

Konfiguration und Fehlerbehebung von Informacast

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Zweck der Funktion](#)

[Einfach und Erweitert](#)

[Verwendete Protokolle](#)

[HTTP und JTAPI](#)

[SIP und CTI](#)

[Konfigurationen](#)

[Netzwerkdiagramm](#)

[Konfigurieren von Call Manager](#)

[Konfigurieren von Informacast](#)

[Konfigurieren von Multicast im Netzwerk](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Häufige Probleme](#)

[Telefone nicht aktiviert](#)

[Telefone nicht erkannt](#)

[SNMP-Fehler: Es können keine Empfängergruppen erstellt werden: java.lang.Exception](#)

[Kein Audio auf den Zieltelefonen](#)

[Zu erfassende Daten](#)

[Leistungsprotokolle](#)

[Paketerfassung](#)

[Beispielanalyse](#)

[SDL Traces](#)

[Leistungsprotokolle](#)

[Konsolenprotokolle \(PRT\)](#)

[Paketerfassung](#)

[Tools für die Fehlerbehebung](#)

[Advance-Lizenz](#)

[Passwörter](#)

[Kennwortwiederherstellung](#)

[JTAPI in Informacast aktualisieren](#)

[Häufige Fehler](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument werden der Cisco Paging-Server (auch InformaCast genannt) und seine Integration in Cisco Unified Communications Manager (CUCM) beschrieben. In diesem Dokument werden der Zweck der Funktion, die Konfiguration der Funktion, die für die Fehlerbehebung zu erfassenden Daten, die Beispielanalyse der Daten und die zugehörigen Ressourcen für weitere Recherchen behandelt.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Unified Communications Manager
- InformaCast
- SIP, CTI, HTTP und SNMP-Protokoll.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- InformaCast Version 11.5.2 - 38
- CUCM-Versionen 11.5.1.14900-8
- CP-8811 und CP-8861 sip88xx.12-0-1SR1-1
- Basislizenz

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle in diesem Dokument verwendeten Geräte begannen mit einer gelöschten (Standard-)Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Hintergrundinformationen

Zweck der Funktion

Der Cisco Paging Server ist eine Paging-/Massenbenachrichtigungslösung für Tausende von Telefonen, Lautsprechern und anderen Geräten. Dies ist besonders in Notfällen mit Live-Audio und/oder Textnachrichten nützlich.

Nach OEM-Vereinbarung (Original Equipment Manufacturer) mit Singlewire (InformaCast-Anbieter) unterstützt das Cisco Technical Assistance Center (TAC) InformaCast ab Version 8.3 zusammen mit CUCM ab Version 8.5. Der einzige vom Cisco TAC unterstützte Modus ist das grundlegende Paging.

Einfach und Erweitert

Der grundlegende Paging-Modus unterstützt Live-Audio-Broadcast nur für bis zu 50 Telefone pro Empfängergruppe und erfordert keine zusätzliche Lizenz. Die im Rahmen von CUCM bereitgestellte InformaCast-Version enthält eine Lizenz für den grundlegenden Paging-Modus. Kunden, die zusätzliche Funktionen benötigen, können auf den erweiterten Benachrichtigungsmodus umsteigen und von SingleWire unterstützt werden.

Eine erweiterte Paging-Lizenz ermöglicht unbegrenzte Paging-Gruppen. Es ermöglicht auch andere erweiterte Funktionen, wie Paging zu Overhead-Analog- und IP-Lautsprechern, Zeitplanung für Signaltöne, Priorisierung von Notfallbenachrichtigungen mit der Anruf-Aufschaltung-Option, vorab aufgezeichnete und nur-Text-Seiten, Integration mit Social Media-Sites für Benachrichtigungen, E-Mail- und SMS-Massenbenachrichtigungen und Überwachung aller Nummern, Notfallwarnungen und Integration mit Cisco Jabber-Clients. Nach der Installation von InformaCast können Sie eine Testversion des erweiterten Benachrichtigungsmodus aktivieren.

Verwendete Protokolle

Der Cisco Paging Server kommuniziert mit Unified CM über SIP, SNMP, AXL und CTI und ab Cisco Paging Server 9.0.1 kann entweder HTTP oder JTAPI für die Kommunikation mit Telefonen verwendet werden.

Der Cisco Paging Server verwendet SNMP, um nach den anderen Unified CM-Knoten sowie nach einer Liste der für die einzelnen Cluster-Mitglieder registrierten Telefone zu suchen. Nach Abschluss der SNMP-Kommunikation verwendet der Cisco Paging Server AXL, um zusätzliche Informationen zu jedem registrierten Telefon zu ermitteln, z. B. Gerätenamen, Beschreibung, Gerätepool, Calling Search Space, Verzeichnisnummer und Standort. Diese Informationen können verwendet werden, um logische Gruppen von Telefonen zu erstellen, so genannte Empfängergruppen. Wie bereits erwähnt, können Empfängergruppen im Cisco Paging Server mit Basislizenz maximal 50 Telefone enthalten.



Anmerkung: Pro Unified CM-Cluster wird nur ein Cisco Paging-Server unterstützt.

HTTP und JTAPI

InformaCast-Versionen vor 9.x verwendeten alle HTTP für die Telefonaktivierung. Im HTTP-Modus sendet der Cisco Paging Server Befehle und Anmeldeinformationen an jeden HTTP-Server eines IP-Telefons. IP-Telefone validieren diese Anmeldeinformationen und führen dann die Befehle aus. Zur Sendezeit kontaktiert InformaCast sie direkt über HTTP mit der XML Services Interface (XSI).

Im JTAPI-Modus sendet Cisco Paging über Unified CM Befehle an jedes Telefon. Cisco Paging Server muss bei jeder Anforderung keine Anmeldeinformationen senden, sodass nicht jedes Telefon seinen Webserver aktivieren muss und Befehle schneller ausgeführt werden. Darüber hinaus ermöglicht der CTI-Modus eine schnellere Überprüfung belegter Telefone und deren

Aktivierung.

Sie können HTTP oder JTAPI verwenden, unabhängig vom Typ der Integration (SIP oder CTI) mit CUCM. Beachten Sie, dass JTAPI auf Telefonen mit nicht englischer Sprache besser funktioniert als HTTP. Um das Gebietsschema für Benutzer zu überprüfen, sehen Sie sich die Telefon-Webseite an.

		
Network setup		
Cisco IP Phone CP-8861 (SEP2C3124C9F8E1)		
Device information	MAC address	2C3124C9F8E1
Network setup	Host name	SEP2C3124C9F8E1
Network statistics	Domain name	
Ethernet information	DHCP server	10.1.61.10
Access	BOOTP server	No
Network	DHCP	Yes
Device logs	IP address	10.1.61.12
Console logs	User locale	English_United_States
Core dumps	Network locale	United_States
Status messages	User locale version	11.0.0.0(1)
Debug display	Network locale version	11.0.0.0(1)

 Anmerkung: Bei der Verwendung von JTAPI muss die CUCM-Version 9.1.2 oder höher sein, und Cisco 3905-, 7902-, 7905- und 7912-Telefone werden nicht unterstützt.

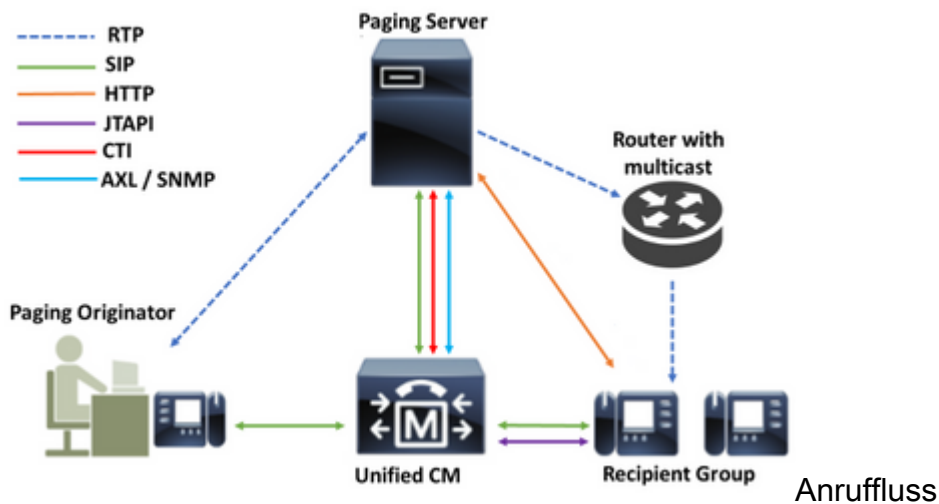
SIP und CTI

Informacast kann Anrufe über CTI und/oder SIP empfangen. Im Fall von CTI werden Anrufe an einem CTI-Routenpunkt verarbeitet (der Cisco Paging Server benötigt keine CTI-Ports, um eingehende Anrufe entgegenzunehmen).

Im Fall von SIP gehen Anrufe über einen SIP-Trunk von Unified CM aus. Sowohl CTI als auch SIP sind gültig und werden unterstützt. Cisco empfiehlt jedoch, SIP-Anrufe über CTI weiterzuleiten, da die Fehlerbehebung bei SIP-Integrationen wesentlich einfacher ist als bei CTI.

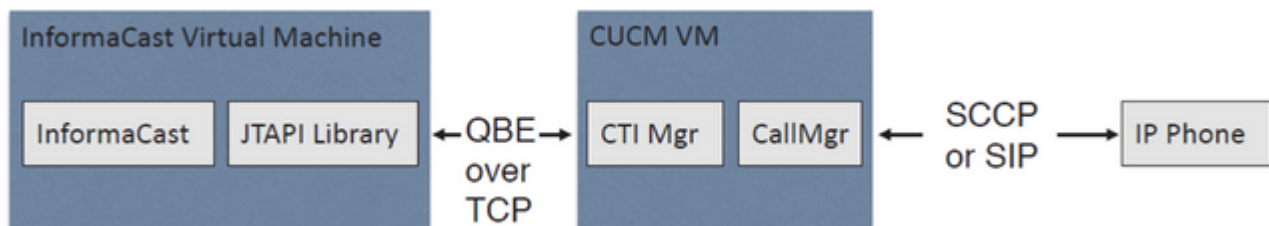
Konfigurationen

Netzwerkdiagramm

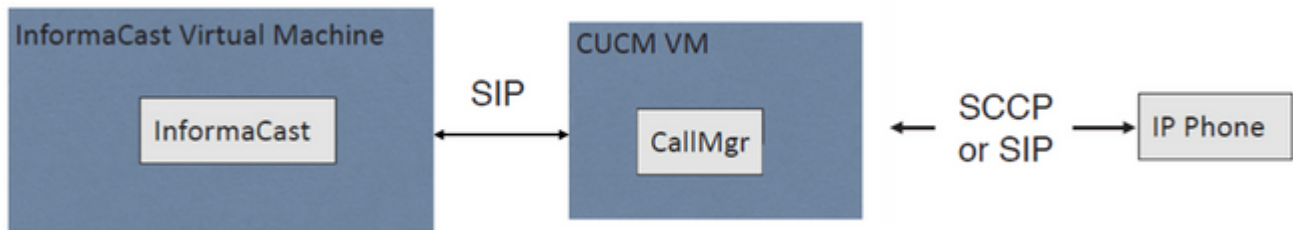


1. Der Anrufer (Paging-Ausgangspunkt) wählt eine vordefinierte Nummer in Unified CM. Beispiel: 7777.
2. Der Unified CM leitet den Anruf entweder über einen SIP-Trunk oder einen CTI-Routing-Punkt an den Cisco Paging-Server weiter.
3. Der Cisco Paging-Server nimmt den Anruf an.
4. Der Anrufer hört einen niedrigen Standton. Während der Cisco Paging Server diesen Ton abspielt, werden Anweisungen über HTTP oder JTAPI an alle Telefone in der Empfängergruppe gesendet, damit diese der Multicast-Gruppe beitreten können.
5. Sobald alle Telefone der Multicast-Gruppe beigetreten sind, gibt der Cisco Paging Server einen hohen "Go-Ahead"-Ton ab. Wenn der Anrufer diesen Ton hört, bedeutet dies, dass der Cisco Paging Server die Audioübertragung empfangen und an die Multicast-IP-Adresse und den Multicast-Port senden kann.
6. Wenn der Anrufer spricht, werden die Medien vom Telefon des Anrufers an den Cisco Paging-Server, dann vom Paging-Server an die Multicast-IP-Adresse und den Multicast-Port und schließlich von der Multicast-IP-Adresse an die empfangenden Telefone gesendet.
7. Wenn der Anrufer den Hörer auflegt, wird die Anweisung an jedes IP-Telefon gesendet. Diesmal wird die Multicast-Gruppe verlassen, und die Übertragung ist beendet.

Wenn InformaCast mithilfe der JTAPI-Bibliothek und des Computer Telephony Integration (CTI) Manager in den Cisco Call Manager integriert wird, verwendet es das Quick Buffer Encoding (QBE)-Protokoll über TCP, wie im Bild gezeigt.



Für SIP-Integrationen verwendet InformaCast das SIP-Protokoll über TCP und den Port 5060, um mit dem Call Manager zu kommunizieren, wie im Bild gezeigt.



Konfigurieren von Call Manager

Schritt 1: Aktivieren Sie die Services, navigieren Sie zu Cisco Unified Serviceability > Tools > Service Activation, und aktivieren Sie die folgenden Services:

- Cisco CallManager
- Cisco CTIManager
- Cisco AXL-Webservice
- Cisco CallManager SNMP-Dienst

 Tipp: Aktivieren Sie SNMP auf allen Knoten, AXL auf mindestens einem Knoten im Cluster und CTI Manager auf mindestens einem Knoten, auf dem der Call Manager-Dienst ausgeführt wird (oder mehr aus Redundanzgründen).

Schritt 2: SNMP konfigurieren (Version 2 oder Version 3)

Für SNMP v2

- Navigieren Sie zu Cisco Unified Serviceability > SNMP > v1/v2.
- Konfigurieren Sie den Community-String-Namen mit der Zugriffsberechtigung ReadOnly.
- Aktivieren Sie, wenn möglich, das Kontrollkästchen Auf alle Knoten anwenden, und klicken Sie auf Speichern.

Status
 ⓘ Status : Ready

Server* 10.1.61.158--CUCM Voice/Video ▼

Community String Information
 Community String Name* ICVA

Host IP Addresses Information
☒ Accept SNMP Packets from any host
☐ Accept SNMP Packets only from these hosts
 Host IP Address
 Insert
 Host IP Addresses
 Remove

Access Privileges
 Access Privileges* ReadOnly ▼
 ⓘ Notify access privilege is required in order to configure Notification Destinations.

☒ Apply To All Nodes

Save Clear All Cancel

Für SNMP v3

- Navigieren Sie zu Cisco Unified Serviceability > SNMP > V3 > User, und erstellen Sie einen Benutzer mit dem Namen ICVA.
- Aktivieren Sie das Kontrollkästchen Authentifizierung erforderlich, geben Sie ein Authentifizierungskennwort ein, und aktivieren Sie das Optionsfeld SHA.
- Aktivieren Sie das Kontrollkästchen Datenschutz erforderlich, geben Sie ein Datenschutzkennwort ein, und aktivieren Sie das Optionsfeld AES128.
- Wählen Sie ReadOnly aus dem Dropdown-Menü Access Privileges (Zugriffsprivilegien) aus, und aktivieren Sie wenn möglich das Kontrollkästchen Apply To All Nodes (Auf alle Knoten anwenden), und klicken Sie auf Save.

Status
 ⓘ Status : Ready

Server* 10.1.61.158--CUCM Voice/Video ▼

User Information
 User Name* ICVA

Authentication Information
☒ Authentication Required
 Password ***** Reenter Password ***** Protocol ☐ MD5 ☒ SHA

Privacy Information
☒ Privacy Required
 Password ***** Reenter Password ***** Protocol ☐ DES ☒ AES128

Host IP Addresses Information
☒ Accept SNMP Packets from any host ☐ Accept SNMP Packets only from these hosts
 Host IP Address
 Insert
 Host IP Addresses
 Remove

Access Privileges
 Access Privileges* ReadOnly ▼
 ⓘ Notify access privilege is required in order to configure Notification Destinations.

☒ Apply To All Nodes

Save Clear All Cancel

Schritt 3: Standard-Codec auf G.711 einstellen

- Navigieren Sie zu CM Administration > System > Region Information > Region, und erstellen Sie eine neue Region, z.B. ICVA.
- Wählen Sie im Bereich Regions (Regionen) alle Regionen aus, und legen Sie als maximale Audio-Bitrate 64 Kbit/s (G.722, G.711) fest.
- Wählen Sie das Optionsfeld Keine in der Max Video Call Bit Rate aus, und klicken Sie auf Speichern.

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

Save Delete Reset Apply Config Add New

Name* ICVA

Region Relationships

Region	Audio Codec Preference List	Maximum Audio Bit Rate	Maximum Session Bit Rate for Video Calls	Maximum Session Bit Rate for Immersive Video Calls
Default	Use System Default (Factory Default low loss)	64 kbps (G.722, G.711)	None	None
ICVA	Use System Default (Factory Default low loss)	64 kbps (G.722, G.711)	None	None
Mex	Use System Default (Factory Default low loss)	64 kbps (G.722, G.711)	None	None
SanJose	Use System Default (Factory Default low loss)	64 kbps (G.722, G.711)	None	None
NOTE: Regions not displayed	Use System Default	Use System Default	Use System Default	Use System Default

Modify Relationship to other Regions

Regions	Audio Codec Preference List	Maximum Audio Bit Rate	Maximum Session Bit Rate for Video Calls	Maximum Session Bit Rate for Immersive Video Calls
Default ICVA Mex SanJose	Keep Current Setting	☒ 64 kbps (G.722, G.711) ☐ kbps	☐ Keep Current Setting ☐ Use System Default ☒ None	☐ Keep Current Setting ☐ Use System Default ☒ None

Anmerkung: Die Multicast-Medien-Streams verwenden immer den G.711-mu-law-Codec. Andere Codecs sind nicht zulässig oder werden nicht unterstützt. Anrufe, die über andere Codecs bei Informacast eingehen, müssen transkodiert werden.

Schritt 4: Erstellen eines Gerätepools

- Navigieren Sie zu CM Administration > System > Device Pool (CM-Verwaltung > System > Gerätepool), und erstellen Sie einen Gerätepool. Geben Sie ihm z. B. den Namen ICVA_DP.
- Fügen Sie die soeben erstellte ICVA-Region hinzu.
- Wählen Sie im Dropdown-Menü SRST-Referenz die Option Disable (Deaktivieren) aus.
- Wählen Sie Ein aus dem Dropdown-Menü Über Linien verbinden und klicken Sie auf Speichern.

Device Pool Configuration

Save Delete Copy Reset Apply Config Add New

Device Pool Settings

Device Pool Name* ICVA_DP

Cisco Unified Communications Manager Group* Default

Calling Search Space for Auto-registration < None >

Adjunct CSS < None >

Reverted Call Focus Priority Default

Intercompany Media Services Enrolled Group < None >

Roaming Sensitive Settings

Date/Time Group* CMLocal

Region* ICVA

Media Resource Group List < None >

Location < None >

Network Locale < None >

SRST Reference* Disable

Connection Monitor Duration***

Single Button Barge* Default

Join Across Lines* On

Physical Location < None >

Device Mobility Group < None >

Wireless LAN Profile Group < None > [View Details](#)

Schritt 5: Erstellen einer Routenpartition, z. B. ICVA_PT.

Schritt 6: Erstellen eines Calling Search Space, z. B. ICVA_CSS Schließen Sie ICVA_PT ein.

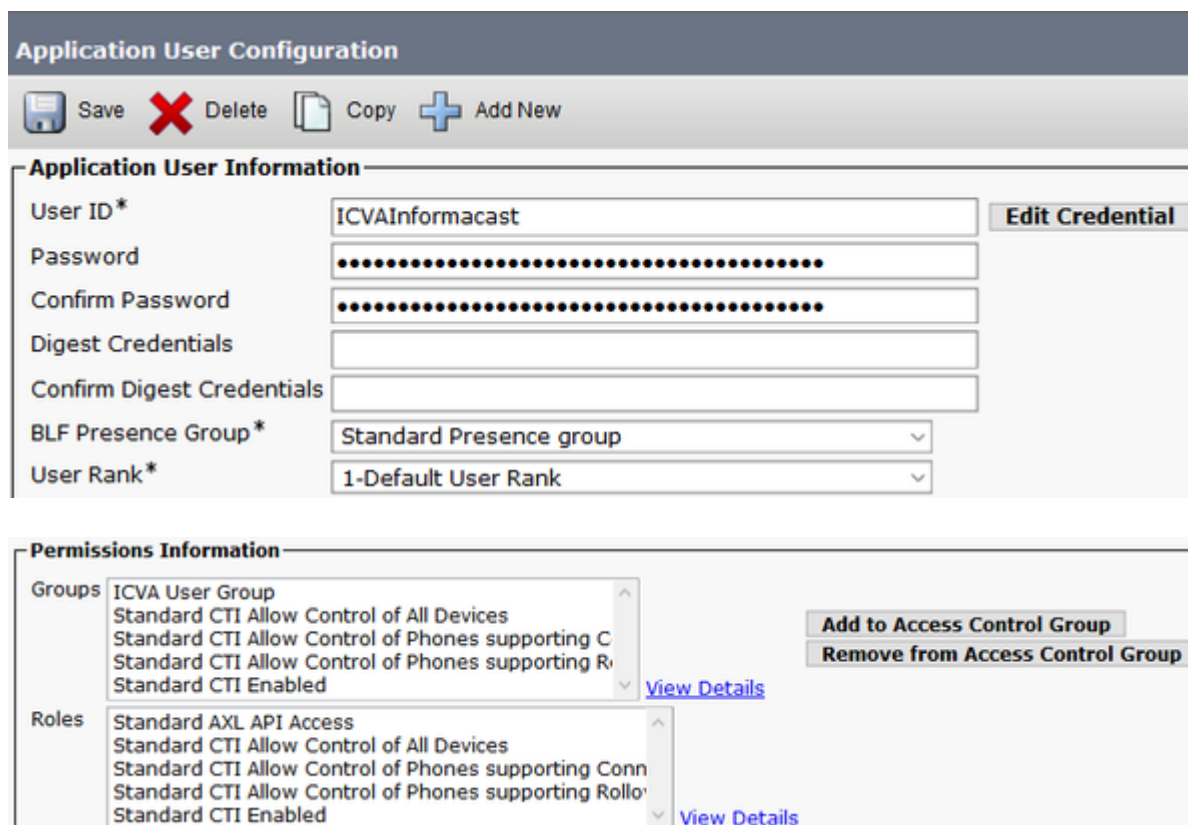
Schritt 7: Erstellen einer Zugriffssteuerungsgruppe (AXL)

- Navigieren Sie zu CM Admin > User Management > User Settings > Access Control Group, und erstellen Sie eine Zugriffskontrollgruppe, z. B. ICVA User Group.
- Fügen Sie die Standard AXL API Access-Rolle hinzu.

 Anmerkung: Möglicherweise haben Sie bereits eine Zugriffssteuerungsgruppe mit dem Namen Standard AXL API Access und der Rolle Standard AXL API Access hinzugefügt, die Sie ebenfalls verwenden können.

Schritt 8: Erstellen eines Anwendungsbenutzers

- Navigieren Sie zu CM Admin > User Management > Application User, und klicken Sie auf Add New. Nennen Sie den Anwendungsbenutzer als ICVA_InformaCast, und weisen Sie ihm die folgenden Rollen zu:
 1. Standard – CTI – aktiviert
 2. ICVA-Benutzergruppe (oder Standard-AXL API-Zugriff)
 3. Standard – CTI – Steuerung von Telefonen zulassen, die verbundenen Transfer und Konferenzen unterstützen.
 4. Standard – CTI – Steuerung von Telefonen zulassen, die den Rollover-Modus unterstützen
 5. Standard-CTI ermöglicht die Steuerung aller Geräte



Application User Configuration

Save Delete Copy Add New

Application User Information

User ID* ICVAInformacast Edit Credential

Password

Confirm Password

Digest Credentials

Confirm Digest Credentials

BLF Presence Group* Standard Presence group

User Rank* 1-Default User Rank

Permissions Information

Groups ICVA User Group
Standard CTI Allow Control of All Devices
Standard CTI Allow Control of Phones supporting C
Standard CTI Allow Control of Phones supporting R
Standard CTI Enabled View Details

Roles Standard AXL API Access
Standard CTI Allow Control of All Devices
Standard CTI Allow Control of Phones supporting Conn
Standard CTI Allow Control of Phones supporting Rollo
Standard CTI Enabled View Details

Add to Access Control Group
Remove from Access Control Group

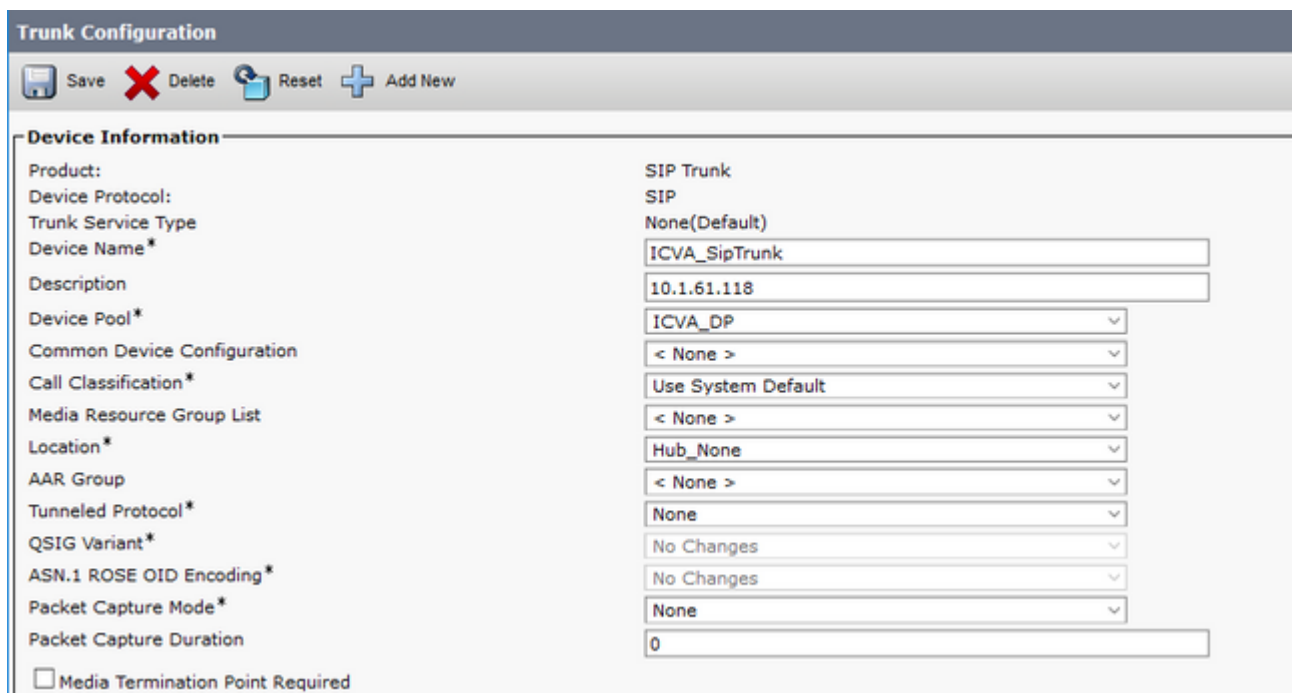
 Warnung: Pro Defekt [CSCve47332](#) wird empfohlen, keine Leerzeichen für die Benutzer-ID

 der Anwendung zu verwenden.

Schritt 9: Integration von Communications Manager in Informacast mithilfe von SIP oder CTI

Erstellen Sie zur SIP-Integration ein SIP-Profil, einen SIP-Trunk und ein Routenmuster.

- Navigieren Sie zu CM Admin > Device > Device Settings > SIP Profile, und klicken Sie auf Standard SIP Profile und dann auf Copy
- Geben Sie dem Profil den Namen ICVA SIP Profile und wählen Sie Best Effort (kein MTP eingefügt). Klicken Sie auf Speichern.
- Navigieren Sie zu CM Admin > Device > Trunk, und klicken Sie auf Add New
- Wählen Sie SIP Trunk aus dem Trunk-Typ-Dropdown-Menü aus. Klicken Sie auf Weiter, und geben Sie einen Namen für Ihren SIP-Trunk ein.
- Wählen Sie den Gerätepool ICVA_DP aus, scrollen Sie nach unten zum Bereich SIP Information, und geben Sie die IP-Adresse Ihres InformaCast-Servers in die Zieladresse ein.
- Stellen Sie sicher, dass der Wert im Feld "Destination Port" 5060 lautet, wählen Sie das nicht sichere SIP-Trunk-Profil aus, und weisen Sie das zuvor erstellte SIP-Profil aus dem Dropdown-Menü "SIP Profile" (SIP-Profil) zu. Klicken Sie auf Speichern.



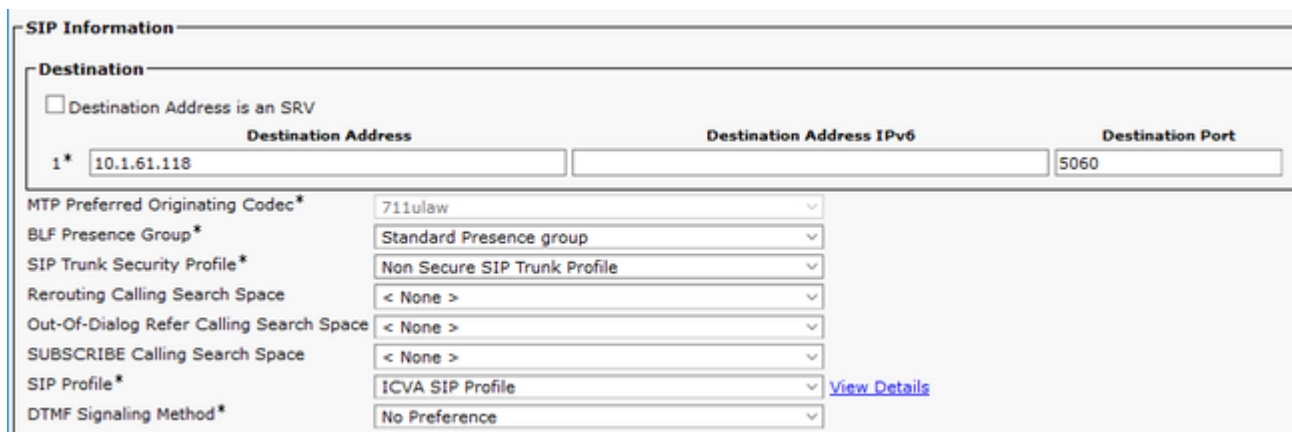
Trunk Configuration

Save Delete Reset Add New

Device Information

Product:	SIP Trunk
Device Protocol:	SIP
Trunk Service Type	None(Default)
Device Name*	ICVA_SipTrunk
Description	10.1.61.118
Device Pool*	ICVA_DP
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



SIP Information

Destination

☐ Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	10.1.61.118		5060

MTP Preferred Originating Codec*	711ulaw
BLF Presence Group*	Standard Presence group
SIP Trunk Security Profile*	Non Secure SIP Trunk Profile
Rerouting Calling Search Space	< None >
Out-Of-Dialog Refer Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile*	ICVA SIP Profile View Details
DTMF Signaling Method*	No Preference

- Erstellen Sie das Routenmuster, navigieren Sie zu CM Admin > Call Routing > Route Hunt > Route pattern, und klicken Sie auf Add New.
- Geben Sie ein Routenmuster ein, z. B. 7777, und konfigurieren Sie eine Partition, die von den Telefonen erreichbar ist, z. B. ICVA_PT.
- Wählen Sie den gerade erstellten SIP-Trunk aus dem Dropdown-Menü Gateway/Routenliste aus.
- Wählen Sie die Optionsfelder Route This Pattern (Dieses Muster weiterleiten) und OnNet aus.
- Deaktivieren Sie das Kontrollkästchen Externen Wählton bereitstellen, und klicken Sie auf Speichern.

Erstellen Sie für die CTI-Integration einen CTI-Routing-Punkt, und ordnen Sie ihn dem in Schritt 8 erstellten Anwendungsbenutzer zu.

- Navigieren Sie zu CM Administration > Device > CTI Route Point, und klicken Sie auf Add new.
- Geben Sie einen Namen ein, z. B. ICVA_CTI_RP (oder wie Sie möchten).
- Weisen Sie den Gerätepool ICVA_DP zu, und klicken Sie auf Speichern.
- Wählen Sie die Zeile 1 aus, geben Sie eine Verzeichnisnummer ein, z. B. 7778, und weisen Sie die kürzlich erstellte Partition (ICVA_PT) zu.
- Konfigurieren Sie die restlichen Informationen wie gewünscht, und klicken Sie auf Speichern.

Fügen Sie den bzw. die CTI-Routenpunkte als gesteuerte Geräte in der Konfiguration des ICVA-Anwendungsbenutzers hinzu.



 **Anmerkung:** InformaCast kann mehrere CTI-Routing-Punkte unterstützen, wenn diese im Communications Manager erstellt und dem Benutzer der InformaCast-Anwendung zugeordnet werden.

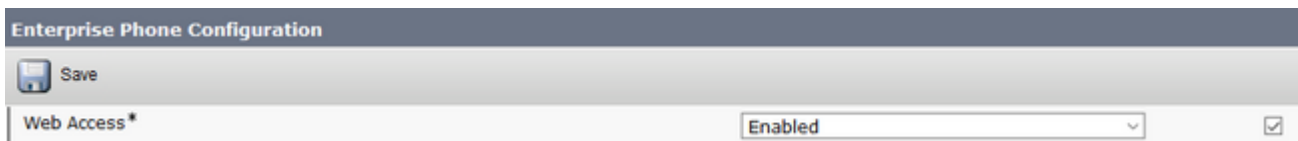
 **Tipp:** Anstatt für jede Nummer, die Sie für DialCasts benötigen, einen CTI-Routing-Punkt zu erstellen, können Sie einem einzelnen CTI-Routing-Punkt auch mehrere Leitungen hinzufügen. Eine weitere Möglichkeit besteht darin, Platzhaltermuster zu verwenden, um einem Nummernbereich zu entsprechen.

Schritt 10: Aktivieren Sie Web Access für Cisco IP-Telefone, um HTTP zur Steuerung der Telefone zu verwenden.

- Der Webzugriff kann auf Gerätebasis, über ein gemeinsames Geräteprofil oder systemweit über die Enterprise Phone Configuration konfiguriert werden.
- Um die Änderung der Telefonkonfigurationen der Enterprise-Klasse anzuwenden, navigieren Sie zu CM Admin > System > Enterprise Phone Configuration, scrollen Sie nach unten zum Dropdown-Menü Web Access (Webzugriff) und wählen Sie Enabled (Aktiviert). Klicken Sie

auf Speichern.

- Setzen Sie die Telefone zurück, um die Änderungen zu übernehmen.



Enterprise Phone Configuration

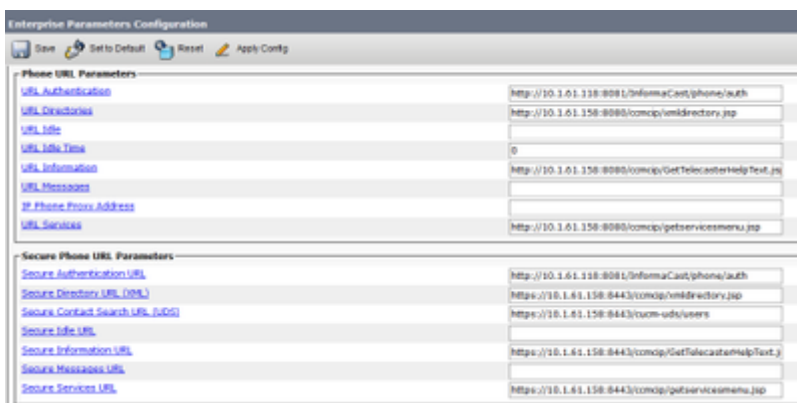
Save

Web Access * Enabled

Schritt 11: Festlegen der Authentifizierungs-URL

Ändern Sie die Authentifizierungs-URL, um Authentifizierungsanforderungen von IP-Telefonen an InformaCast zu senden. Alle Nicht-InformaCast-Authentifizierungsanforderungen werden zurück an die Standard-CUCM-Authentifizierungs-URL umgeleitet.

- Navigieren Sie zu CM Administration > System > Enterprise-Parameter.
- Geben Sie im Feld für die URL-Authentifizierung und die URL für die sichere Authentifizierung `http://<IP-Adresse der virtuellen InformaCast-Appliance>:8081/InformaCast/phone/auth` ein.
- Klicken Sie auf Speichern, Konfiguration übernehmen und die Telefone zurücksetzen.



Enterprise Parameters Configuration

Save Set to Default Reset Apply Config

Phone URL Parameters

URL Authentication	<code>http://10.1.61.158:8081/InformaCast/phone/auth</code>
URL Directories	<code>http://10.1.61.158:8080/cucmp/umdirectories.jsp</code>
URL Info	
URL Info Time	0
URL Information	<code>http://10.1.61.158:8080/cucmp/GetTelecastertHelpText.jsp</code>
URL Messages	
IP Phone Proxy Address	
URL Services	<code>http://10.1.61.158:8080/cucmp/getservicesmenu.jsp</code>

Secure Phone URL Parameters

Secure Authentication URL	<code>http://10.1.61.158:8081/InformaCast/phone/auth</code>
Secure Directory URL (DNIS)	<code>https://10.1.61.158:8443/cucmp/umdirectories.jsp</code>
Secure Contact Search URL (JCS)	<code>https://10.1.61.158:8443/cucm-uds/users</code>
Secure Info URL	
Secure Information URL	<code>https://10.1.61.158:8443/cucmp/GetTelecastertHelpText.jsp</code>
Secure Messages URL	
Secure Services URL	<code>https://10.1.61.158:8443/cucmp/getservicesmenu.jsp</code>

 Anmerkung: Bei der URL wird die Groß-/Kleinschreibung beachtet. Achten Sie also darauf, dass die Buchstaben "I" und "C" im Wort "InformaCast" großgeschrieben werden. Sowohl die URL für die sichere Authentifizierung als auch die Authentifizierungs-URL müssen auf denselben Wert, die HTTP-URL, festgelegt werden.

Schritt 12: Festlegen der Authentifizierungsmethode für den API-Browserzugriff

- Wenn Sie Unified Communications Manager 11.5.1 oder höher verwenden, scrollen Sie auf der Seite nach unten zum Bereich "Sicherheitsparameter", und wählen Sie im Dropdown-Menü "Authentifizierungsmethode für API-Browserzugriff" die Option Basics (Grundlegend) aus.

Schritt 13: Testen Sie Ihre Telefone, und wählen Sie z. B. 7777 (für die SIP-Integration) oder 7778 (für die CTI-Integration).

 Anmerkung: Wenn Sie Unified Communications Manager im gemischten Modus ausführen, stellen Sie sicher, dass Anrufe bei und von InformaCast nicht mit verschlüsselten Medien

 erfolgen.

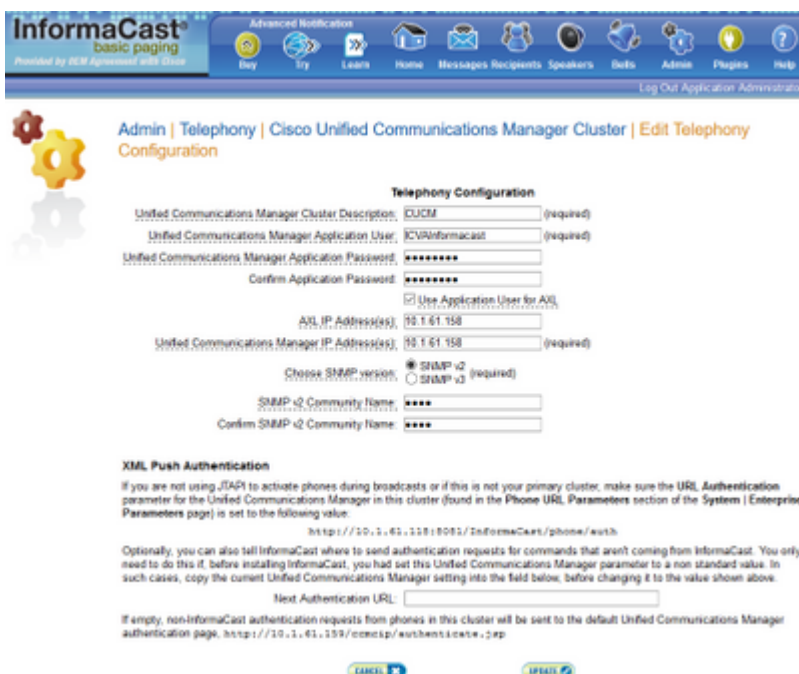
Konfigurieren von Informacast

Schritt 1: Konfigurieren des Communications Manager-Clusters in Informacast

- Melden Sie sich bei Informacast an, und navigieren Sie zu Admin > Telephony > Unified Communications Manager Cluster. Klicken Sie auf "Bearbeiten".
- Geben Sie den Benutzernamen und das Kennwort des Anwendungsbenutzers für den Anwendungsbenutzer ein, den Sie in Schritt 8 erstellt haben.
- Vergewissern Sie sich, dass das Kontrollkästchen Anwendungsbenutzer für AXL verwenden aktiviert ist, d. h. dass Ihre Anmeldeinformationen für Anwendungsbenutzer beim Erstellen des Telefoncaches von InformaCast verwendet werden.

 **Anmerkung:** Wenn Sie dieses Feld leer lassen, versucht InformaCast, einen Server zu finden, auf dem der AXL-Dienst ausgeführt wird, und zwar auf den Servern, auf denen der CallManager-Dienst ausgeführt wird.

- Geben Sie die IP-Adresse des/der Unified Communications Manager-Server(s) in das Feld Communications Manager-IP-Adresse(n) ein. Verwenden Sie numerische IP-Adressen anstelle von DNS-Namen.
- Wählen Sie das Optionsfeld SNMP v2 oder SNMP v3 aus. Geben Sie die gleichen Informationen ein, die in CUCM konfiguriert wurden. Klicken Sie auf Aktualisieren.



InformaCast
basic paging
Powered by BCM Application Event Server

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

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

Telephony Configuration

Unified Communications Manager Cluster Description: CUCM (required)

Unified Communications Manager Application User: ICVInformacast (required)

Unified Communications Manager Application Password: *****

Confirm Application Password: *****

☒ Use Application User for AXL

AXL IP Address(es): 10.1.61.158

Unified Communications Manager IP Address(es): 10.1.61.158 (required)

Choose SNMP version:
☒ SNMP v2 ☐ SNMP v3 (required)

SNMP v2 Community Name: ****

Confirm SNMP v2 Community Name: ****

XML Push Authentication

If you are not using J2API to activate phones during broadcasts or if this is not your primary cluster, make sure the URL, Authentication parameter for the Unified Communications Manager in this cluster (found in the Phone URL, Parameters section of the System | Enterprise Parameters page) is set to the following value:
http://10.1.61.158:8081/InformaCast/phone/auth

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

Next Authentication URL:

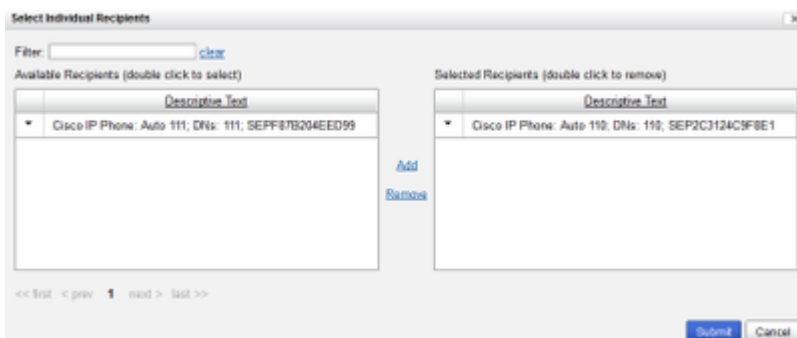
If empty, non-InformaCast authentication requests from phones in this cluster will be sent to the default Unified Communications Manager authentication page, http://10.1.61.158/cmsep/authenticate.jsp

Schritt 2: Konfigurieren der Empfängergruppe

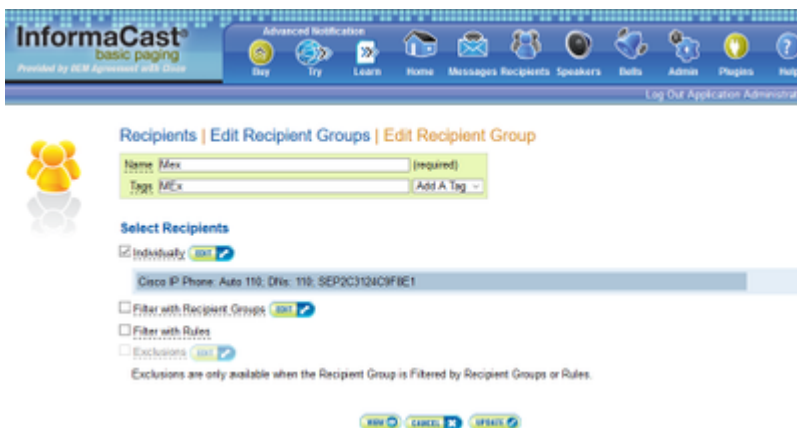
- Navigieren Sie zu Empfänger > Empfängergruppen bearbeiten, und klicken Sie auf Aktualisieren, um alle in CUCM registrierten und von InformaCast erkannten Telefone anzuzeigen.



- Um eine neue Empfängergruppe zu erstellen, klicken Sie auf Hinzufügen, geben Sie einen Namen ein, und klicken Sie dann auf Bearbeiten, um die Telefone für diese Empfängergruppe hinzuzufügen. Sobald die Telefone dem Empfänger hinzugefügt wurden, klicken Sie auf Senden.

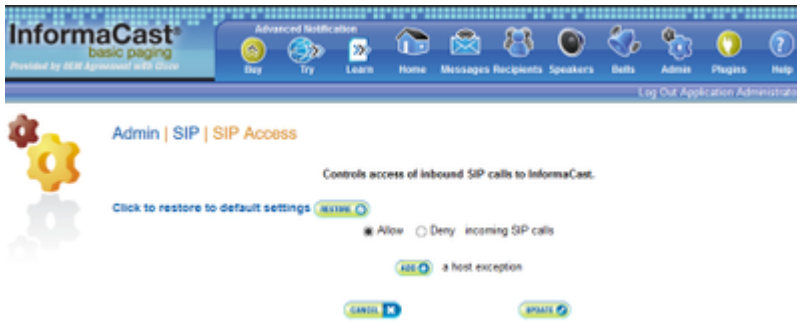


- Um die Änderungen zu speichern, klicken Sie auf Aktualisieren.



Schritt 3: SIP-Zugriff auf InformaCast zulassen/deaktivieren

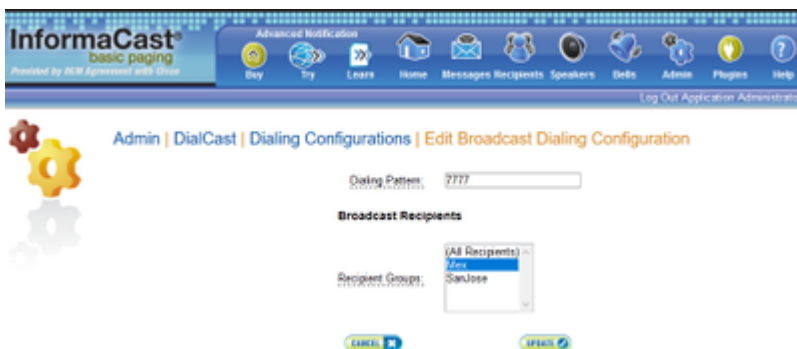
- Navigieren Sie zu Admin > SIP > SIP Access. Standardmäßig werden alle SIP-Anrufe abgelehnt.
- Aktivieren Sie das Optionsfeld Zulassen, um alle SIP-Anrufe zuzulassen, oder klicken Sie auf Hinzufügen, um Ausnahmen von dieser Einschränkung zuzulassen.



 Tipp: Stellen Sie beim Definieren von Ausnahmen sicher, dass Sie den Host angeben, der die INVITE-Anforderung direkt an InformaCast sendet. Dies kann ein SIP-Proxy-Server sein, wenn sich die Proxys zwischen InformaCast und dem anrufenden Host befinden.

Schritt 4: Hinzufügen einer Broadcast-Wählkongfiguration

- Gehen Sie zu Admin > DialCast > Dialing Configurations, und klicken Sie auf Add.
- Geben Sie ein Wählmuster (z. B. 7777, 7778) in das Feld Wählmuster gemäß dem in CUCM erstellten Routenmuster (für SIP-Integration) oder CTI-Routenpunkt (für CTI-Integration) ein.
- Wählen Sie die Empfängergruppen aus der Liste aus, und klicken Sie auf Aktualisieren.



Schritt 5: Konfigurieren Sie die Broadcast-Parameter.

- Navigieren Sie zu Admin > Broadcast-Parameter.
- Konfigurieren der IP für Multicast Die Standard-IP-Adresse (239.0.1.2) wird häufig verwendet.
- Aktivieren Sie das Kontrollkästchen JTAPI, wenn Sie die Befehle als JTAPI an die Telefone senden möchten. Andernfalls werden HTTP-Nachrichten verwendet.



Stellen Sie sicher, dass dieser Bereich Ihren Netzwerkinfrastruktureinstellungen entspricht und

alle Empfängergruppen abdeckt. Bei Bereitstellungen mit mehreren Standorten empfehlen Singlewire und Cisco die Verwendung eines Adressenbereichs. Dieser Bereich sollte groß genug sein, um eine Adresse für jeden gleichzeitigen Broadcast zu verarbeiten.

 Anmerkung: Die Verwendung von JTAPI über HTTP wird empfohlen, da es den Status von Telefonen besser überwacht und mit mehr Gebietsschemas arbeitet.

 Tipp: Die Standardeinstellungen für die Webschnittstelle melden Sie nach fünf Minuten ab. Navigieren Sie zu Admin > Network Parameters > Session Timeouts, und ändern Sie das Feld General Session Timeout (seconds) (Allgemeines Sitzungstimeout (Sekunden)) von 300 in den neuen Wert.

Konfigurieren von Multicast im Netzwerk

Wenn sich der Cisco Paging-Server und die IP-Telefone in separaten IP-Subnetzen befinden, müssen die Router zwischen diesen beiden Subnetzen für das Multicast-Routing konfiguriert werden.

Der Cisco Paging Server erfordert keine bestimmte Multicast-Routing-Methode (SM, DM, S-DM, SSM usw.). Einige WAN-Umgebungen unterstützen kein Multicast-Routing. In diesen Umgebungen können GRE-Tunnel zwischen Standorten gebaut und für den Transport von Multicast verwendet werden.

Das Design und die Konfiguration von Multicast in Ihrer Umgebung werden in diesem Dokument nicht behandelt. Die folgenden Ressourcen sind jedoch möglicherweise hilfreich:

- [Multicast-Whitepaper](#)
- [Multicast-Testtool](#)

 Anmerkung: Wenn Sie Meraki Switches verwenden, ist IGMP-Snooping standardmäßig aktiviert. Dies kann zu Problemen führen und muss von Meraki deaktiviert werden. Wenn Sie den Kontakt hergestellt und das IGMP-Snooping deaktiviert haben, testen Sie das Paging erneut.

Überprüfung

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Häufige Probleme

Telefone nicht aktiviert

Berücksichtigen Sie, dass Informacast alle Telefone überspringt, die während der Übertragung genutzt werden (besetzt).

InformaCast verwendet verschiedene Besetzt-Erkennungsmethoden, je nachdem, wie Sie Nachrichten an die Telefone senden (HTTP oder JTAPI).

HTTP: Die Besetzterkennung funktioniert nur bei Gebietsschemas, auf denen englische Lasten ausgeführt werden.

CTI: Funktioniert mit anderen Sprachen als Englisch

Die Besetzt-Erkennung funktioniert je nach Protokoll, Leitungstyp und Leitungsstatus auch unterschiedlich.

Leitungsstatus	CTI-Besetzt-Erkennung	HTTP-Besetzt-Erkennung
Gemeinsam genutzte Leitung mit Anruf, der auf einem anderen Telefon verwendet wird, kein gehaltener Anruf	Inaktiv	Inaktiv
Hörer abnehmen, Ziffern erfassen	Besetzt	Nicht beschäftigt
Gespräch, aktiver Anruf	Besetzt	Besetzt
In Haltestellung, inaktiver Anruf auf gemeinsam genutzter Leitung	Besetzt	Nicht beschäftigt
In Haltestellung, inaktiver Anruf auf eindeutiger Leitung	Besetzt	Nicht beschäftigt

 Anmerkung: Wenn versucht wird, gleichzeitig zu senden, spielt Informacast zuerst die erste Übertragung ab (die zweite Übertragung wird blockiert).

Sammeln Sie bei der Fehlerbehebung eines nicht aktivierten Telefons die folgenden Daten:

- Leistungsprotokolle von Informacast
- Konsolenprotokolle (PRT) vom Telefon aus.

Telefone nicht erkannt

Nur registrierte Telefone werden von InformaCast erkannt. Wenn ein IP-Telefon registriert, aber nicht erkannt wurde, überprüfen Sie die SNMP-Dienstkonfiguration in Informacast und den CUCM-Knoten, bei dem das Telefon registriert ist. Der SNMP-Dienst und der Community String müssen für alle Knoten konfiguriert werden, auf denen der Call Manager-Dienst aktiviert ist.

SNMP-Fehler: Es können keine Empfängergruppen erstellt werden: java.lang.Exception



1. Der Fehler bedeutet, dass SNMP aufgrund der DNS-Konnektivität oder -Auflösung nicht rechtzeitig auf Abfragen antwortet.
2. Bestätigen Sie, dass der UDP-Port 161 vom InformaCast-Server für alle Unified Communications Manager-Clusterknoten blockiert wird.
3. Bestätigen Sie, dass die SNMP-Informationen richtig sind. Navigieren Sie zu Admin > Telephony > Unified Communications Manager Cluster, und geben Sie, falls möglich, einen neuen SNMP-String ein. Konfigurieren Sie die neue Zeichenfolge in CUCM.
4. Möglicherweise verwenden Sie auch einen Community-String, der die maximale Zeichenanzahl für den Community-String überschreitet. Wenn Sie den Community-String aus CUCM kopieren und in die Informacast-Konfiguration einfügen, versuchen Sie, ihn einzugeben, um zu sehen, ob Sie den gesamten String eingeben können. In der Informacast-Version 11 sind maximal 18 Zeichen zulässig.
5. Überprüfen Sie, ob Ihre DNS-Konfiguration auf dem CUCM korrekt ist, und stellen Sie sicher, dass Sie nicht mit dem Defekt [CSCtb70375](#) übereinstimmen.

Kein Audio auf den Zieltelefonen

Wenn Telefone aufleuchten, aber kein Ton abgespielt wird, hängt das Problem höchstwahrscheinlich mit Multicast-Routing zusammen und nicht mit Ihrem CUCM-Server oder Ihren IP-Telefonen.

Zu erfassende Daten

Bei der Fehlerbehebung von Informacast sollten Sie die folgenden Daten erfassen:

1. Leistungsprotokolle von Informacast
2. Paketerfassung von Informacast.
3. Paketerfassung von den Telefonen.
4. Paketerfassung vom CUCM.
5. SDL Protokolle vom CUCM

6. PRT (Konsolenprotokolle)

Leistungsprotokolle

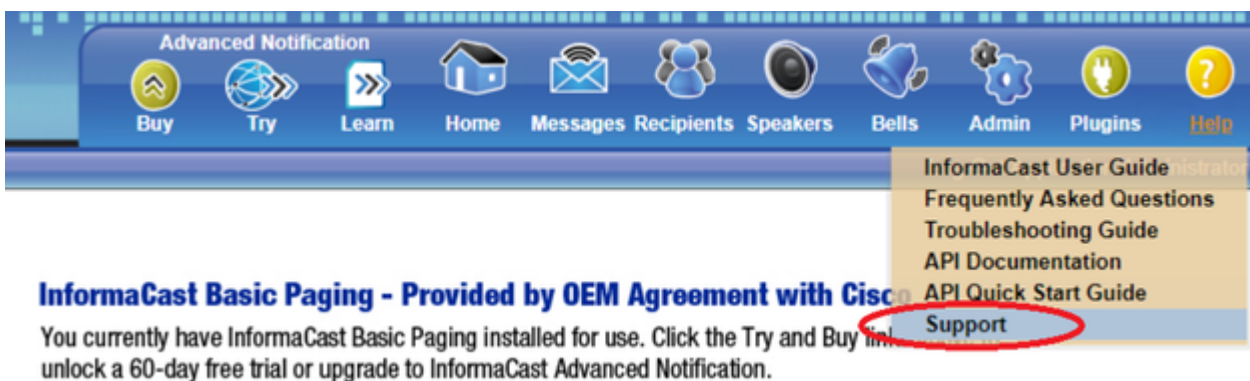
Es gibt zwei Methoden, um die Leistungsprotokolle von Informacast abzurufen.

Methode 1

1. Navigieren Sie zu <https://<Informacast IP>:8444/InformaCast/logs/performance.log>
2. Kopieren Sie die Datei, und speichern Sie das Protokoll in einer TXT-Datei.

Methode 2

1. Öffnen Sie die Informacast IP in einem Webbrowser, https://<informacast_IP> und wählen Sie Informacast aus.
2. Melden Sie sich mit Ihren Anmeldeinformationen an, und navigieren Sie zu Hilfe > Support.



3. Klicken Sie auf Performance Logs unter dem Bereich Tools, wie im Bild gezeigt.

Tools

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

[API Log](#) Shows requests made to the InformaCast REST API.

[Calling Terminal Diagnostics](#) Shows the CTI ports and route points registered with InformaCast.

[Call Detail Records Directory](#) Shows the directory containing the call detail records.

[InformaCast Logs Directory](#) Shows the directory containing the InformaCast logs.

[Log Tool](#) Collects and analyzes Singlewire log files for errors.

[Performance Log](#) Contains information logged by InformaCast.

[SIP Stack Log](#) Contains information logged by the SIP stack.

[Summary Log](#) Contains a summary of broadcasts sent by InformaCast.

Paketerfassung

Von Informacast

Es gibt drei Methoden, um eine Paketerfassung von Informacast zu erhalten.

Methode 1

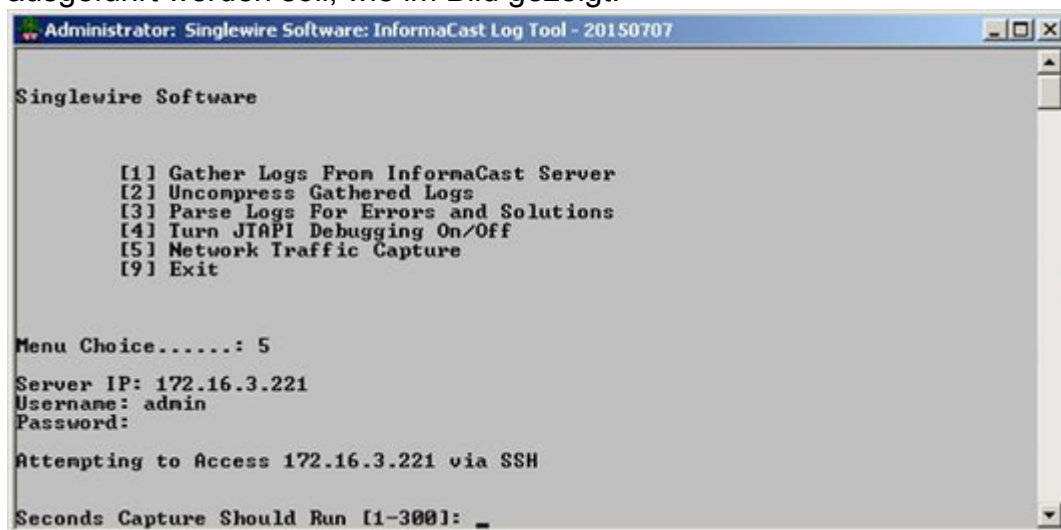
1. Herstellen einer Verbindung zur CLI der Informacast-Box über SSH

2. Führen Sie den Befehl `sudo capturePackets test.cap` aus, um die Erfassung zu starten und eine Datei mit dem Namen `test.cap` zu erstellen.
3. Rufen Sie die Telefone auf, die nicht funktionieren.
4. Drücken Sie `Strg + C`, um den `pcap` zu beenden.
5. Führen Sie `ls` aus, um sicherzustellen, dass die Paketerfassung einsatzbereit ist.
6. Verwenden Sie SFTP oder Secure Copy (SCP), um die Datei auf Ihren PC zu übertragen.

```
admin@singlewire:~$ sudo capturePackets test.cap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 1514 bytes
^C34 packets captured
36 packets received by filter
0 packets dropped by kernel
admin@singlewire:~$ sftp cisco@10.1.61.20
Authenticated with partial success.
cisco@10.1.61.20's password:
Hello, I'm freeFTPD 1.0Connected to 10.1.61.20.
sftp>
sftp>
sftp> put test.cap
Uploading test.cap to /test.cap
test.cap
sftp>
```

Methode 2

1. Laden Sie [InformaCast LogTool](#) aus dem Internet herunter und installieren Sie es.
2. Führen Sie die Software aus, und wählen Sie die Option [5]. Schreiben Sie die IP-Adresse von Informacast, die Anmeldedaten und die Sekunden, in denen die Paketerfassung ausgeführt werden soll, wie im Bild gezeigt.



3. Die Erfassung beginnt nicht sofort, sodass Sie Ihre Testumgebung vorbereiten können. Wenn Sie bereit sind, wählen Sie Option [1] aus, und drücken Sie die Eingabetaste, um die Paketerfassung wie im Bild dargestellt zu starten.

```
Seconds Capture Should Run [1-300]: 60

[1] Start 60 Second Capture
[9] Return to Main Menu

Menu Choice.....: 1
Traffic Capture Started: 60 Seconds
00:00:51
```

4. Das Tool zeigt einen Countdown-Timer mit der ausstehenden Dauer der Erfassung an. Replizieren Sie das Problem während dieser Zeit, und wenn der Erfassungszähler den Wert Null erreicht, ist die Erfassung abgeschlossen und wird beendet.

5. Das Tool bündelt die Paketerfassung und alle Protokolle in einer .tgz-Datei und überträgt diese an Ihre Workstation. Dies entspricht Option 1 zum Sammeln von Protokollen, umfasst jedoch auch die Erfassung des Netzwerkverkehrs.
6. Das Tool erstellt einen Ordner mit der Paketerfassung im Basisverzeichnis von Informacast_LogTool.exe, wie im Bild dargestellt.

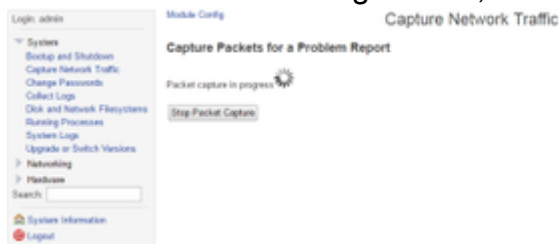


Methode 3 (verfügbar ab Version 12.0.1)

1. Melden Sie sich bei <Informacast_IP> an:10000
2. Navigieren Sie zu System > Capture Network Traffic (System > Netzwerkverkehr erfassen).

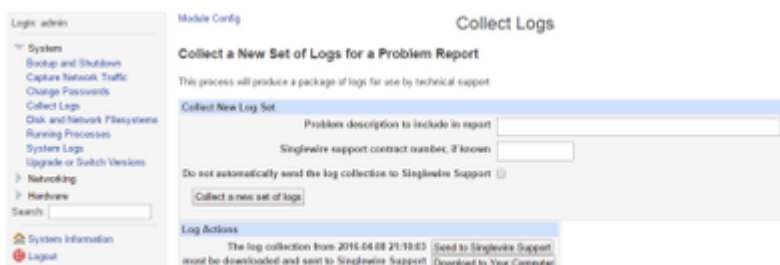


3. Klicken Sie auf Neue Paketerfassung starten, und replizieren Sie das Problem wie im Bild



dargestellt.

4. Klicken Sie auf Stopp Packet Capture (Paketerfassung beenden), wenn das Problem vollständig repliziert wird, oder beenden Sie es von selbst, nachdem Sie 33.000 Pakete erfasst haben.
5. Navigieren Sie zu System > Collect Logs, geben Sie eine kurze Beschreibung des Problems ein, und klicken Sie auf Collect a new set of logs.
6. Um die Protokolle zu speichern, klicken Sie auf Auf Ihren Computer herunterladen, wie im Bild gezeigt.



Methode 4 (verfügbar ab Version 12.0.1)

In Version 12.0.1 und neueren Versionen ist sudo nicht mehr erforderlich. Um eine Paketerfassung auszuführen, verwenden Sie den Befehl capture-packages <Name der Datei> <Anzahl der Pakete> wie im Beispiel gezeigt:

```

admin@informacast:~$ capture-packets test
Saving up to 33000 packets to /var/log/capture-packets/test
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 1514
bytes
^C13 packets captured
15 packets received by filter
0 packets dropped by kernel
Interrupt signaled. Cleaning up.

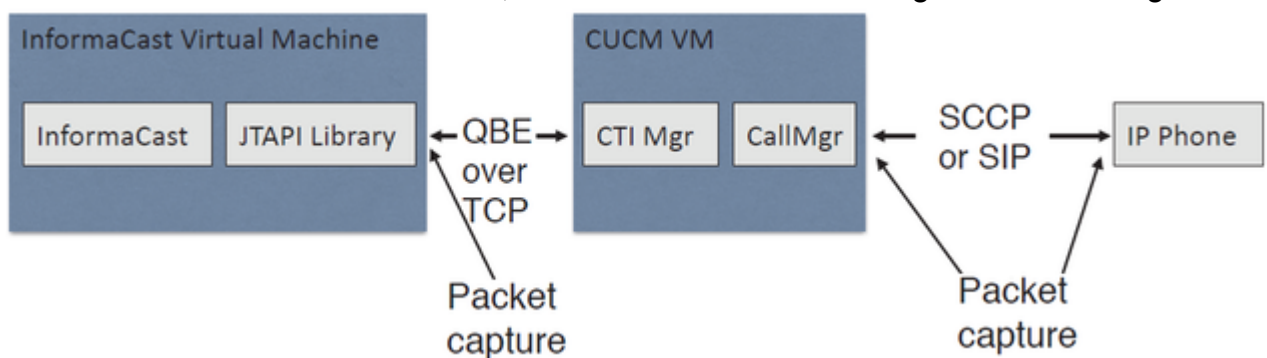
```

 Anmerkung: Die GUI-Methode ist besser als die CLI, da es keine Abhängigkeit von einem SFTP-Server gibt und Sie die Paketerfassung von der Webseite starten, stoppen und herunterladen können.

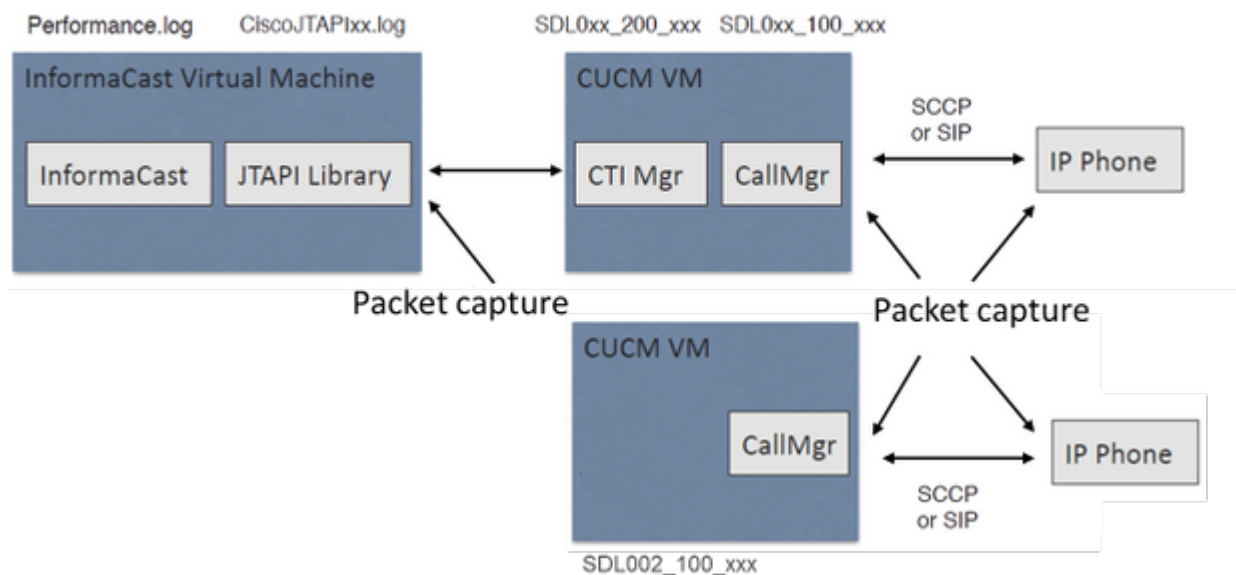
Von CUCM

Definieren Sie, von wo aus Sie die Paketerfassung gemäß Ihrer Bereitstellung erhalten müssen. Sie können nur einen CUCM-Knoten oder mehrere CUCMs im Cluster haben.

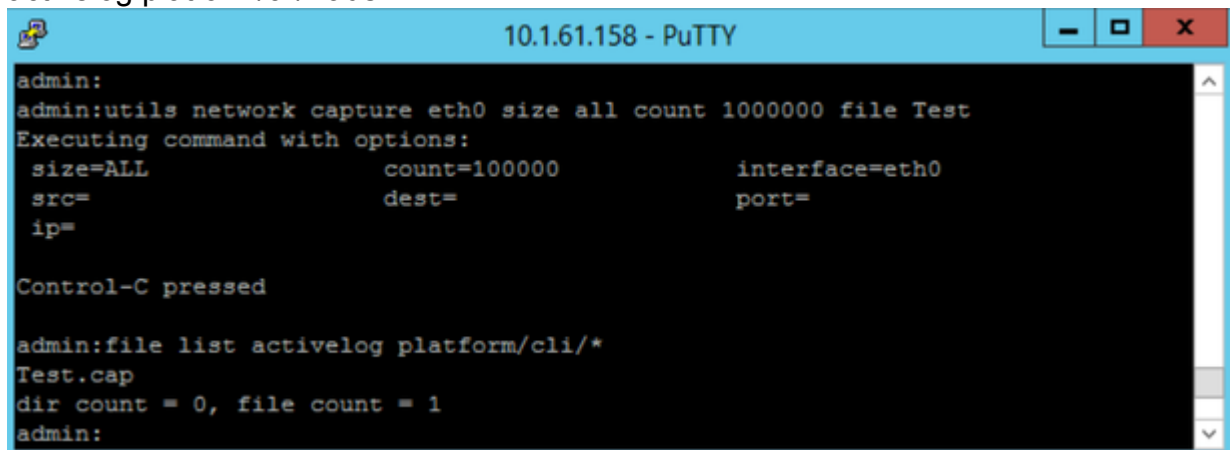
- Wenn Sie einen CUCM-Knoten haben, rufen Sie die Paketerfassung wie im Bild dargestellt



- Wenn Sie einen CUCM-Cluster haben und ein Knoten mit Informacast kommuniziert, aber ein anderer mit den Telefonen kommuniziert, holen Sie die Paketerfassung wie im Bild gezeigt ein.



1. Öffnen Sie eine SSH-Sitzung für den Knoten, den Sie erfassen müssen.
2. Führen Sie den Befehl `utils network capture eth0 size all count 1000000 file Test` aus, um die Paketerfassung zu starten.
3. Problem replizieren
4. Stoppen der Paketerfassung mit Strg + C
5. Um zu bestätigen, dass die Paketerfassung gespeichert wurde, führen Sie den Befehl `file list activelog platform/cli/*` aus.

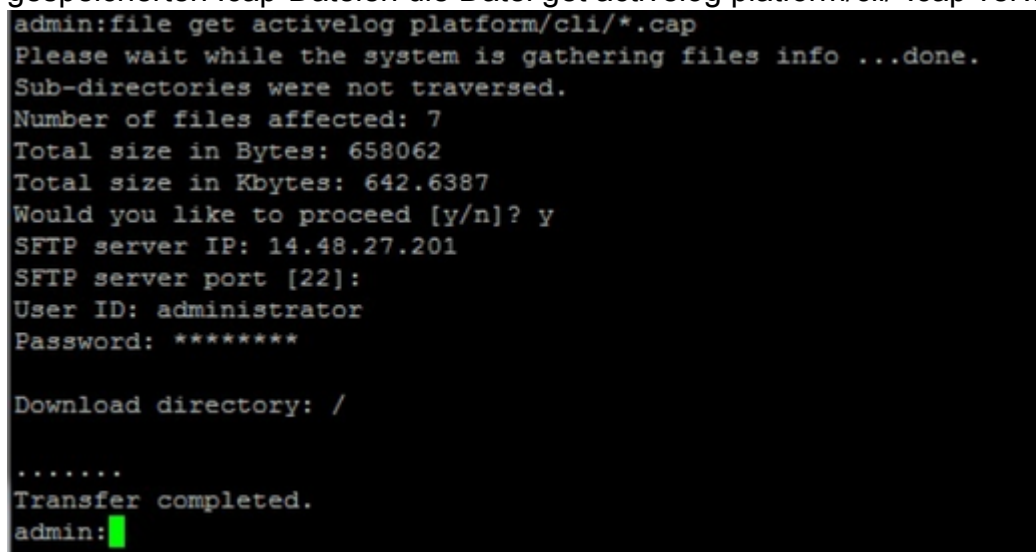


```
admin:
admin:utils network capture eth0 size all count 1000000 file Test
Executing command with options:
  size=ALL          count=100000      interface=eth0
  src=              dest=            port=
  ip=

Control-C pressed

admin:file list activelog platform/cli/*
Test.cap
dir count = 0, file count = 1
admin:
```

6. Verwenden Sie den Befehl `file get activelog platform/cli/Test.cap`, um die Paketerfassung an einen SFTP-Server zu senden. Alternativ können Sie zum Sammeln aller auf dem Server gespeicherten .cap-Dateien die Datei `get activelog platform/cli/*.cap` verwenden.

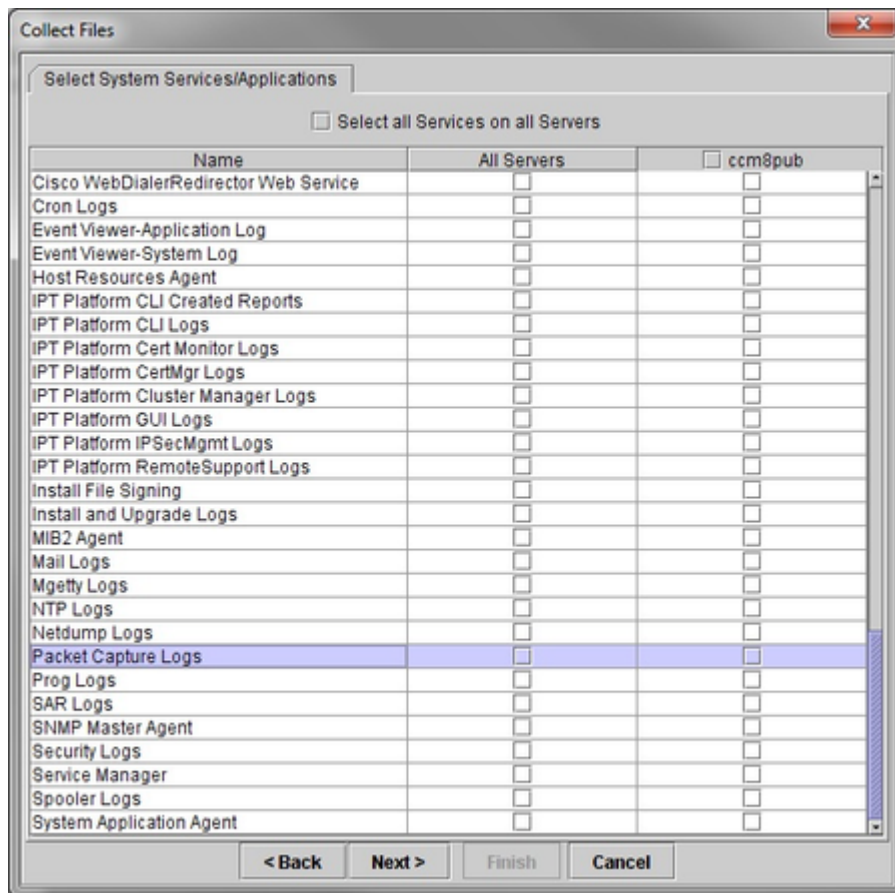


```
admin:file get activelog platform/cli/*.cap
Please wait while the system is gathering files info ...done.
Sub-directories were not traversed.
Number of files affected: 7
Total size in Bytes: 658062
Total size in Kbytes: 642.6387
Would you like to proceed [y/n]? y
SFTP server IP: 14.48.27.201
SFTP server port [22]:
User ID: administrator
Password: *****

Download directory: /

.....
Transfer completed.
admin:
```

7. Verwenden Sie RTMT, falls Sie keinen SFTP-Server verwenden können. Navigieren Sie zu System > Trace & Log Central > Collect Files. Klicken Sie auf Weiter, und aktivieren Sie das Kontrollkästchen Paketerfassungsprotokolle, wie im Bild gezeigt.



8. Klicken Sie auf Weiter, wählen Sie ein Download-Dateiverzeichnis und klicken Sie auf Fertig stellen.
9. Löschen Sie das Paket mit der Befehlsdatei delete activelog platform/cli/Test.cap

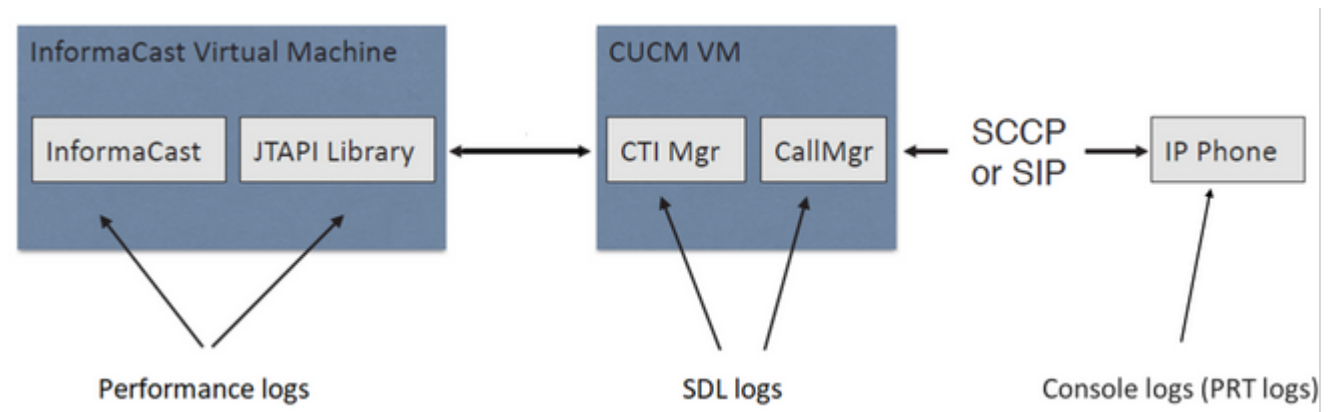
Über das Telefon

1. Aktivieren Sie den SPAN-PC-Port. Navigieren Sie zu CM Admin page > Device > phone, und suchen Sie nach dem Telefon mit den gemeldeten Problemen.
2. Suchen Sie im Abschnitt "Produktspezifisches Konfigurationslayout" nach Span to PC Port, und wählen Sie Aktivieren aus dem Dropdown-Menü aus. Klicken Sie auf Speichern und dann auf Konfiguration übernehmen.
3. Schließen Sie einen Laptop an den PC-Port des Telefons an.
4. Führen Sie die Paketanalysesoftware auf dem Laptop aus. Sie können Wireshark (oder andere Paketerfassungssoftware) verwenden.
5. Replizieren Sie das Problem.
6. Wenn das Problem vollständig repliziert wurde, beenden Sie die Paketerfassung.

Weitere Informationen finden Sie unter dem folgenden Link:

<https://supportforums.cisco.com/document/44741/collecting-packet-capture-cisco-ip-phone>

Beispielanalyse



SDL Traces

Für SIP-Integration und JTAPI-gesteuerte Telefone

CUCM: 10.1.61.158

Informacast: 10.1.61.118

Telefon A

DN: 110

Modell: KP-8861

Firmware-Version: sip88xx.12-0-1SR1-1

IP-Adresse des Telefons A: 10.1.61.12

MAC, SEP2C3124C9F8E1

Telefon B

DN: 111

Modell: KP-8811

Firmware-Version: sip88xx.12-0-1SR1-1

IP-Adresse von Telefon B: 10.1.61.11

MAC SEPF87B204EED99

Wählnummer: 7777

<#root>

CUCM receives the invite from Phone A

71439050.002 |19:00:35.206 |AppInfo |SIPtcp - wait_SdlReadRsp: Incoming SIP TCP message from 10.1.61.12 [431528,NET]

INVITE sip:7@10.1.61.158;user=phone SIP/2.0
Via: SIP/2.0/TCP 10.1.61.12:51600;branch=z9hG4bK18a14280
From: "PhoneA" <sip:110@10.1.61.158>;tag=2c3124c9f8e10c3c246b7956-5c62fa57
To: <sip:7@10.1.61.158>
Call-ID: 2c3124c9-f8e1000d-00337209-0547bb10@10.1.61.12
Max-Forwards: 70
Session-ID: 712c9e1f00105000a0002c3124c9f8e1;remote=00000000000000000000000000000000
Date: Tue, 10 Sep 2019 00:00:37 GMT
CSeq: 101 INVITE
User-Agent: Cisco-CP8861/12.0.1
Contact: <sip:142b9f25-7f2b-48a8-9ff9-377f616f3084@10.1.61.12:51600;transport=tcp>;+u.sip!devicename.cc
Expires: 180
Accept: application/sdp
Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,UPDATE,SUBSCRIBE,INFO
Remote-Party-ID: "PhoneA" <sip:110@10.1.61.158>;party=calling;id-type=subscriber;privacy=off;screen=yes
Supported: replaces,join,sdp-anat,norefersub,resource-priority,extended-refer,X-cisco-callinfo,X-cisco-
Allow-Events: kpml,dialog
Recv-Info: conference
Recv-Info: x-cisco-conference
Content-Length: 548
Content-Type: application/sdp
Content-Disposition: session;handling=optional

v=0
o=Cisco-SIPUA 11811 0 IN IP4 10.1.61.12
s=SIP Call
b=AS:4064
t=0 0
m=audio 22018 RTP/AVP 114 9 124 0 8 116 18 101
c=IN IP4 10.1.61.12
b=TIAS:64000
a=rtpmap:114 opus/48000/2
a=fmtp:114 maxplaybackrate=16000;sprop-maxcapture=16000;maxaveragebitrate=64000;stereo=0;sprop-ster
a=rtpmap:9 G722/8000
a=rtpmap:124 ISAC/16000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:116 iLBC/8000
a=fmtp:116 mode=20
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=yes
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=sendrecv

CUCM performs digit analysis for the dialed digits (dd="7777")

71439203.000	19:00:36.580	SdISig	DaReq	wait
71439203.001	19:00:36.580	AppInfo	Digit Analysis: star_DaReq: daReq.partitionSearchSpace(8653f609-0	
71439203.002	19:00:36.580	AppInfo	Digit Analysis: Host Address=10.1.61.158 MATCHES this node's IPv4	
71439203.003	19:00:36.580	AppInfo	Digit Analysis: star_DaReq: Matching SIP URL, Numeric User, user=	
71439203.012	19:00:36.588	AppInfo	Digit analysis: match(pi="2", fqcn="110", cn="110", plv="5", pss="	
71439203.013	19:00:36.588	AppInfo	Digit analysis: analysis results	
71439203.014	19:00:36.588	AppInfo	PretransformCallingPartyNumber=110	
			CallingPartyNumber=110	
			DialingPartition=Informacast_PT	
			DialingPattern=7777	
			FullyQualifiedCalledPartyNumber=7777	
			DialingPatternRegularExpression=(7777)	
			DialingWhere=	
			PatternType=Enterprise	
			PotentialMatches=NoPotentialMatchesExist	

|DialingSdlProcessId=(0,0,0)
|PretransformDigitString=7777
|PretransformTagsList=SUBSCRIBER
|PretransformPositionalMatchList=7777
|CollectedDigits=7777
|UnconsumedDigits=
|TagsList=SUBSCRIBER
|PositionalMatchList=7777
|VoiceMailbox=
|VoiceMailCallingSearchSpace=
|VoiceMailPilotNumber=
|RouteBlockFlag=RouteThisPattern
|RouteBlockCause=0
|AlertingName=
|UnicodeDisplayName=
|CallableEndPointName=[ddef6b78-6232-f5eb-b286-79292be99bb5]

CUCM determines call must stay on the same node, then it sends the call to SIP Trunk PID=SIPD(1,100)

71439207.001 |19:00:36.588 |AppInfo |Digit analysis: wait_DmPidRes- Partition=[107a02ea-a384-5219-3670

CUCM extends the call to the Informacast SIP Trunk

71439248.001 |19:00:36.643 |AppInfo |SIPTcp - wait_SdlSPISignal: Outgoing SIP TCP message to 10.1.61.1
[431545,NET]

INVITE sip:7777@10.1.61.118:5060 SIP/2.0

Via: SIP/2.0/TCP 10.1.61.158:5060;branch=z9hG4bK1996d1e0c5e3e

From: "PhoneA" <sip:110@10.1.61.158>;tag=229417~7cc9781e-f7e3-4c51-a2b9-de353a4e7d6f-19282343

To: <sip:7777@10.1.61.118>

Date: Tue, 10 Sep 2019 00:00:36 GMT

Call-ID: 2d72f80-d761e7a4-1996c-9e3d010a@10.1.61.158

Supported: timer,resource-priority,replaces

Min-SE: 1800

User-Agent: Cisco-CUCM11.5

Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY

CSeq: 101 INVITE

Expires: 180

Allow-Events: presence, kpm1

Supported: X-cisco-srtp-fallback,X-cisco-original-called

Call-Info: ;method="NOTIFY;Event=telephone-event;Duration=500"

Call-Info: ;x-cisco-video-traffic-class=DESKTOP

Session-ID: 712c9e1f00105000a0002c3124c9f8e1;remote=00000000000000000000000000000000

Cisco-Guid: 0047656832-0000065536-0000000001-2654798090

Session-Expires: 1800

P-Asserted-Identity: "PhoneA" <sip:110@10.1.61.158>

Remote-Party-ID: "PhoneA" <sip:110@10.1.61.158>;party=calling;screen=yes;privacy=off

Contact: <sip:110@10.1.61.158:5060;transport=tcp>;+u.sip!devicename.ccm.cisco.com="SEP2C3124C9F8E1"

Max-Forwards: 69

Content-Type: application/sdp

Content-Length: 552

v=0

o=CiscoSystemsCCM-SIP 229417 1 IN IP4 10.1.61.158

s=SIP Call

c=IN IP4 10.1.61.12

b=TIAS:64000

b=AS:64

t=0 0

m=audio 22018 RTP/AVP 114 9 124 0 8 116 18 101

b=TIAS:64000

a=rtpmap:114 opus/48000/2
a=fmtp:114 maxplaybackrate=16000;prop-maxcapture=16000;maxaveragebitrate=64000;stereo=0;prop-ster
a=rtpmap:9 G722/8000
a=rtpmap:124 iSAC/16000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:116 iLBC/8000
a=maxptime:20
a=fmtp:116 mode=20
a=rtpmap:18 G729/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15

Informacast replies with 200 OK (Call established using codec PCMU)

71439316.004 |19:00:36.849 |AppInfo |SIPtcp - wait_SdReadRsp: Incoming SIP TCP message from 10.1.61.1
[431549,NET]
SIP/2.0 200 OK
CSeq: 101 INVITE
Call-ID: 2d72f80-d761e7a4-1996c-9e3d010a@10.1.61.158
From: "PhoneA" <sip:110@10.1.61.158>;tag=229417~7cc9781e-f7e3-4c51-a2b9-de353a4e7d6f-19282343
To: <sip:7777@10.1.61.118>;tag=2c9be8b4
Via: SIP/2.0/TCP 10.1.61.158:5060;branch=z9hG4bK1996d1e0c5e3e;rport=43802
Content-Type: application/sdp
Contact: "InformaCast" <sip:7777@10.1.61.118;transport=tcp>
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,NOTIFY
Accept: application/sdp
Accept-Encoding: identity
Accept-Language: en
Supported:
Call-Info: <sip:7777@10.1.61.118:5060>;method="NOTIFY;Event=telephone-event;Duration=500"
Content-Length: 248

v=0
o=SingewireInformaCast-SIP 1568074182370 1 IN IP4 10.1.61.118
s=SIP Call
c=IN IP4 10.1.61.118
b=TIAS:64000
b=AS:64
t=0 0
m=audio 32070 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20

ACK from CUCM to Informacast

71439319.001 |19:00:36.850 |AppInfo |SIPtcp - wait_SdSPISignal: Outgoing SIP TCP message to 10.1.61.1
[431550,NET]
ACK sip:7777@10.1.61.118;transport=tcp SIP/2.0
Via: SIP/2.0/TCP 10.1.61.158:5060;branch=z9hG4bK1996e72237022
From: "PhoneA" <sip:110@10.1.61.158>;tag=229417~7cc9781e-f7e3-4c51-a2b9-de353a4e7d6f-19282343
To: <sip:7777@10.1.61.118>;tag=2c9be8b4
Date: Tue, 10 Sep 2019 00:00:36 GMT
Call-ID: 2d72f80-d761e7a4-1996c-9e3d010a@10.1.61.158
User-Agent: Cisco-CUCM11.5
Max-Forwards: 70
CSeq: 101 ACK
Allow-Events: presence, kpm
Content-Length: 0

CUCM sends 200 OK to Phone A with codec PCMU

71439437.001 |19:00:36.884 |AppInfo |SIPTcp - wait_SdISPISignal: Outgoing SIP TCP message to 10.1.61.1
[431551,NET]

SIP/2.0 200 OK

Via: SIP/2.0/TCP 10.1.61.12:51600;branch=z9hG4bK18a14280

From: "PhoneA" <sip:110@10.1.61.158>;tag=2c3124c9f8e10c3c246b7956-5c62fa57

To: <sip:7@10.1.61.158>;tag=229414~7cc9781e-f7e3-4c51-a2b9-de353a4e7d6f-19282342

Date: Tue, 10 Sep 2019 00:00:35 GMT

Call-ID: 2c3124c9-f8e1000d-00337209-0547bb10@10.1.61.12

CSeq: 101 INVITE

Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY

Allow-Events: presence

Supported: replaces

Server: Cisco-CUCM11.5

Call-Info: ; security= NotAuthenticated; orientation= to; gci= 1-15008; isVoip; call-instance= 1

Send-Info: conference, x-cisco-conference

Remote-Party-ID: <sip:7777@10.1.61.158>;party=called;screen=no;privacy=off

Session-ID: ddef6b786232f5ebb2867929ab229417;remote=712c9e1f00105000a0002c3124c9f8e1

Remote-Party-ID: <sip:7777@10.1.61.158;user=phone>;party=x-cisco-original-called;privacy=off

Contact: <sip:7@10.1.61.158:5060;transport=tcp>

Content-Type: application/sdp

Content-Length: 235

v=0

o=CiscoSystemsCCM-SIP 229414 1 IN IP4 10.1.61.158

s=SIP Call

c=IN IP4 10.1.61.118

b=AS:64

t=0 0

m=audio 32070 RTP/AVP 0 101

b=TIAS:64000

a=ptime:20

a=rtpmap:0 PCMU/8000

a=rtpmap:101 telephone-event/8000

a=fmtp:101 0-15

ACK from Phone A to CUCM

71439438.002 |19:00:36.950 |AppInfo |SIPTcp - wait_SdIReadRsp: Incoming SIP TCP message from 10.1.61.1
[431552,NET]

ACK sip:7@10.1.61.158:5060;transport=tcp SIP/2.0

Via: SIP/2.0/TCP 10.1.61.12:51600;branch=z9hG4bK20553712

From: "PhoneA" <sip:110@10.1.61.158>;tag=2c3124c9f8e10c3c246b7956-5c62fa57

To: <sip:7@10.1.61.158>;tag=229414~7cc9781e-f7e3-4c51-a2b9-de353a4e7d6f-19282342

Call-ID: 2c3124c9-f8e1000d-00337209-0547bb10@10.1.61.12

Max-Forwards: 70

Session-ID: 712c9e1f00105000a0002c3124c9f8e1;remote=ddef6b786232f5ebb2867929ab229417

Date: Tue, 10 Sep 2019 00:00:39 GMT

CSeq: 101 ACK

User-Agent: Cisco-CP8861/12.0.1

Remote-Party-ID: "PhoneA" <sip:110@10.1.61.158>;party=calling;id-type=subscriber;privacy=off;screen=yes

Content-Length: 0

Recv-Info: conference

Recv-Info: x-cisco-conference

Since integration is with JTAPI, CUCM sends REFER to the phone with instructions to join to the IP

71439541.002 |19:00:38.199 |AppInfo |SIPTcp - wait_SdISPISignal: Outgoing SIP TCP message to 10.1.61.1

[431557,NET]
REFER sip:e2881942-2853-4eab-a0d9-96228c79d062@10.1.61.11:51784;transport=tcp SIP/2.0
Via: SIP/2.0/TCP 10.1.61.158:5060;branch=z9hG4bK19970687ccd2b
From: <sip:111@10.1.61.158>;tag=1598606730
To: <sip:111@10.1.61.11>
Call-ID: 4085c80-d761e7a6-1996d-9e3d010a@10.1.61.158
CSeq: 101 REFER
Max-Forwards: 70
Contact: <sip:111@10.1.61.158:5060;transport=tcp>
User-Agent: Cisco-CUCM11.5
Expires: 30
Refer-To: cid:1234567890@10.1.61.158
Content-Id: <1234567890@10.1.61.158>
Content-Type: multipart/mixed;boundary=uniqueBoundary
Mime-Version: 1.0
Referred-By: <sip:111@10.1.61.158>
Content-Length: 682

--uniqueBoundary
Content-Type:application/x-cisco-remotecc-request+xml
<x-cisco-remotecc-request>
<datapasssthroughreq>
<applicationid>0</applicationid>
<lineid>0</lineid>
<transactionid>109</transactionid>
<stationsequence>StationSequenceLast</stationsequence>
<displaypriority>2</displaypriority>
<appinstance>0</appinstance>
<routingid>0</routingid>
<confid>0</confid>
<featureddata></featureddata>
</datapasssthroughreq>

</x-cisco-remotecc-request>
--uniqueBoundary
Content-Type:application/x-cisco-remote-cm+xml
<CiscoIPPhoneExecute><ExecuteItem URL="

RTPMRx:239.0.1.2:20480

"/></CiscoIPPhoneExecute>
--uniqueBoundary--

Phone B replies with 202 Accepted

71439542.002 |19:00:38.215 |AppInfo |SIPTcp - wait_SdReadRsp: Incoming SIP TCP message from 10.1.61.1
[431558,NET]
SIP/2.0 202 Accepted
Via: SIP/2.0/TCP 10.1.61.158:5060;branch=z9hG4bK19970687ccd2b
From: <sip:111@10.1.61.158>;tag=1598606730
To: <sip:111@10.1.61.11>;tag=f87b204eed990c3a4020c613-5969341f
Call-ID: 4085c80-d761e7a6-1996d-9e3d010a@10.1.61.158
Session-ID: f9d4984b00105000a000f87b204eed99;remote=00000000000000000000000000000000
Date: Tue, 10 Sep 2019 00:00:40 GMT
CSeq: 101 REFER
Server: Cisco-CP8811/12.0.1
Contact: <sip:e2881942-2853-4eab-a0d9-96228c79d062@10.1.61.11:51784;transport=tcp>;+u.sip!devicename.cc
Content-Length: 0

Phone B sends a NOTIFY to indicate that it was activated (Data="Success")

71439548.004 |19:00:38.453 |AppInfo |SIPTcp - wait_SdReadRsp: Incoming SIP TCP message from 10.1.61.11
[431559,NET]
NOTIFY sip:111@10.1.61.158:5060;transport=tcp SIP/2.0
Via: SIP/2.0/TCP 10.1.61.11:51784;branch=z9hG4bK08ccf329
To: <sip:111@10.1.61.158>;tag=1598606730
From: <sip:111@10.1.61.11>;tag=f87b204eed990c3a4020c613-5969341f
Call-ID: 4085c80-d761e7a6-1996d-9e3d010a@10.1.61.158
Session-ID: f9d4984b00105000a000f87b204eed99;remote=00000000000000000000000000000000
Date: Tue, 10 Sep 2019 00:00:40 GMT
CSeq: 1000 NOTIFY
Event: refer
Subscription-State: terminated; reason=timeout
Max-Forwards: 70
Contact: <sip:e2881942-2853-4eab-a0d9-96228c79d062@10.1.61.11:51784;transport=tcp>;+u.sip!devicename.cc
Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,UPDATE,SUBSCRIBE
Content-Type: multipart/mixed; boundary=uniqueBoundary
Mime-Version: 1.0
Content-Length: 1199

--uniqueBoundary
Content-Type:application/x-cisco-remotecc-response+xml
Content-Disposition_session;handling=required

```
<?xml version=1.0" encoding="UTF-8"?>
<x-cisco-remotecc-response>
<response>
<code>200</code>
<reason></reason>
<applicationid>0</applicationid>
<transactionid>109</transactionid>
<stationsequence>StationSequenceLast</stationsequence>
<displaypriority>2</displaypriority>
<appinstance>0</appinstance>
<linenumber>0</linenumber>
<routingid>0</routingid>
<confid>0</confid>
<callid></callid>
```

```
<options_ind>
<combine max="0">
<service-control></service-control>
</combine>
```

```
<dialog usage="">
<unot></unot>
<sub></sub>
</dialog>
<presence usage="">
<unot></unot>
<sub></sub>
</presence>
```

```
</options_ind>
</response>
</x-cisco-remotecc-response>
```

--uniqueBoundary
Content-Type:application/x-cisco-remote-cm+xml
Content-Disposition:session;handling=required
<?xml version="1.0" encoding="utf-8"?>
<CiscoIPPhoneResponse>
<ResponseItem URL="

RTPMRx:239.0.1.2:20480

"

Data="Success" Status="0"/>

</CiscoIPPhoneResponse>

--uniqueBoundary--

CUCM send a 200 OK for the NOTIFY received

71439556.001 |19:00:38.464 |AppInfo |SIPTcp - wait_SdSPISignal: Outgoing SIP TCP message to 10.1.61.1

[431560,NET]

SIP/2.0 200 OK

Via: SIP/2.0/TCP 10.1.61.11:51784;branch=z9hG4bK08ccf329

From: <sip:111@10.1.61.11>;tag=f87b204eed990c3a4020c613-5969341f

To: <sip:111@10.1.61.158>;tag=1598606730

Date: Tue, 10 Sep 2019 00:00:38 GMT

Call-ID: 4085c80-d761e7a6-1996d-9e3d010a@10.1.61.158

CSeq: 1000 NOTIFY

Server: Cisco-CUCM11.5

Content-Length: 0

CUCM sends to the phone B a REFER to stop receiving multicast audio

71442357.002 |19:01:10.795 |AppInfo |SIPTcp - wait_SdSPISignal: Outgoing SIP TCP message to 10.1.61.1

[431582,NET]

REFER sip:e2881942-2853-4eab-a0d9-96228c79d062@10.1.61.11:51784;transport=tcp SIP/2.0

Via: SIP/2.0/TCP 10.1.61.158:5060;branch=z9hG4bK199754588a6e3

From: <sip:111@10.1.61.158>;tag=928499252

To: <sip:111@10.1.61.11>

Call-ID: 171b2c80-d761e7c6-19970-9e3d010a@10.1.61.158

CSeq: 101 REFER

Max-Forwards: 70

Contact: <sip:111@10.1.61.158:5060;transport=tcp>

User-Agent: Cisco-CUCM11.5

Expires: 30

Refer-To: cid:1234567890@10.1.61.158

Content-Id: <1234567890@10.1.61.158>

Content-Type: multipart/mixed;boundary=uniqueBoundary

Mime-Version: 1.0

Referred-By: <sip:111@10.1.61.158>

Content-Length: 683

--uniqueBoundary

Content-Type: application/x-cisco-remotecc-request+xml

<x-cisco-remotecc-request>

<datapasssthroughreq>

<applicationid>0</applicationid>

<lineid>0</lineid>

<transactionid>109</transactionid>

<stationsequence>StationSequenceLast</stationsequence>

<displaypriority>2</displaypriority>

<appinstance>0</appinstance>

<routingid>0</routingid>

<confid>0</confid>

<featureddata></featuredata>

</datapasssthroughreq>

</x-cisco-remotecc-request>

--uniqueBoundary

Content-Type: application/x-cisco-remote-cm+xml

<CiscoIPPhoneExecute><ExecuteItem Priority="0" URL="

RTPMRx:Stop

```
"/></CiscoIPPhoneExecute>  
--uniqueBoundary--
```

Phone B sends to CUCM a 202 Accepted

```
71442358.002 |19:01:10.802 |AppInfo |SIPTcp - wait_SdReadRsp: Incoming SIP TCP message from 10.1.61.11  
[431583,NET]  
SIP/2.0 202 Accepted  
Via: SIP/2.0/TCP 10.1.61.158:5060;branch=z9hG4bK199754588a6e3  
From: <sip:111@10.1.61.158>;tag=928499252  
To: <sip:111@10.1.61.11>;tag=f87b204eed990c3e1c1bfe96-1d092704  
Call-ID: 171b2c80-d761e7c6-19970-9e3d010a@10.1.61.158  
Session-ID: f9d4984b00105000a000f87b204eed99;remote=00000000000000000000000000000000  
Date: Tue, 10 Sep 2019 00:01:12 GMT  
CSeq: 101 REFER  
Server: Cisco-CP8811/12.0.1  
Contact: <sip:e2881942-2853-4eab-a0d9-96228c79d062@10.1.61.11:51784;transport=tcp>;+u.sip!devicename.cc  
Content-Length: 0
```

A NOTIFY is sent from the phone B to CUCM to indicate that it stopped receiving multicast audio

```
71442417.004 |19:01:11.069 |AppInfo |SIPTcp - wait_SdReadRsp: Incoming SIP TCP message from 10.1.61.11  
[431584,NET]  
NOTIFY sip:111@10.1.61.158:5060;transport=tcp SIP/2.0  
Via: SIP/2.0/TCP 10.1.61.11:51784;branch=z9hG4bK68d7f530  
To: <sip:111@10.1.61.158>;tag=928499252  
From: <sip:111@10.1.61.11>;tag=f87b204eed990c3e1c1bfe96-1d092704  
Call-ID: 171b2c80-d761e7c6-19970-9e3d010a@10.1.61.158  
Session-ID: f9d4984b00105000a000f87b204eed99;remote=00000000000000000000000000000000  
Date: Tue, 10 Sep 2019 00:01:13 GMT  
CSeq: 1000 NOTIFY  
Event: refer  
Subscription-State: terminated; reason=timeout  
Max-Forwards: 70  
Contact: <sip:e2881942-2853-4eab-a0d9-96228c79d062@10.1.61.11:51784;transport=tcp>;+u.sip!devicename.cc  
Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,UPDATE,SUBSCRIBE  
Content-Type: multipart/mixed; boundary=uniqueBoundary  
Mime-Version: 1.0  
Content-Length: 1187
```

```
--uniqueBoundary  
Content-Type: application/x-cisco-remotecc-request+xml  
Content-Disposition: session; handling=required
```

```
<?xml version="1.0" encoding="UTF-8"?>  
<x-cisco-remotecc-response>  
<response>  
<code>200</code>  
<reason></reason>  
<applicationid>0</applicationid>  
<transactionid>117</transactionid>  
<stationsequence>StationSequenceLast</stationsequence>  
<displaypriority>2</displaypriority>  
<appinstance>0</appinstance>  
<linenumber>0</linenumber>  
<routingid>0</routingid>  
<confid>0</confid>  
<callid></callid>
```

```

<options_ind>
  <combine max="0">
    <service-control></service-control>
  </combine>
  <dialog usage="">
    <unot></unot>
    <sub></sub>
  </dialog>
  <presence usage="">
    <unot></unot>
    <sub></sub>
  </presence>
</options_ind>
</response>
</x-cisco-remotecc-response>
--uniqueBoundary
Content-Type: application/x-cisco-remotecc-cm+xml
Content-Disposition: session;handling=required
<?xml version="1.0" encoding="utf-8"?>
<CiscoIPPhoneResponse>
<ResponseItem URL="RTPRx:Stop" Data="Success" Status="0" />
</CiscoIPPhoneResponse>
--uniqueBoundary-

```

CUCM replies with 200 OK

```

71442425.001 |19:01:11.070 |AppInfo |SIPtcp - wait_SdSPISignal: Outgoing SIP TCP message to 10.1.61.1
[431585,NET]
SIP/2.0 200 OK
Via: SIP/2.0/TCP 10.1.61.11:51784;branch=z9hG4bK68d7f530
From: <sip:111@10.1.61.11>;tag=f87b204eed990c3e1c1bfe96-1d092704
To: <sip:111@10.1.61.158>;tag=928499252
Date: Tue, 10 Sep 2019 00:01:11 GMT
Call-ID: 171b2c80-d761e7c6-19970-9e3d010a@10.1.61.158
CSeq: 1000 NOTIFY
Server: Cisco-CUCM11.5
Content-Length: 0

```

Für CTI-Integration und HTTP-gesteuerte Telefone

CUCM: 10.1.61.158

Informacast: 10.1.61.118

Telefon A

DN: 110

Modell: KP-8861

Firmware-Version: sip88xx.12-0-1SR1-1

IP-Adresse des Telefons A: 10.1.61.12

MAC: SEP2C3124C9F8E1

Telefon B

DN: 111

Modell: KP-8811

Firmware-Version: sip88xx.12-0-1SR1-1

IP-Adresse von Telefon B: 10.1.61.11

MAC: SEPF87B204EED99

Wählnummer: 7778

<#root>

CUCM receives the INVITE from phone A (Call Manager SDL Log)

```
71531116.002 |19:15:32.972 |AppInfo |SIPtcp - wait_SdlReadRsp: Incoming SIP TCP message from 10.1.61.11
[431985,NET]
INVITE sip:7@10.1.61.158;user=phone SIP/2.0
Via: SIP/2.0/TCP 10.1.61.12:51600;branch=z9hG4bK112766fc
From: "PhoneA" <sip:110@10.1.61.158>;tag=2c3124c9f8e10c541ed075c2-67793e32
To: <sip:7@10.1.61.158>
Call-ID: 2c3124c9-f8e10011-0bb54030-57b0a7c8@10.1.61.12
Max-Forwards: 70
Session-ID: 02023b9b00105000a0002c3124c9f8e1;remote=00000000000000000000000000000000
Date: Tue, 10 Sep 2019 00:15:35 GMT
CSeq: 101 INVITE
User-Agent: Cisco-CP8861/12.0.1
Contact: <sip:142b9f25-7f2b-48a8-9ff9-377f616f3084@10.1.61.12:51600;transport=tcp>;+u.sip!devicename.ccm
Expires: 180
Accept: application/sdp
Allow: ACK,BYE,CANCEL,INVITE,NOTIFY,OPTIONS,REFER,REGISTER,UPDATE,SUBSCRIBE,INFO
Remote-Party-ID: "PhoneA" <sip:110@10.1.61.158>;party=calling;id-type=subscriber;privacy=off;screen=yes
Supported: replaces,join,sdp-anat,norefersub,resource-priority,extended-refer,X-cisco-callinfo,X-cisco-
Allow-Events: kpml,dialog
Recv-Info: conference
Recv-Info: x-cisco-conference
Content-Length: 548
Content-Type: application/sdp
Content-Disposition: session;handling=optional
v=0
o=Cisco-SIPUA 19108 0 IN IP4 10.1.61.12
s=SIP Call
b=AS:4064
t=0 0
m=audio 19104 RTP/AVP 114 9 124 0 8 116 18 101
c=IN IP4 10.1.61.12
b=TIAS:64000
a=rtpmap:114 opus/48000/2
a=fmtp:114 maxplaybackrate=16000;sprop-maxcapture=16000;maxaveragebitrate=64000;stereo=0;sprop-ster
a=rtpmap:9 G722/8000
a=rtpmap:124 ISAC/16000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:116 iLBC/8000
a=fmtp:116 mode=20
a=rtpmap:18 G729/8000
```

a=fmtp:18 annexb=yes
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=sendrecv

Digit analysis for the dialed number 7778

71531367.000 |19:15:34.231 |SdISig |DaReq |wait
71531367.001 |19:15:34.231 |AppInfo |Digit Analysis: star_DaReq: daReq.partitionSearchSpace(8653f609-0
71531367.002 |19:15:34.231 |AppInfo |Digit Analysis: Host Address=10.1.61.158 MATCHES this node's IPv4
71531367.003 |19:15:34.231 |AppInfo |Digit Analysis: star_DaReq: Matching SIP URL, Numeric User, user=
71531367.004 |19:15:34.232 |AppInfo |Digit Analysis: getDaRes data: daRes.ssType=[0] Intercept DAMR.ss
71531367.005 |19:15:34.232 |AppInfo |Digit Analysis: getDaRes - Remote Destination [] isURI[1]
71531367.006 |19:15:34.232 |AppInfo |Digit analysis: patternUsage=2
71531367.007 |19:15:34.232 |AppInfo |Digit analysis: match(pi="2", fqcn="110", cn="110",plv="5", pss=""
71531367.008 |19:15:34.232 |AppInfo |Digit analysis: analysis results
71531367.009 |19:15:34.232 |AppInfo ||PretransformCallingPartyNumber=110
|CallingPartyNumber=110
|DialingPartition=Informacast_PT
|DialingPattern=7778
|FullyQualifiedCalledPartyNumber=7778
|DialingPatternRegularExpression=(7778)
|DialingWhere=
|PatternType=Enterprise
|PotentialMatches=NoPotentialMatchesExist
|DialingSdIProcessId=(0,0,0)
|PretransformDigitString=7778
|PretransformTagsList=SUBSCRIBER
|PretransformPositionalMatchList=7778
|CollectedDigits=7778
|UnconsumedDigits=
|TagsList=SUBSCRIBER
|PositionalMatchList=7778
|VoiceMailbox=
|VoiceMailCallingSearchSpace=
|VoiceMailPilotNumber=
|RouteBlockFlag=RouteThisPattern
|RouteBlockCause=0
|AlertingName=InformacastCTIRP
|UnicodeDisplayName=InformacastCTIRP
|DisplayNameLocale=1
|OverlapSendingFlagEnabled=0
|WithTags=
|WithValues=
|CallingPartyNumberPi=NotSelected
|ConnectedPartyNumberPi=NotSelected
|CallingPartyNamePi=NotSelected
|ConnectedPartyNamePi=NotSelected
|CallManagerDeviceType=NoDeviceType
|PatternPrecedenceLevel=Routine
|CallableEndPointName=[4db482c3-64c3-5adf-33c5-a11c890d96d0]
|PatternNodeId=[4db482c3-64c3-5adf-33c5-a11c890d96d0]
|AARNeighborhood=[]
|AARDestinationMask=[]
|AARKeepCallHistory=true
|AARVoiceMailEnabled=false
|NetworkLocation=OnNet
|Calling Party Number Type=Cisco Unified CallManager
|Calling Party Numbering Plan=Cisco Unified CallManager
|Called Party Number Type=Cisco Unified CallManager
|Called Party Numbering Plan=Cisco Unified CallManager
|ProvideOutsideDialtone=false

|AllowDeviceOverride=false
|IsEmergencyNumber=false
|AlternateMatches=
|TranslationPatternDetails=
|ResourcePriorityNamespace=
|PatternRouteClass=RouteClassDefault

CUCM extends the call to the Line control associated to the CTI Route Point ICVA_CTI_RP (Call Manager SDL Log)

71531370.001 |19:15:34.232 |AppInfo |Digit analysis: wait_DmPidRes- Partition=[107a02ea-a384-5219-3670-
71531386.001 |19:15:34.233 |AppInfo |LineCdpc(20): -dispatchToAllDevices-, sigName=CcSetupReq, device=

CUCM sends the CTI New call notify (Call Manager SDL Log)

71531404.000 |19:15:34.235 |SdISig-O |CtiNewCallNotify |NA RemoteSignal

CTI process receives the CtiNewCallNotify from CallManager process (CTI Manager SDL Trace)

04961495.000 |19:15:34.236 |SdISig-I |CtiNewCallNotify |ready

CTI process sends the NewCallEvent to Informacast server (CTI Manager SDL Trace)

04961497.003 |19:15:34.236 |AppInfo |[CTI-APP] [CTIHandler::OutputCtiMessage] CTI NewCallEvent
ICVA_CTI_RP

cgpn=110 Presentation=1 cgpn NameInfo=locale: 1 pi: 1 Name: PhoneA UnicodeName: PhoneA cdpn=7778 Presentation=1

CTI process receives the LineCallAcceptRequest from Informacast server (CTI Manager SDL Trace)

04961500.002 |19:15:34.242 |AppInfo |[CTI-APP] [CTIHandler::processIncomingMessage] CTI LineCallAcceptRequest

CTI process sends the answer to Call Manager process (CTI Manager SDL Trace)

04961503.000 |19:15:34.242 |SdISig-O |CtiLineCallAcceptReq |NA RemoteSignal

Call Manager process receives the answer from CTI process (Call Manager SDL Log)

71531414.000 |19:15:34.243 |SdISig-I |CtiLineCallAcceptReq |restart0

CTI Process receives from Informacast the port to be used to receive the audio (CTI Manager SDL Trace)

04961525.002 |19:15:34.256 |AppInfo |[CTI-APP] [CTIHandler::processIncomingMessage] CTI DeviceSetRTPForCallReq

CTI Process sends the port to Call manager process (CTI Manager SDL Trace)

04961528.000 |19:15:34.256 |SdISig-O |CtiDeviceSetRTPForCallReq |NA RemoteSignal

CUCM sends the 200 OK to the Phone A (Codec PCMU, IP and port of Informacast)

71531593.001 |19:15:34.258 |AppInfo |SIPtcp - wait_SdISPISignal: Outgoing SIP TCP message to 10.1.61.12
[432000,NET]
SIP/2.0 200 OK
Via: SIP/2.0/TCP 10.1.61.12:51600;branch=z9hG4bK112766fc
From: "PhoneA" <sip:110@10.1.61.158>;tag=2c3124c9f8e10c541ed075c2-67793e32
To: <sip:7@10.1.61.158>;tag=229579~7cc9781e-f7e3-4c51-a2b9-de353a4e7d6f-19282358
Date: Tue, 10 Sep 2019 00:15:32 GMT
Call-ID: 2c3124c9-f8e10011-0bb54030-57b0a7c8@10.1.61.12

CSeq: 101 INVITE
Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY
Allow-Events: presence
Supported: replaces
Server: Cisco-CUCM11.5
Call-Info: <urn:x-cisco-remotecc:callinfo>; security= NotAuthenticated; orientation= to; gci= 1-15018;
Send-Info: conference, x-cisco-conference
Session-ID: 5ee92aa5415831d8b114c4ba19282359;remote=02023b9b00105000a0002c3124c9f8e1
Remote-Party-ID: "InformacastCTIRP" <sip:7778@10.1.61.158>;party=called;screen=yes;privacy=off
Contact: <sip:7@10.1.61.158:5060;transport=tcp>
Content-Type: application/sdp
Content-Length: 179
v=0
o=CiscoSystemsCCM-SIP 229579 1 IN IP4 10.1.61.158
s=SIP Call
c=IN IP4 10.1.61.118
b=AS:64
t=0 0
m=audio 32080 RTP/AVP 0
b=TIAS:64000
a=ptime:20

a=rtpmap:0 PCMU/8000

ACK from Phone A to CUCM

71531622.002 |19:15:34.473 |AppInfo |SIPTcp - wait_SdReadRsp: Incoming SIP TCP message from 10.1.61.118 [432004,NET]
ACK sip:7@10.1.61.158:5060;transport=tcp SIP/2.0
Via: SIP/2.0/TCP 10.1.61.12:51600;branch=z9hG4bK4fcbad6d
From: "PhoneA" <sip:110@10.1.61.158>;tag=2c3124c9f8e10c541ed075c2-67793e32
To: <sip:7@10.1.61.158>;tag=229579~7cc9781e-f7e3-4c51-a2b9-de353a4e7d6f-19282358
Call-ID: 2c3124c9-f8e10011-0bb54030-57b0a7c8@10.1.61.12
Max-Forwards: 70
Session-ID: 02023b9b00105000a0002c3124c9f8e1;remote=5ee92aa5415831d8b114c4ba19282359
Date: Tue, 10 Sep 2019 00:15:37 GMT
CSeq: 101 ACK
User-Agent: Cisco-CP8861/12.0.1
Remote-Party-ID: "PhoneA" <sip:110@10.1.61.158>;party=calling;id-type=subscriber;privacy=off;screen=yes
Content-Length: 0
Recv-Info: conference
Recv-Info: x-cisco-conference

NOTE: At this point the call from phone A to Informacast has been established successfully. For this scenario

Leistungsprotokolle

Für SIP-Integration

<#root>

Informacast receives an INVITE sent by CUCM

2019-09-09 19:09:42,323 [pool-41-thread-1] INFO ba [] - Received INVITE request; call ID 2d72f80-d761e

Informacast sends a 200 OK to CUCM

2019-09-09 19:09:42,508 [pool-41-thread-1] INFO ba [] - Sent INVITE response; status OK (200) ; call ID

CUCM replies with ACK to Informacast

2019-09-09 19:09:42,527 [pool-41-thread-1] INFO ba [] - Received ACK request; call ID 2d72f80-d761e7a4

Informacast provides the IP and port

2019-09-09 19:09:42,871 [pool-1264-thread-1] INFO u [] - providing address: 239.0.1.2

2019-09-09 19:09:42,885 [pool-1264-thread-1] INFO t [] - Gathering information required to send the message

2019-09-09 19:09:42,904 [pool-1264-thread-1] INFO t [] - Broadcast will be sent on port: 20480

Stream settings:

2019-09-09 19:09:43,556 [Signaler # 1 run 1] INFO Signaler [] - Stream settings:

General info: User=dialcast(System User), BroadcastInitiator=10.1.61.12, SourceType=CallingPhone, MessageID=

Audio details: AudioFile=null, AudioFormat=ULAW 8000.0 Hz, 8 bit, mono, 1 bytes/frame, , RemoteAddress=

Confirmation details: CollectConfirmations=false

Informacast sends the instruction message to 1 participant (SEPF87B204EED99)

2019-09-09 19:09:43,555 [Signaler # 1 run 1] INFO Signaler [] - Sending message to 1 participants

2019-09-09 19:09:43,643 [Push:10.1.61.11-pool-1269-thread-1] INFO i [1 run 1] - Started device instruction

Informacast received the response via JTAPI from the phone

2019-09-09 19:09:44,126 [Push:10.1.61.11-pool-1269-thread-1] INFO i [1 run 1] - The response from the phone

```
<?xml version="1.0" encoding="UTF-8"?>
<CiscoIPPhoneResponse>
<ResponseItem URL="RTPMRx:239.0.1.2:20480" Data="Success" Status="0" />
</CiscoIPPhoneResponse>
```

Informacast starts broadcasting

2019-09-09 19:09:44,151 [pool-1269-thread-1] INFO ah [] - Starting broadcast for inbound call 2d72f80-d761e7a4

Informacast receives the BYE to end the paging

2019-09-09 19:10:15,222 [pool-41-thread-1] INFO ba [] - Received BYE request; call ID 2d72f80-d761e7a4

Informacast sends to the phone the instruction to stop receiving audio

2019-09-09 19:10:16,403 [Push:10.1.61.11-pool-1269-thread-3] INFO i [1 run 1] - Pushing stop command to the phone

Informacast receives the response from the phone

2019-09-09 19:10:16,732 [Push:10.1.61.11-pool-1269-thread-3] INFO i [1 run 1] - The response from the phone

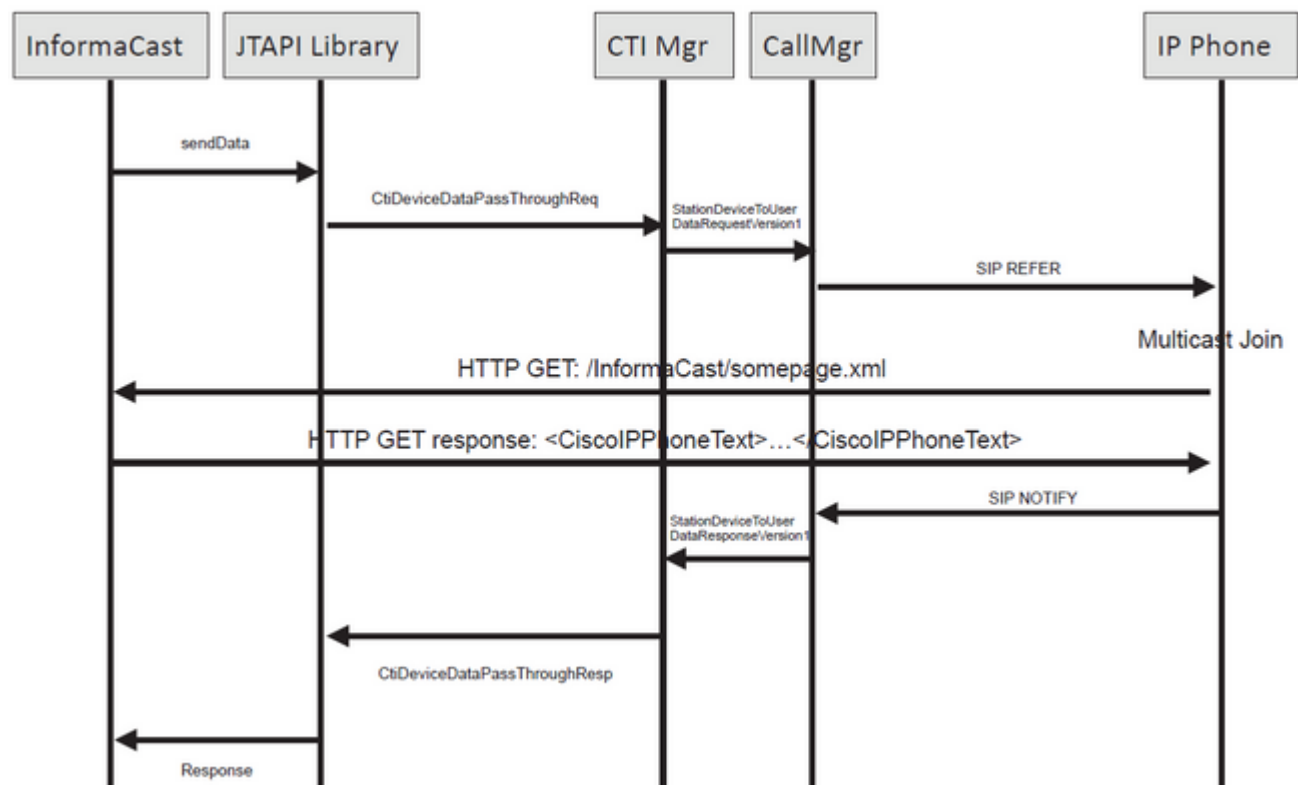
```
<?xml version="1.0" encoding="UTF-8"?>
<CiscoIPPhoneResponse>
<ResponseItem URL="RTPMRx:Stop" Data="Success" Status="0" />
```

</CiscoIPPhoneResponse>

Task ended

2019-09-09 19:10:19,357 [DeviceDeactivator-pool-1268-thread-1] INFO ah [1] - Canceling live broadcast :
2019-09-09 19:11:45,250 [Timer-0] INFO JavaExchangeAdapter [] - Task Ended: checkpoint command to comp

Für CTI-Integration



<#root>

Informacast receives the request to route the call

2019-09-09 19:24:39,936 [RouteCall:15018/1Thread] INFO av [] - Route request for call [CiscoCallID=150

Dialing pattern matches

2019-09-09 19:24:39,942 [ObserverThread(af@feaf7c)] INFO V [] - Dialing pattern "7778" matched dialed

Informacast provides the IP and port for multicast

2019-09-09 19:24:40,020 [pool-1287-thread-1] INFO u [] - providing address: 239.0.1.2
2019-09-09 19:24:40,020 [pool-1287-thread-1] INFO t [] - Gathering information required to send the me
2019-09-09 19:24:40,023 [pool-1287-thread-1] INFO t [] - Broadcast will be sent on port: 20486

Informacast sends the message to all devices in the recipient group, in this case to only 1 device

```

2019-09-09 19:24:40,262 [Signaler # 4 run 1] INFO Signaler [] - Sending message to 1 participants

#### Informacast starts the live broadcast over the IP and port

2019-09-09 19:24:40,263 [Signaler # 4 run 1] INFO ah [] - Starting live broadcast alert for inbound call

#### Informacast sends the instruction activate the phone (SEPF87B204EED99) and join to the multicast address

2019-09-09 19:24:40,278 [Push:10.1.61.11-pool-1269-thread-10] INFO i [4 run 1] - Started device instruction

#### Informacast receives the response from the phone

2019-09-09 19:24:40,624 [Push:10.1.61.11-pool-1269-thread-10] INFO i [4 run 1] - The response from the phone

#### Informacast starts the broadcast over the IP and port

2019-09-09 19:24:40,637 [pool-1269-thread-10] INFO ah [] - Starting broadcast for inbound call 15018/15019

#### Informacast receives the notification that the call has ended

2019-09-09 19:25:21,253 [ObserverThread(af@feaf7c)] INFO af [] - RTP input stopped event received for call 15018/15019

#### Informacast sends the instruction to the phones in order to stop receiving audio

2019-09-09 19:25:21,865 [Push:10.1.61.11-pool-1269-thread-12] INFO i [4 run 1] - Pushing stop command to phone

#### Informacast receives the response from the phone

2019-09-09 19:25:22,123 [Push:10.1.61.11-pool-1269-thread-12] INFO i [4 run 1] - The response from the phone

#### Deactivation done

2019-09-09 19:25:22,134 [pool-1269-thread-12] INFO ah [] - Canceling live broadcast for inbound call 15018/15019
2019-09-09 19:25:22,134 [pool-1269-thread-12] INFO Signaler [] - Notifying signaler that the deactivation is done

```

Konsolenprotokolle (PRT)

<#root>

```

#### The same IP and port for multicast provided by Informacast is shown in the console logs

5311 INF Sep 10 00:15:34.434302 (701:844) JAVA-PushThread|cip.push.PushThread:execute - Sleep for 100ms
5312 DEB Sep 10 00:15:34.535773 (701:832) JAVA-SIPCC-MSP: mp_create_rtp_session: scheme_specific=239.0.0.1
5313 DEB Sep 10 00:15:34.535893 (701:832) JAVA-SIPCC-MSP: mp_create_rtp_session: precedence=0 mixingmode=0
5314 DEB Sep 10 00:15:34.535980 (701:832) JAVA-SIPCC-MSP: mp_create_rtp_session: ipv4 address/port/type=

```

Create receive session only

```
5315 DEB Sep 10 00:15:34.536032 (701:832) JAVA-SIPCC-MSP: mp_create_rtp_session: Create Rx only stream.
5316 NOT Sep 10 00:15:34.536151 (408:408) ms-MSAPI.ms_forceReserveMediaPort port 20486
5317 NOT Sep 10 00:15:34.536291 (701:832) JAVA-SIPCC-MED_API: 0/-1, mp_create_rx_session: MCAP 0:GRP -1
5320 DEB Sep 10 00:15:34.536489 (701:832) JAVA-mp_create_rx_session:type=1, addr=239.0.1.2, ip4=-285212
5321 DEB Sep 10 00:15:34.536525 (701:832) JAVA-mp_create_rx_session:addr_str=239.0.1.2
5323 DEB Sep 10 00:15:34.536661 (701:832) JAVA-mp_create_rx_session:[ToMS] payload=4 dynpayload=0 pkt_p
5326 NOT Sep 10 00:15:34.537528 (408:408) ms-RTPSESSION.createRTPSession media [ipv4=239.0.1.2][port=20
```

Start RTCP

```
5385 NOT Sep 10 00:15:34.673264 (408:408) ms-RTCPMGR.rtcpm_startRtcp[A:6:5:8] [local IPv4:port=239.0.1.
```

Start RTP session RX

```
5388 NOT Sep 10 00:15:34.673917 (408:408) ms-RTPSESSION.ms_startRTPSessionRx[A:6] START RX [stream=5][m
```

Release connection

```
5536 NOT Sep 10 00:16:16.173301 (701:832) JAVA-SIPCC-MED_API: mp_session_cmd: release local rtp port 20
5537 NOT Sep 10 00:16:16.173396 (408:408) ms-MSAPI.ms_releaseRxPort : port 20486
```

Paketerfassung

Sammeln Sie eine Paketerfassung vom Telefon, und überprüfen Sie die HTTP-XSI-Befehle von InformaCast. Eine IGMP-Nachricht (Internet Group Management Protocol) wird gesendet, um dem Multicast-Stream beizutreten. Wenn nach der IGMP-Nachricht kein Multicast Real-Time Transport Protocol (RTP)-Stream angezeigt wird, können Sie eine Paketerfassung von InformaCast durchführen, bestätigen, dass der Informacast-Server das RTP an die IP-Adresse und den Port gesendet hat, und dann Ihre Netzwerkinfrastruktur überprüfen.

Paketerfassung am Telefon (gesteuert über HTTP)

- CUCM: 10.1.61.158
- Informacast: 10.1.61.118
- IP-Adresse von Telefon B: 10.1.61.11
- Modell: KP-8811
- Firmware-Version: sip88xx.12-0-1SR1-1
- eth.addr==SEPF87B204EED99

Die auf den Telefonen empfangenen HTTP- und IGMP-Nachrichten werden im Bild angezeigt.

Informacast sends IP and port for multicast

The phone authenticates with Informacast

Informacast replies with 200 OK

The phone joins to the Membership (IP and port)

Informacast gives the order to leave

The phone leaves the IGMP group

```

No.    Time           Source            Destination      Protocol  Length  Info
1771 00:24:39.352999 10.1.61.22       173.36.89.68    HTTP      2295    CCM_POST /ccm_system/request HTTP/1.1 (text/plain)
1777 00:24:39.404529 173.36.89.68     10.1.61.22      HTTP      394     HTTP/1.1 200 OK (text/plain)
1905 00:24:49.392163 10.1.61.118      10.1.61.11      HTTP      223     GET /StreamingStatisticsX?1 HTTP/1.1
1911 00:24:49.444329 10.1.61.11       10.1.61.118     HTTP/XML   1452    HTTP/1.1 200 OK
1917 00:24:49.453245 10.1.61.118      10.1.61.11      HTTP      399     POST /CGI/Execute HTTP/1.1 (application/x-www-form-urlencoded)
1922 00:24:49.479784 10.1.61.11       10.1.61.118     HTTP      457     GET /InformaCast/phone/auth?UserID=ICVAInformacast&Password=rtppavvid&devicename=SEPF87B204EED99 HTTP/1.1
1926 00:24:49.483773 10.1.61.118      10.1.61.11      HTTP      76      HTTP/1.1 200 OK (text/html)
1932 00:24:49.610049 10.1.61.11       239.0.1.2       IGMPv2    60      Membership Report group 239.0.1.2
1941 00:24:49.735551 10.1.61.11       10.1.61.118     HTTP/XML   474     HTTP/1.1 200 OK
1965 00:24:50.999400 10.1.61.11       239.0.1.2       IGMPv2    60      Membership Report group 239.0.1.2
2070 00:24:58.399806 10.1.61.11       239.0.1.2       IGMPv2    60      Membership Report group 239.0.1.2
2512 00:25:30.985190 10.1.61.118      10.1.61.11      HTTP      404     POST /CGI/Execute HTTP/1.1 (application/x-www-form-urlencoded)
2516 00:25:31.228042 10.1.61.11       224.0.0.2       IGMPv2    60      Leave Group 239.0.1.2
2518 00:25:31.234468 10.1.61.11       10.1.61.118     HTTP/XML   462     HTTP/1.1 200 OK
  
```

Hypertext Transfer Protocol

```

POST /CGI/Execute HTTP/1.1\r\n
Authorization: Basic SUMaQUuZm9ybWIFjYXN0OnJ0cGF2dmk\r\n
User-Agent: Jakarta Commons-HttpClient/3.1\r\n
Host: 10.1.61.11\r\n
Content-Length: 116\r\n
Content-Type: application/x-www-form-urlencoded\r\n
\r\n
[Full request URI: http://10.1.61.11/CGI/Execute]
[HTTP request 1/1]
[Response in frame: 1941]
File Data: 116 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "XML" = "<CiscoIPPhoneExecute><ExecuteItem URL='RTPPRx:239.0.1.2:20486'/></CiscoIPPhoneExecute>"
  
```

Paketerfassung am Telefon (gesteuert durch JTAPI)

- CUCM: 10.1.61.158
- Informacast: 10.1.61.118
- IP-Adresse von Telefon B: 10.1.61.11
- Modell: KP-8811
- Firmware-Version: sip88xx.12-0-1SR1-1
- MAC SEPF87B204EED99

Wie im Konfigurationsabschnitt erläutert, können Telefone von JTAPI gesteuert werden, d. h., dass die Option "Send Commands to Phones by Jtapi" aktiviert ist, wie im Bild gezeigt.

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

Advanced Notification
Buy Try Learn

Admin | Broadcast Parameters

Send Commands to Phones by JTAPI: ☒

Create Telephony Terminals for all Phones: ☐

Starting Multicast IP Address: 239.0.1.2 (required)

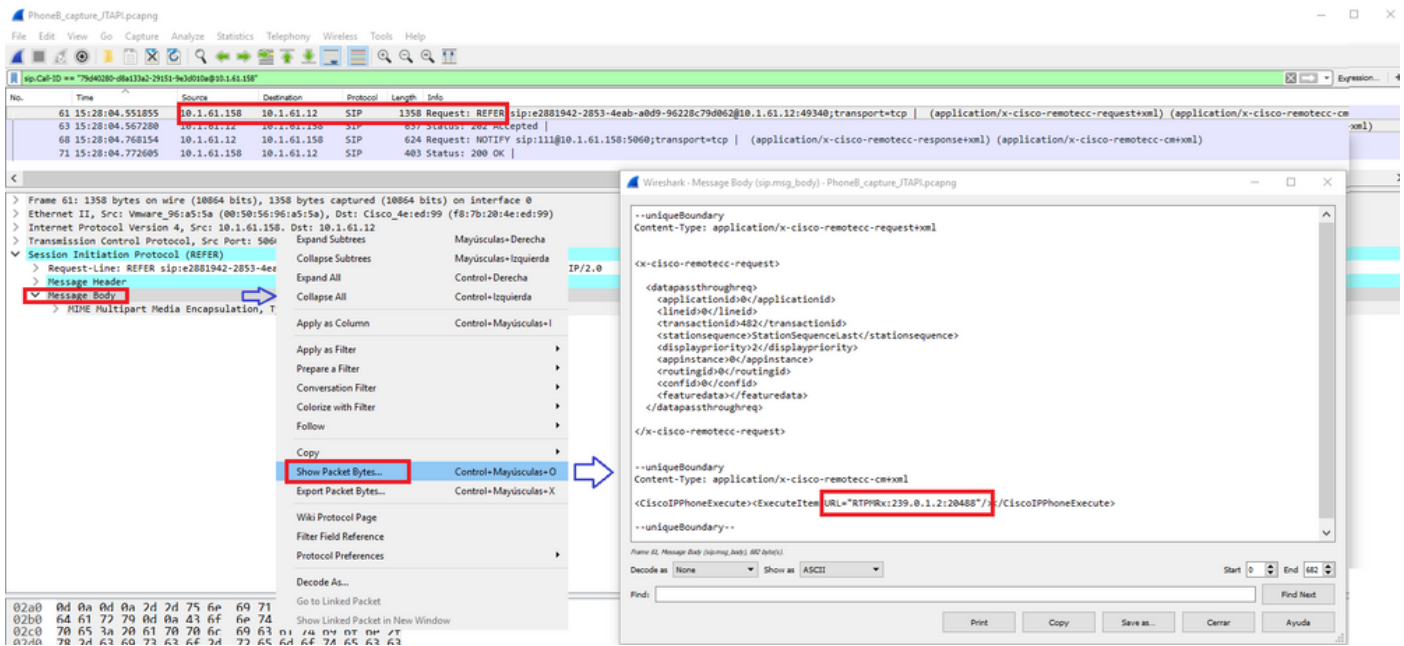
Ending Multicast IP Address: 239.0.1.2 (required)

See <http://www.iana.org/assignments/multicast-addresses>

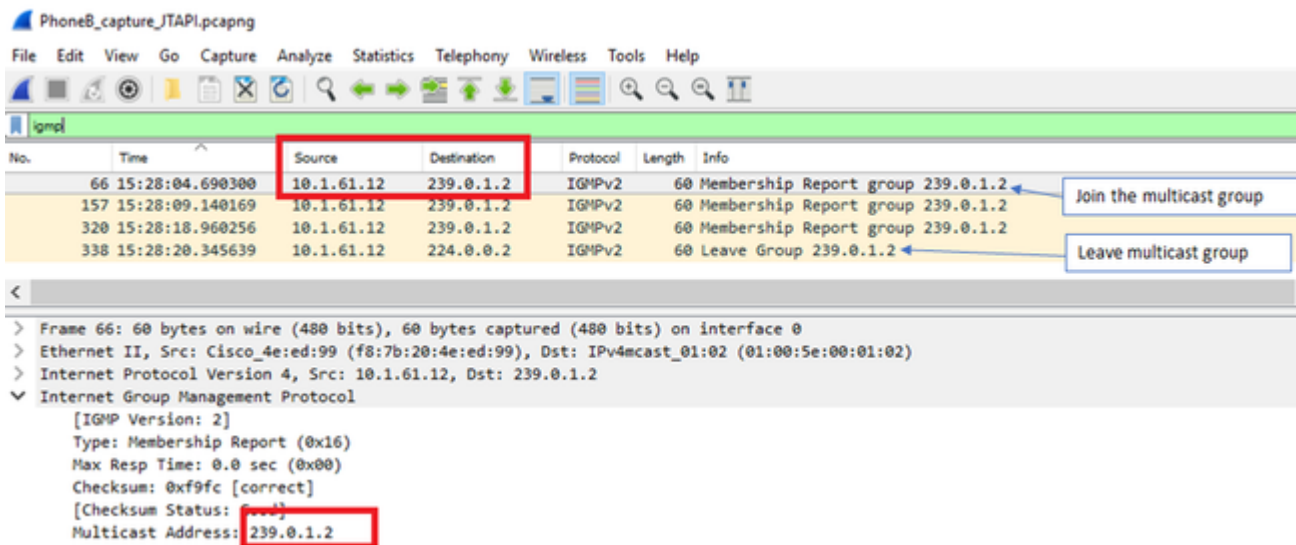
Multicast TTL: 16 (required)

CANCEL UPDATE

In diesem Fall empfängt das Telefon B vom CUCM-Server die IP-Adresse und den Port für Multicast über eine SIP-REFER. Sie können auf die SIP REFER-Nachricht klicken, dann mit der rechten Maustaste auf den Nachrichtentext klicken und Paketbytes anzeigen auswählen, wie im Bild gezeigt.



Sobald das Telefon die Anweisung empfängt, verbindet es sich mit der Multicast-IP-Adresse und dem Port mit einer IGMP-Nachricht. Das Telefon versucht dreimal so oft wie möglich, Audio zu empfangen. Wenn das Paging endet, senden die Telefone in der Empfängergruppe die Nachricht "Leave Group" (Gruppe verlassen), um die Multicast-Sitzung zu beenden.



Tools für die Fehlerbehebung

[Das Multicast-Testtool](#) unterstützt Sie bei der weiteren Fehlerbehebung für SNMP.

[InformaCast LogTool](#) unterstützt Sie bei der Behebung gängiger Probleme bei der Implementierung und Wartung von InformaCast in Ihrem Netzwerk.

Advance-Lizenz

Kunden mit dem erweiterten Benachrichtigungsmodus werden von SingleWire unterstützt. Wenden Sie sich für weitere Unterstützung an sales@singlewire.com.

Der SingleWire-Support ist von Montag bis Freitag von 7 bis 18 Uhr CDT unter +1 608 661 1140 (Option 2) verfügbar.

Passwörter

In Informacast gibt es mehrere Arten von Passwörtern:

Betriebssystem-Anmeldedaten: Wird verwendet, um Webmin und das Kontrollzentrum (<https://x.x.x.x:10000>) zu öffnen und wenn SSH für den Zugriff auf die virtuelle InformaCast-Appliance verwendet wird. Der Standardbenutzer ist admin, während das Kennwort changeMe lautet.

Administratorkennwort: Wird verwendet, um sich bei der Admin-Schnittstelle (<https://x.x.x.x:8444/InformaCast/admin>) anzumelden.

Kennsatz: Wird verwendet, um Ihre Backups der virtuellen InformaCast-Appliance zu sichern. Sie müssen sich diese Passphrase merken. Das Personal des SingleWire-Supports kann die Daten nicht wiederherstellen, wenn sie verloren gehen.

Kennwortwiederherstellung

Für Cisco Paging-Server 12.5.1 und höher:

[https://www.singlewire.com/help/InformaCast/v12.5.1/advanced/cucm/index.htm#t=InformaCast_Fusion%](https://www.singlewire.com/help/InformaCast/v12.5.1/advanced/cucm/index.htm#t=InformaCast_Fusion%20)

JTAPI in Informacast aktualisieren

Wenn Sie die virtuelle InformaCast-Appliance installieren oder die Versionen von CUCM ändern, müssen Sie die von der virtuellen InformaCast-Appliance verwendete JTAPI-Bibliothek auf die gleiche Version aktualisieren, die vom CUCM-Server verwendet wird.

Durch die Aktualisierung von JTAPI über die virtuelle Appliance wird die JTAPI-Version für alle SingleWire-Anwendungen aktualisiert, die JTAPI verwenden.

Die Schritte werden im Abschnitt JTAPI aktualisieren in Informacast im folgenden Leitfaden beschrieben <https://community.cisco.com/t5/collaboration-voice-and-video/integrating-basic-cisco-paging-basic-informacast-with-cucm/ta-p/3161322>

Häufige Fehler

[CSCve47332](#)  Cisco IP-Telefone der Serie 69XX können keine Leerzeichen in Anwendungsbenutzern für Informacast verarbeiten.

[CSCuy56088](#)  Telefon der Serie 8800 ohne Multicast-Audio

[CSKut91894](#)  Verbindungen von FF37 & Chrome zu InformaCast scheitern nach FF/Chrome Update

[CSCtb70375](#)  SNMP muss den Benutzer über DNS-Verbindungsprobleme informieren.

Zugehörige Informationen

- CUCM-Kompatibilitätsmatrix: <https://www.singlewire.com/matrix/cisco-platforms>
- Telefonmatrix: <https://www.singlewire.com/matrix/cisco-phones>
- Aktualisierungspfad: <https://www.singlewire.com/matrix/ic-upgrades>
- Serverplattformen: <https://www.singlewire.com/matrix/server-platforms>
- Hardwareanforderungen: <https://www.singlewire.com/informacast-hardware-requirements>
- Technischer Support und Dokumentation - Cisco Systems SRND:
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab12/collab12.pdf
- CUCM-Integration mit Cisco Paging-Server/InformaCast - Konfigurationsbeispiel:
<https://www.cisco.com/c/en/us/support/docs/unified-communications/paging-server/117059-configure-informacast-00.html>
- Cisco Paging Server - Kurzreferenz:
https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cucm/cisco_paging_server/12_5_1/QSG

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.