCast's logging configuration, which may be useful when validating that the logging information you entered is correct or when troubleshooting the reason you're receiving too many logs or not enough.

- **New Upgrade File for pre-12.0.1 Versions of InformaCast.** A new file (CiscoPagingServer\_UpgradeFrom115To-12.17.1.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-12.17.1.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-12.17.1.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-12.17.1.iso)
  - For 11.5.1 or 11.5.2 to the current version, you will attach one ISO file (CiscoPagingServer\_UpgradeFrom115To-12.17.1.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 12.17.1. 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 12.17.1. 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 12.17.1. For 11.5.1 and 11.5.2 versions of the Virtual Appliance, you can upgrade directly to 12.17.1.

If you're already using InformaCast 12.0.1 or later, ignore this note; [your upgrade process](#) involves fewer steps and files.

## Announcements

- **Discontinued Support for Cisco Unified Communications Manager 10.x.x.** InformaCast no longer supports 10.x.x versions of Cisco Unified Communications Manager due to these versions reaching Cisco's end of software maintenance date.
- **Discontinuing Support for Cisco Unified Communications Manager 11.0.x.** In a subsequent release of InformaCast, 11.0.x versions of Cisco Unified Communications Manager will no longer be supported due to these versions reaching Cisco's impending end of software maintenance date.

## 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 12.15.1

The following information pertains to InformaCast 12.15.1.

### Compatibility

InformaCast is compatible with the following versions of Cisco Unified Communications Manager server (including Business Edition 6000): 10.5.2, 11.0.1, 11.5.1, 12.0.1, and 12.5.1.

### New Feature

**New Upgrade File for pre-12.0.1 Versions of InformaCast.** A new file (CiscoPagingServer\_UpgradeFrom115To-12.15.1.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-12.15.1.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-12.15.1.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-12.15.1.iso)
- For 11.5.1 or 11.5.2 to the current version, you will attach one ISO file (CiscoPagingServer\_UpgradeFrom115To-12.15.1.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 12.15.1. 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 12.15.1. 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 12.15.1. For 11.5.1 and 11.5.2 versions of the Virtual Appliance, you can upgrade directly to 12.15.1.

If you're already using InformaCast 12.0.1 or later, ignore this note; [your upgrade process](#) involves fewer steps and files.

### Announcement

**Streamlining Support for Cisco Unified Communications Manager 10.x.x.** In a mid-2020 release of InformaCast, 10.x.x versions of Cisco Unified Communications Manager will no longer be supported due to these versions reaching Cisco's end of software maintenance date.

### 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 12.13.1

The following information pertains to InformaCast 12.13.1.

### Compatibility

InformaCast is compatible with the following versions of Cisco Unified Communications Manager server (including Business Edition 6000): 10.5.2, 11.0.1, 11.5.1, 12.0.1, and 12.5.1.

### New Features

- **Newly Redesigned User Interface.** Notice something different? InformaCast now has an entirely redesigned user interface. This new UI enhances in-application navigation, provides upfront feature explanations, improves accessibility, and raises application and browser security. Learn more by [taking a tour through the new UI](#).
- **New Upgrade File for pre-12.0.1 Versions of InformaCast.** A new file (CiscoPagingServer\_UpgradeFrom115To-12.13.1.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-12.13.1.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-12.13.1.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-12.13.1.iso)
  - For 11.5.1 or 11.5.2 to the current version, you will attach one ISO file (CiscoPagingServer\_UpgradeFrom115To-12.13.1.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 12.13.1. 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 12.13.1. 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 12.13.1. For 11.5.1 and 11.5.2 versions of the Virtual Appliance, you can upgrade directly to 12.13.1.

If you're already using InformaCast 12.0.1 or later, ignore this note; [your upgrade process](#) involves fewer steps and files.

### Known Issue

**Upgrades to InformaCast 12.13.1 Require a Browser Restart.** If you are upgrading to InformaCast 12.13.1, you must close your browser window/tabs before you will be allowed to log into InformaCast.



## 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 12.11.1

The following information pertains to InformaCast 12.11.1.

### Compatibility

InformaCast is compatible with the following versions of Cisco Unified Communications Manager server (including Business Edition 6000): 10.5.2, 11.0.1, 11.5.1, 12.0.1, and 12.5.1.

### New Features

- **New CTI Security for InformaCast and CTI-connected Plugins.** Computer Telephony Integration over Transport Layer Security (CTI over TLS) and CTI with Secure Real-Time Transport Protocol (CTI with SRTP) are now available with InformaCast. CTI over TLS ensures that communication between InformaCast and Unified Communications Manager is secure, and CTI with SRTP ensures that communication between InformaCast and its Cisco IP phones is secure. Aside from increased security, some environments, such as Cisco's Hosted Collaboration Solution for Government (HCS-G), require it.
- **New InformaCast Physical Appliance.** Previously available only as a virtual appliance, the InformaCast server is now also available as a physical appliance. The InformaCast Physical Appliance (model number IPTA-IAS) has an Intel Celeron N3160 1.6GHz quad core processor with 4GB of RAM and a 128GB solid state drive (SSD). Having a physical appliance instead of a virtual one allows you to run InformaCast without also having to run VMware.



---

**Note** The InformaCast Physical Appliance is not available with InformaCast Basic Paging.

---

- **New InformaCast Terminology.** Due to the addition of a physical appliance, InformaCast Virtual Appliance will now be known as InformaCast Appliance. The "InformaCast Appliance" term applies to both InformaCast as a bundled package, i.e. InformaCast the application, PushToTalk, InformaCast the server, Control Center, etc., or as the platform on which everything rests, i.e. InformaCast the server. Where there are differences between administering the virtual server and the physical one, InformaCast Virtual Appliance and InformaCast Physical Appliance will be used, respectively.
- **New Upgrade File for pre-12.0.1 Versions of InformaCast.** A new file (CiscoPagingServer\_UpgradeFrom115To-12.11.1.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-12.11.1.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-12.11.1.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-12.11.1.iso)
- For 11.5.1 or 11.5.2 to the current version, you will attach one ISO file (CiscoPagingServer\_UpgradeFrom115To-12.11.1.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 12.11.1. 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 12.11.1. 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 12.11.1. For 11.5.1 and 11.5.2 versions of the Virtual Appliance, you can upgrade directly to 12.11.1.

If you're already using InformaCast 12.0.1 or later, ignore this note; [your upgrade process](#) involves fewer steps and files.

## Announcements

- **Newly Redesigned User Interface.** Coming soon! A subsequent version of InformaCast boasts an entirely redesigned user interface. This new UI enhances in-application navigation, provides upfront feature explanations, improves accessibility, and raises application and browser security. Learn more by [taking a tour through the new UI](#).
- **New API Opt-in Discussion Group.** Sign up to the API Developer Announcements broadcast-only discussion group within Singlewire's Support Community (<http://support.singlewire.com/s/api>) and receive updates on additions and changes to InformaCast's API environment.
- **Streamlined Support for Cisco Unified Communications Manager 10.0.x.** 10.0.x versions of Cisco Unified Communications Manager are no longer supported due to these versions reaching Cisco's end of software maintenance date.
- **Streamlined Support for Internet Explorer 11.** In a 2019 fourth quarter release of InformaCast, Internet Explorer 11 will no longer be a supported web browser due to its inherent security issues and poor support for essential InformaCast components.
- **Streamlining Support for Cisco Unified Communications Manager 10.x.x.** In a mid-2020 release of InformaCast, 10.x.x versions of Cisco Unified Communications Manager will no longer be supported due to these versions reaching Cisco's [end of software maintenance date](#).

## 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 12.5.1

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 Cisco TAC 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."<sup>2</sup> 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.
- **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.

2. <https://github.com/vmware/open-vm-tools>



- **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 its communication with Unified Communication Manager. In order for this communication to work properly, if you are using Unified Communications Manager 11.5.1 and later, you need to set your authentication method for API browser access to **Basic**.
- **New Call Detail Records Collection.** You can collect call detail records and set a retention period that will eliminate saved records older than the set period through a scheduled job that runs every day at 3:30 a.m. When configured, InformaCast creates a call detail record for every SIP call it receives or makes, e.g. calls made through DialCasts. InformaCast collects call data, such as changes to the call state and DTMF sent and received, as it interacts with a call and Unified Communications Manager. When the call ends, the collected data is written to an InformaCast directory accessible through the **Call Detail Records Directory** link on the Support page.
- **New SRTP Support.** For Unified Communications Managers 10.x and later in mixed mode, InformaCast now supports SRTP packets in unicast streams. SRTP provides encryption, message authentication, integrity, and replay protection for RTP packets. With the addition of SRTP support, InformaCast is interoperable with Unified Communications Manager in FIPS and FedRAMP modes. If you were previously using SIP and you had configured it to work with TLS, you will need to select the **Secure Signaling Required** checkbox on the SIP Call Security page before any InformaCast features using SIP will work.
- **Improved Logging for the SIP Stack.** The SIP Stack log (available by going to **Help | Support**) has been improved to log the message body of SIP requests along with the headers that were already being monitored. This more robust logging can further aid in troubleshooting various SIP issues.
- **New CTI Connection Information.** InformaCast's Overview page has a new table column, CTI Provider, that lists the Unified Communications Manager with which it has established a connection. If no connection has been established, "DISCONNECTED" will appear.
- **Newly Supported Phone.** InformaCast now supports the 8851NR Cisco IP phone model.
- **New Operating System.** The Virtual Appliance is now running an updated operating system that includes the latest bug fixes and security patches.
- **New Upgrade File.** A new file (CiscoPagingServer\_11.5.1.deb) has been added to the upgrade process. Depending on the version of InformaCast Virtual Appliance from which you are starting, you will install different package files:
  - For 8.3 or 8.4 versions to the current version, you will install three package files (CiscoPagingServer\_8.5.1.deb, CiscoPagingServer\_9.1.1.deb, and CiscoPagingServer\_11.5.1.deb)

- For 8.5.1, 9.0.1, or 9.0.2 to the current version, you will install two package files (CiscoPagingServer\_9.1.1.deb and CiscoPagingServer\_11.5.1.deb)
- For 9.1.1, 11.0.1, 11.0.2, or 11.0.5 to the current version, you will install one package file (CiscoPagingServer\_11.5.1.deb)

InformaCast Virtual Appliance 8.5.1 and 9.1.1 are waypoints in the upgrade process. For 8.3 or 8.4 versions of the Virtual Appliance, you must upgrade to 8.5.1, reboot the Virtual Appliance, upgrade to 9.1.1, reboot the Virtual Appliance, and then continue to upgrade to 11.5.1. For 8.5.1, 9.0.1, or 9.0.2 versions of the Virtual Appliance, you must upgrade to 9.1.1, reboot the Virtual Appliance, and then continue to upgrade to 11.5.1. For 9.1.1, 11.0.1, 11.0.2, and 11.0.5 versions of the Virtual Appliance, you can upgrade directly to 11.5.1.

## Resolved Issues

**Establish CTI Connections After InformaCast’s Initialization.** In previous versions of InformaCast, CTI connections were being established while InformaCast was still initializing. This could cause problems if calls arrived during initialization because InformaCast was not prepared to start broadcasts. CTI connections are now established after InformaCast initializes, which solves the issue.

## Resolved Caveats

CDETs ID	Title
CSCux54435	Remove SSLRC4 Cipher Suites
CSCux97095	InformaCast and CVE-2016-0777 and CVE-2016-0778
CSCuy36612	Evaluation of informacast for glibc_feb_2016
CSCuy54654	Evaluation of informacast for OpenSSL March 2016
CSCuz52548	Evaluation of informacast for OpenSSL May 2016

## InformaCast 11.0.5

### Compatibility

InformaCast is compatible with the following versions of Cisco Unified Communications Manager server (including Business Edition 6000): 8.5.1, 8.6.1, 9.0.1, 9.1.2, 10.0.1, 10.5.2, or 11.0.1.

### New Features

- **New Password Security.** For new installations of InformaCast 11.0.5, you are now required to set both your OS and Application Administrator passwords before the Virtual Appliance is completely installed. Similarly, if you are upgrading to InformaCast 11.0.5 and your password was previously changeMe, you will be forced to change your password. By default, both your OS and Application Administrator usernames are “admin.” Your OS credentials allow you to enter Webmin and Control Center as an administrator or access the Virtual Appliance’s command line through SSH. Your application credentials allow you to enter InformaCast as an administrator. When setting your OS or Application Administrator passwords, you cannot use “changeMe.”

- **New Support for the E.164 Dial Plan.** InformaCast supports the E.164 dial plan. You can now use E.164 DNs in the InformaCast web and phone user interfaces. In addition, you no longer have to enter a leading backslash when creating rules for your recipient groups on the Add/Edit Recipient Group page. Adjust your filters from \+<DN> to +<DN> and your matched DNs should appear.
- **New Supported ESXi Version.** VMware ESXi 6.0 is now supported by the Virtual Appliance.
- **New Supported SNMP Version.** InformaCast now supports SNMP v3, which allows encryption of phone information traffic between InformaCast and Cisco Unified Communications Manager. When configuring SNMP in Unified Communications Manager, you can set up the V3 option and then enter the corresponding SNMP v3 user's name and password information in InformaCast's updated Edit Telephony Configuration page (**Admin** | **Telephony** | **Cisco Unified Communications Manager Cluster** | **Edit** button).
- **Updated SIP Stack Logging.** The two previous logs generated for the SIP stack have been combined into one, sipStack.log, which is accessible through the Support page (**Help** | **Support**).
- **Enhanced Retention of Log Files.** As InformaCast is in use in increasingly busier environments, more is being written to the Performance and Summary log files. Previously, InformaCast retained 10 of each, but with increased logging these can roll over quickly, and if not checked immediately, relevant information can be lost. Therefore, 100 Performance and Summary log files are now kept to alleviate this situation.
- **New Upgrade File.** A new file (CiscoPagingServer\_11.0.5.deb) has been added to the upgrade process. Depending on the version of InformaCast Virtual Appliance from which you are starting, you will install different package files:
  - For 8.3 or 8.4 versions to the current version, you will install three package files (CiscoPagingServer\_8.5.1.deb, CiscoPagingServer\_9.1.1.deb, and CiscoPagingServer\_11.0.5.deb)
  - For 8.5.1, 9.0.1, or 9.0.2 to the current version, you will install two package files (CiscoPagingServer\_9.1.1.deb and CiscoPagingServer\_11.0.5.deb)
  - For 9.1.1, 11.0.1, or 11.0.2 to the current version, you will install one package file (CiscoPagingServer\_11.0.5.deb)

InformaCast Virtual Appliance 8.5.1 and 9.1.1 are waypoints in the upgrade process. For 8.3 or 8.4 versions of the Virtual Appliance, you must upgrade to 8.5.1, reboot the Virtual Appliance, upgrade to 9.1.1, reboot the Virtual Appliance, and then continue to upgrade to 11.0.5. For 8.5.1, 9.0.1, or 9.0.2 versions of the Virtual Appliance, you must upgrade to 9.1.1, reboot the Virtual Appliance, and then continue to upgrade to 11.0.5. For 9.1.1, 11.0.1, and 11.0.2 versions of the Virtual Appliance, you can upgrade directly to 11.0.5.

- **API Troubleshooting.** The API documentation ([www.singlewire.com/help/InformaCastAPI/v11.0.5/index.html](http://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 <b>Update</b> 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](http://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 15-8.

### 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 15-5.

**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 15-5.
- 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 Appliance**

Singlewire's bundled package for virtualized environments. It contains an operating system and InformaCast.

**InformaCast Appliance Landing Page**

The InformaCast Appliance landing page is accessible through a web browser addressed with the IP address of the InformaCast Appliance, and it contains links to your applications' user interfaces, the Control Center, and Webmin.

**Invalid License Audio**

When you pick up a phone and dial your set pattern for a DialCast broadcast, if that pattern matches a configuration you've set and the SIP trunk used, and InformaCast has an invalid license, you hear this message.

**IOS**

The Cisco Internetworking Operating System (IOS) is a sophisticated operating system optimized for internetworking. Cisco IOS provides the unifying principles around which an internetwork can be maintained cost-effectively over time. It is a software architecture, disassociated from hardware, that can be dynamically upgraded to adapt to changing technologies (hardware and software) as they evolve within a networking infrastructure. Cisco IOS can be thought of as an internetworking brain, a highly intelligent administrator that manages and controls complex, distributed network resources and functions.

**IP Address**

Internet Protocol Address. A 32-bit address assigned to hosts using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as four octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, while the host number is used to address an individual host within the network or subnetwork. A subnet mask is used to extract network and subnetwork information from the IP address. Also known as an Internet address. See also "Subnet Mask" on page 15-9.

**IP Phone**

See "Cisco IP Phone" on page 15-2.

**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 15-10.

**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 15-3.

**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 throughout InformaCast's recipient-specific features.

**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.

**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 15-6. 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 15-7.

**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 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

## A

### Access

- Advanced InformaCast 1-1
- InformaCast Appliance Landing Page 1-1
- InformaCast Interfaces 1-1
- Logs 1-62

### Add

- Dialing Configuration 1-2
- Login Banners 1-5
- Route Pattern 1-83
- SIP Profile 1-60
- SIP Trunk Security Profile 1-58
- SIP User Credentials 1-94
- TLS SIP Trunk 1-74
- TLS SIP Trunk Security Profile 1-71
- Unified Communications Manager Cluster 1-1

### Administer

- InformaCast 1-1
- Recipients 1-47

### Advanced Functionality Definition 1-7, 1-1

### AES 1-26

### API 1-1, 1-12

### Application Credentials 1-1

### AXL Credentials 1-1, 1-11, 1-14

## B

### Back Up InformaCast 1-11, 1-14

- Back Up InformaCast's Configuration 1-14
- Configure InformaCast's Connection to an SFTP Server 1-11

### Basic Functionality Definition 1-7, 1-1

### Basic License Definition 1-7

### Broadcast

- Cancel 1-6
- Send 1-6

### Broadcast Management 1-1

### Broadcast Parameters 1-1

### Broadcast to IP Phones 1-1

### Broadcasts 1-1

### Buy Advanced Notification 1-5

## C

### Call Detail Records

- Collect 1-7
- Manage 1-7
- View 1-9

### Cancel Audio Broadcast 1-6

### Capture Network Traffic 1-53

### Cause Tag 1-54

### Certificate Authority 1-124, 1-125

### Certificates 1-124, 1-125

- Create Signed 1-125
- Display Local Trust 1-133
- Display Trusted 1-131
- Manage Trust 1-124
- Regenerate Trust 1-136
- Remove Trust 1-134

### Challenge Response 1-84, 1-101

### Change

- Application Administrator Password 1-1
- Hostname 1-41
- IP Address 1-37
- OS Administrator Password 1-98
- Security Passphrase 1-114

### Cisco Unified Communications Manager

- Access Control Group 1-24
- Application User 1-28
- Application User CAPF Profile 1-31
- Authentication URL 1-40
- Calling Search Space 1-17
- Community String 1-7
- CTI Ports 1-19
- Device Pool 1-14
- G.711 Codec 1-12
- Integrate 1-3
- Reboot Phones 1-43
- Route Partition 1-16
- SNMP 1-4
- Test Phones 1-45
- Web Access for Phones 1-32

### Collect Call Detail Records 1-7

### Collect InformaCast's Logs 1-67

### collect-logs 1-70

### Command-line Interface 1-13

- Access Logs 1-64
- Change the Security Passphrase 1-114
- Collect Logs 1-70
- Configure SNMP Monitoring 1-26
- Create and Install a Signed Certificate 1-125
- Disable the Support Account 1-84
- Display Current Firewall State 1-51
- Display Current SNMP Monitoring Configuration 1-32
- Display InformaCast's Logging Configuration 1-80
- Display Local Trust 1-133
- Display Remote SSL Certificates 1-121
- Display Trusted Certificates 1-131
- Enable the Support Account 1-84
- Factory Reset 1-180
- Import Signed SSL Certificate 1-122
- Log In 1-16
- Manage SNMP Monitoring 1-23
- Reboot InformaCast Appliance 1-19
- Regenerate Trust Certificates 1-136
- Remove Added Trust Certificates 1-134

- Remove Current SNMP Monitoring Configuration 1-35
- Restart a Service 1-17
- Restart Network 1-43
- Restart SNMP Monitoring Service 1-34
- Send Logs to Local Server 1-75
- Set Allowed SSL Protocols 1-117
- Set System Time 1-43
- Set the IGMP Version 1-49
- Show Appliance Type 1-95
- Show BIOS Version 1-96
- Show Latest Consent Token 1-88
- Show Monit Status 1-92
- Show Multicast Statistics 1-22
- Show Network Configuration 1-36
- Show Phone Caches 1-74
- Show System Health 1-54
- Show Technical Support Information 1-82
- Show the InformaCast Appliance's Version 1-94
- Shut Down InformaCast Appliance 1-20
- Start a Service 1-17
- Switch Versions 1-179
- Configure 1-1
  - Host Trust 1-48
  - Pathways 1-1
  - Session Timeouts 1-3
  - SIP Trunk Connection 1-57
  - SNMP Monitoring 1-26
- configure-recovery 1-101
- configure-snmp 1-26
- configure-ssl-parameters 1-117
- configure-time 1-43
- Consent Token 1-88
- Control Center Interface 1-12
- Control Center, Log In 1-12
- Copy, Recipient Group 1-37
- Create
  - Application User CAPF Profile 1-31
  - Recipient Groups 1-18
  - Signed Certificate 1-125
  - SIP Trunk 1-62
  - SNMP v3 User 1-9
- create-certificate-signing-request 1-125
- CTI Certificates
  - Delete 1-55
  - Install 1-51
  - View Installed 1-53
- CTI Credentials 1-1, 1-11, 1-14
- CTI Security
  - Create Application User CAPF Profile 1-31
  - Delete Certificates 1-55
  - Install Certificates 1-51
  - Manage 1-49
  - Manage Certificates 1-51
  - Verify Secure Connection 1-55
  - View Installed Certificates 1-53
- D**
- Defunct Phones 1-42
- Delete
  - CTI Certificates 1-55
  - Defunct Phones from InformaCast 1-42
  - Dialing Configuration 1-5
  - Login Banners 1-10
  - Recipient Group 1-43
  - SIP User Credentials 1-98
  - Unified Communications Manager Cluster 1-14
- Demonstration License Definition 1-7
- Deploy InformaCast Virtual Appliance 1-17
- Diagnostics, InformaCast 1-1
- DialCasts
  - Add Dialing Configuration 1-2
  - Cancel 1-6
  - Delete Dialing Configuration 1-5
  - Edit Dialing Configuration 1-4
  - Manage 1-1
  - Manage Dialing Configurations 1-2
  - Manage SIP Functionality 1-56
  - Send 1-6
- Dialing Configuration
  - Add 1-2
  - Delete 1-5
  - Edit 1-4
  - Manage 1-2
- Disable
  - Password Recovery 1-101
  - SNMP Monitoring 1-26, 1-35
  - Support Account 1-84
- disable-support 1-84
- Display 1-80
  - Current Firewall State 1-51
  - Current Network Configuration 1-36
  - InformaCast's Logging Configuration 1-80
  - Local Trust 1-133
  - Remote SSL Certificates 1-121
  - SNMP Monitoring Configuration 1-32
  - Trusted Certificates 1-131
- E**
- Edit
  - Dialing Configuration 1-4
  - Login Banners 1-9
  - Recipient Group 1-31
  - SIP User Credentials 1-96
  - Unified Communications Manager Cluster 1-11
- Enable
  - Password Recovery 1-101
  - SNMP Monitoring 1-26
  - Support Account 1-84
  - Web Access for Individual Phones 1-36
  - Web Access for Multiple Phones 1-33, 1-34
  - Web Access for Phones 1-32
- enable-support 1-84
- Encrypted Media 1-3
- ESXi 1-17
- F**
- Factory Reset the InformaCast Appliance 1-180
- factory-reset 1-180
- Find a Phone's Recipient Groups 1-30
- Free Trial 1-3
- H**
- halt-appliance 1-20

Host Trust 1-48  
 Hostname, Change Appliance 1-41

## I

### Import

Signed SSL Certificate 1-122

import-signed-certificate 1-125

### InformaCast

Administer 1-1

Application Credentials 1-1

Application, Definition of 1-1

Backups 1-11

Broadcast Management 1-1

DSCP Quality of Service Policies 1-6

Log Directory 1-1

Log In 1-9

Log In Initially 1-3

Manage Recipients 1-1

Overview 1-1

Summary and Diagnostics 1-1

Upgrade to Advanced 1-1

### InformaCast Appliance

Access Interfaces 1-1

Access Landing Page 1-1

API 1-1, 1-12

Authentication URL 1-40

Capture Network Traffic 1-53

Change Hostname 1-41

Change OS Administrator Password 1-98

Change the IP Address 1-37

Change the Security Passphrase 1-114

Collect Logs 1-67

Command Line Interface 1-13

Control Center Interface 1-12

Definition of 1-1

Deploy Virtual Machine 1-17

Display a List of Running Processes 1-90

Display Current Firewall State 1-51

Display Logging Configuration 1-80

Display Remote SSL Certificates 1-121

Enable the Support Account 1-84

Factory Reset 1-180

Hardware Requirements 1-4

Install 1-17

Install Cisco Unified Communications Manager Certificates 1-77

Install SIP Certificate 1-64

Installation 1-1

Intended Audience 1-2

Interface Orientation 1-8

Interface Permissions 1-14

Keyboard and Monitor Interface 1-14

Landing Page 1-9

License 1-2

Licensing 1-7

Logs 1-62

Manage Backups 1-11

Manage Password Recovery 1-101

Manage SNMP Monitoring 1-23

Multicast 1-2, 1-7, 1-13, 1-14, 1-15

Notification Boxes Explained 1-3

Plan your Multicast Environment 1-1

Port Configuration 1-5

Prepare your Multicast Environment 1-1

Prerequisites 1-3

Reboot 1-12, 1-19

Reboot Phones 1-43

Remove Defunct Phones 1-42

Restart Network 1-21, 1-43

Restart Service 1-10, 1-17

Restore from Backup 1-20

Set Allowed SSL Protocols 1-117

Set Initial Configuration 1-31

Set the IGMP Version 1-49

Set the System Time 1-43

Show Appliance Type 1-95

Show BIOS Version 1-96

Show Monit Status 1-92

Show Multicast Statistics 1-22

Show Network Configuration 1-36

Show Technical Support Information 1-82

Show Version 1-94

Shut Down 1-20

Start Service 1-9, 1-17

Switch Versions 1-179

Technical Support 1-15

Test Multicast 1-2

Test Phones 1-45

Upgrade 1-139

Upgrade Open VM Tools 1-168

Upgrade, Determine Version 1-139

Upgrade, Upload New License 1-2

User Guide Standards 1-2

Version 1-16

Versions 1-139

Web Interface 1-10

Webmin 1-13

### Install 1-1

Cisco Unified Communications Manager Certificates on InformaCast 1-77

CTI Certificates 1-51

InformaCast Appliance 1-17

InformaCast SIP Certificate 1-64

Set Initial Configuration 1-31

Signed Certificate 1-125

### Interface Orientation 1-8

### Interface Permissions 1-14

### Intermediate Certificate 1-124, 1-125

### IP Address, Change 1-37

### IP Phones, Manage 1-1

## J

JTAPI, Update 1-10

## K

Keyboard and Monitor Interface 1-14

## L

Landing Page 1-9, 1-1

License 1-7

Demonstration, Definition of 1-7

Perpetual, Definition of 1-8

Subscription, Definition of 1-7

Trial, Definition of 1-7

License Key 1-7, 1-2

Upload New 1-2

- Live Audio Broadcast 1-6
- Log Directory 1-1
- Log Files 1-62, 1-67, 1-75, 1-80
- Log into InformaCast 1-9
- Log into InformaCast Initially 1-3
- Log into PushToTalk 1-11
- Log into the Command-line Interface 1-16
- Log into the Control Center 1-12
- Log into Webmin 1-14

- Login Banners 1-4

- Add 1-5
  - Delete 1-10
  - Edit 1-9
  - Manage 1-4

- Logs

- Directory 1-1
  - Redact IP Addresses 1-72

## M

- Manage

- Broadcast Parameters 1-1
  - Broadcasts 1-1
  - Call Detail Records 1-7
  - CTI Certificates 1-51
  - CTI Security 1-49
  - DialCasts 1-1
  - Dialing Configuration 1-2
  - Digest Authentication with SIP User Credentials 1-93
  - InformaCast Backups 1-11
  - IP Phones 1-1
  - Login Banners 1-4
  - Messages 1-1
  - New License 1-2
  - Password Recovery 1-101
  - Phone Updates 1-15
  - Recipient Administration 1-47
  - Recipient Groups 1-17
  - Recipients 1-1
  - SIP Access to InformaCast 1-85
  - SIP Call Security 1-88
  - SIP Functionality 1-56
  - SIP Stack 1-99
  - Trust Certificates 1-124

- Messages, Manage 1-1

- Mixed Mode 1-3

- Multicast

- IGMP Snooping 1-15
  - IGMPv3 1-15
  - MPLS Provider 1-14
  - Network Capture 1-7, 1-11
  - PIM 1-13
  - Plan your environment 1-1
  - Prepare your Environment 1-1
  - Review Configuration 1-6
  - Test Configuration 1-2
  - Testing Tool 1-2
  - Traffic Capture 1-7

## N

- Network DSCP QoS 1-6

- Network Traffic Capture
- Obtain 1-7

- Read 1-11
- Notification Box
- Caution 1-3
  - Note 1-3
  - Tip 1-3
  - Warning 1-3
- NTP 1-43
- ntpd 1-43

## O

- Open VM Tools 1-168
- OS Credentials 1-98, 1-101
- Overview Page, InformaCast 1-1

## P

- Packet Capture 1-53
- Password Recovery 1-88, 1-101
- Pathways
- Broadcast to IP Phones 1-1
  - Configuration 1-1
  - Secure CTI Communication 1-2
  - Send a DialCast 1-3
  - Validate Certificates 1-2
- Performance Log 1-75
- Perpetual InformaCast 1-5
- Perpetual License Definition 1-7, 1-8
- Phone Cache 1-74
- Phones, Reboot 1-43
- Phones, Test 1-45
- Port Configuration 1-5
- PushToTalk, Definition of 1-1

## R

- Reboot
- InformaCast Appliance 1-12, 1-19
  - Phones 1-43
- Recipient Group Tags
- Add 1-44
  - Delete 1-47
  - Description of 1-44
  - Edit 1-46
- Recipient Groups
- Advanced Matching 1-48
  - Copy 1-37
  - Create 1-18
  - Delete 1-43
  - Edit 1-31
  - Find Phone Members 1-30
  - Manage 1-17
  - Remove Defunct Phones 1-42
  - Tag 1-44, 1-46, 1-47
  - View Recipients 1-27
- Recipients
- Administration 1-47
  - Manage 1-1
  - Manage IP Phones 1-1
- recovery 1-101
- Regenerate Trust Certificates 1-136
- regenerate-ssl-certificates 1-136
- Release Notes 1-1
- 11.0.1 1-31

- 11.0.1.a 1-31
- 11.0.2 1-30
- 11.0.5 1-28
- 11.5.1 1-26
- 8.3 1-40
- 8.3.a 1-39
- 8.4.a 1-37
- 8.5.1 1-37
- 9.0.1 1-35
- 9.0.2 1-34
- 9.1.1 1-33
- InformaCast 11.5.2 1-26
- InformaCast 12.0.1 1-23
- InformaCast 12.0.2 1-22
- InformaCast 12.1.1 1-20
- InformaCast 12.11.1 1-16
- InformaCast 12.13.1 1-15
- InformaCast 12.15.1 1-14
- InformaCast 12.17.1 1-12
- InformaCast 12.19.1 1-10
- InformaCast 12.19.2 1-9
- InformaCast 12.20.1 1-8
- InformaCast 12.22.2 1-7
- InformaCast 12.5.1 1-18
- InformaCast 14.0.1 1-5
- InformaCast 14.2.1 1-4
- InformaCast 14.4.1 1-2
- InformaCast 14.4.2 1-1
- Remove
  - Defunct Phones 1-42
  - SNMP Monitoring Configuration 1-35
  - Trust Certificates 1-134
- remove-all-user-added-trusted-certificates 1-134
- remove-snmp-configuration 1-35
- Restart
  - Network 1-21, 1-43
  - Service 1-10, 1-17
  - SIP 1-101
  - SNMP Monitoring Service 1-34
- restart-appliance 1-19
- restart-network 1-21, 1-43
- Restore InformaCast from Backup 1-20
- Return the InformaCast Appliance to Original State 1-180
- Root Certificate 1-124, 1-125
- Running Processes 1-90
- S**
- Secure CTI Communication 1-2
- Security Passphrase 1-114
- Self-signed Certificate 1-124, 1-125
- Send
  - DialCasts 1-3, 1-6
  - Live Audio Broadcast 1-6
  - Logs to Local Server 1-75
- Session Timeouts, Configure 1-3
- Set
  - Allowed SSL Protocols 1-117
  - IGMP Version 1-49
  - Initial Configuration 1-31
  - System Time 1-43
- Set Authentication URL 1-40
- set-ipv4-igmp-version 1-49
- SFTP Server 1-11
- SHA 1-26
- Show
  - Appliance Type 1-95
  - BIOS Version 1-96
  - Monit Status 1-92
  - Multicast Statistics 1-22
  - Network Configuration 1-36
  - Phone Caches 1-74
  - System Health 1-54
  - Technical Support Information 1-82
- show-appliance-type 1-95
- show-bios-version 1-96
- show-certificate-from-network command 1-121
- show-firewall 1-51
- show-local-trust 1-133
- show-logging 1-80
- show-monit-status 1-92
- show-multicast-statistics 1-22
- show-network-configuration 1-36
- show-phone-caches 1-74
- show-snmp-configuration 1-32
- show-tech-support 1-82
- show-time-configuration 1-43
- show-time-status 1-43
- show-trusted-certificates 1-131
- show-version 1-94
- Shut Down InformaCast Appliance 1-14, 1-20
- Signed Certificate 1-2, 1-122, 1-125
- SIP 1-56
  - Add a Profile 1-60
  - Add a Route Pattern 1-83
  - Add a SIP Trunk Security Profile 1-58
  - Add a TLS SIP Trunk 1-74
  - Add a TLS SIP Trunk Security Profile 1-71
  - Add User Credentials 1-94
  - Allow/Deny Access to InformaCast 1-85
  - Call Detail Records 1-7, 1-9
  - Configure a Secure SIP Trunk 1-122
  - Configure a SIP Trunk Connection 1-57
  - Create a SIP Trunk 1-62
  - Delete SIP User Credentials 1-98
  - Edit User Credentials 1-96
  - Enable Digest Authentication with SIP User Credentials 1-93
  - Enable SIP Call Security 1-88
  - Import a Signed SSL Certificate 1-122
  - Install Cisco Unified Communications Manager Certificates on InformaCast 1-77
  - Install InformaCast SIP Certificate 1-64
  - Manage 1-56
  - Manage SIP Stack 1-99
  - Restart 1-101
- SNMP
  - Configure Monitoring 1-26
  - Disable 1-35
  - Display Monitoring Configuration 1-32
  - Enable Monitoring 1-26
  - Manage Monitoring 1-23
  - Remove Monitoring 1-35
  - Restart Monitoring Service 1-34
- SNMP Enable Monitoring 1-26



- SNMP v2 1-7
  - SNMP v3 1-9
  - snmp-service disable 1-34
  - S RTP 1-60
  - SSL 1-122
  - SSL Certificates 1-48, 1-125
  - SSL, Display Remote Certificates 1-121
  - Start a Service 1-9, 1-17
  - Start InformaCast 1-9
  - Stop InformaCast 1-7
  - Subscription InformaCast 1-5
  - Subscription License Definition 1-7
  - Summary, InformaCast 1-1
  - Support Account 1-84, 1-88
  - Switch Versions 1-179
  - switch-version 1-179
  - System Health 1-54
  - System Logs 1-62, 1-67, 1-75
  - System Management
    - Display InformaCast's Logging Configuration 1-80
    - Display Your Consent Token 1-88
    - Send Logs to Local Server 1-75
    - Show Phone Caches 1-74
    - Show System Health Information 1-54
- T**
- Technical Support 1-15
  - Test
    - Multicast 1-2
    - Phones 1-45
  - test-network-connectivity 1-21
  - TLS
    - Add a SIP Profile 1-60
    - Add a SIP Trunk 1-74
    - Add a SIP Trunk Security Profile 1-71
    - Definition 1-57
    - Install Cisco Unified Communications Manager Certificates on InformaCast 1-77
    - Install the InformaCast SIP Certificate 1-64
  - Token ID Number 1-84, 1-101
  - Trial License Definition 1-7
  - Trust Certificates 1-124, 1-125
    - Create 1-125
    - Display 1-131
    - Display Local Trust 1-133
    - Manage 1-124
    - Regenerate 1-136
    - Remove 1-134
  - Trust, Host 1-48
  - Try Advanced Notification 1-3
- U**
- Unified Communications Manager
    - Add Cluster 1-1
    - Configure XML Push Authentication 1-8
    - Create an SNMP v3 User 1-9
    - Delete Cluster 1-14
    - Edit Cluster 1-11
    - Maximum Devices Per Provider 1-8
    - Mixed Mode, Encrypted Media 1-3
    - Save and Set Cluster Security 1-8
  - Set Authentication Method for API Browser Access 1-42
  - Set AXL Configuration 1-4
  - Set JTAPI or HTTP Configuration 1-7
  - Set Secure CTI Configuration 1-6
  - Set SNMP Configuration 1-5
  - Set Telephony Configuration 1-2
  - Update JTAPI 1-11
  - Update Recipients 1-10
  - Update InformaCast's Phone Information 1-15
  - Update JTAPI 1-10
  - Upgrade 1-139, 1-168
    - Basic to Advanced 1-1
    - Buy Advanced Notification 1-5
    - Determine Your Current Version 1-139
    - Differences Between Versions 1-1, 1-139
    - InformaCast 12.0.1 and Later 1-168
    - InformaCast 12.0.1 and Later in the CLI 1-175
    - InformaCast 12.0.1 and Later in Webmin 1-169
    - InformaCast Pre-12.0.1 1-140
    - Open VM Tools 1-168
    - Try Advanced Notification 1-3
    - Understand the Architecture 1-168
    - Upload New License 1-2
- V**
- Validate Certificates 1-2
  - Verify Secure CTI Connection 1-55
  - Version, InformaCast Appliance 1-16, 1-94, 1-139
  - View
    - Call Detail Records 1-9
    - CTI Certificates 1-53
    - License Key 1-2
    - Recipients in a Recipient Group 1-27
  - VMware 1-17, 1-168
  - vSphere
    - Access Logs 1-66
- W**
- Web Access, Individual Phones 1-36
  - Web Access, Multiple Phones 1-33, 1-34
  - Web Access, Phones 1-32
  - Web Interface 1-10
  - Webmin 1-13
    - Access Logs 1-62, 1-63
    - Back Up InformaCast 1-11
    - Capture Network Traffic 1-53
    - Change OS Credentials 1-98
    - Change the InformaCast Appliance's Hostname 1-41
    - Change the InformaCast Appliance's IP Address 1-37
    - Collect Logs 1-68
    - Display a List of Running Processes 1-90
    - Log In 1-14
    - Reboot InformaCast Appliance 1-12
    - Restart a Service 1-10
    - Start a Service 1-9
  - Website Certificate 1-125