Prime Collaboration Assurance (PCA) configureren - vergaderdiagnostiek

Inhoud

Inleiding

Dit document beschrijft hoe u uw implementatie voor Conference Diagnostics binnen Prime Collaboration Assurance (PCA) moet configureren en instellen, om spraaktelefoniestatistieken/videoconferentiestatistieken proactief te controleren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Aanmelden voor Call Manager Admin
- PCA-inloggen
- Uw TelePresence Monitor Server (TMS)
- Core/Express-referenties, indien van toepassing

Gebruikte componenten

De informatie in dit document is gebaseerd op PCA versies 11.x - 12.x.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Cisco Prime Collaboration 11.x ondersteunt deze soorten zichtbaarheid:

- Full Visibility - Call detectie met het gebruik van JTAPI/HTTP-feedback en real-time monitoringinformatie zoals conferentiestatistieken, en conferentieinformatie wordt ondersteund.
- Beperkte zichtbaarheid - Automatische gespreksdetectie met het gebruik van JTAPI/ HTTP-feedback vindt plaats, maar real-time bewakingsinformatie zoals conferentiestatistieken, en conferentieinformatie wordt niet ondersteund. Endpoints met beperkte zichtbaarheid worden aangegeven met een halfverduisterd pictogram in de vergadertopologie.

Cisco Prime Collaboration 12.x ondersteunt deze soorten zichtbaarheid:

- Full Visibility - Call detectie met het gebruik van JTAPI/HTTP-feedback en real-time monitoringinformatie zoals conferentiestatistieken, en conferentieinformatie wordt ondersteund.
- Geen zichtbaarheid - gespreksdetectie met het gebruik van JTAPI/ HTTP-feedback en real-time bewakingsinformatie worden niet ondersteund. Deze eindpunten worden weergegeven op de pagina Conference Monitoring met een volledig beeld.

Beperking van endpoints ingesteld op beperkte of volledige zichtbaarheid per OVA

- Small Open Virtualization Archief (OVA) ondersteunt maximaal 500 endpoints
- Medium-OVA ondersteunt maximaal 1000 endpoints
- Grote OVA-ondersteuning tot 1800 endpoints
- Zeer grote OVA-ondersteuning tot 2000 endpoints

Een lijst van de ondersteunde apparatuur per partnerschaps- en samenwerkingsovereenkomst voor conferenties en onze ondersteunde sessies is te zien in de tabel hier.

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.

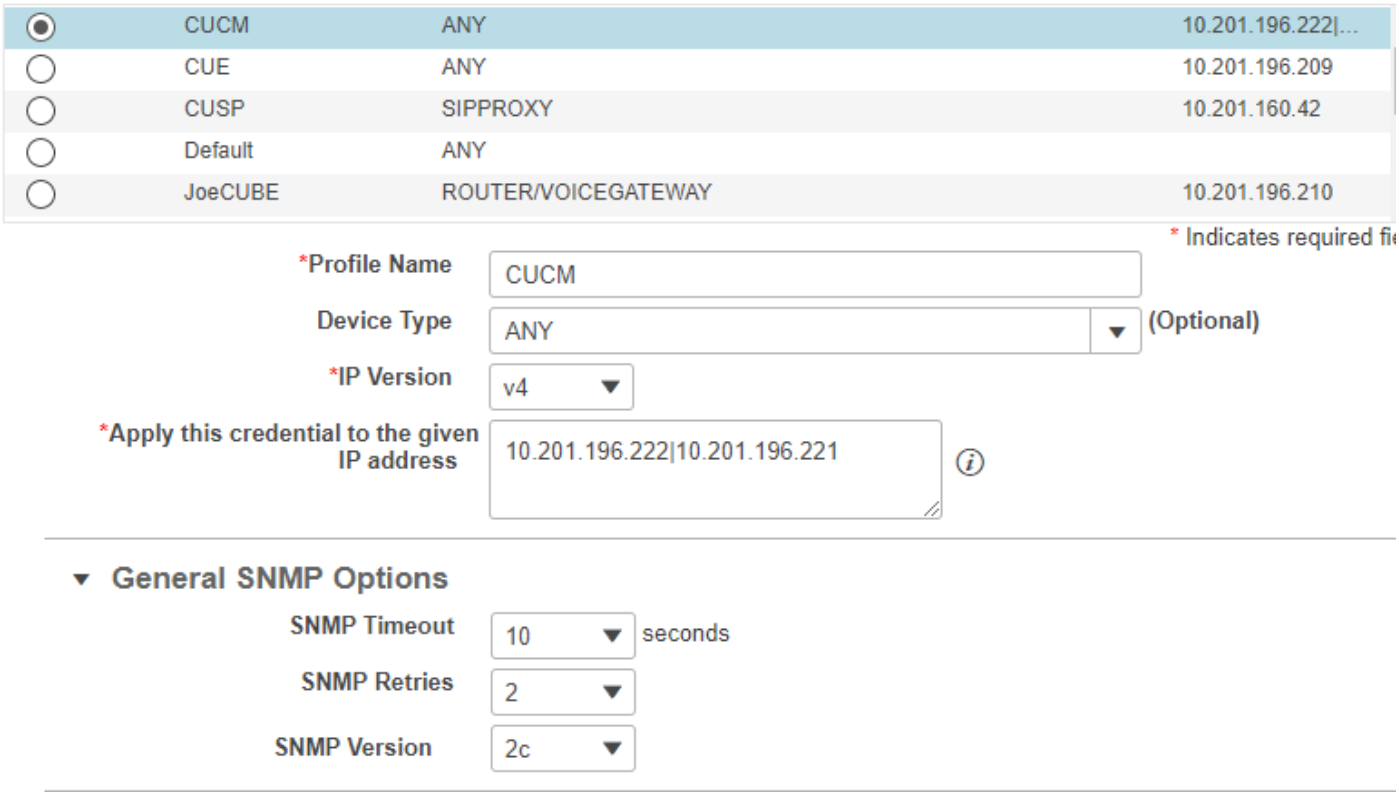
Configureren

Scenario 1. Conferentie met video-endpoints die zijn geregistreerd in Call Manager

Stap 1. Eerst moet u ervoor zorgen dat de Call Managers in een beheerde staat zijn.

navigeren naar **inventaris > Voorraadbeheer > Credentials beheren > Een profiel maken** voor de Call Manager cluster.

> Opmerking: Onthoud dat elk gecrediteerd profiel dezelfde geloofsbrieven gebruikt voor elke ip die binnen het profiel wordt vermeld. Dus als u een lijst maakt van de Uitgever en de Subscriber van Call Manager binnen hetzelfde Credentials Profile, gebruikt het deze zelfde geloofsbrieven om beide ip adressen te ontdekken. Als u geen dirigent in uw opstelling hebt, ontdekt u de dirigent eerst en dan Cisco Call Manager zoals in de afbeelding.



Stap 2. Zorg ervoor dat u Hypertext Transfer Protocol (HTTP), Simple Name Management Protocol (SNMP) en Java Telephony API (JTAPI)-aanmeldingsgegevens hebt ingevoerd

Daarnaast moet u de Cisco Computer Telephony Integration (CTI) Service in Call Manager Services inschakelen.

Installatie van Cisco Unified Communications Manager

HTTP inschakelen

U hoeft geen nieuwe gebruiker te maken als u Cisco Prime Collaboration-applicaties wilt gebruiken om admin-aanmeldingsgegevens te gebruiken. In plaats hiervan moet u, als u Cisco Prime Collaboration Manager wilt toestaan om de juiste aanmeldingsgegevens te gebruiken om in Cisco Unified Communications Manager te loggen, een nieuwe HTTP-gebruikersgroep en een correspondent-gebruiker maken die Cisco Prime Collaboration kan gebruiken om te communiceren.

Volg deze stappen om een gebruiker te maken:

Stap 1. Meld u aan bij de Cisco Unified CM-beheerwebinterface met uw beheeraccount.

Stap 2. Maak een gebruikersgroep met voldoende rechten. Navigeer naar **gebruikersbeheer>Gebruikersinstellingen>Toegangsbeheer** Groepering en maak een nieuwe gebruikersgroep met een geschikte naam, **PC_HTTP_Gebruikers** in dit geval. **Selecteer** nu **Opslaan**.

Stap 3. Navigeer naar **gebruikersbeheer>Gebruikersinstellingen>Toegangscontrolegroep** en **selecteer** Zoeken. Vind de groep die u hebt gedefinieerd en klik op het pictogram rechts.

Stap 4. **Selecteer** Rol **toewijzen** aan Groepering en selecteer deze rollen:

- Standaard AXL API-toegang
- Standaard CCM-beheergebruikers
- Standaard SERVICEABILITEITSBEHEER

Stap 5. Klik op **Opslaan**.

Stap 6. Klik in het hoofdmenu op **Gebruikersbeheer>Toepassingsgebruikers>Een nieuwe gebruiker maken**.

Specificeer een geschikt wachtwoord op **de** pagina **Application User** Configuration. U kunt alleen bepaalde typen apparaten uit het tekstgebied Beschikbare apparaten selecteren of u kunt Cisco Prime Collaboration-software toestaan om alle apparaten te controleren

Stap 7. In **het gedeelte** Informatie over **toegangsrechten**, **selecteert uAdd to User** Groepering en selecteert u de groep die in Stap 1 is gemaakt. (bijvoorbeeld PC_HTTP_Gebruikers).

Stap 8. **Klik op Opslaan**. De pagina is ververst en de juiste privileges worden weergegeven.

SNMP activeren

SNMP is niet standaard ingeschakeld in Cisco Unified Communications Manager.

Zo schakelt u SNMP in:

Stap 1. Meld u aan bij **de** weergave **van Cisco Unified** Services in de Cisco Unified Communications Manager-webGUI.

Stap 2. Navigeer naar **Gereedschappen > Serviceactivering**.

Stap 3. Selecteer **Uitgeverij**.

Stap 4. Navigeer naar **Performance > Monitoring Services en selecteer het aankruisvakje voor Cisco Call Manager SNMP Service.**

Stap 5. Selecteer **Opslaan** onder in het scherm.

Zo maakt u een SNMP-community-string:

Stap 1. Meld u aan bij **de Cisco Unified** Services **en** bekijkt de Cisco Unified Communications Manager-webGUI.

Stap 2. Klik in het hoofdmenu van de Cisco Unified Services-weergave op **SNMP > v1/v2c > Community-string**.

Stap 3. Selecteer een server en **klik op Zoeken**.
Als de community-string al is gedefinieerd, wordt de Community String Name in de Search Results weergegeven.

Stap 4. **Klik op** Add newto om een nieuwe string toe te voegen als er geen resultaten worden weergegeven.

Stap 5. Specificeer de gewenste SNMP-informatie en slaat de configuratie op.

Opmerking: Alleen SNMP-Lezen (RO) is nodig.

Start CTI-service

Voer de procedure uit voor het Cisco Unified Communications Manager-knooppunt dat u wilt, is het beter om deze op twee knooppunten in te stellen.

Stap 1. Meld u aan bij Cisco Unified Services, gezien in de grafische gebruikersinterface van Cisco Unified Communications Manager.

Stap 2. Navigeer naar Gereedschappen > Serviceactivering.

Stap 3. Selecteer een server in de vervolgkeuzelijst.

Stap 4. Controleer het aankruisvakje Cisco CTI Manager in het gedeelte CM-services.

Stap 5. Selecteer Opslaan bovenop het scherm

Toepassingsgebruiker maken voor PCA CTI-controle (JTAPI-gebruiker)

JTAPI wordt gebruikt om de informatie over de sessiestatus van het apparaat te herstellen. U moet een Application gebruiker voor CTI Control in de telefoonprocessor maken met de vereiste toestemming om JTAPI-gebeurtenissen op endpoints te ontvangen. Prime Collaboration beheert meerdere clusters van gespreksprocessors. U moet ervoor zorgen dat de cluster-ID's uniek zijn. Maak een nieuwe toepassingsgebruiker om Cisco Prime Collaboration te helpen de benodigde informatie te verkrijgen.

Om een nieuwe JTAPI-toepassingsgebruiker te maken, volgt u deze stappen:

Stap 1. Meld u aan bij de Cisco Unified CM-beheerwebinterface via uw beheeraccount.

Stap 2. Maak een gebruikersgroep met voldoende rechten. Navigeer naar gebruikersbeheer>Gebruikersinstellingen>Toegangsbeheer Groepering en maak een nieuwe gebruikersgroep met een geschikte naam, PC_HTTP_Gebruikers in dit geval. Selecteer nu Opslaan.

Stap 3. Kies Gebruikersbeheer>Gebruikersinstellingen>Toegangscontrolegroep en klik op Zoeken. Vind de groep die u hebt gedefinieerd en selecteer het pictogram aan de rechterkant.

Stap 4. Klik op Rol toewijzen aan Groepering en selecteer deze rollen:

- Standaard CTI toestaan van gespreksbewaking
- Standaard CTI-enabled
- Standaard CTI voor controle van telefoons die aangesloten Xfer en conf ondersteunen

Stap 5. Selecteer Opslaan.

Stap 6. Klik in het hoofdmenu op Gebruikersbeheer>Toepassingsgebruikers>Een nieuwe gebruiker maken.
Specificeer een geschikt wachtwoord op de pagina Application User Configuration. U kunt bepaalde typen apparaten uit het tekstgebied Beschikbare apparaten selecteren of u kunt Cisco Prime Collaboration toestaan om alle apparaten te controleren.

Opmerking: Het wachtwoord mag geen puntkomma (;) of gelijken (=) bevatten.

Stap 7. In **het gedeelte** Informatie over **toegangsrechten** selecteert u **Add to Access Control** Group en selecteert u de groep die in Stap 1 is gemaakt. (bijvoorbeeld PC_HTTP_Gebruikers).

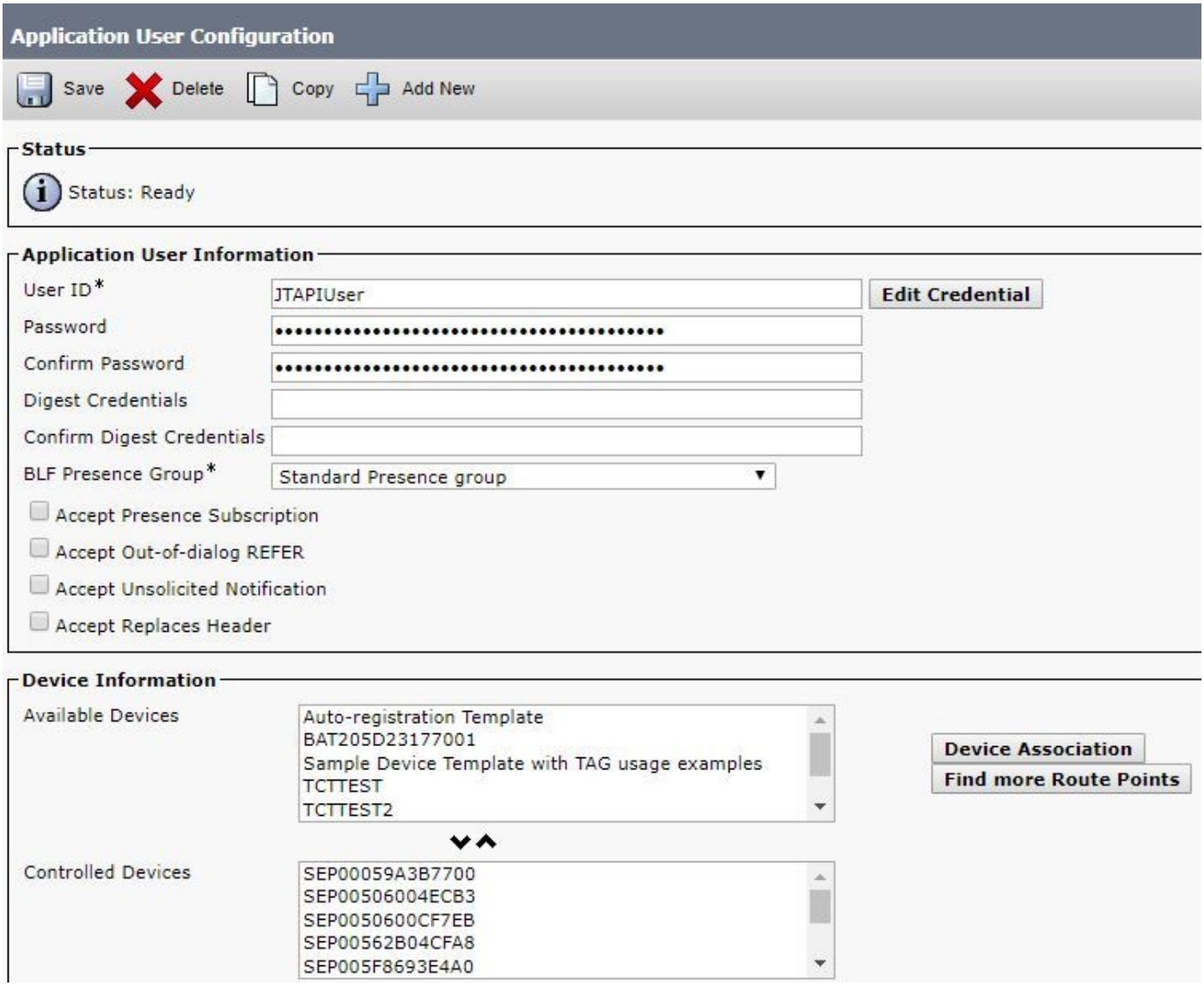
Stap 8. **Klik op Opslaan**. De pagina is ververst en de juiste privileges worden weergegeven.

Opmerking: Als de Call Manager is beheerd voordat u de JTAPI-gebruiker toevoegt, zorg er dan voor dat de JTAPI-gebruiker in het Credentials profiel voor de Call Manager wordt toegevoegd en herhaal het.

Vervolg op Scenario 1. Stappen:

Stap 3. Navigeer naar de Call Manager JTAIP-toepassingsgebruiker die u hebt gemaakt, en verplaats de ondersteunde endpoints van Beschikbare apparaten naar gecontroleerde apparaten.

U kunt dit uitvoeren door de functie Apparaatassociatie uit te voeren zoals in de afbeelding wordt weergegeven.

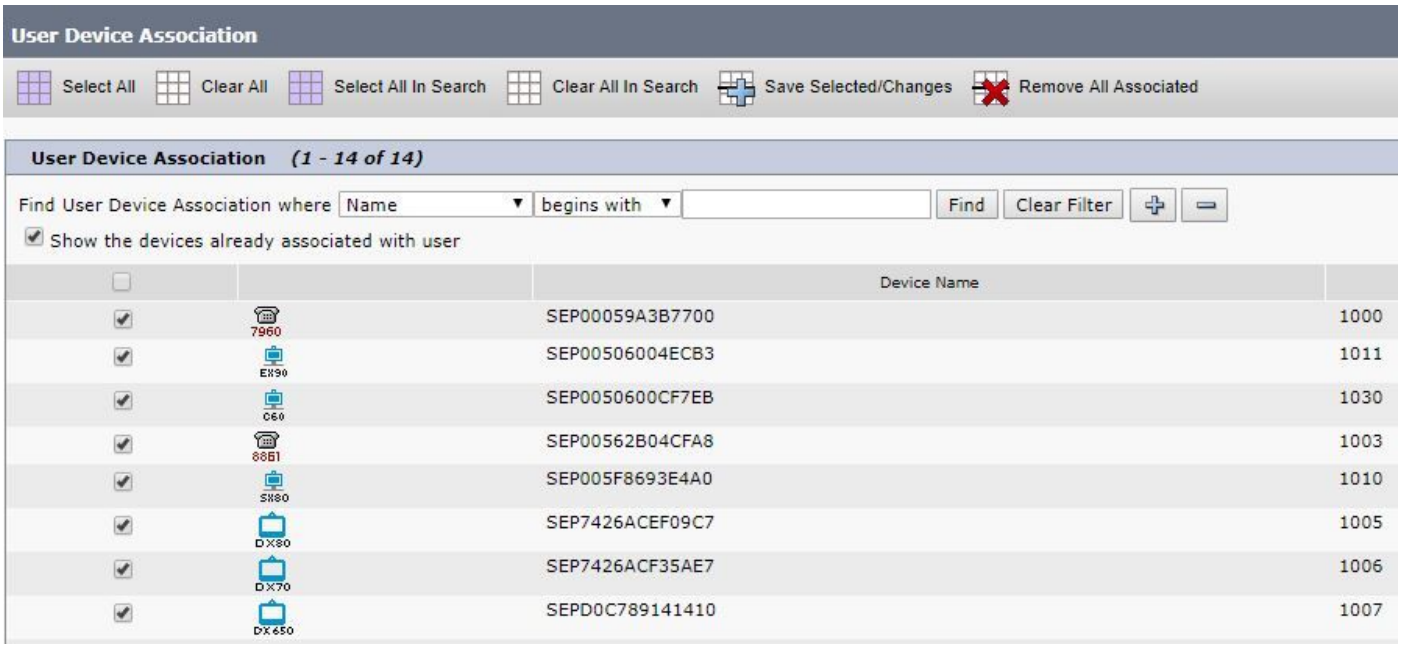


Als u terugverwijst naar de beperking van de reeks-endpoints op de beperkte of volledige

zichtbaarheid per OVA, kunt u controleren hoeveel apparaten u aan de OVA-grootte hebt toegevoegd.

Binnen dit scherm kunt u door Apparaatnaam, Beschrijving of Map Nummer filteren om u te helpen deze apparaten te beheren en te filteren zoals in de afbeelding.

Het is handig om deze apparaten op te merken zoals ze in stap 7 zijn toegevoegd.

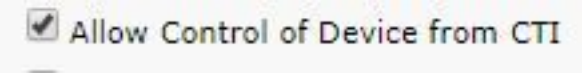


Zorg ervoor dat ook de juiste gebruikersrollen zijn toegevoegd voor deze JTAPI-gebruiker:

- Standaard CTI toestaan van gespreksbewaking
- Standaard CTI-enabled
- Standaard CTI voor controle van telefoons die Connected Xfer en conf ondersteunen zoals in de afbeelding.

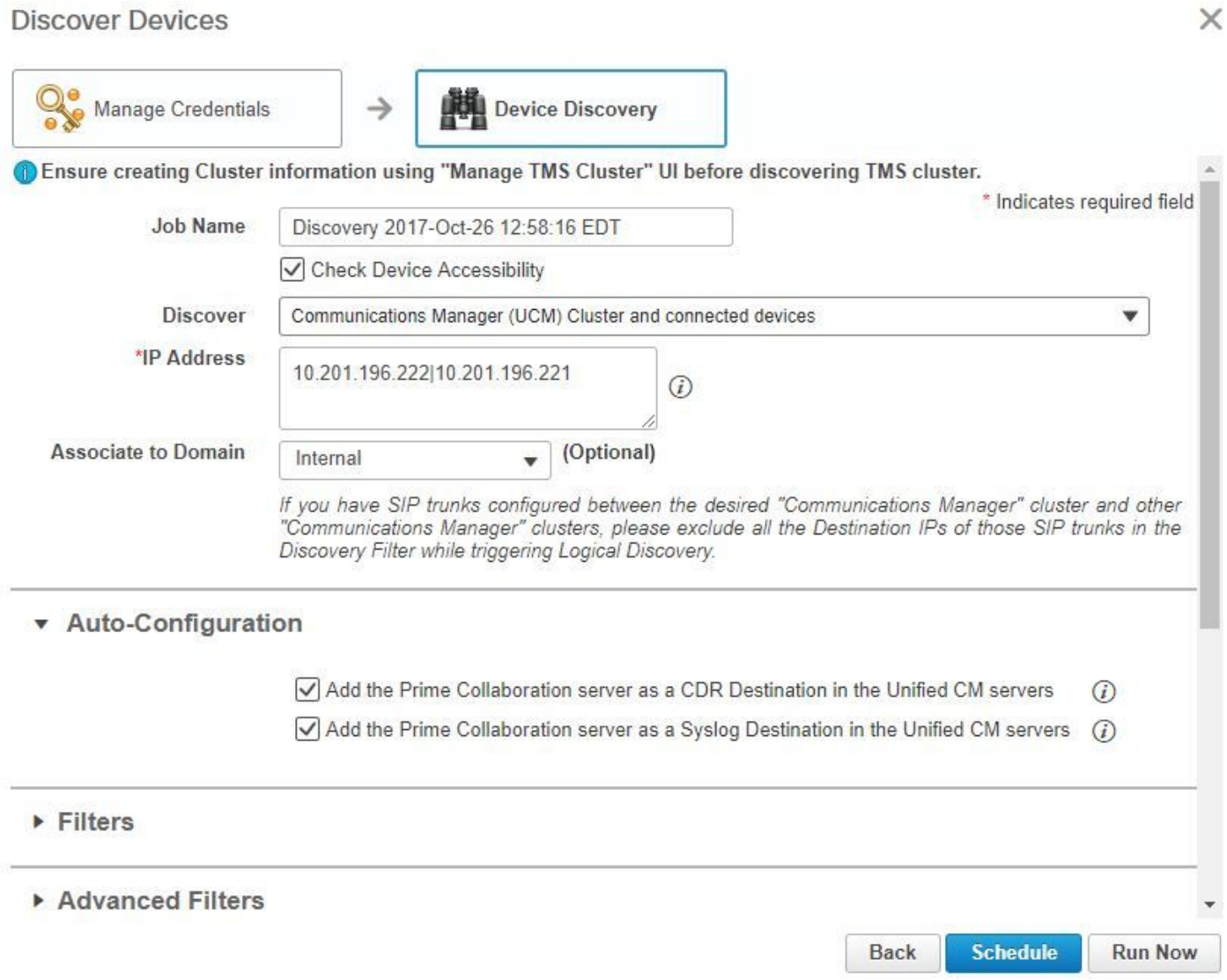
Voor een lijst van ondersteunde apparatuur per partnerschaps- en samenwerkingsovereenkomst, met betrekking tot conferenties en onze ondersteunde sessies, wordt verwezen naar de afdeling Achtergrondinformatie.

> Opmerking: Zorg er bovendien voor dat de apparaten die door de CTI-toepassingsgebruiker worden gecontroleerd het aankruisvakje voor toegangscontrole van het apparaat van CTI hebben ingeschakeld onder de informatie van het apparaat zoals in de afbeelding wordt getoond.



Opmerking: Het is belangrijk om nota te nemen alvorens u te werk gaat dat als u de endpoints hebt die zijn geregistreerd om Call Manager te bellen en Call Manager is geïntegreerd met VCS/TMS, dan ontdekt u eerst uw VCS/TMS en ontdekt dan laatst uw Call Manager. Deze manier vanuit het inventarisperspectief, is al uw infrastructuur in kaart gebracht aan de juiste plaats. Wanneer u de VCS/TMS ontdekt, dient u bovendien het tabblad Default Discovery in te stellen op het betreffende apparaat van TMS/VCS of Call Manager.

Stap 4. Selecteer vervolgens in PCA de optie **Apparaatdetectie** en -invoer in de IP-adressen van uw gespreksbeheer, selecteer de twee vinkjes in **Auto-configuratie** en selecteer **Nu uitvoeren** zoals in de afbeelding.



Stap 5. Nadat de Call Manager in een beheerde staat is, gaat u naar Stap 6.

Opmerking: Als de Call Manager niet in een beheerde staat is, is deze meestal te wijten aan HTTP of SNMP als verdere assistentie nodig is om een TAC-case te openen om de Call Manager in een beheerde staat te krijgen.

Stap 6. Navigeer naar **inventaris > Tijdschema > Cluster Data Discovery Schedule** en selecteer **nu uitvoeren**.

> Opmerking: Dit is afhankelijk van het aantal geregistreerde/niet-geregistreerde apparaten dat u hebt. Dit proces kan van een paar minuten tot een paar uur duren. Controleer de gehele dag door deze pagina te verfrissen. Bovendien, brengt dit uw cluster van de Call Manager samen in kaart en wint al uw eindpunten terug. Nadat dit volledig is, ga naar de volgende stap.

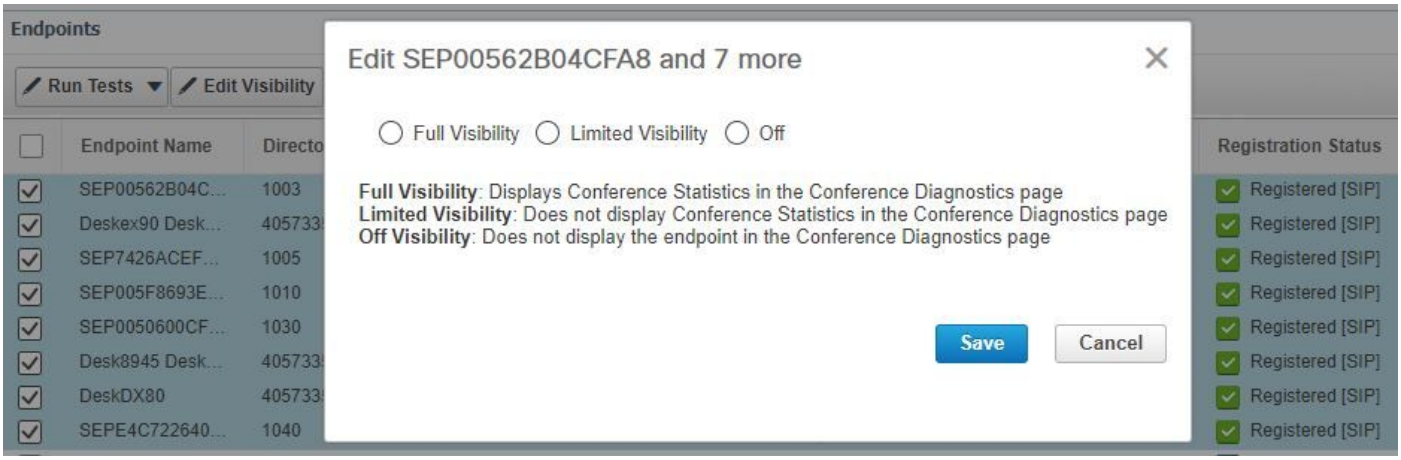
> Opmerking: Het is belangrijk om in de partnerschaps- en samenwerkingsovereenkomst te vermelden als er eindpunten zijn waar u conferentiestatistieken wilt hebben die worden ondersteund. Zorg ervoor dat deze goed worden beheerd voor verslagen en alle statistieken om de juiste informatie te tonen.

Stap 7. Navigeer naar **Diagnose > Endpoint Diagnostics**.

Om bijgewerkte statistieken te verkrijgen voor uw conferentie eindpunten moet u hun zichtbaarheid op het hoogst mogelijke niveau instellen dat door het systeem wordt toegestaan.

Selecteer alle endpoints die u in het programma Conferencing wilt controleren en klik vervolgens op **Visibility** bewerken en selecteer vervolgens **Full Visibility** zoals in de afbeelding.

Beperkte zichtbaarheid toont het apparaat alleen binnen de topologie maar geen statistieken en het is niet in staat om toepasbare alarmen op te halen voor die apparatuur die verband houdt met Conference Diagnostics.

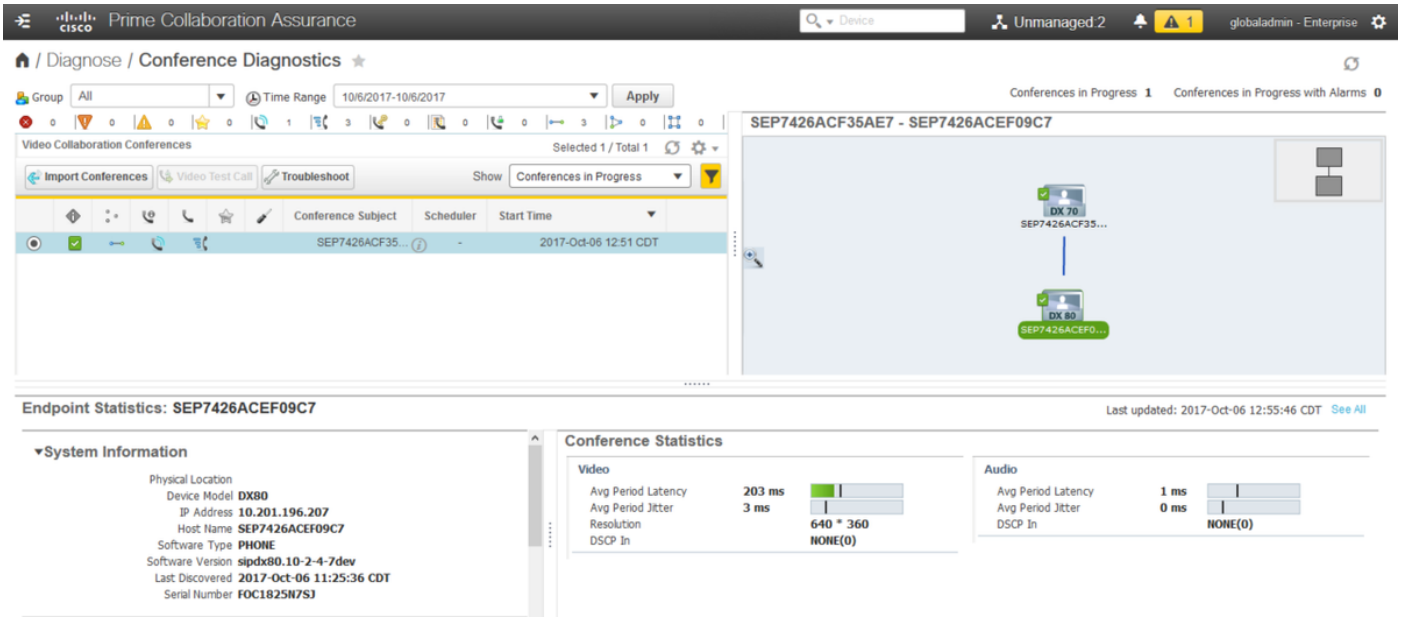


The following table lists the default and maximum visibility details for the endpoints:

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

Opmerking: Als u bijvoorbeeld 10 eindpunten selecteert en Full Visibility and (Volledig zichtbaarheid) selecteert, wordt het hoogste niveau van de zichtbaarheidsondersteuning per apparaat geselecteerd.

Stap 8. Om te testen, navigeer naar **Diagnose > Conference Diagnostics** en een conferentie in uitvoering of voltooid shows, zoals in de afbeelding.



Binnen deze conferenties kunt u het gemiddelde pakketverlies, de latentie en de Jitter voor audio en video gesprekken bekijken.

Zorg ook voor een topologie van de sessie en de betrokken apparaten.

Op dit moment onthult de Conference Diagnostics de informatie die is gebaseerd op DNA en als je milieu DNA's heeft gedeeld, haalt PCA de eerste die ze voor de conferentie ontvangt.

Verwante alarmen voor conferenties

Voor Conference Diagnostics kunt u drie verschillende alarmen voor elke sessie ontvangen en hun drempels instellen:

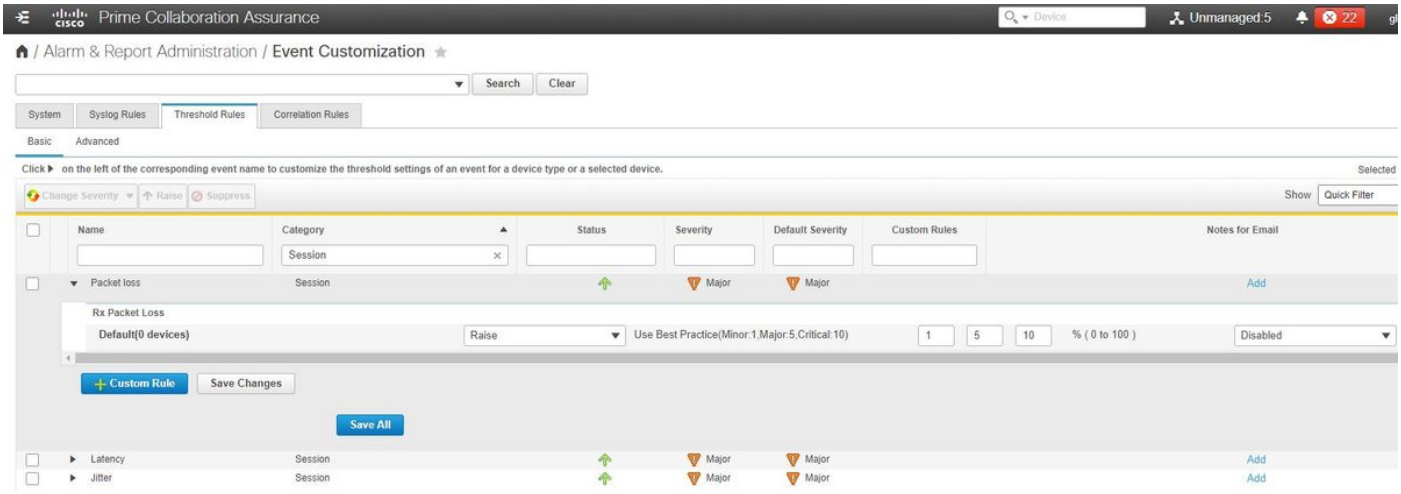
- Packet Loss
- Latentie
- Jitter

Voor elk van deze, kunt u de standaarddrempel wijzigen, deze onderdrukken of bepalen welke apparaten u aan dit alarm wilt koppelen.

Stap 1. Navigeer naar **Alarm & Report Administratie > Aanpassing van gebeurtenissen**.

Stap 2. Selecteer **Drempelregels** en controleer of u **basisregels** hebt geselecteerd.

Stap 3. Scrolt of filter naar rechts voor de categorie Benoemde sessie zoals in de afbeelding.



Stap 4. Selecteer de vervolgkeuzelijst naast het alarm. U wilt de mindere, grote of kritieke percentages voor pakketverlies, Jitter of Latency wijzigen en kunt u deze wijzigen.

Stap 5. Als u wilt surfen, schakelt u de hoogte in overdrukken.

Stap 6. Als u de eindpunten wilt definiëren die aan het alarm zijn gekoppeld, kunt u Aangepaste regel selecteren.

Stap 7. Selecteer vervolgens het **apparaattype > Alle apparaten** of **selecteerbare apparaten** die u voor dit alarm wilt selecteren en klik op **Opslaan**.

Verwante verslagen van de conferentie

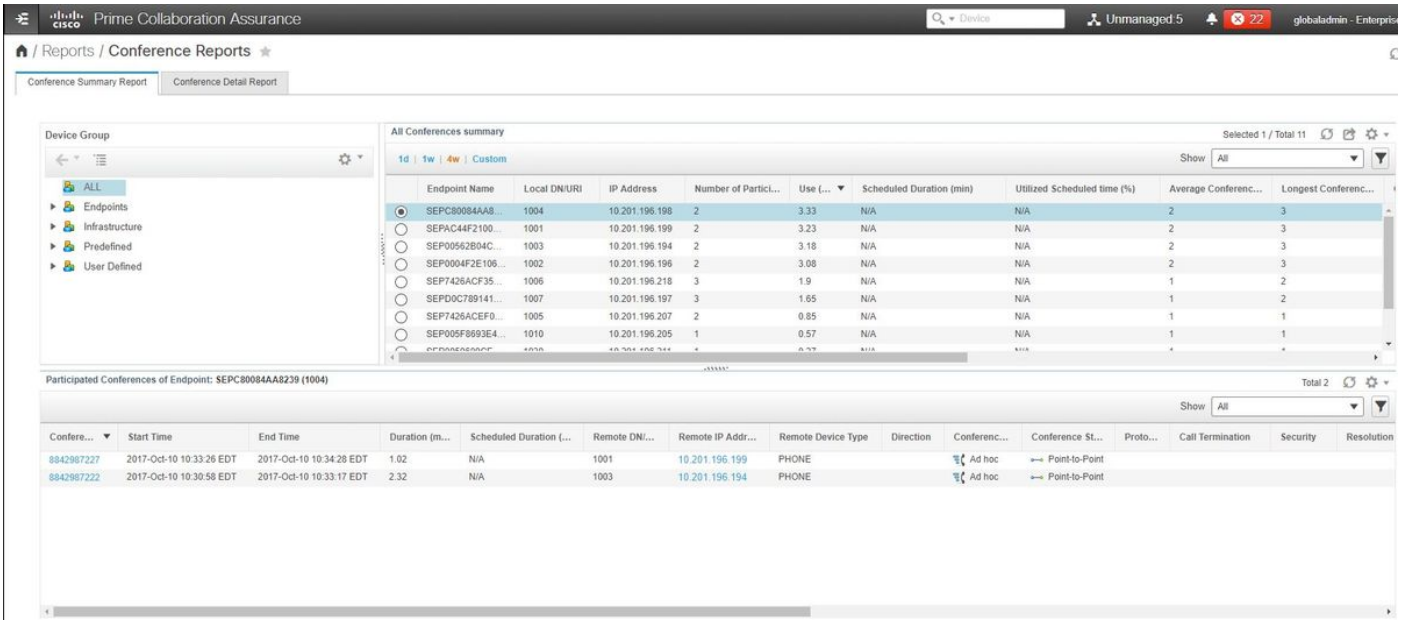
Voor de Conference Diagnostics kunnen rapporten worden opgezocht en bekeken.

Er zijn twee rapporten:

- Conferentieverslagen
- TelePresence-endpointrapporten

Voor vergaderverslagen kunt u een lijst van alle conferenties binnen een tijdsbestek van één tot vier weken of een aangepaste periode bekijken zoals nodig is.

Stap 1. Navigeer naar **Rapporten > Conferentieverslagen** zoals in de afbeelding.



Rapport van de conferentie

Dit rapport biedt een overzicht van elk eindpunt dat u als beperkt/volledig zicht en hun conferenties hebt geselecteerd.

De hier getoonde statistieken zijn:

- Gemiddelde conferentiegebruik
- Zorgen in verband met de conferentie
- Gemiddeld pakketverlies, Jitter en Latentie
- Langste conferentie

Dit kan u helpen een granulaire weergave te realiseren van onderwerpen waar u binnen uw spraak/video-netwerk kunt klikken om te bepalen welke endpoints de meeste problemen hebben.

U kunt ook uw bandbreedte gebruiken in overeenstemming per gebruik.

Tabblad Conference Detail-rapport

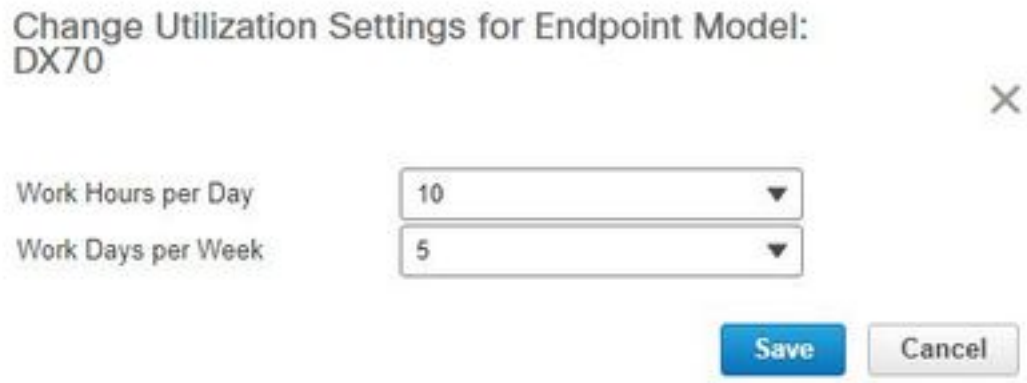
Als u een alarm voor een conferentie tegenkomt kunt u naar het tabblad **Rapport** van de **Conferentie** navigeren.

Nadat u de Conferentie hebt geselecteerd, kunt u deze verfijnen om de naam van het Endpoint, de softwareversie en andere details te vinden waarin u mogelijk geïnteresseerd bent.

Voor TelePresence Endpoint Rapporten kunt u per eindpunt de volgende informatie bekijken:

- Aantal conferenties die dit apparaat had
- Gebruikerspercentage
- Endpoint model
- Gebruik

Daarnaast kunt u de Utilization-parameters wijzigen in het tabblad **Change Utilization** zoals in de afbeelding.



Dit stelt de parameters voor dat apparaat in zodat het systeem van het gebruik weet welk percentage te tonen is.

Het rapport No Show Endpoint toont de endpoints die geplande conferencing hadden gemist.

Binnen deze grafiek, kunt u ook het Eindpunt en hoeveel Totaal Geplande Conferenties en hoeveel van deze voorkwamen en geen shows waren.

Conference Video Test Call

U kunt point-to-point videotestoproepen tussen twee video-endpoints in beheerde toestand maken om uw netwerk te testen. U kunt gebeurtenissen en alarmen, sessiestatistieken, eindpuntstatistieken en netwerktopologie met statistieken zoals andere vraag zien. Alleen de CTS-, C- en EX-series worden voor deze oproep ondersteund.

Daarnaast kan dit worden gebruikt om alles te valideren functioneert met de diagnostiek van conferenties.

Voorwaarden

- Deze optie wordt niet ondersteund voor de E20-codec-serie.
- Om deze optie te gebruiken, moeten CLI-referenties voor de eindpunten worden toegevoegd.
- Zorg ervoor dat de endpoints worden geregistreerd en JTAPI is ingeschakeld voor endpoints (als deze zijn geregistreerd op Unified CM).
- De functie Video Test Call is niet beschikbaar als u Cisco Prime Collaboration-software in MSP-modus hebt uitgevoerd.

Stap 1. Navigeer naar **Diagnose > Endpoint Diagnostics**.

Stap 2. Selecteer twee toepasbare eindpunten in overeenstemming met de vermelde voorwaarden.

Stap 3. Selecteer **Start tests > Video Test Call**.

Stap 4. U kunt de Video Test Call plannen om nu of op een herhalingsschema te starten.

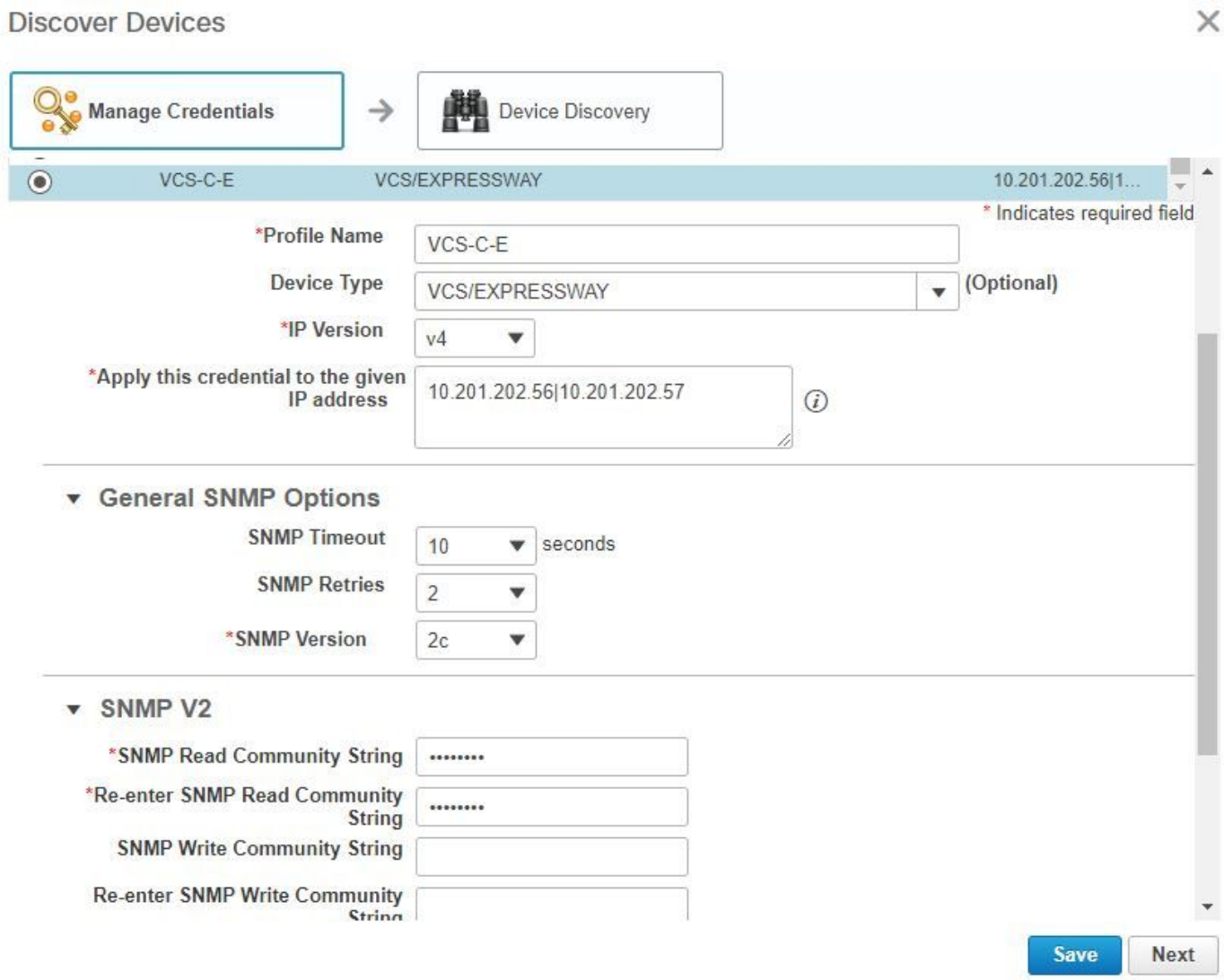
Stap 5. Deze Video Test Call toont vervolgens in het Scherm voor Conferentie van diagnostiek.

Scenario 2. Conferentie met geregistreerde endpoints voor niet Call Manager

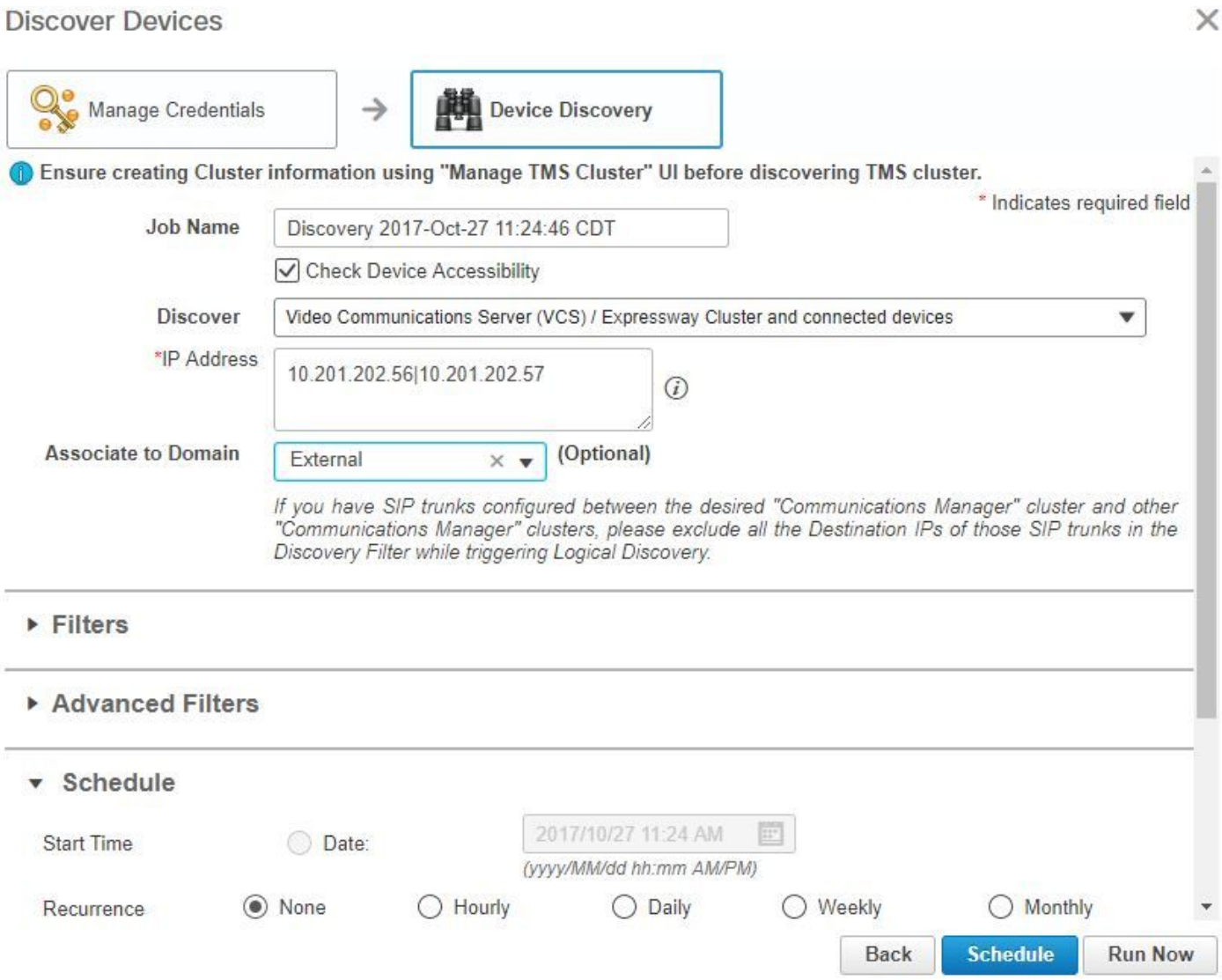
Stap 1. Zorg ervoor dat de aanmeldingsgegevens van TelePresence Management Suite (TMS) en Video Communications Server(s) (VCS) beschikbaar zijn.

> Opmerking: Wanneer u in dit scenario uw VCS/TMS ontdekt, is het zoekproces belangrijk. Als u een Call Manager in uw opstelling hebt, ontdek eerst de geleider en dan Cisco Call Manager.

Stap 2. Navigeer naar **inventaris > Voorzieningsbeheer > Credentials beheren >** Selecteer **Add** en voer vervolgens de informatie voor uw TMS in terwijl u een afzonderlijk geloofwaardig profiel voor uw VCS zoals in de afbeelding maakt.



Stap 3. Zodra het crediteurenprofiel is gecreëerd, selecteert u **Apparaatdetectie**, voert u de **IP-adressen** in en selecteert u **VCS** op het tabblad Discovery en ontdekt u de VCS-apparaten. Selecteer ook **TMS** voor de TMS en voer u het IP-adres in. Klik op **Nu uitvoeren** zoals in de afbeelding.

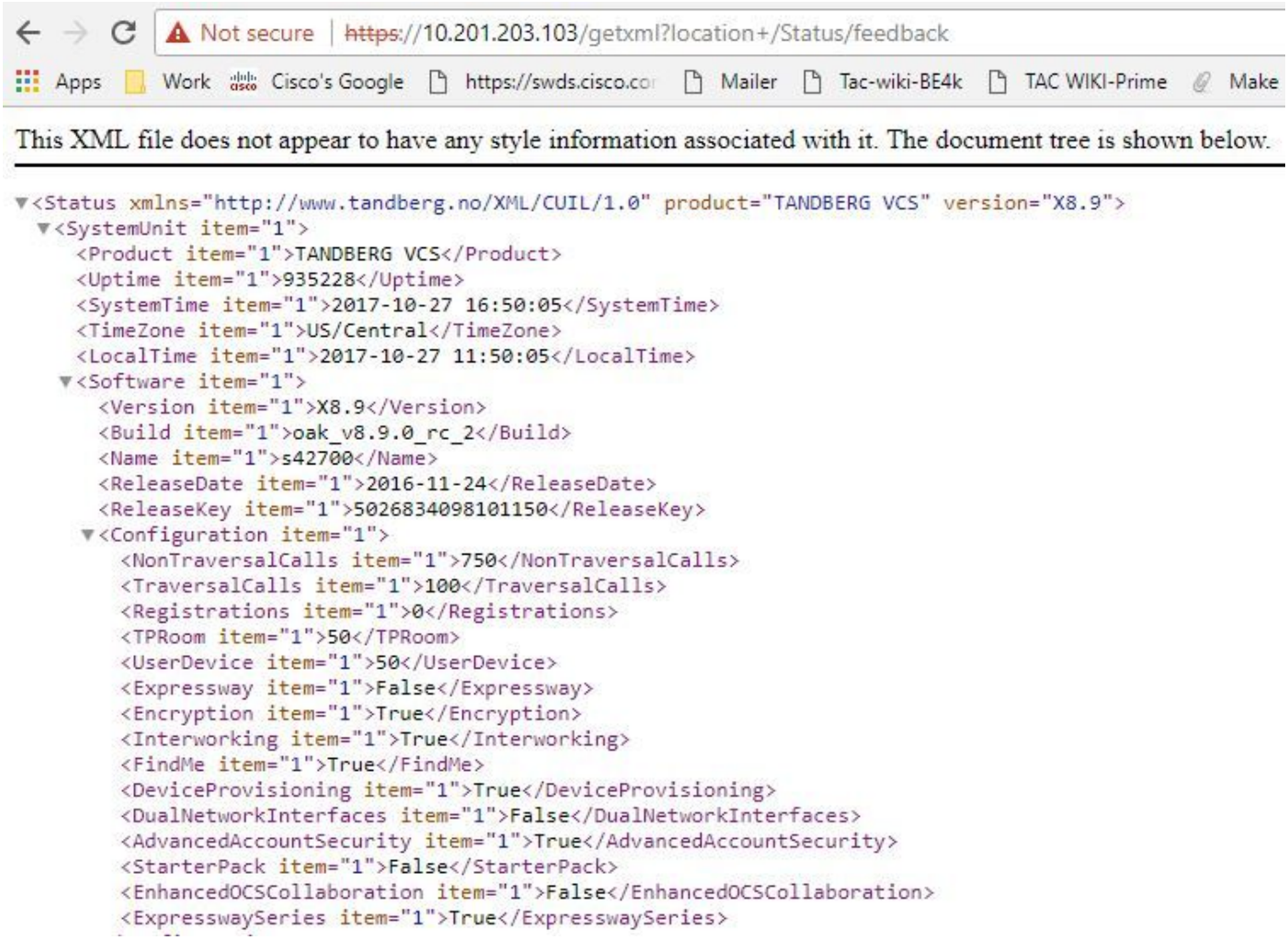


Stap 4. Zorg ervoor dat de VCS en TMS in een beheerde staat zijn.

Opmerking: Als de VCS of TMS zich niet in een beheerde staat bevindt, is dat meestal te danken aan HTTP of SNMP, als verdere assistentie nodig is om een TAC-case te openen om VCS/TMS in een beheerde staat te krijgen.

Opmerking: Gebruik deze URL en vervang de IP_Address_of_VCS_Server door het juiste IP-adres zodra de VCS in een beheerde staat is.De PC-server moet worden geregistreerd als een terugkoppelingsserver naar VCS, dit garandeert dat wanneer een conferentiesessie eindigt, er geen probleem is met de gegevens die VCS terugstuurt naar een PCA.

https://<IP_Address_of_VCS_Server>/getxml?location+/Status/feedback, de http geloofsbrieven worden gevraagd en zodra u wordt ingevoerd, moet u een antwoord ontvangen zoals in de afbeelding wordt getoond.



> Opmerking: Als Prime Collaboration niet via een HTTP-feedback-abonnement op VCS is geabonneerd, hoeft deze niet door VCS te worden aangemeld wanneer een geregistreerd eindpunt toetreedt of een sessie verlaat, of registers of registers aan VCS laat. Stel in dit geval de zichtbaarheid van deze eindpunt(en) in op volledig of beperkt zoals vereist en zorg ervoor dat uw VCS in beheerde toestand verkeert.

Stap 5. Navigeer naar **inventaris > Tijdschema > Cluster Data Discovery Schedule** en selecteer **nu uitvoeren**.

> Opmerking: Dit proces kan enige tijd in beslag nemen terwijl het deze functie over alle infrastructurele apparaten uitvoert. Als het na een paar minuten niet is voltooid, moet u dit na 1-2 uur opnieuw controleren. Zeer grote systemen kunnen tot 4 uur duren. Het is belangrijk om in de partnerschaps- en samenwerkingsovereenkomst te vermelden of er eindpunten zijn waar u conferentiestatistieken wilt hebben die worden ondersteund en dat u er ook voor zorgt dat deze ook worden beheerd voor verslagen en alle statistieken om de juiste informatie te tonen.

Voor een lijst van ondersteunde apparaten, zoals die in de partnerschaps- en samenwerkingsovereenkomst voor conferenties en onze ondersteunde sessies staat, zie de afdeling Achtergrondinformatie.

Stap 6. Navigeer naar **Diagnose > Endpoint Diagnostics**.

Om de juiste statistieken voor de eindpunten van de conferentie te verkrijgen, moet u hun

zichtbaarheid op het hoogst mogelijke niveau instellen dat door het systeem wordt toegestaan.

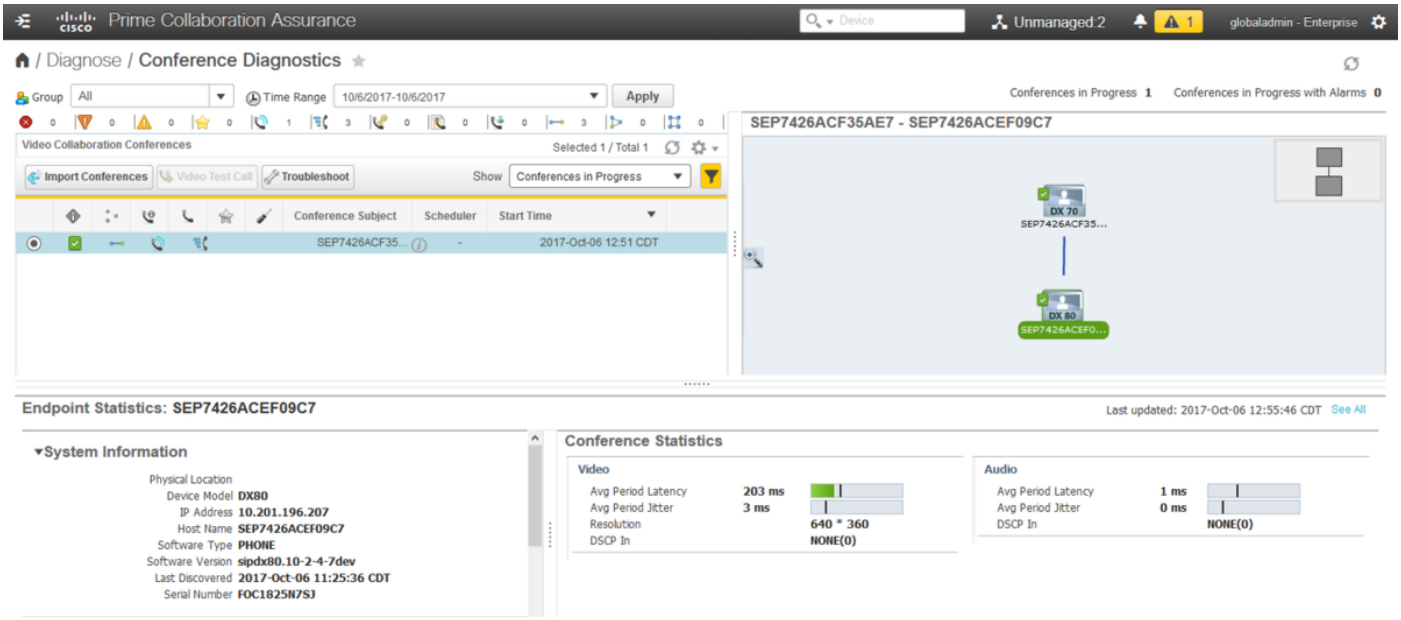
Selecteer alle endpoints die u in het programma Conferencing wilt controleren en klik vervolgens op **Visibility** bewerken en selecteer het maximale zicht.

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

> **Opmerking**: Als u bijvoorbeeld 10 eindpunten selecteert en Full Visibility and (Volledig zichtbaarheid) selecteert, wordt het hoogste niveau van de zichtbaarheidsondersteuning per apparaat geselecteerd.

Stap 7. Om te testen, nAfwijken tot **Diagnose > Conference Diagnostics** en een conferentie die in uitvoering of voltooid is, is zoals getoond in de afbeelding.



Binnen deze conferenties kunt u het gemiddelde pakketverlies, de latentie en de Jitter voor audio en video gesprekken bekijken.

U verkrijgt ook een topologie van de Sessie en de betrokken apparaten.

Verwante alarmen voor conferenties

Voor Conference Diagnostics kunt u elke sessie drie verschillende alarmsignalen ontvangen en hun drempels instellen:

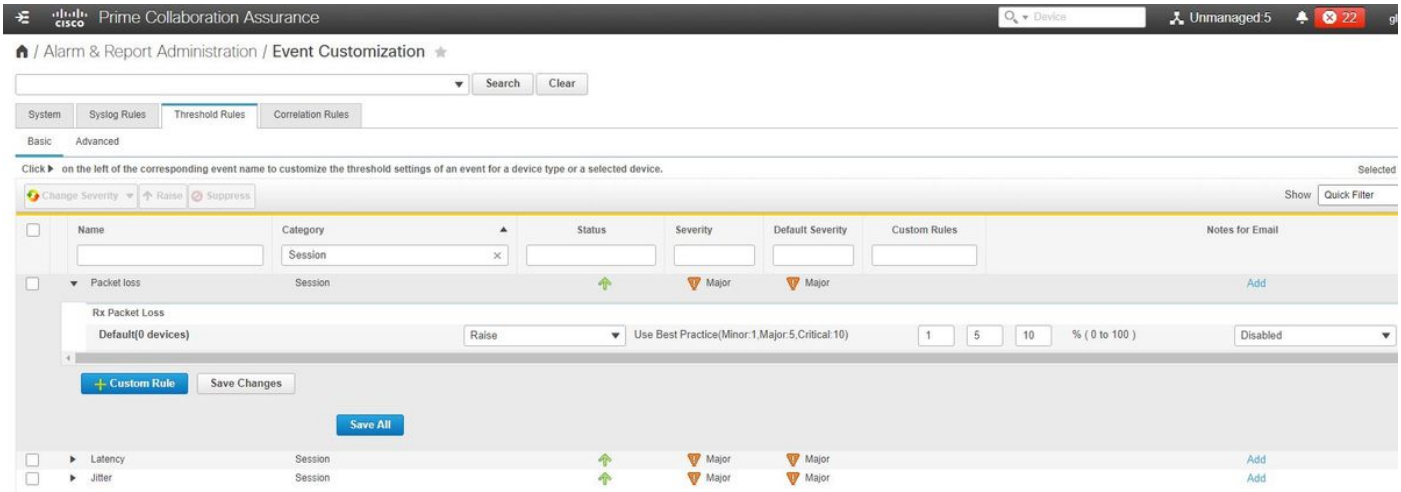
- Packet Loss
- Latentie
- Jitter

Elk van deze u kunt de standaarddrempel wijzigen, geheel uitschakelen of bepalen welke apparaten u aan dit alarm wilt koppelen.

Stap 1. Navigeer naar **Alarm & Report Administratie >Aanpassing van gebeurtenissen**.

Stap 2. Selecteer **Drempelregels** en controleer of u **basisregels** hebt geselecteerd.

Stap 3. Scrolt of filter naar rechts voor de categorie Benoemde sessie zoals in de afbeelding.



Stap 4. Selecteer de pijl omlaag naast het alarm dat u wilt wijzigen en u kunt de mindere, grote of kritieke percentages voor Packet Loss, Jitter of Latency wijzigen.

Stap 5. Als u het beeld wilt onderdrukken, schakelt u de Omhoog in omlaag.

Stap 6. Als u de eindpunten wilt definiëren die aan het alarm zijn gekoppeld, selecteert u Aangepaste regel.

Stap 7. Selecteer vervolgens **het type apparaat >** selecteer **Alle apparaten** of **selecteerbare apparaten** die u voor dit alarm wilt en klik op **Opslaan**.

Verwante verslagen van de conferentie

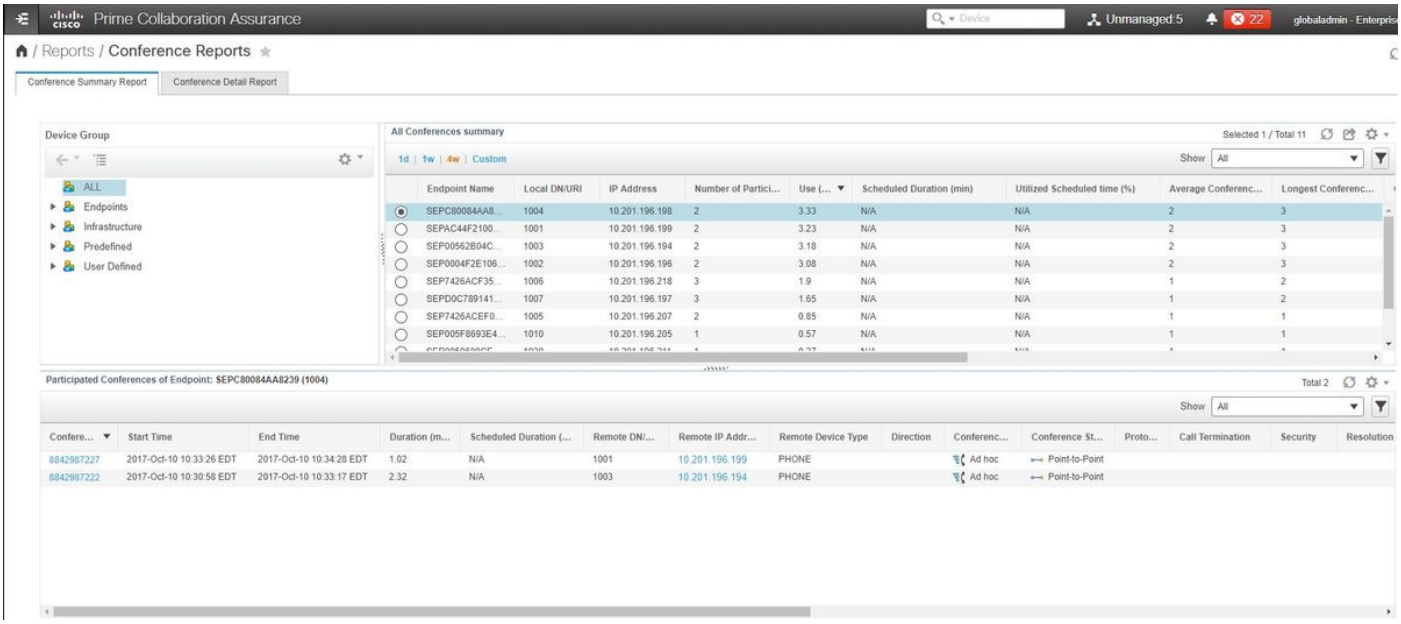
Voor de Conference Diagnostics kunnen rapporten worden opgezocht en bekeken.

Er zijn twee rapporten:

- Conferentieverslagen
- TelePresence-endpointrapporten

Voor vergaderverslagen kunt u een lijst van alle conferenties binnen een tijdsbestek van één tot vier weken of een aangepaste periode bekijken zoals nodig is.

Stap 1. navigeren om **rapporten van vergaderingen** zoals in de afbeelding te **melden**.



Rapport van de conferentie

Dit rapport biedt een overzicht van elk eindpunt dat u als beperkt/volledig zicht en hun conferenties hebt geselecteerd.

De hier getoonde statistieken zijn:

- Gemiddelde conferentiegebruik
- Zorgen in verband met de conferentie
- Gemiddeld pakketverlies, Jitter en Latentie
- Langste conferentie

Dit kan u helpen een granulaire weergave te realiseren van problemen die u binnen uw spraak/video-netwerk kunt hebben om te bepalen welke endpoints de meeste problemen hebben.

Gebruik ook uw bandbreedte per gebruik

Tabblad Conference Detail-rapport

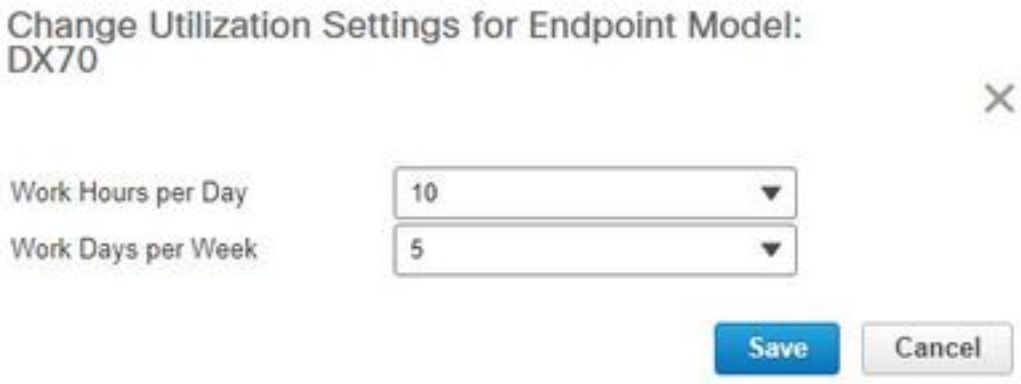
Als u een alarm voor een Conferentie tegenkomt, kunt u naar het tabblad Rapport van de Conferentie navigeren.

Nadat u de Conferentie hebt geselecteerd, kunt u de naam van het Endpoint, de softwareversie en andere details die u mogelijk interesseert, verfijnen.

Voor TelePresence Endpoint Rapporten kunt u per eindpunt de - bekijken

- Aantal conferenties die dit apparaat had
- Gebruikerspercentage
- Endpoint model
- Gebruik

Daarnaast kunt u de Utilization-parameters wijzigen via het tabblad Change Utilization zoals in de afbeelding weergegeven.



Dit stelt de parameters voor dat apparaat in zodat het systeem van het gebruik weet welk percentage te tonen is.

Het rapport No Show Endpoint toont de endpoints die geplande conferencing hadden gemist.

Binnen deze grafiek, kunt u het Endpoint bekijken en hoeveel Totaal Geplande Conferenties en hoeveel van deze voorkwamen en geen shows waren.

Conference Video Test Call

U kunt point-to-point videotestoproepen maken tussen twee video-endpoints die in een beheerde toestand verkeren om uw netwerk te testen. U kunt gebeurtenissen en alarmen zien, sessiestatistieken, eindpuntstatistieken en netwerktopologie. Alleen de CTS-, C- en EX-series worden voor deze oproep ondersteund.

Daarnaast kan dit worden gebruikt om alle functionaliteit te valideren is correct met de conferentiediagnostiek.

Voorwaarden

- Deze optie wordt niet ondersteund voor de E20-codec-serie.
- Om deze optie te gebruiken, moeten CLI-referenties voor de eindpunten worden toegevoegd.
- Zorg ervoor dat de endpoints worden geregistreerd en JTAPI is ingeschakeld voor endpoints (als deze zijn geregistreerd op Unified CM).
- De functie Video Test Call is niet beschikbaar als u Cisco Prime Collaboration-software in MSP hebt geïmplementeerd.

Stap 1. Navigeer naar **Diagnose > Endpoint Diagnostics**.

Stap 2. Selecteer twee toepasbare eindpunten in overeenstemming met de vereisten.

Stap 3. Selecteer **Start tests > Video Test Call**.

Stap 4. U kunt de Video Test Call plannen om nu of op een herhalingsschema te starten.

Stap 5. Deze Video Test Call toont vervolgens in het Scherm voor Conferentie van diagnostiek.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

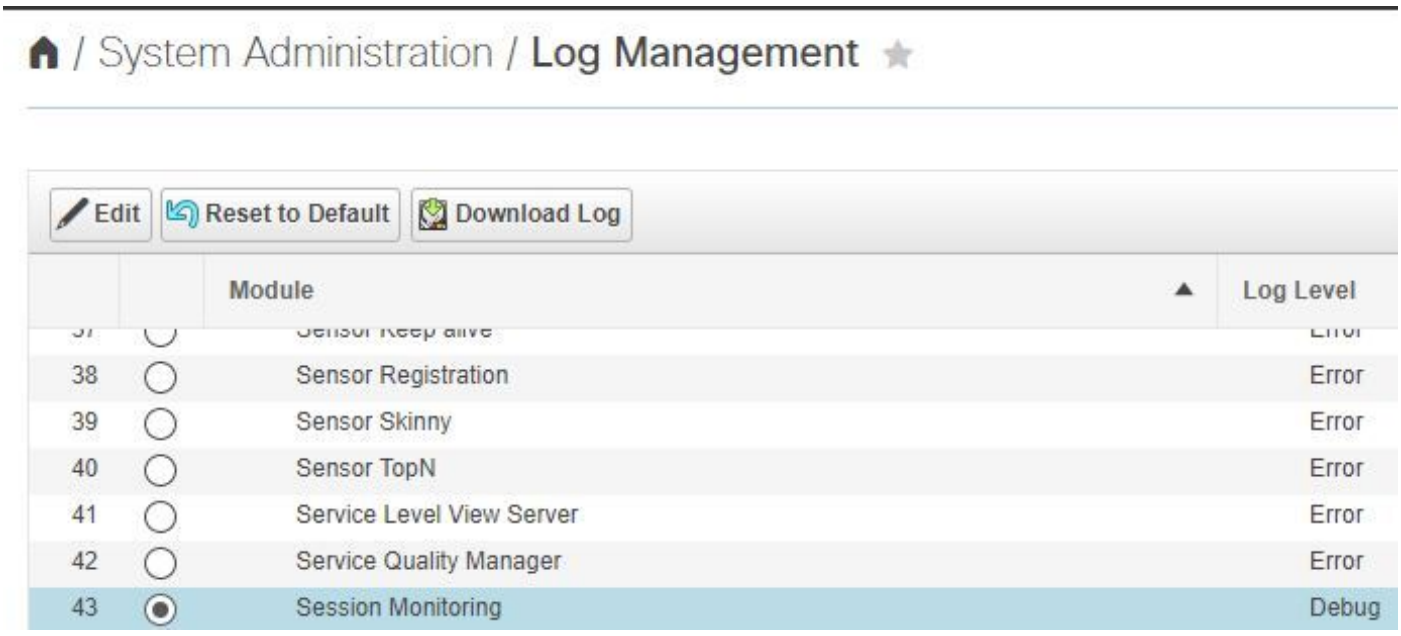
Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

Aanmelden om te verzamelen voor probleemoplossing

Stap 1. Navigeer naar **systeembeheer > logbeheer**.

Stap 2. Scrolt naar de module en selecteer **Sessiebewaking** en selecteer **Bewerken** zoals in de afbeelding.



Stap 3. Wijzig het logniveau om te debug en klik op **Opslaan**.

Stap 4. Reinig het probleem en kom vervolgens terug op het scherm voor logbeheer.

Stap 5. Nadat u het probleem hebt gereproduceerd, selecteert u **Sessiebewaking** en vervolgens selecteert u **Downloadlogboek**.

Stap 6. Nadat u het zip-bestand hebt gedownload.

Stap 7. Open het zip-bestand en navigeer naar de locaties voor nuttige logbestanden:

/opt/emms/emsam/log/SessionMon/

- CUCMJTAPI.log
- CUCMJTAPIDiag.log
- CSMTracker
- CSMTrackerDiag.log
- CSMTrackerDataSource.log
- PostInitSessionMuon.log