Konfigurieren von Prime Collaboration Assurance (PCA) - Conference Diagnostics

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie die Bereitstellung für Konferenzdiagnosen im Rahmen von Prime Collaboration Assurance (PCA) konfigurieren und einrichten, um Statistiken zu Sprach-/Videokonferenzen proaktiv zu überwachen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Anmeldung beim Call Manager Admin
- PCA-Anmeldung
- Ihr Telepresence Monitor Server (TMS)
- Core/Expressway-Anmeldeinformationen (falls zutreffend)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den PCA-Versionen 11.x - 12.x.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Cisco Prime Collaboration 11.x unterstützt folgende Arten von Transparenz:

- Vollständige Transparenz - Die Anrufabdeckung wird mithilfe von JTAPI-/HTTP-Feedback und Echtzeitüberwachungsinformationen wie Konferenzstatistiken und Konferenzinformationen unterstützt.
- Eingeschränkte Transparenz - Die automatische Anrufererkennung erfolgt mithilfe von JTAPI/HTTP-Feedback. Echtzeitüberwachungsinformationen wie Konferenzstatistiken und Konferenzinformationen werden jedoch nicht unterstützt. Endpunkte mit eingeschränkter Transparenz werden in der Konferenztopologie durch ein halbdunkles Symbol gekennzeichnet.

Cisco Prime Collaboration 12.x unterstützt folgende Arten von Transparenz:

- Vollständige Transparenz - Die Anrufabdeckung wird mithilfe von JTAPI-/HTTP-Feedback und Echtzeitüberwachungsinformationen wie Konferenzstatistiken und Konferenzinformationen unterstützt.
- Keine Transparenz - Anrufabdeckung mit JTAPI-/HTTP-Feedback und Echtzeitüberwachungsinformationen werden nicht unterstützt. Diese Endpunkte werden auf der Seite für die Konferenzüberwachung mit einem vollständig abgedunkelten Symbol angezeigt.

Begrenzung der Endgeräte auf eine begrenzte oder vollständige Transparenz pro OVA

- Small Open Virtualization Archive (OVA) unterstützt bis zu 500 Endgeräte
- Mittlere OVA unterstützt bis zu 1.000 Endpunkte
- Große OVA unterstützt bis zu 1.800 Endpunkte
- Sehr große OVA unterstützt bis zu 2.000 Endpunkte

Eine Liste der unterstützten Geräte pro PCA in Bezug auf Konferenzen und die von uns unterstützten Sitzungen finden Sie in der Tabelle unten.

Session Scenarios

The various session scenarios that are monitored in Cisco Prime Collaboration are as follows:

Table 1 Session Scenarios

Session Classification	Session Type	Session Structure	Session Topology Elements
Cisco Unified CM *intracluster* and *intercluster* sessions	Ad hoc,Scheduled	Point-to-point	Cisco TelePresence System 500, 1000, 3000, TX9000 Series.
Cisco Unified CM *intracluster* and *intercluster* sessions	Ad hoc,ScheduledStatic	Multipoint	Cisco TelePresence System 500, 1000, 3000, TX9000 Series, and CTMS.
Cisco VCS *intracluster* and *intercluster* sessions	Ad hoc,Scheduled	Point-to-point	Cisco C series, EX Series, Cisco MX series, Cisco MXP Series, Cisco IP Video Phone E20, Cisco Cius, and Cisco Jabber. If a call is identified as a traversal call, Cisco VCS Control or Cisco VCS Expressway is displayed in the session topology.
Cisco VCS *intracluster* and *intercluster* sessions (with MCU)	Ad hoc,ScheduledPermanent (displayed as static)	Multipoint	Cisco C series, EX Series, Cisco MCU, Cisco MSE[1], or Cisco TelePresence Server. If a call is identified as a traversal call, Cisco VCS Control or Cisco VCS Expressway is displayed in the session topology.
Cisco VCS *intracluster* and *intercluster* sessions (without MCU)	Ad hoc,Scheduled	Multisite	Cisco C series, EX Series, Cisco MX, Cisco MXP Series, Cisco IP Video Phone E20. If a call is identified as a traversal call, Cisco VCS Control or Cisco VCS Expressway is displayed in the session topology.
Sessions between Cisco Unified CM and Cisco VCS clusters [2]	Ad hoc	Point-to-pointMultipoint	• Cisco C series, EX Series, Cisco MX series, Cisco MXP Series, Cisco IP Video Phone E20 • Cisco TelePresence System 500, 1000, 3000, and TX9000 Series • Cisco TelePresence Server • IX 5000 series TelePresence endpoints
Cisco Unified CM (8.6(1), 8.6(2), and 9.0) *intracluster* sessions[3]	Ad hoc	Point-to-point	• Cisco C series, EX Series, Cisco MX series • Cisco TelePresence System 500, 1000, 3000, and TX9000 Series • IX 5000 series TelePresence endpoints
Cisco Unified CM (8.6(1), 8.6(2), and 9.0) *intracluster* sessions	Ad hoc,Scheduled **Note** Scheduler must be CTS-Manager 1.7, 1.8, or 1.9.	Multipoint	• Cisco C series, EX Series, Cisco MX series, Cisco IP Video Phone E20 • Cisco TelePresence System 500, 1000, 3000, and TX9000 Series • CTMS 1.8 or Cisco TelePresence Server
Sessions outside the enterprise firewall - Cisco VCS Expressway	Ad hocPermanent (displayed as static)	Point-to-point,Multipoint, Multisite	• Cisco C series, EX Series, Cisco MX series, Cisco MXP Series, Cisco IP Video Phone E20 • Cisco MCU or Cisco TelePresence Server • Cisco VCS Control and Cisco VCS Expressway

Endpoints in a call (with an MCU in the call) work as a conferencing bridge in Cisco Unified CM.	Ad hoc	Point-to-point When a call is put in a conference mode or when merged with another call, it becomes Multipoint. The session does not show the MCU. When the first participant leaves the call, the session shows it is connected to the MCU, while the second and third participants continue in the same call as a point-to-point call. **Note** This scenario is applicable when in-built video bridge capability is not present in the endpoint.	Multipoint conferencing devices and video endpoints. For a list of devices supported by Cisco Prime Collaboration 11.0, see Supported Devices for Prime Collaboration Assurance.
Sessions between MRA endpoints- Cisco Jabber or Cisco TelePresence MX Series or Cisco TelePresence System EX Series or Cisco TelePresence SX Series	Ad hoc, Scheduled	Point-to-point,Multipoint, Multisite **Note** Cisco Prime Collaboration does not monitor a Multisite session where an MRA endpoint acts as a conference bridge.	Cisco Jabber, Cisco TelePresence MX Series, Cisco TelePresence System EX Series, and Cisco TelePresence SX Series.

[1] The codian software must be running on Cisco MSE.
[2] This scenario is supported on CTS 1.7.4, and TC 4.1 to 7.0.
[3] The troubleshooting workflow is supported on TC 4.2, 5.0, and above.

Note
- Cisco Cius and Cisco Jabber devices support only ad hoc sessions.

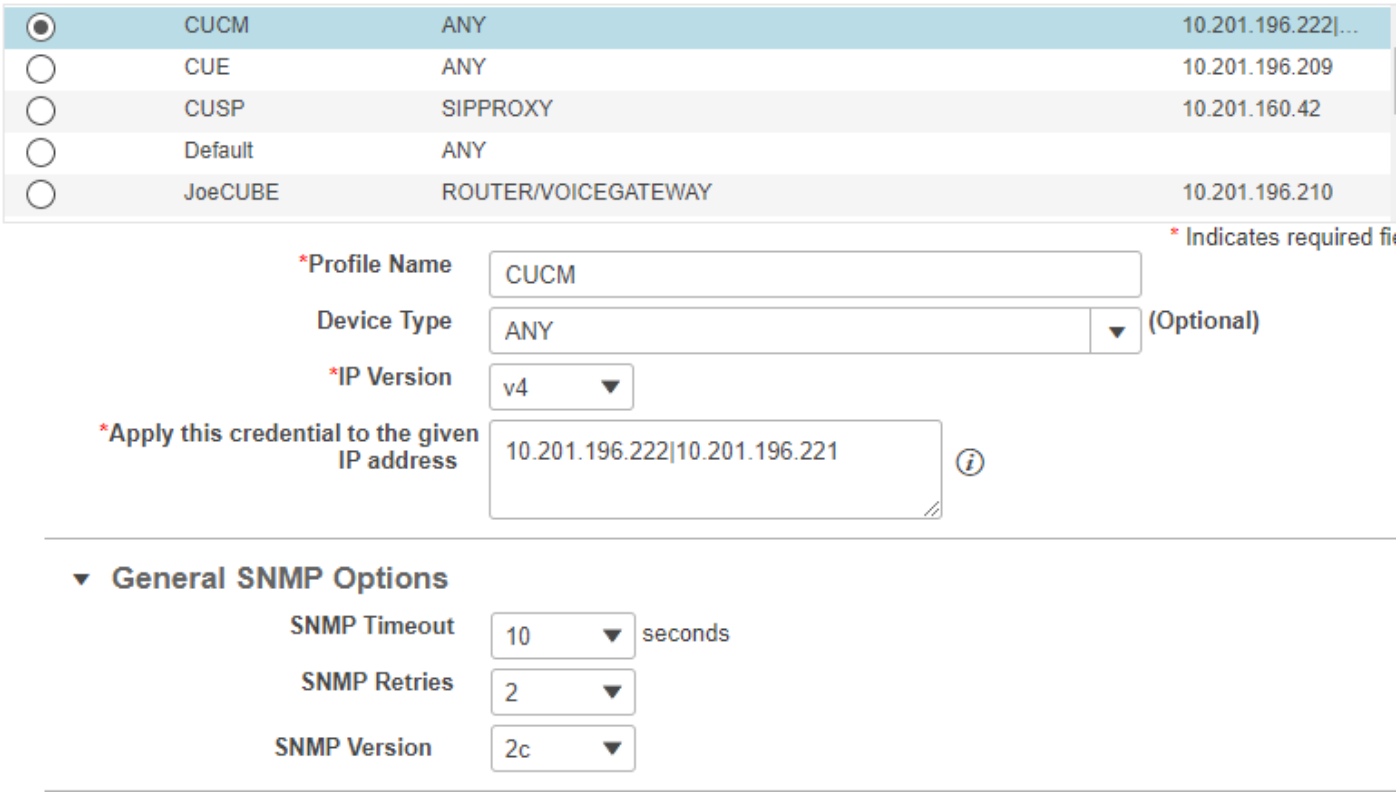
Konfigurieren

Szenario 1. Konferenz mit Video-Endpunkten, die zum Call Manager registriert sind

Schritt 1: Zuerst müssen Sie sicherstellen, dass sich die Call Manager im Managed-Zustand befinden.

Navigieren Sie zu **Inventory > Inventory Management > Manage Credentials (Anmeldeinformationen verwalten) > Create a profile** for the Call Manager cluster.

> **Hinweis**: Denken Sie daran, dass jedes Berechtigungsprofil für jede im Profil aufgeführte IP dieselben Anmeldeinformationen verwendet. Wenn Sie also Call Manager Publisher und Subscriber im gleichen Credential-Profil auflisten, werden diese beiden IP-Adressen mit denselben Anmeldeinformationen ermittelt. Wenn Sie einen Leiter in Ihrer Einrichtung haben, suchen Sie zuerst nach dem Leiter und dann nach dem Cisco Call Manager, wie im Bild gezeigt.



Schritt 2: Stellen Sie sicher, dass Sie über die Anmeldeinformationen für Hypertext Transfer Protocol (HTTP), Simple Name Management Protocol (SNMP) und Java Telefony API (JTAPI) verfügen.

Darüber hinaus müssen Sie den Cisco Computer Telefony Integration (CTI) Service in Call Manager Serviceability aktivieren.

Einrichtung von Cisco Unified Communications Manager

HTTP aktivieren

Wenn Sie zulassen möchten, dass Cisco Prime Collaboration Administratorberechtigungen verwendet, müssen Sie keinen neuen Benutzer erstellen. Wenn Sie Cisco Prime Collaboration Manager die richtigen Anmeldeinformationen für die Anmeldung bei Cisco Unified Communications Manager zuweisen möchten, müssen Sie eine neue HTTP-Benutzergruppe und einen entsprechenden Benutzer erstellen, den Cisco Prime Collaboration für die Kommunikation verwenden kann.

Um einen Benutzer zu erstellen, gehen Sie wie folgt vor:

Schritt 1: Melden Sie sich mit Ihrem Administratorkonto bei der Webschnittstelle von Cisco Unified CM Administration an.

Schritt 2: Erstellen Sie eine Benutzergruppe mit ausreichenden Berechtigungen. Navigieren Sie zu **User Management>User Settings>Access Control** Group, und erstellen Sie eine neue Benutzergruppe mit dem passenden Namen **PC_HTTP_Users** in diesem Fall. **Wählen Sie** jetzt **Speichern aus**.

Schritt 3: Navigieren Sie zu **Benutzerverwaltung>Benutzereinstellungen>Zugriffskontrollgruppe,** und **wählen Sie Suchen aus**. Suchen Sie die Gruppe, die Sie definiert haben, und klicken Sie auf das Symbol rechts.

Schritt 4: **Wählen Sie Rolle der** Gruppe **zuweisen** und wählen Sie die folgenden Rollen aus:

- Standard-API-Zugriff über AXL
- Standard-CCM-Administratorbenutzer
- Standard-SERVICEABILITÄTSmanagement

Schritt 5: Klicken Sie auf **Speichern**.

Schritt 6: Navigieren Sie im Hauptmenü **zuBenutzerverwaltung>Anwendungsbenutzer>Neuen Benutzer erstellen**.

Geben Sie ein geeignetes Kennwort auf **der** Seite **Anwendungsbenutzerkonfiguration** an. Sie können im Textbereich "Verfügbare Geräte" nur bestimmte Gerätetypen auswählen oder Cisco Prime Collaboration zum Überwachen aller Geräte zulassen.

Schritt 7: Wählen Sie **im** Abschnitt Berechtigungsinformationen **die Option Zu** Benutzergruppe **hinzufügen** aus, und wählen Sie die Gruppe aus, die in Schritt 1 erstellt wurde. (z. B. PC_HTTP_Users).

Schritt 8: **Klicken Sie auf Speichern**. Die Seite wird aktualisiert und die richtigen Berechtigungen werden angezeigt.

SNMP aktivieren

SNMP ist in Cisco Unified Communications Manager standardmäßig nicht aktiviert.

So aktivieren Sie SNMP:

Schritt 1: Melden Sie sich in **der** Web-Benutzeroberfläche von Cisco Unified Communications Manager **bei** der **Cisco Unified** ServiceView an.

Schritt 2: Navigieren Sie zu **Extras > Service-Aktivierung**.

Schritt 3: Wählen Sie **Publisher Server aus**.

Schritt 4: Navigieren Sie zu **Leistung > Überwachungsdienste, und aktivieren Sie das Kontrollkästchen für den Cisco Call Manager SNMP Service.**

Schritt 5: Wählen Sie unten im Bildschirm **Speichern aus**.

So erstellen Sie einen SNMP Community String:

Schritt 1: Melden Sie sich bei **Cisco Unified** Service **an**, um die Web-Benutzeroberfläche von Cisco Unified Communications Manager anzuzeigen.

Schritt 2: Navigieren Sie im Hauptmenü in der Ansicht "Cisco Unified Services" **zuSNMP > v1/v2c > Community String**.

Schritt 3: Wählen Sie einen Server aus, und **klicken Sie auf Suchen**.
Wenn der Community-String bereits definiert ist, wird der Community String Name in den Suchergebnissen angezeigt.

Schritt 4: **Klicken Sie auf** Neu **hinzufügen**, um eine neue Zeichenfolge hinzuzufügen, wenn keine

Ergebnisse angezeigt werden.

Schritt 5: Geben Sie die erforderlichen SNMP-Informationen an, und speichern Sie die Konfiguration.

Hinweis: Es wird nur SNMP Read Only (RO)-Zugriff benötigt.

CTI-Service starten

Führen Sie das gewünschte Verfahren für den Cisco Unified Communications Manager-Knoten durch. Es empfiehlt sich, diesen auf zwei Knoten festzulegen.

Schritt 1: Melden Sie sich bei der Cisco Unified Serviceability an, die in der grafischen Benutzeroberfläche von Cisco Unified Communications Manager angezeigt wird.

Schritt 2: Navigieren Sie **zu Extras > Service-Aktivierung**.

Schritt 3: Wählen Sie einen Server aus der Dropdown-Liste aus.

Schritt 4: Aktivieren Sie im Bereich CM Services **das** Kontrollkästchen **Cisco CTI** Manager.

Schritt 5: Wählen Sie oben im Bildschirm **Speichern aus.**

Erstellen eines Anwendungsbenutzers für PCA CTI Control (JTAPI-Benutzer)

JTAPI wird verwendet, um die Sitzungsstatusinformationen vom Gerät abzurufen. Sie müssen im Anrufprozessor einen Anwendungsbenutzer für CTI Control mit der erforderlichen Berechtigung zum Empfang von JTAPI-Ereignissen auf Endpunkten erstellen. Prime Collaboration verwaltet mehrere Anrufprozessor-Cluster. Sie müssen sicherstellen, dass die Cluster-IDs eindeutig sind. Erstellen Sie einen neuen Anwendungsbenutzer, damit Cisco Prime Collaboration die erforderlichen Informationen erhält.

Um eine neue JTAPI-Anwendung zu erstellen, gehen Sie wie folgt vor:

Schritt 1: Melden Sie sich über Ihr Administratorkonto bei der Webschnittstelle von Cisco Unified CM Administration an.

Schritt 2: Erstellen Sie eine Benutzergruppe mit ausreichenden Berechtigungen. Navigieren Sie zu **User Management>User Settings>Access Control** Group, und erstellen Sie eine neue Benutzergruppe mit dem passenden Namen **PC_HTTP_Users** in diesem Fall. **Wählen Sie** jetzt **Speichern aus**.

Schritt 3: Wählen Sie **User Management>User Settings>Access Control Group (Benutzerverwaltung > Benutzereinstellungen > Zugriffskontrollgruppe),** und **klicken Sie auf Find**. Suchen Sie die Gruppe, die Sie definiert haben, und wählen Sie das Symbol auf der rechten Seite aus.

Schritt 4: **Klicken Sie auf Rolle der** Gruppe **zuweisen** und wählen Sie die folgenden Rollen aus:

- Standard-CTI erlaubt Anrufüberwachung

- Standard-CTI aktiviert
- Standard-CTI ermöglicht die Steuerung von Telefonen, die angeschlossene Xfer- und conf-Verbindungen unterstützen

Schritt 5: **Wählen Sie Speichern aus**.

Schritt 6: Navigieren Sie im Hauptmenü **zuBenutzerverwaltung>Anwendungsbenutzer>Neuen Benutzer erstellen**.
Geben Sie ein geeignetes Kennwort auf **der** Seite **Anwendungsbenutzerkonfiguration** an. Sie können bestimmte Gerätetypen aus dem Textbereich Verfügbare Geräte auswählen oder Cisco Prime Collaboration zum Überwachen aller Geräte zulassen.

> **Hinweis**: Das Kennwort darf kein Semikolon (;) oder Gleichheitszeichen (=) enthalten.

Schritt 7: Wählen Sie **im** Abschnitt Berechtigungsinformationen **die Option Zu Zugriffskontrollgruppe hinzufügen** aus, und wählen Sie die Gruppe aus, die in Schritt 1 erstellt wurde. (z. B. PC_HTTP_Users).

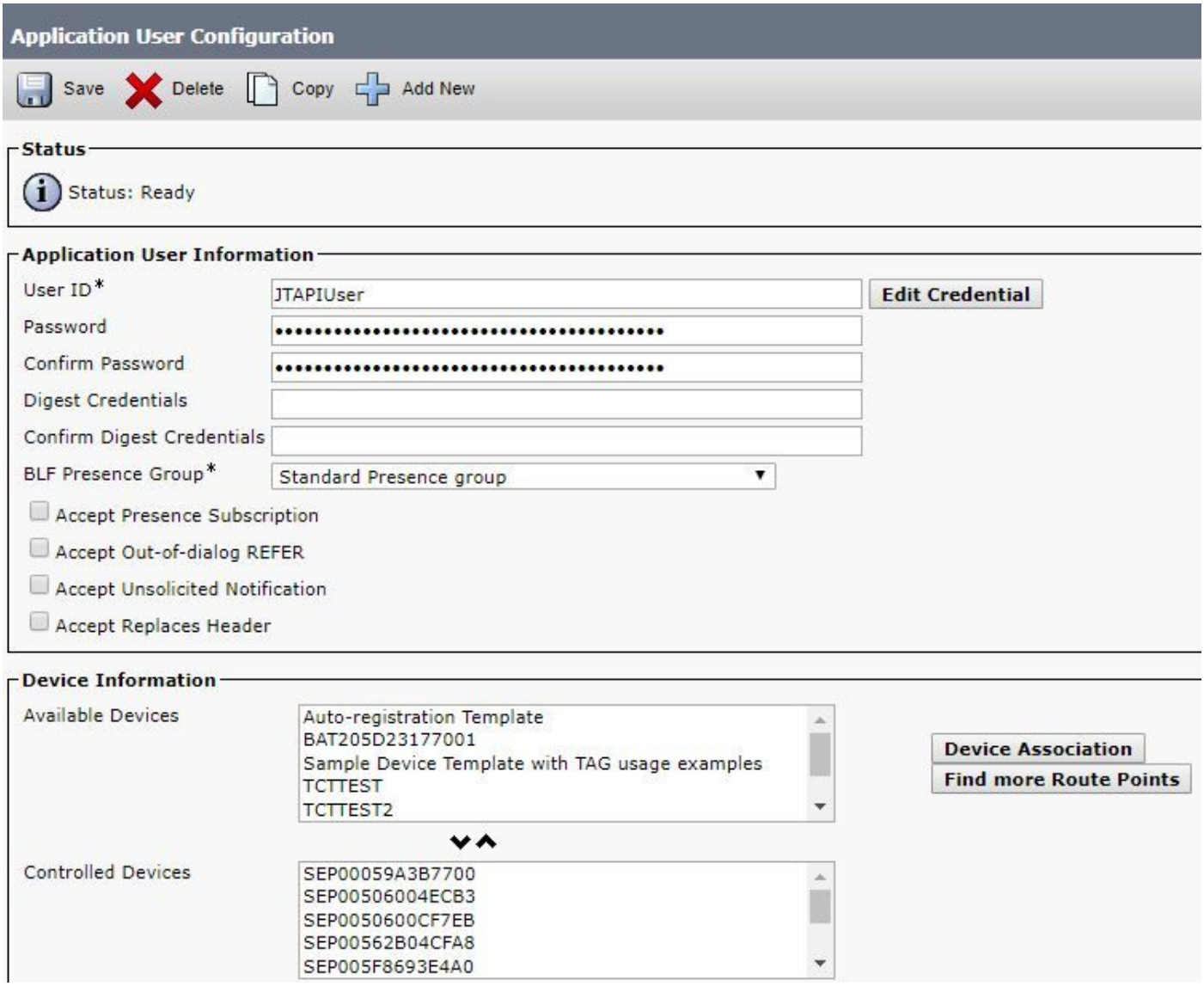
Schritt 8: **Klicken Sie auf Speichern**. Die Seite wird aktualisiert und die richtigen Berechtigungen werden angezeigt.

> **Hinweis**: Wenn der Call Manager vor dem Hinzufügen des JTAPI-Benutzers verwaltet wurde, stellen Sie sicher, dass der JTAPI-Benutzer dem Credential-Profil für den Call Manager hinzugefügt wurde, und ermitteln Sie ihn erneut.

Fortsetzung von Szenario 1. Schritte:

Schritt 3: Navigieren Sie zum von Ihnen erstellten Call Manager JTAPI-Anwendungsbenutzer, und verschieben Sie die unterstützten Endpunkte von Verfügbaren Geräten auf Kontrollierte Geräte.

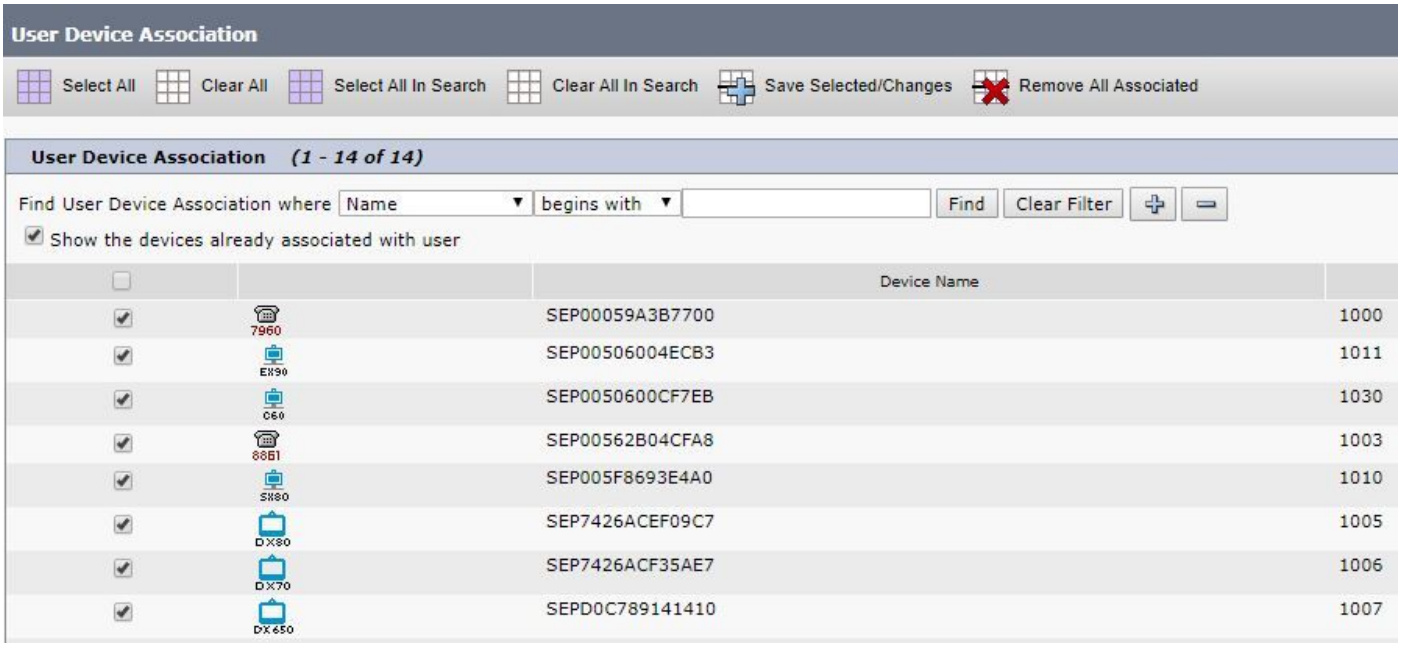
Sie können dies mithilfe der Device Association-Funktion (Gerätezuweisung) wie im Bild gezeigt durchführen.



Wenn Sie auf die Beschränkung von Endpunkten auf "Eingeschränkte" oder "Vollständige Transparenz pro OVA" zurückgreifen, können Sie überprüfen, wie viele Geräte Sie der OVA-Größe hinzugefügt haben.

In diesem Bildschirm können Sie nach Gerätename, Beschreibung oder Verzeichnisnummer filtern, um Sie bei der Verwaltung und Filterung dieser Geräte zu unterstützen, wie im Bild gezeigt.

Es ist hilfreich, diese Geräte zu beachten, da sie in Schritt 7 hinzugefügt wurden.



Stellen Sie sicher, dass für diesen JTAPI-Benutzer die richtigen Benutzerrollen hinzugefügt werden:

- Standard-CTI erlaubt Anrufüberwachung
- Standard-CTI aktiviert
- Standard CTI ermöglicht die Steuerung von Telefonen, die angeschlossene Xfer- und conf-Verbindungen unterstützen, wie im Bild gezeigt.

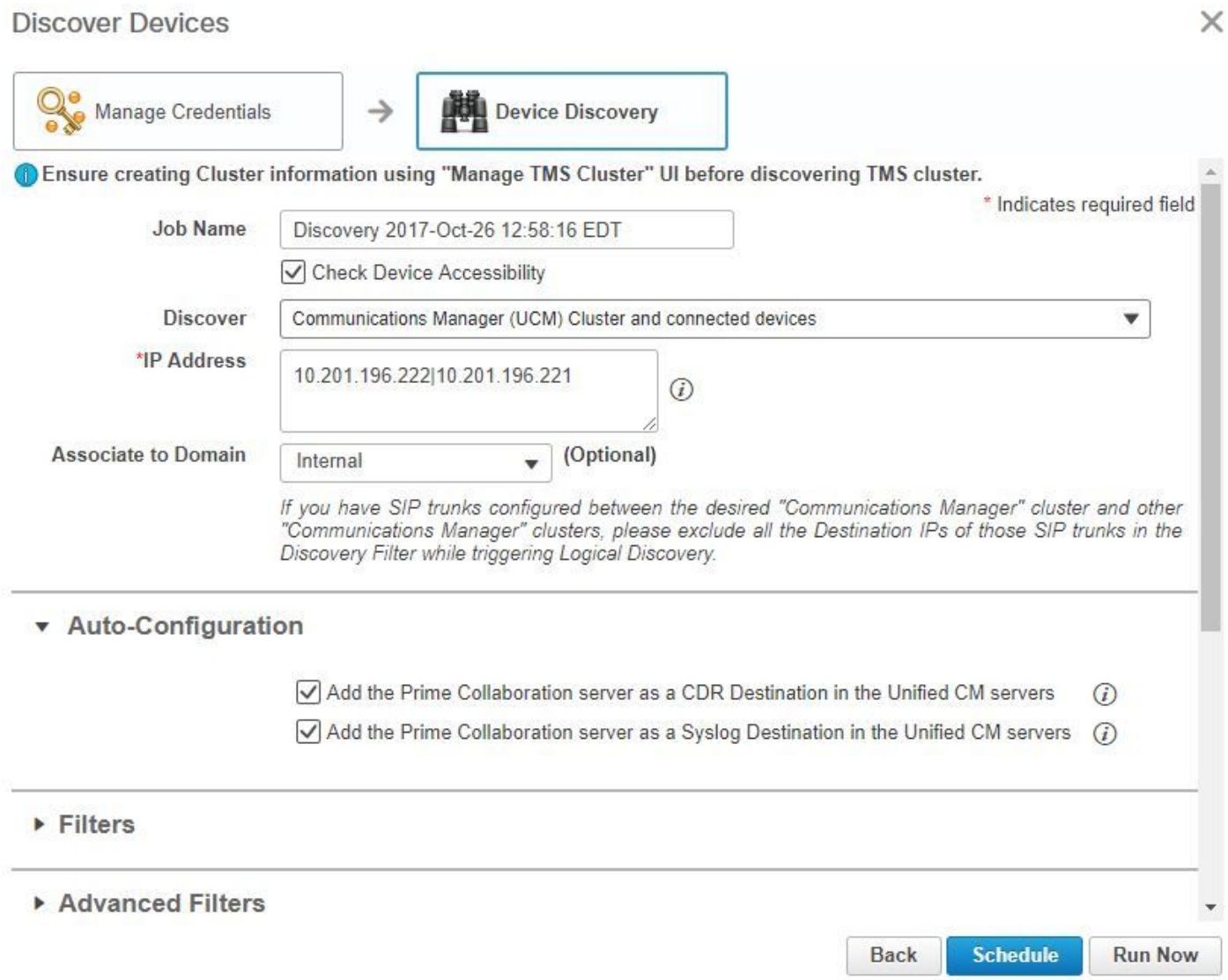
Eine Liste der unterstützten Geräte pro PCA bezüglich Konferenzen und unterstützter Sitzungen finden Sie im Abschnitt Hintergrundinformationen.

Hinweis: Stellen Sie außerdem sicher, dass für die vom CTI-Anwendungsbenutzer kontrollierten Geräte das Kontrollkästchen Device Control of Device from CTI (Gerätesteuerung vom CTI zulassen) unter den Geräteinformationen wie im Bild gezeigt aktiviert ist.

Hinweis: Bevor Sie fortfahren, sollten Sie beachten, dass wenn Sie die Endpunkte für Call Manager registriert haben und Call Manager in VCS/TMS integriert ist, Sie zuerst Ihr VCS/TMS erkennen und dann zuletzt Ihren Call Manager aufrufen. Aus Inventarsicht wird Ihre gesamte Infrastruktur dem richtigen Standort zugeordnet. Wenn Sie das VCS/TMS erkennen, stellen Sie außerdem sicher, dass Sie die Standard-Registerkarte "Discover"

(Erkennung) auf das entsprechende Gerät von TMS/VCS oder Call Manager ändern.

Schritt 4: Wählen Sie anschließend im PCA **Device Discovery** (Geräteerkennung) aus, und geben Sie die IP-Adressen Ihrer Call Manager ein. Aktivieren Sie die beiden Kontrollkästchen **Auto-Configuration (Automatische Konfiguration),** und wählen Sie **Run Now (Jetzt ausführen)** wie im Bild gezeigt aus.



Schritt 5: Wenn sich die Call Manager im Managed-Zustand befinden, fahren Sie mit Schritt 6 fort.

Hinweis: Wenn sich der Call Manager nicht in einem verwalteten Zustand befindet, ist dies meistens auf HTTP oder SNMP zurückzuführen. Wenn weitere Unterstützung erforderlich ist, öffnen Sie ein TAC-Ticket, um den Call Manager in einen verwalteten Zustand zu versetzen.

Schritt 6: Navigieren Sie zu **Inventory > Inventory Schedule > Cluster Data Discovery Schedule**, und wählen Sie **Run Now (Jetzt ausführen)**.

Hinweis: Dies hängt von der Anzahl der registrierten/nicht registrierten Geräte ab. Dieser Vorgang kann zwischen einigen Minuten und einigen Stunden dauern. Überprüfen Sie den ganzen Tag durch eine Aktualisierung der Seite. Darüber hinaus ordnet dies Ihrem Call Manager-Cluster zu und ruft alle Endpunkte ab. Fahren Sie nach Abschluss dieses

Vorgangs mit dem nächsten Schritt fort.

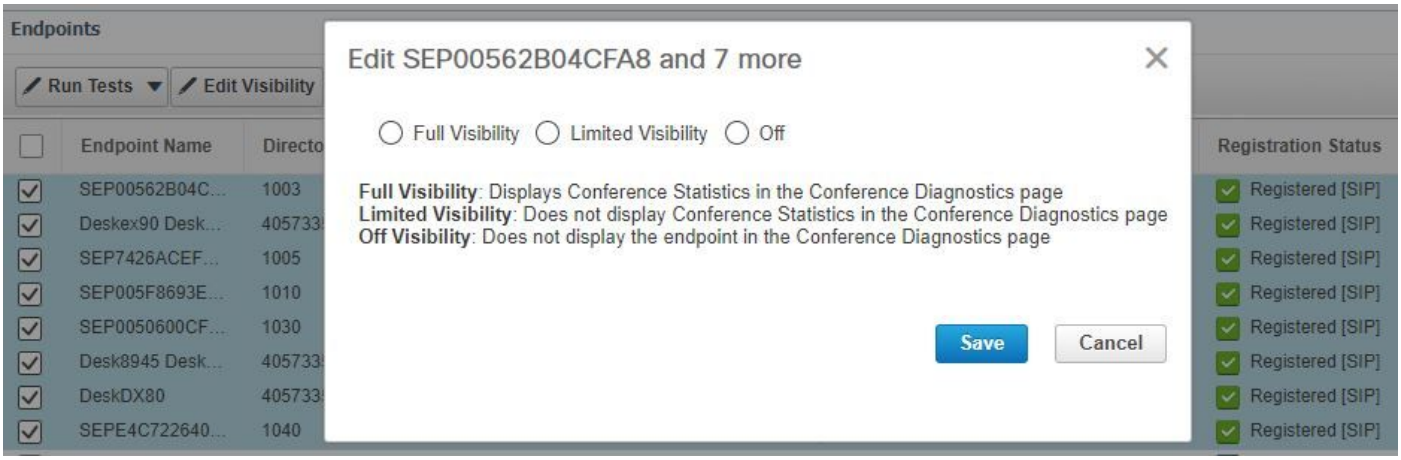
Hinweis: Es ist wichtig, im PCA-Bestand anzugeben, ob es Endpunkte gibt, für die Konferenzstatistiken unterstützt werden sollen. Stellen Sie sicher, dass diese Berichte und alle Statistiken gut verwaltet werden, um die richtigen Informationen anzuzeigen.

Schritt 7: Navigieren Sie zu **Diagnose > Endpunktdiagnose**.

Um aktuelle Statistiken für Ihre Konferenzendpunkte zu erhalten, müssen Sie deren Sichtbarkeit auf die höchstmögliche vom System zulässige Ebene einstellen.

Wählen Sie alle Endpunkte aus, die Sie in der Konferenz-Diagnose überwachen möchten, klicken Sie dann auf **Sichtbarkeit bearbeiten** und wählen Sie dann **Vollständige Transparenz** aus, wie im Bild gezeigt.

Die eingeschränkte Transparenz zeigt nur das Gerät in der Topologie an, aber keine Statistiken. Außerdem ist es nicht in der Lage, die entsprechenden Alarme für die Geräte abzurufen, die mit der Konferenzdiagnose in Zusammenhang stehen.

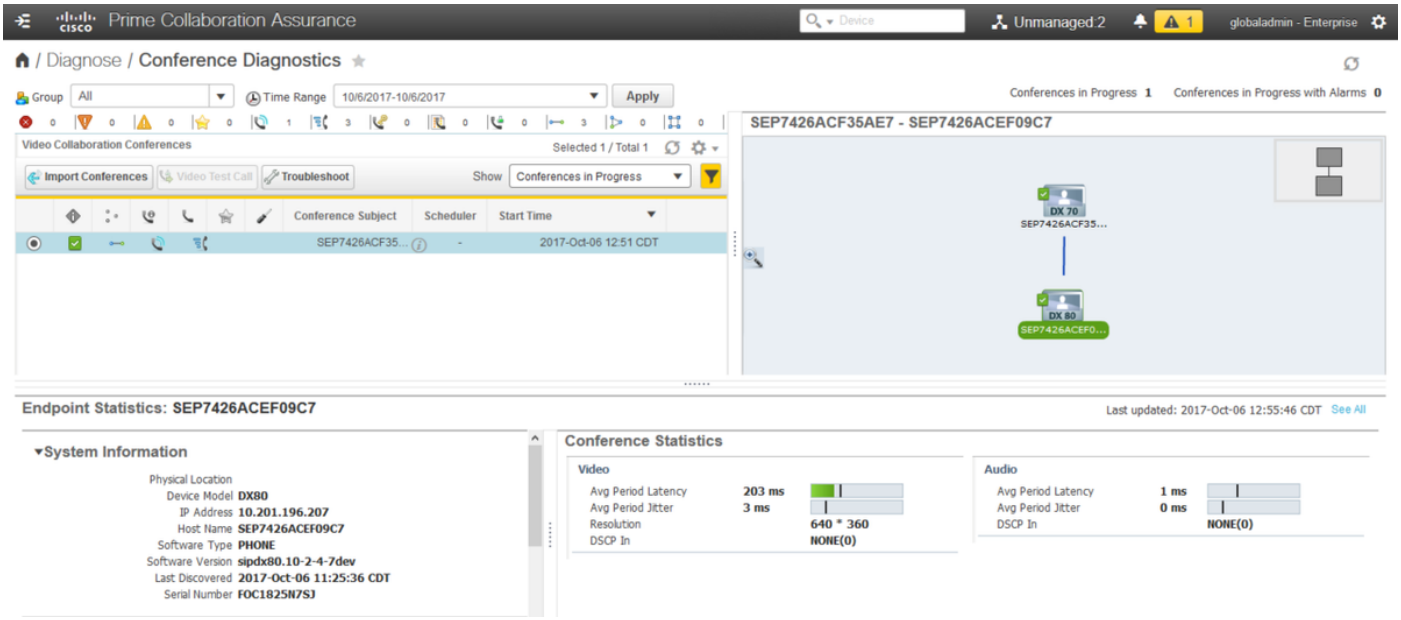


The following table lists the default and maximum visibility details for the endpoints:

Endpoint Type	Default Visibility	Maximum Visibility
• CTS 500, 1000, and 3000 Series • Cisco Codec • Cisco TelePresence SX20 • Cisco TelePresence MXP Series • Cisco IP Video Phone E20	Full	Full
• Cisco Jabber Video for TelePresence (Movi) • Polycom	Limited	Limited
Cisco Cius	Off	Full
Cisco IP Phones (89xx, 99xx)	Off	Full
Cisco Desktop Collaboration Experience DX650 and DX630	Off	Full
• Cisco SX80 and Cisco SX10 • • Cisco MX200 G2, Cisco MX300 G2, Cisco MX700, and Cisco MX800	Full	Full
Cisco DX70 and DX80	Off	Full
MRA Endpoints: • Cisco Jabber • Cisco TelePresence MX Series • Cisco TelePresence System EX Series • Cisco TelePresence System SX Series	Limited	Limited

Hinweis: Wenn Sie z. B. 10 Endpunkte auswählen und Full Visibility (Vollständige Transparenz) auswählen, wird die höchste Unterstützung für Transparenz pro Gerät ausgewählt.

Schritt 8: Um zu testen, navigieren Sie zu **Diagnose > Conference Diagnostics (Diagnose > Konferenzdiagnose)** und zu einer Konferenz In progress (Konferenz läuft) oder Complete (Abgeschlossen), wie im Bild gezeigt.



Auf diesen Konferenzen können Sie den durchschnittlichen Paketverlust, die Latenz und Jitter für Audio- und Videoanrufe anzeigen.

Rufen Sie außerdem eine Topologie der Sitzung und der beteiligten Geräte ab.

Derzeit ruft die Konferenzdiagnose die Informationen auf Basis der DN ab. Wenn Ihre Umgebung über gemeinsam genutzte DNs verfügt, ruft PCA das erste System ab, das für die Konferenz empfangen wird.

Konferenzrelevante Alarme

Für Konferenzdiagnosen können Sie drei verschiedene Alarme für jede Sitzung empfangen und deren Schwellenwerte festlegen:

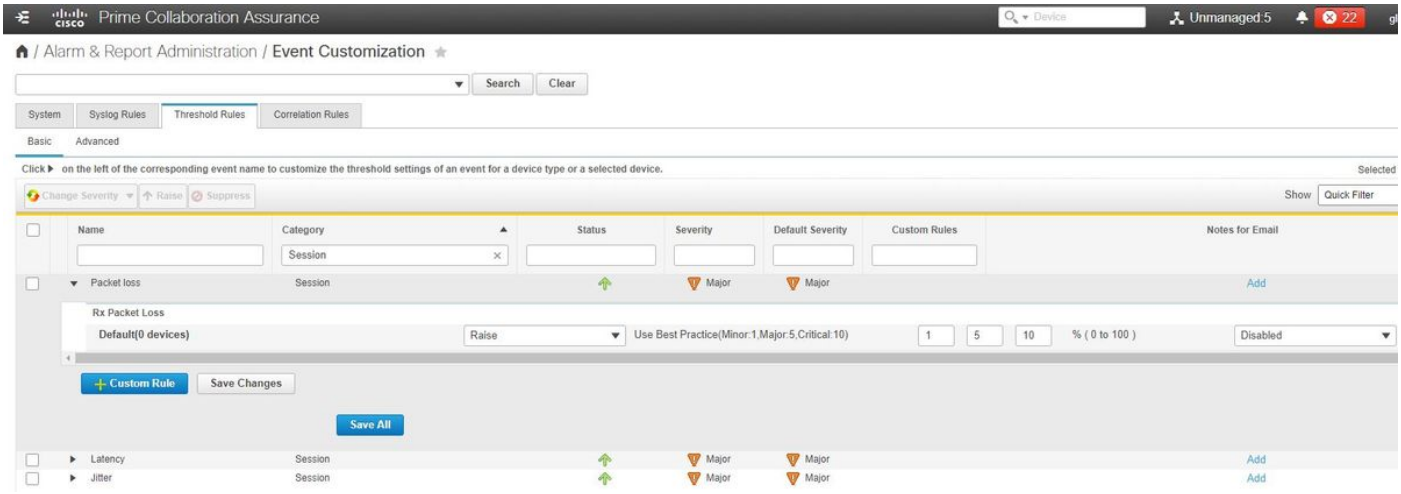
- Paketverlust
- Latenz
- Jitter

Für jeden dieser Werte können Sie den Standard-Schwellenwert ändern, diesen drücken oder festlegen, welche Geräte diesem Alarm zugeordnet werden sollen.

Schritt 1: Navigieren Sie zu **Alarm & Report Administration > Event Customization**.

Schritt 2: Wählen Sie **Schwellenwertregeln aus**, und stellen Sie sicher, dass **Basic (Grundlegende** Auswahl) ausgewählt ist.

Schritt 3: Blättern Sie nach unten, oder filtern Sie nach rechts, um die Kategorie Sitzung wie im Bild gezeigt anzuzeigen.



Schritt 4: Wählen Sie den Dropdown-Pfeil neben dem Alarm aus. Sie möchten die Prozentsätze für kleine, mittlere oder kritische Pakete für Paketverlust, Jitter oder Latenz ändern.

Schritt 5: Wenn Sie die Taste drücken möchten, wechseln Sie zum Überdrücken.

Schritt 6: Wenn Sie die dem Alarm zugeordneten Endpunkte definieren möchten, können Sie die Option Benutzerdefinierte Regel auswählen.

Schritt 7: Wählen Sie als Nächstes den **Gerätetyp aus > Alle Geräte** oder **wählbare Geräte**, die Sie für diesen Alarm auswählen möchten, und klicken Sie auf **Speichern**.

Konferenzrelevante Berichte

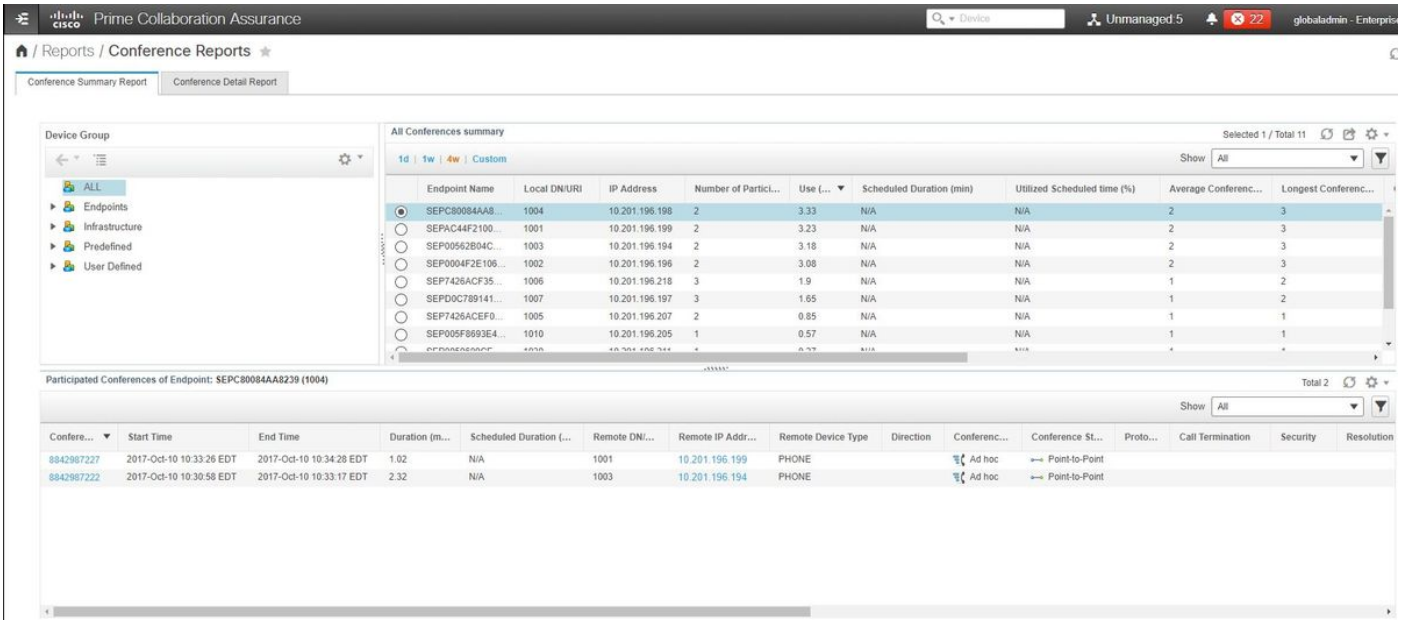
Für die Konferenzdiagnoseberichte können Berichte abgerufen und angezeigt werden.

Es gibt zwei Berichte:

- Konferenzberichte
- TelePresence-Endgeräteberichte

Bei Konferenzberichten können Sie eine Liste aller Konferenzen innerhalb eines Zeitrahmens von einem bis vier Wochen oder nach Bedarf in einem benutzerdefinierten Zeitraum anzeigen.

Schritt 1: Navigieren Sie zu **Reports > Conference Reports (Berichte > Konferenzberichte)**, wie im Bild gezeigt.



Berichte zur Konferenzzusammenfassung

Diese Berichte bieten eine Ansicht aller von Ihnen ausgewählten Endpunkte mit eingeschränkter bzw. vollständiger Transparenz und deren Konferenzen.

Hier werden folgende Statistiken angezeigt:

- Durchschnittliche Konferenznutzung
- Konferenzalarme
- Durchschnittlicher Paketverlust, Jitter und Latenz
- Längste Konferenz

Auf diese Weise können Sie einen detaillierten Überblick über Probleme in Ihrem Sprach-/Videonetzwerk erhalten, um festzustellen, auf welchen Endgeräten die meisten Probleme auftreten.

Außerdem können Sie die Bandbreite entsprechend der Nutzung nutzen.

Registerkarte "Conference Detail Report"

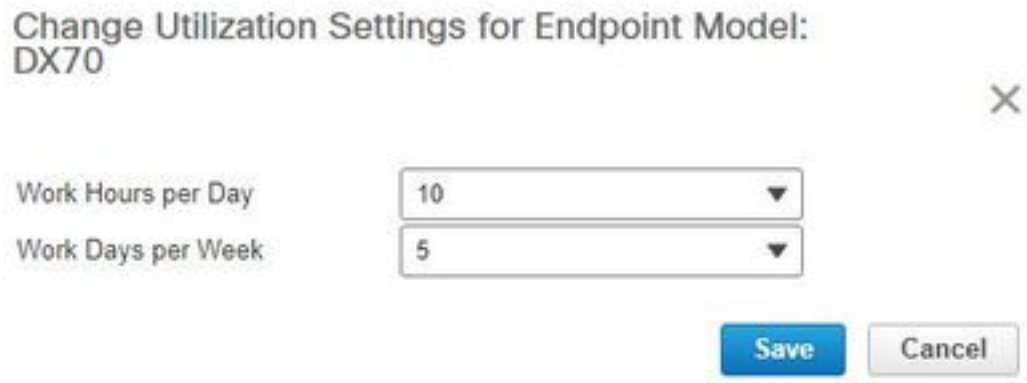
Wenn Sie eine Warnmeldung für eine Konferenz erhalten, können Sie zur Registerkarte **Conference Detail Report (Konferenzdetailbericht)** navigieren.

Nachdem Sie die Konferenz ausgewählt haben, können Sie sie verfeinern, um den Namen des Endpunkts, die Softwareversion und andere Details zu finden, die Sie interessieren.

Für Berichte zu Telepresence-Endgeräten können Sie Folgendes pro Endgerät anzeigen:

- Anzahl der Konferenzen, die dieses Gerät hatte
- Auslastungsprozentsatz
- Endgerätemodell
- Verwendung

Darüber hinaus können Sie die Utilization Paramaters (Auslastungsparameter) über die Registerkarte **Change Utilization (Auslastung ändern)** ändern, wie im Bild gezeigt.



Dadurch werden die Parameter für das Gerät festgelegt, sodass das System anhand der Nutzung weiß, welcher Prozentsatz angezeigt werden soll.

Der zusammenfassende Bericht "Endgeräte nicht anzeigen" zeigt die Endpunkte an, die geplante Konferenzen verpasst haben.

In diesem Diagramm können Sie auch den Endpunkt und die Gesamtzahl der geplanten Konferenzen sowie die Anzahl der Konferenzen anzeigen, die stattgefunden haben und bei denen es sich nicht um Shows handelt.

Videokonferenz-Testanruf

Sie können Video-Point-to-Point-Testanrufe zwischen zwei Video-Endpunkten im verwalteten Zustand erstellen, um Ihr Netzwerk zu testen. Sie können Ereignisse und Alarme, Sitzungsstatistiken, Endpunktstatistiken und Netzwerktopologie mit Statistiken wie andere Anrufe anzeigen. Für diesen Anruf werden nur die Codecs der CTS-, C- und EX-Serie unterstützt.

Darüber hinaus können Sie mit dieser Funktion prüfen, ob die Konferenzdiagnose alle Funktionen bietet.

Voraussetzungen

- Diese Funktion wird für die Codec-Serie E20 nicht unterstützt.
- Um dieses Feature zu verwenden, müssen CLI-Anmeldeinformationen für die Endpunkte hinzugefügt werden.
- Stellen Sie sicher, dass die Endpunkte registriert sind und JTAPI für Endpunkte aktiviert ist (wenn sie für Unified CM registriert sind).
- Wenn Sie Cisco Prime Collaboration im MSP-Modus implementiert haben, ist die Funktion für Videotest-Anrufe nicht verfügbar.

Schritt 1: Navigieren Sie zu **Diagnose > Endpunktdiagnose**.

Schritt 2: Wählen Sie je nach den genannten Voraussetzungen zwei geeignete Endpunkte aus.

Schritt 3: Wählen Sie **Tests ausführen > Videotest-Anruf aus**.

Schritt 4: Sie können den Videotest-Anruf so planen, dass er jetzt oder zu einem Wiederholungszeitpunkt ausgeführt wird.

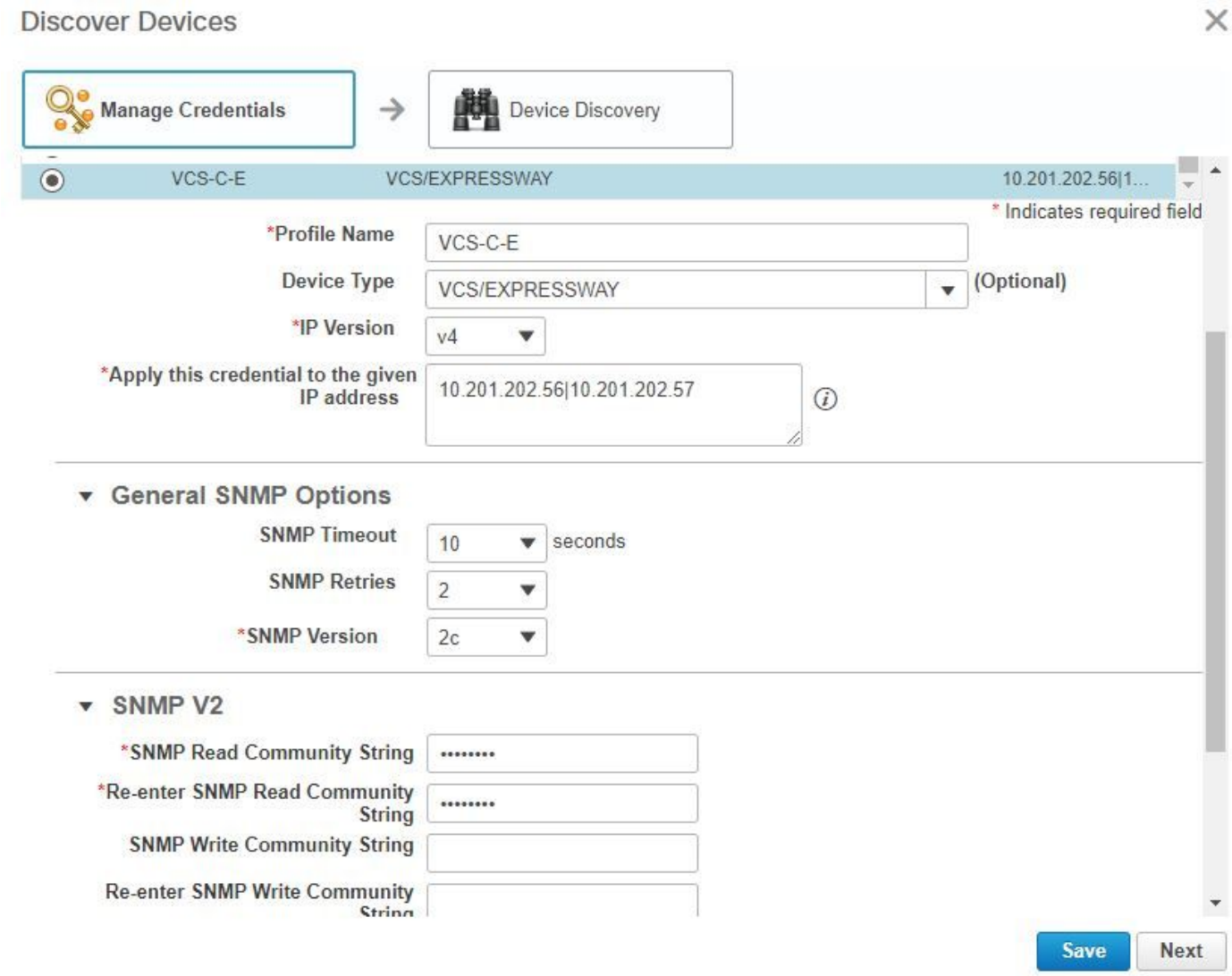
Schritt 5: Dieser Videotest-Anruf wird dann im Bildschirm "Conference Diagnostics" (Konferenzdiagnose) angezeigt.

Szenario 2. Konferenz mit registrierten Endgeräten ohne Call Manager

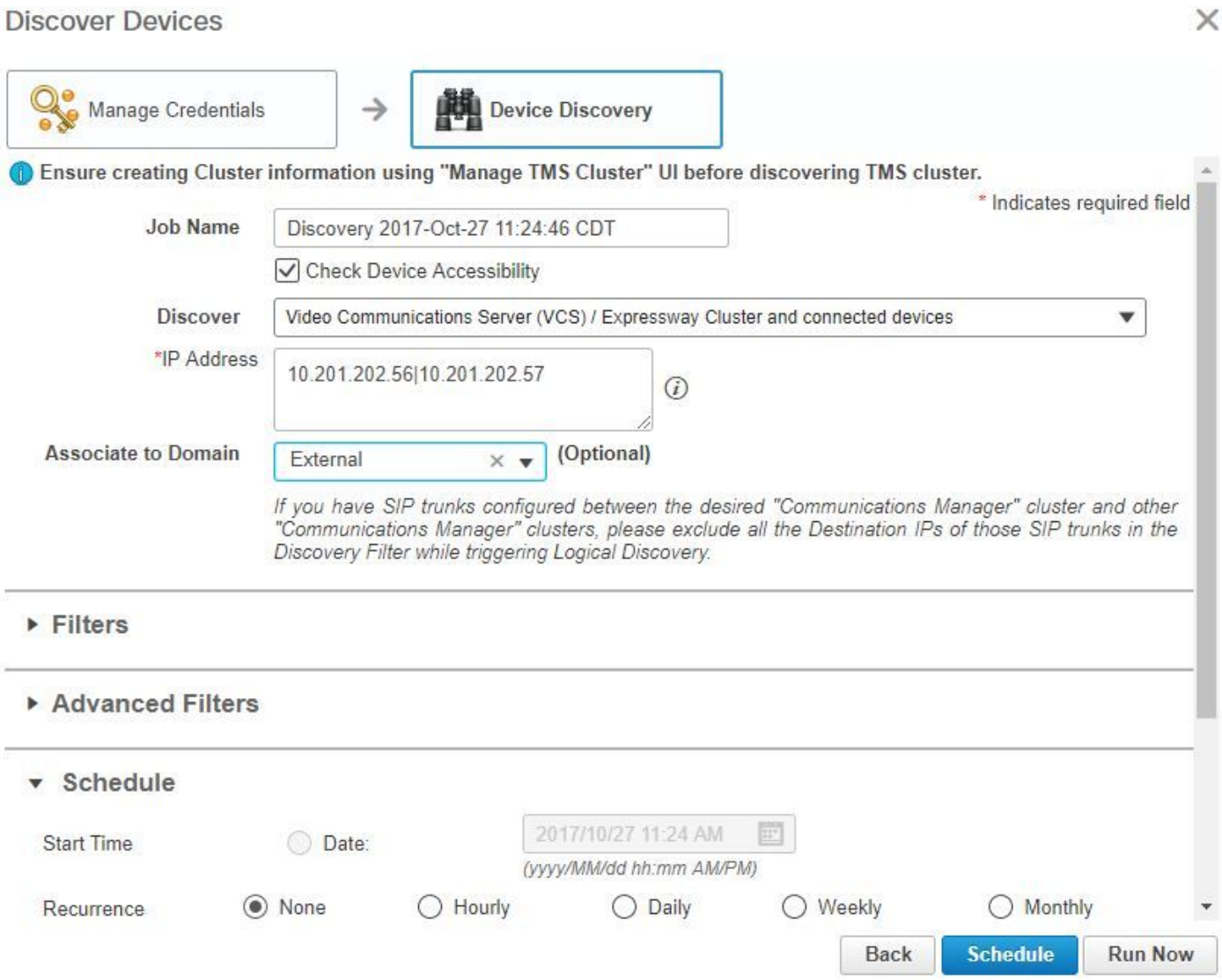
Schritt 1: Stellen Sie sicher, dass die Anmeldeinformationen für die Telepresence Management Suite (TMS) und den Video Communications Server (VCS) verfügbar sind.

> **Hinweis**: Wenn Sie in diesem Szenario Ihr VCS/TMS erkennen, ist der Erkennungsprozess wichtig. Wenn Sie einen Anrufmanager in Ihrer Konfiguration haben, suchen Sie zuerst nach dem Leiter und dann nach dem Cisco Call Manager.

Schritt 2: Navigieren Sie zu **Inventory > Inventory Management > Manage Credentials (Anmeldeinformationen verwalten) >** Wählen Sie **Add** aus, und geben Sie dann die Informationen für Ihr TMS ein. Erstellen Sie gleichzeitig ein separates Anmeldeinformationsprofil für Ihre VCS, wie im Bild gezeigt.



Schritt 3: Wählen Sie nach dem Erstellen des Anmeldeinformationsprofils **Device Discovery (Geräteerkennung)**, geben Sie die **IP-Adressen ein**, und wählen Sie auf der Registerkarte Discovery (Erkennung) **VCS** aus, und ermitteln Sie die VCS-Geräte. Wählen Sie außerdem **TMS** für das TMS aus, und geben Sie die IP-Adresse des TMS ein. Klicken Sie auf **Jetzt ausführen**, wie im Bild gezeigt.

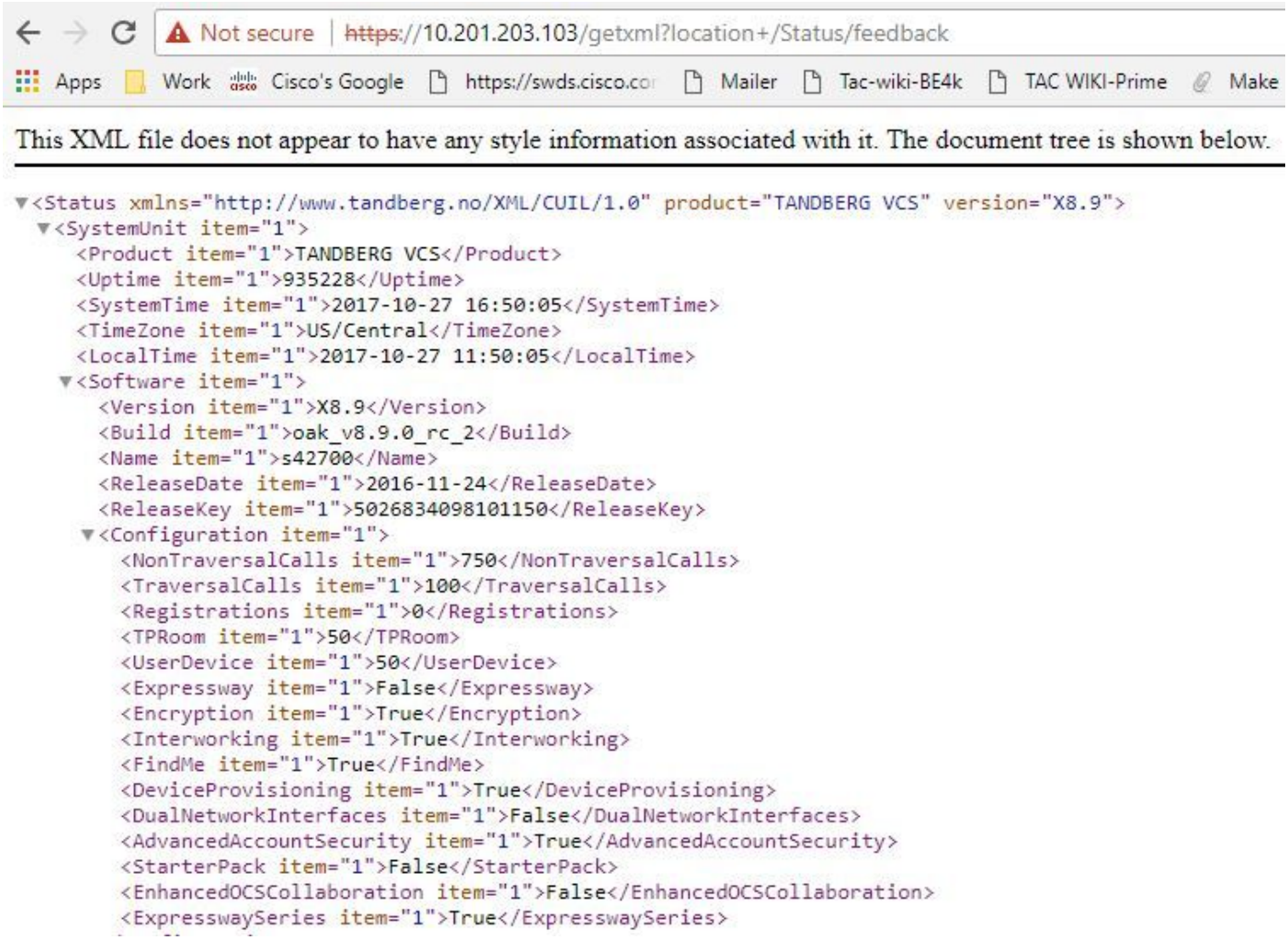


Schritt 4: Vergewissern Sie sich, dass sich VCS und TMS im Managed-Zustand befinden.

Hinweis: Wenn sich der VCS oder das TMS nicht in einem verwalteten Zustand befindet, ist dies meistens auf HTTP oder SNMP zurückzuführen. Wenn weitere Unterstützung erforderlich ist, wird ein TAC-Fall geöffnet, um das VCS/TMS in einen verwalteten Zustand zu versetzen.

Hinweis: Verwenden Sie diese URL, und ersetzen Sie IP_Address_of_VCS_Server durch die entsprechende IP-Adresse, sobald sich der VCS in einem verwalteten Zustand befindet.Der PCA-Server muss als Feedback-Server für VCS registriert werden, sodass bei Beendigung einer Konferenzsitzung kein Problem mit dem Daten-VCS auftritt, der an PCA zurückgesendet wird.

https://<IP_Address_of_VCS_Server>/getxml?location+/Status/Feedback , die http-Anmeldeinformationen werden angefordert, und nach der Eingabe müssen Sie eine Antwort erhalten, wie im Bild gezeigt.



Hinweis: Wenn Prime Collaboration nicht über ein HTTP-Feedback-Abonnement für VCS registriert ist, ist eine Benachrichtigung des VCS nicht erforderlich, wenn ein registrierter Endpunkt eine Sitzung hinzufügt oder verlässt oder sich beim VCS anmeldet oder die Registrierung aufhebt. Stellen Sie in diesem Fall die Sichtbarkeit dieser Endpunkte je nach Bedarf auf vollständig oder begrenzt ein, und stellen Sie sicher, dass sich Ihr VCS in einem Managed-Zustand befindet.

Schritt 5: Navigieren Sie zu **Inventory > Inventory Schedule > Cluster Data Discovery Schedule**, und wählen Sie **Run Now (Jetzt ausführen)**.

Hinweis: Dieser Prozess kann einige Zeit in Anspruch nehmen, da er diese Funktion für alle Infrastrukturgeräte durchführt. Wenn der Vorgang nach einigen Minuten nicht abgeschlossen ist, überprüfen Sie ihn daher nach 1-2 Stunden erneut. Sehr große Systeme können bis zu 4 Stunden dauern. Es ist wichtig, im PCA-Bestand zu erwähnen, ob es Endpunkte gibt, für die Konferenzstatistiken unterstützt werden sollen, und sicherzustellen, dass diese auch für Berichte und alle Statistiken verwaltet werden, um die richtigen Informationen anzuzeigen.

Eine Liste der unterstützten Geräte gemäß PCA in Bezug auf Konferenzen und unsere unterstützten Sitzungen finden Sie im Abschnitt Hintergrundinformationen.

Schritt 6: Navigieren Sie zu **Diagnose > Endpunktdiagnose**.

Um korrekte Statistiken für die Konferenzendpunkte zu erhalten, müssen Sie deren Sichtbarkeit auf die höchstmögliche, vom System erlaubte Ebene einstellen.

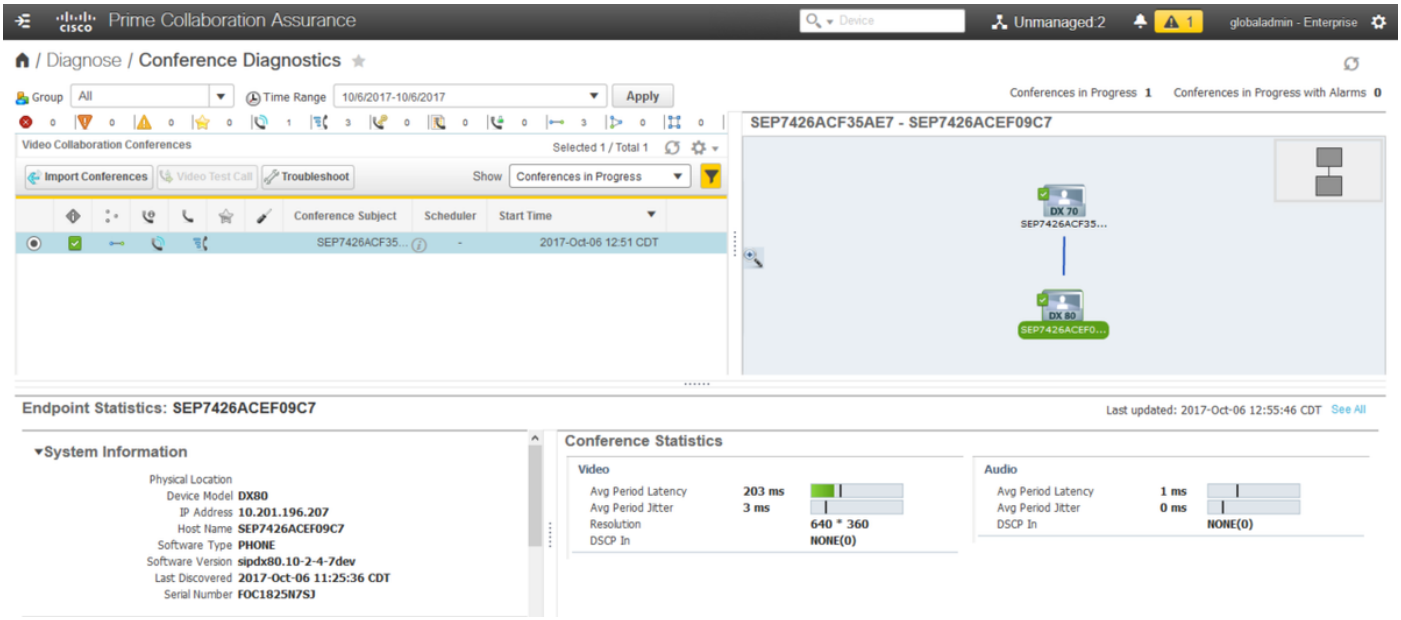
Wählen Sie alle in der Konferenzdiagnose zu überwachenden Endpunkte aus, klicken Sie dann auf **Sichtbarkeit bearbeiten**, und wählen Sie die maximale Sichtbarkeit aus.

The following table lists the default and maximum visibility details for the endpoints:

Endpoint Type	Default Visibility	Maximum Visibility
• CTS 500, 1000, and 3000 Series • Cisco Codec • Cisco TelePresence SX20 • Cisco TelePresence MXP Series • Cisco IP Video Phone E20	Full	Full
• Cisco Jabber Video for TelePresence (Movi) • Polycom	Limited	Limited
Cisco Cius	Off	Full
Cisco IP Phones (89xx, 99xx)	Off	Full
Cisco Desktop Collaboration Experience DX650 and DX630	Off	Full
• Cisco SX80 and Cisco SX10 • • Cisco MX200 G2, Cisco MX300 G2, Cisco MX700, and Cisco MX800	Full	Full
Cisco DX70 and DX80	Off	Full
MRA Endpoints: • Cisco Jabber • Cisco TelePresence MX Series • Cisco TelePresence System EX Series • Cisco TelePresence System SX Series	Limited	Limited

> **Hinweis**: Wenn Sie z. B. 10 Endpunkte auswählen und Full Visibility (Vollständige Transparenz) auswählen, wird die höchste Unterstützung für Transparenz pro Gerät ausgewählt.

Schritt 7: Um zu testen, nSie können **Diagnose > Conference Diagnostics (Diagnose > Konferenzdiagnose)** und eine laufende oder abgeschlossene Konferenz anzeigen, wie im Bild gezeigt.



Auf diesen Konferenzen können Sie den durchschnittlichen Paketverlust, die Latenz und Jitter für Audio- und Videoanrufe anzeigen.

Außerdem erhalten Sie eine Topologie der Sitzung und der beteiligten Geräte.

Konferenzrelevante Alarme

Für die Konferenzdiagnose können Sie drei verschiedene Alarme jeder Sitzung empfangen und deren Schwellenwerte festlegen:

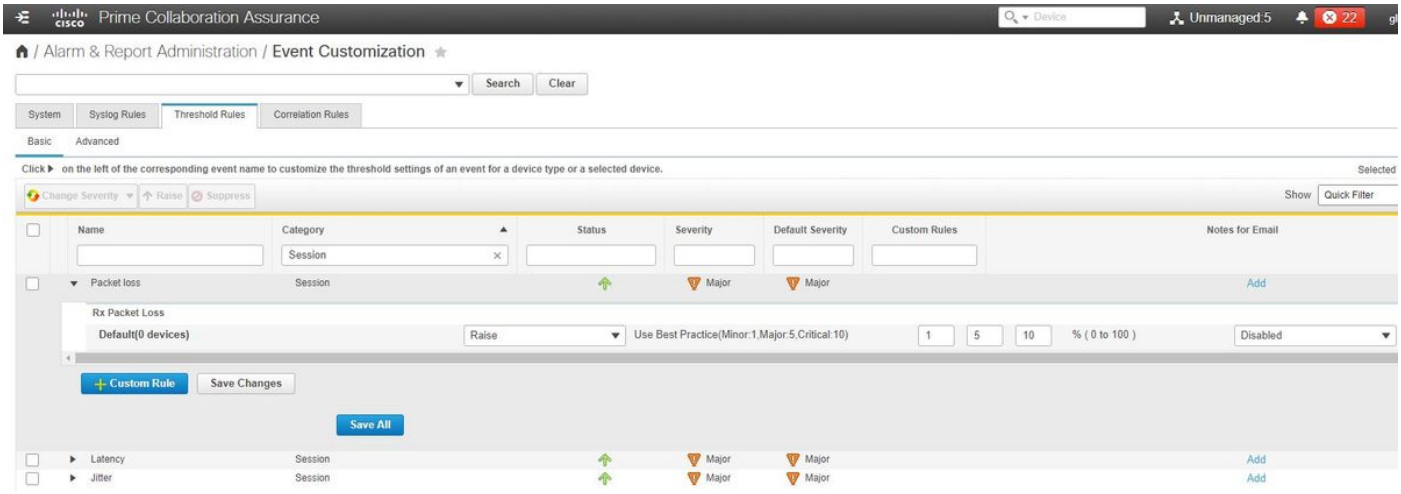
- Paketverlust
- Latenz
- Jitter

Jeder dieser Parameter kann den Standard-Grenzwert ändern, ihn vollständig deaktivieren oder festlegen, welche Geräte diesem Alarm zugeordnet werden sollen.

Schritt 1: Navigieren Sie zu **Alarm & Report Administration > Event Customization**.

Schritt 2: Wählen Sie **Schwellenwertregeln aus**, und stellen Sie sicher, dass **Basic (Grundlegende** Auswahl) ausgewählt ist.

Schritt 3: Blättern Sie nach unten, oder filtern Sie nach rechts, um die Kategorie Sitzung wie im Bild gezeigt anzuzeigen.



Schritt 4: Wählen Sie den Dropdown-Pfeil neben der Erinnerung aus, die Sie ändern möchten, und Sie können die Prozentwerte für kleine, mittlere oder kritische Prozentwerte für Paketverluste, Jitter oder Latenz ändern.

Schritt 5: Wenn Sie sie überdrücken möchten, wechseln Sie auf "Höhen zu Überdrücken".

Schritt 6: Wenn Sie die dem Alarm zugeordneten Endpunkte definieren möchten, wählen Sie Benutzerdefinierte Regel.

Schritt 7: Wählen Sie als Nächstes **Gerätetyp >** Alle **Geräte** oder **wählbare Geräte aus**, die Sie für diesen Alarm auswählen möchten, und klicken Sie auf **Speichern**.

Konferenzrelevante Berichte

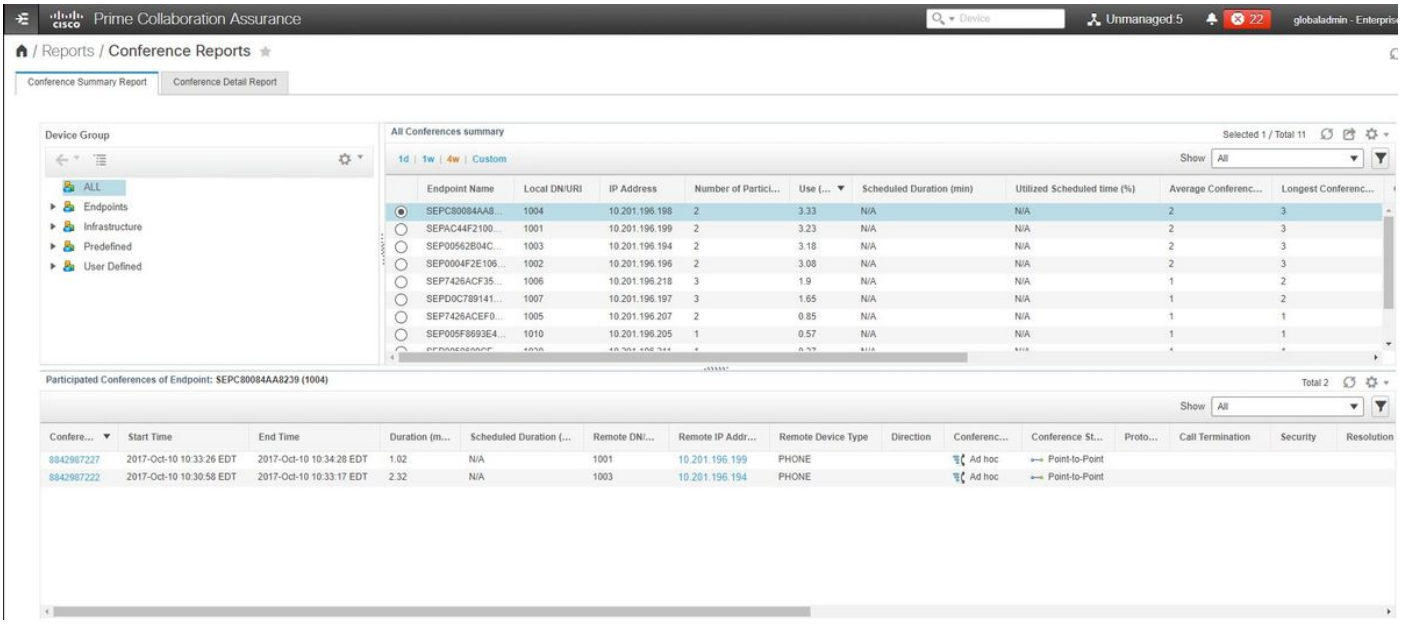
Für die Konferenzdiagnoseberichte können Berichte abgerufen und angezeigt werden.

Es gibt zwei Berichte:

- Konferenzberichte
- TelePresence-Endgeräteberichte

Bei Konferenzberichten können Sie eine Liste aller Konferenzen innerhalb eines Zeitrahmens von einem bis vier Wochen oder nach Bedarf in einem benutzerdefinierten Zeitraum anzeigen.

Schritt 1: Navigieren Sie zu **Bericht > Konferenzberichte,** wie im Bild gezeigt.



Berichte zur Konferenzzusammenfassung

Diese Berichte bieten eine Ansicht aller von Ihnen ausgewählten Endpunkte mit eingeschränkter bzw. vollständiger Transparenz und den zugehörigen Konferenzen.

Hier werden folgende Statistiken angezeigt:

- Durchschnittliche Konferenznutzung
- Konferenzalarme
- Durchschnittlicher Paketverlust, Jitter und Latenz
- Längste Konferenz

So können Sie eine detaillierte Ansicht der Probleme in Ihrem Sprach-/Videonetzwerk erhalten, um festzustellen, welche Endgeräte die meisten Probleme haben.

Nutzen Sie auch die Bandbreite entsprechend der Nutzung.

Registerkarte "Conference Detail Report"

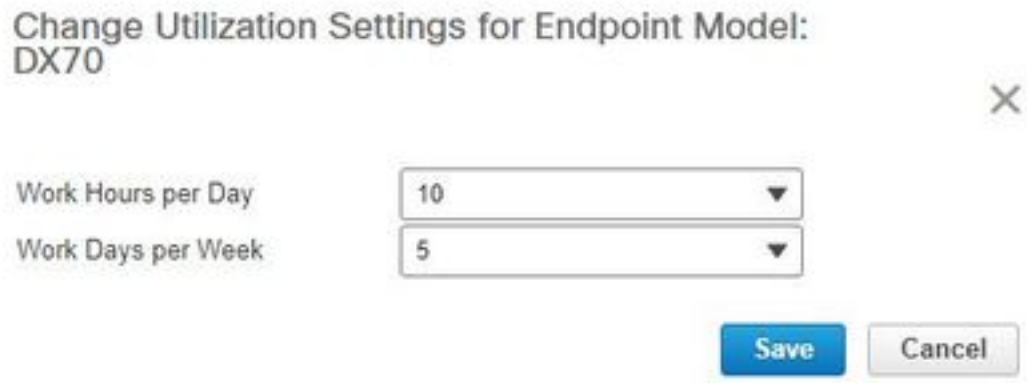
Wenn bei einer Konferenz ein Alarm ausgelöst wird, können Sie zur Registerkarte "Conference Detail Report" (Detailbericht Konferenz) navigieren.

Wenn Sie die Konferenz ausgewählt haben, können Sie den Namen des Endpunkts, die Softwareversion und weitere Details festlegen, die Sie interessieren.

Bei TelePresence-Endgeräteberichten können Sie die

- Anzahl der Konferenzen, die dieses Gerät hatte
- Auslastungsprozentsatz
- Endgerätemodell
- Verwendung

Darüber hinaus können Sie die Utilization Paramaters (Auslastungsparameter) über die Registerkarte Change Utilization (Auslastung ändern) ändern, wie im Bild gezeigt.



Dadurch werden die Parameter für das Gerät festgelegt, sodass das System anhand der Nutzung weiß, welcher Prozentsatz angezeigt werden soll.

Der zusammenfassende Bericht "Endgeräte nicht anzeigen" zeigt die Endpunkte an, die geplante Konferenzen verpasst haben.

In diesem Diagramm können Sie den Endpunkt und die Gesamtzahl geplanter Konferenzen sowie die Anzahl der Konferenzen anzeigen, die stattgefunden haben und bei denen es sich nicht um Shows handelt.

Videokonferenz-Testanruf

Zum Testen Ihres Netzwerks können Sie Videotestanrufe zwischen zwei Videoendpunkten erstellen, die sich in einem verwalteten Zustand befinden. Sie sehen Ereignisse und Alarme, Sitzungsstatistiken, Endpunktstatistiken und Netzwerktopologie. Für diesen Anruf werden nur die Codecs der CTS-, C- und EX-Serie unterstützt.

Darüber hinaus kann mit dieser Funktion überprüft werden, ob alle Funktionen mit der Konferenzdiagnose korrekt sind.

Voraussetzungen

- Diese Funktion wird für die Codec-Serie E20 nicht unterstützt.
- Um dieses Feature zu verwenden, müssen CLI-Anmeldeinformationen für die Endpunkte hinzugefügt werden.
- Stellen Sie sicher, dass die Endpunkte registriert sind und JTAPI für Endpunkte aktiviert ist (wenn sie für Unified CM registriert sind).
- Wenn Sie Cisco Prime Collaboration im MSP-Modus implementiert haben, ist die Funktion für Videotest-Anrufe nicht verfügbar.

Schritt 1: Navigieren Sie zu **Diagnose > Endpunktdiagnose**.

Schritt 2: Wählen Sie je nach den Voraussetzungen zwei geeignete Endpunkte aus.

Schritt 3: Wählen Sie **Tests ausführen > Videotest-Anruf aus**.

Schritt 4: Sie können den Videotest-Anruf so planen, dass er jetzt oder zu einem Wiederholungszeitpunkt ausgeführt wird.

Schritt 5: Dieser Videotest-Anruf wird dann im Bildschirm "Conference Diagnostics" (Konferenzdiagnose) angezeigt.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

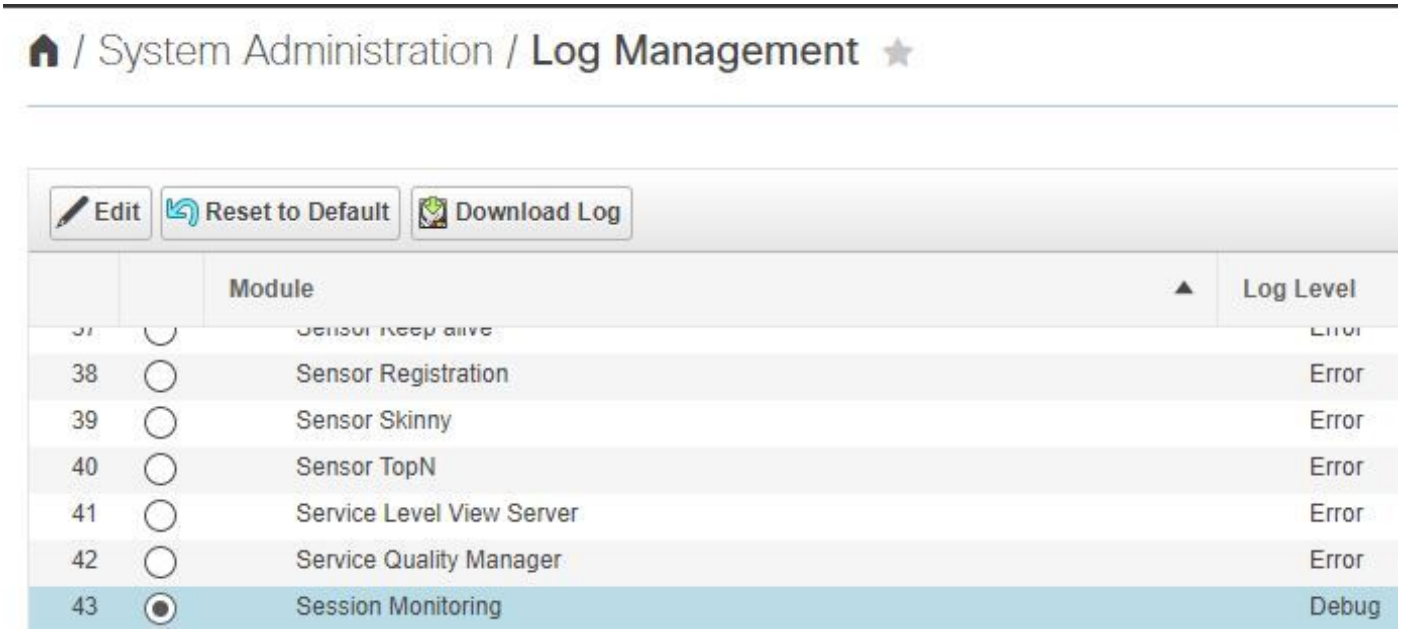
Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Zu sammelnde Protokolle zur Fehlerbehebung

Schritt 1: Navigieren Sie zu **Systemverwaltung > Protokollverwaltung**.

Schritt 2: Blättern Sie nach unten zum Modul, wählen Sie **Sitzungsüberwachung** aus, und wählen Sie **Bearbeiten** aus, wie im Bild gezeigt.



Schritt 3: Ändern Sie die Protokollstufe in debug, und klicken Sie auf **Speichern**.

Schritt 4: Reproduzieren Sie das Problem, und kehren Sie dann zum Bildschirm für die Protokollverwaltung zurück.

Schritt 5: Nachdem Sie das Problem reproduziert haben, wählen Sie **Sitzungsüberwachung** aus, und wählen Sie **Protokoll herunterladen aus**.

Schritt 6: Extrahieren Sie die ZIP-Datei nach dem Download.

Schritt 7: Öffnen Sie die ZIP-Datei, und navigieren Sie zu den Speicherorten für nützliche Protokolle:

/opt/emms/emsam/log/SessionMon/

- CUCMJTAPI.log
- CUCMJTAPIDiag.log

- CSMTracker
- CSMTrackerDiag.log
- CSMTrackerDataSource.log
- PostInitSessionMon.log