Configurar Prime Collaboration Assurance (PCA): Diagnósticos de conferencia

Contenido

Introducción

En este documento se describe cómo configurar y configurar la implementación de los diagnósticos de conferencia en Prime Collaboration Assurance (PCA) para supervisar de forma proactiva las estadísticas de las conferencias de voz y vídeo.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Inicio de sesión de Call Manager Admin
- Inicio de sesión en PCA
- Su Telepresence Monitor Server (TMS)

- Credenciales de Core/Expressway, si procede

Componentes Utilizados

La información de este documento se basa en las versiones 11.x - 12.x de PCA.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

Cisco Prime Collaboration 11.x admite estos tipos de visibilidad:

- Visibilidad total: se admite la detección de llamadas mediante la retroalimentación JTAPI/ HTTP y la información de supervisión en tiempo real, como las estadísticas de la conferencia y la información de la conferencia.
- Visibilidad limitada: se produce la detección automática de llamadas con el uso de información JTAPI/ HTTP, pero no se admite la información de supervisión en tiempo real, como las estadísticas de la conferencia y la información de la conferencia. Los terminales con visibilidad limitada se indican con un icono de semidombra en la topología de conferencia.

Cisco Prime Collaboration 12.x admite estos tipos de visibilidad:

- Visibilidad total: se admite la detección de llamadas mediante la retroalimentación JTAPI/ HTTP y la información de supervisión en tiempo real, como las estadísticas de la conferencia y la información de la conferencia.
- Sin visibilidad: no se admite la detección de llamadas con el uso de información de seguimiento en tiempo real y comentarios JTAPI/ HTTP. Estos extremos se muestran en la página Supervisión de conferencia con un icono completamente atenuado.

Limitación de los terminales establecidos en Visibilidad limitada o total por OVA

- Small Open Virtualization Archive (OVA) admite hasta 500 terminales
- OVA medio admite hasta 1000 terminales
- OVA de gran tamaño admite hasta 1800 terminales
- OVA muy grande admite hasta 2000 terminales

En la imagen de la tabla siguiente se muestra una lista de los dispositivos compatibles por PCA en lo que respecta a las conferencias y nuestras sesiones compatibles.

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.

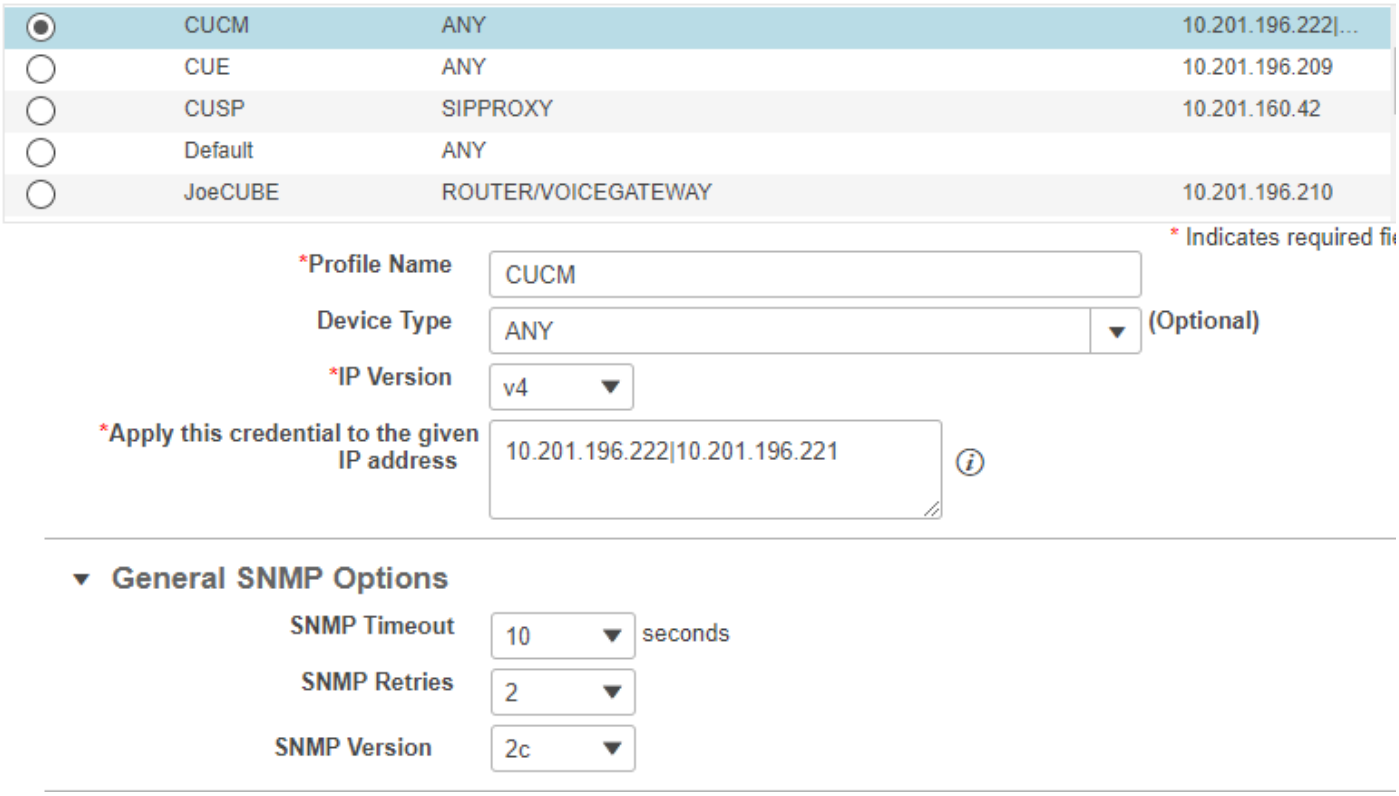
Configurar

Escenario 1. Conferencia con terminales de vídeo registrados en Call Manager

Paso 1. En primer lugar, debe asegurarse de que los Call Managers se encuentran en el estado Managed (Gestionado).

Vaya a Inventario > Gestión de inventario > Gestionar credenciales > Crear un perfil para el clúster de Call Manager.

Nota: Recuerde que cada perfil de credencial utiliza las mismas credenciales para cada dirección IP incluida en el perfil. Por lo tanto, si enumera el editor y el suscriptor de Call Manager dentro del mismo perfil de credenciales, utiliza esas mismas credenciales para detectar ambas direcciones IP. Si tiene un conductor en la configuración, descubra primero el conductor y luego el Cisco Call Manager como se muestra en la imagen.



Paso 2. Asegúrese de haber configurado las credenciales de protocolo de transferencia de hipertexto (HTTP), protocolo simple de administración de nombres (SNMP) y API de telefonía Java (JTAPI)

Además, debe habilitar el servicio Cisco Computer Telephony Integration (CTI) en Call Manager Serviceability.

Configuración de Cisco Unified Communications Manager

Habilitar HTTP

No es necesario crear un nuevo usuario si desea permitir que Cisco Prime Collaboration utilice las credenciales de administrador para iniciar sesión. Asimismo, si desea permitir que Cisco Prime Collaboration Manager utilice las credenciales adecuadas para iniciar sesión en Cisco Unified Communications Manager, debe crear un nuevo grupo de usuarios HTTP y un usuario correspondiente que Cisco Prime Collaboration pueda utilizar para comunicarse.

Para crear un usuario, siga estos pasos:

Paso 1. Inicie sesión en la interfaz web de administración de Cisco Unified CM con su cuenta de administrador.

Paso 2. Cree un grupo de usuarios con privilegios suficientes. Navegue hasta Administración de usuarios>Configuración de usuario>Grupo de control de acceso y cree un nuevo grupo de usuarios con un nombre adecuado, PC_HTTP_Users en este caso. Ahora, seleccione Guardar.

Paso 3. Navegue hasta Administración de usuarios>Configuración de usuario>Grupo de control de acceso y seleccione Buscar. Busque el grupo que ha definido y haga clic en el icono de la

derecha.

Paso 4. Seleccione Asignar rol a grupo y seleccione estos roles:

- Acceso API AXL estándar
- Usuarios administrativos de CCM estándar
- Administración de MANTENIMIENTO estándar

Paso 5. Click Save.

Paso 6. En el menú principal, vaya aAdministración de usuarios>Usuarios de la aplicación>Crear un nuevo usuario.

Especifique una contraseña adecuada en la páginaConfiguración de usuario de aplicación. Solo puede seleccionar determinados tipos de dispositivos en el área de texto Dispositivos disponibles o permitir que Cisco Prime Collaboration supervise todos los dispositivos

Paso 7. En la secciónInformación de Permiso, seleccione Agregar al grupo de usuarios y seleccione el grupo que se creó en el paso 1. (por ejemplo, PC_HTTP_Users).

Paso 8. Haga clic en Guardar. La página se actualiza y se muestran los privilegios adecuados.

Activar SNMP

SNMP no está activado en Cisco Unified Communications Manager de forma predeterminada.

Para habilitar SNMP:

Paso 1. Inicie sesión en la vistaServicio de Cisco Unified en la GUI web de Cisco Unified Communications Manager.

Paso 2. Vaya a Herramientas > Activación de servicio.

Paso 3. Seleccione Publisher Server.

Paso 4. Navegue hasta Performance > Monitoring Services y seleccione la casilla de verificación para Cisco Call Manager SNMP Service.

Paso 5. Seleccione Save en la parte inferior de la pantalla.

Para crear una cadena de comunidad SNMP:

Paso 1. Inicie sesión en Serviciabilidad de Cisco Unified para ver la GUI web de Cisco Unified Communications Manager.

Paso 2. En el menú principal de la vista Serviciabilidad de Cisco Unified, vaya aSNMP > v1/v2c > Cadena de comunidad.

Paso 3. Seleccione un servidor y haga clic en Buscar.
Si la cadena de comunidad ya está definida, el nombre de la cadena de comunidad se muestra en

los resultados de la búsqueda.

Paso 4. Haga clic en Add newpara agregar una nueva cadena si no se muestra ningún resultado.

Paso 5. Especifique la información SNMP necesaria y guarde la configuración.

Nota: Sólo se necesita acceso de solo lectura (RO) SNMP.

Iniciar servicio CTI

Realice el procedimiento del nodo de Cisco Unified Communications Manager que desee; es preferible configurarlo en dos nodos.

Paso 1. Inicie sesión en Serviciabilidad de Cisco Unified, en la interfaz gráfica de usuario de Cisco Unified Communications Manager.

Paso 2. Vaya aHerramientas > Activación de servicio.

Paso 3. Seleccione un servidor de la lista desplegable.

Paso 4. En la sección Servicios de CM, marque la casilla Cisco CTI Manager.

Paso 5. Seleccione Save en la parte superior de la pantalla

Crear usuario de aplicación para el control CTI de PCA (usuario JTAPI)

JTAPI se utiliza para recuperar la información de estado de sesión del dispositivo. Debe crear un usuario de aplicación para control CTI en el procesador de llamadas con el permiso necesario para recibir eventos JTAPI en los terminales. Prime Collaboration gestiona varios clústeres de procesadores de llamadas. Debe asegurarse de que los ID de clúster son únicos. Cree un nuevo usuario de la aplicación para ayudar a Cisco Prime Collaboration a obtener la información necesaria.

Para crear un nuevo usuario de la aplicación JTAPI siga estos pasos:

Paso 1. Inicie sesión en la interfaz web de administración de Cisco Unified CM a través de su cuenta de administrador.

Paso 2. Cree un grupo de usuarios con privilegios suficientes. Navegue hasta Administración de usuarios>Configuración de usuario>Grupo de control de acceso y cree un nuevo grupo de usuarios con un nombre adecuado, PC_HTTP_Users en este caso. Ahora, seleccione Guardar.

Paso 3. Elija User Management>User Settings>Access Control Group y haga clic en Find. Busque el grupo que ha definido y seleccione el icono de la derecha.

Paso 4. Haga clic en Asignar rol a grupo y seleccione estos roles:

- Standard CTI Allow Call Monitoring

- Standard CTI Enabled
- CTI estándar permite el control de teléfonos compatibles con Xfer y conf conectados

Paso 5. Seleccione Guardar.

Paso 6. En el menú principal, vaya aAdministración de usuarios>Usuarios de la aplicación>Crear un nuevo usuario.
Especifique una contraseña adecuada en la páginaConfiguración de usuario de aplicación. Puede seleccionar determinados tipos de dispositivos en el área de texto Dispositivos disponibles o permitir que Cisco Prime Collaboration supervise todos los dispositivos.

Nota: La contraseña no debe incluir un punto y coma (;) ni ser igual a (=).

Paso 7. En la secciónInformación de permiso, seleccione Agregar al grupo de control de acceso y seleccione el grupo que se creó en el paso 1. (por ejemplo, PC_HTTP_Users).

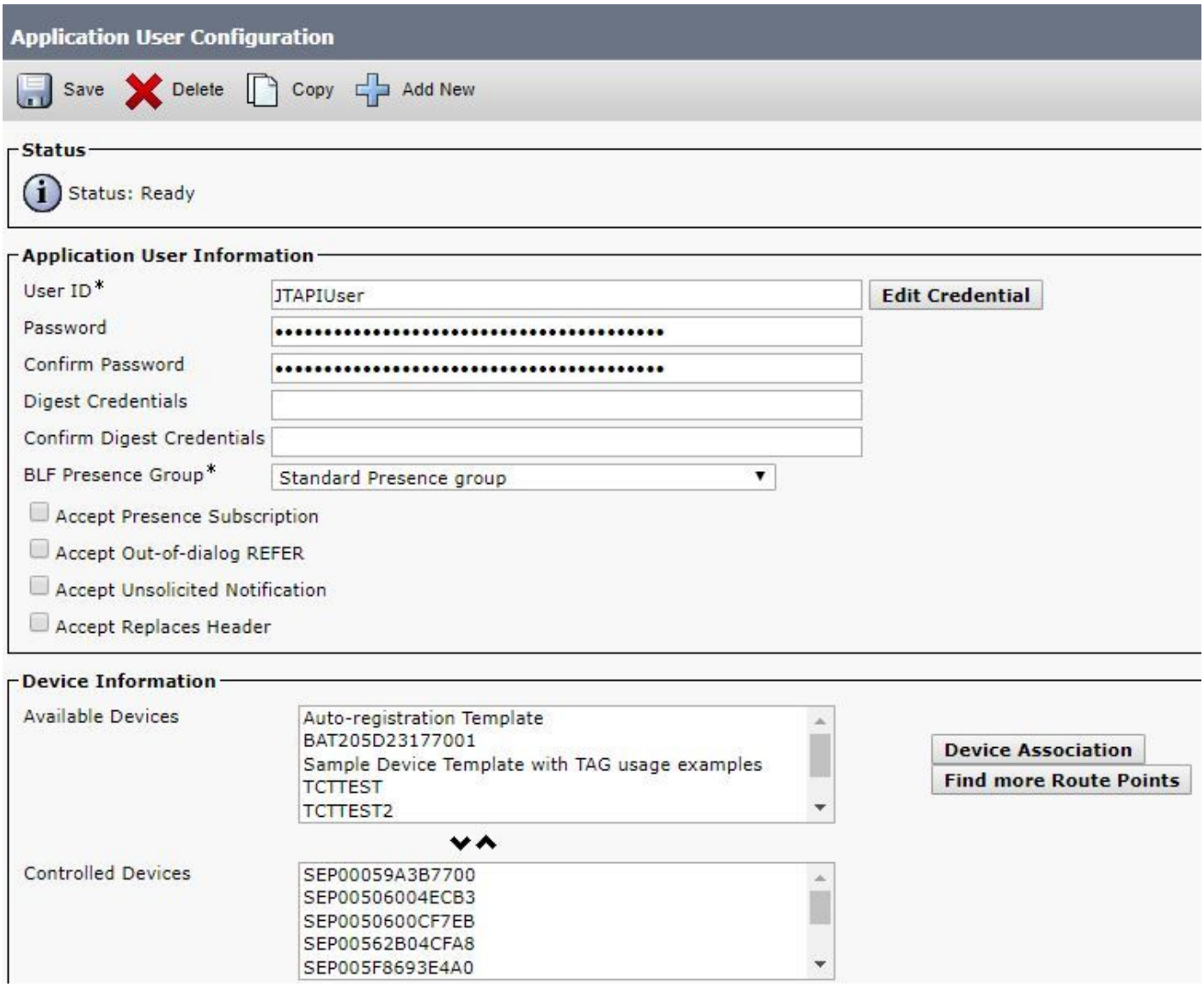
Paso 8. Haga clic en Guardar. La página se actualiza y se muestran los privilegios adecuados.

Nota: Si Call Manager se administró antes de agregar el usuario JTAPI, asegúrese de que el usuario JTAPI se agrega en el perfil de credenciales para Call Manager y vuelva a descubrirlo.

Continuación de la situación 1. Pasos:

Paso 3. Desplácese hasta el usuario de la aplicación JTAPI de Call Manager que creó y mueva los terminales compatibles de Dispositivos disponibles a Dispositivos controlados.

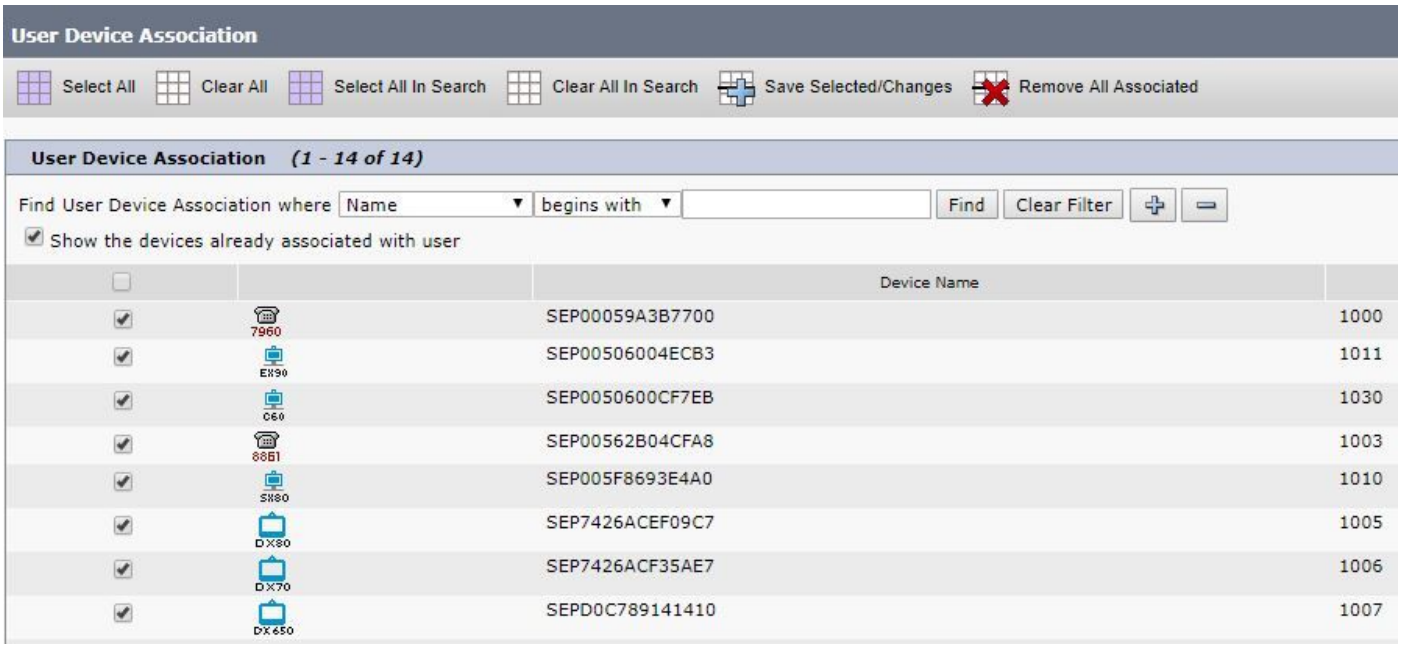
Puede hacerlo mediante la función Device Association, como se muestra en la imagen.



Si vuelve a hacer referencia a la limitación de los terminales establecidos en Visibilidad limitada o Visibilidad completa por OVA, puede verificar la cantidad de dispositivos que ha agregado al tamaño de OVA.

En esta pantalla, puede filtrar por nombre de dispositivo, descripción o número de directorio para ayudarle a administrar y filtrar estos dispositivos, como se muestra en la imagen.

Es útil tener en cuenta estos dispositivos, ya que se agregan en el paso 7.



Asegúrese también de agregar las funciones de usuario correctas para este usuario JTAPI:

- Standard CTI Allow Call Monitoring
- Standard CTI Enabled
- El CTI estándar permite el control de los teléfonos que admiten Connected Xfer y conf, como se muestra en la imagen.

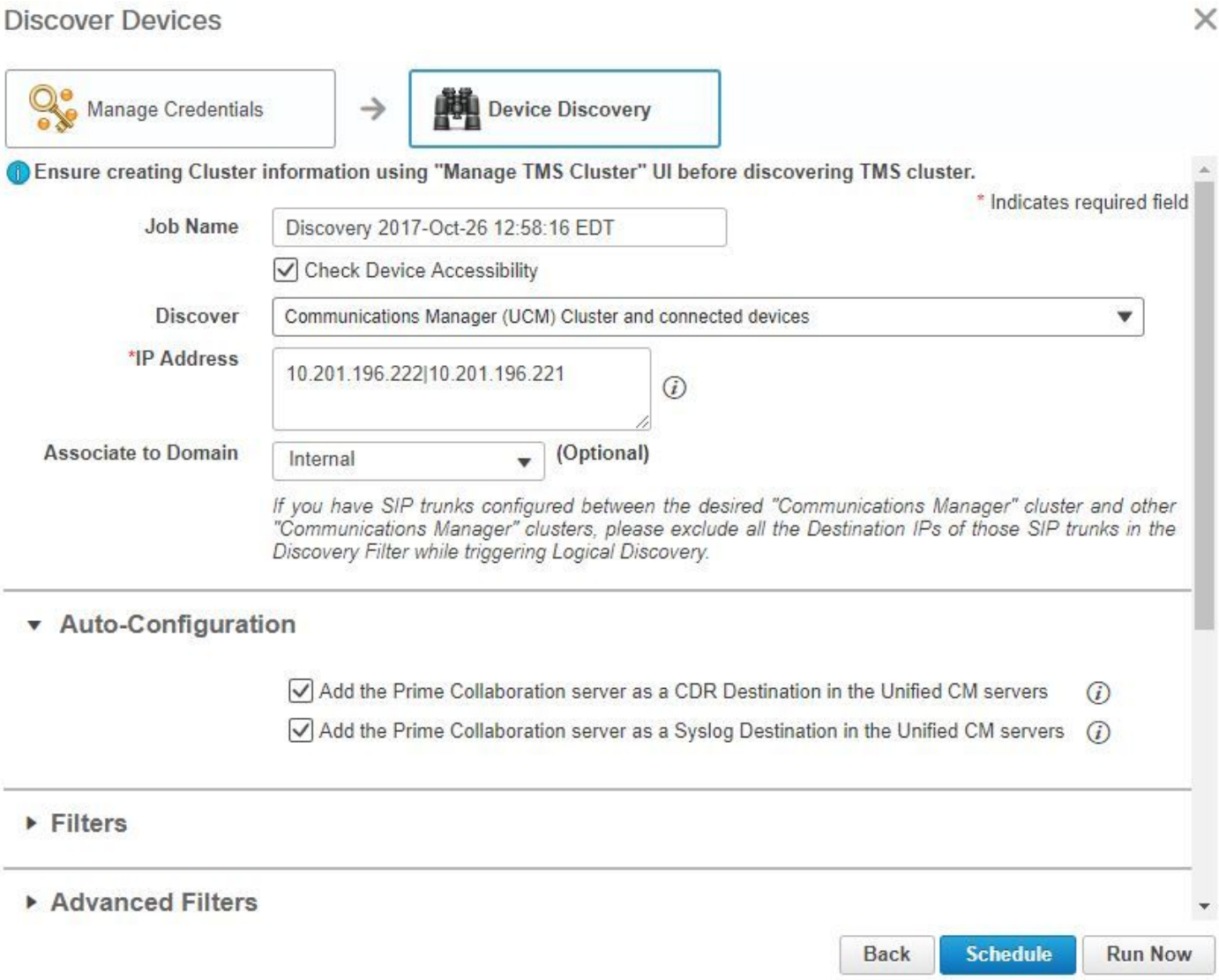
Para obtener una lista de los dispositivos compatibles por PCA, en lo que respecta a las conferencias y nuestras sesiones compatibles, consulte la sección Información general.

Nota: Además, asegúrese de que los dispositivos controlados por el usuario de la aplicación CTI tengan marcada la casilla de verificación Permitir el control del dispositivo desde CTI en la información del dispositivo, como se muestra en la imagen.

Nota: Es importante tener en cuenta antes de continuar que si tiene los terminales

registrados en Call Manager y Call Manager está integrado con VCS/TMS, primero descubra su VCS/TMS y luego descubra su Call Manager al final. De esta manera, desde la perspectiva del inventario, toda su infraestructura se asigna a la ubicación correcta. Además, cuando descubra el VCS/TMS, asegúrese de cambiar la ficha Detectar predeterminada por el dispositivo correspondiente de TMS/VCS o Call Manager.

Paso 4. A continuación, en PCA, seleccione Device Discovery e ingrese en las Direcciones IP de sus Call Managers, seleccione las dos casillas de verificación en Auto-Configuration y seleccione Run Now como se muestra en la imagen.



Paso 5. Una vez que los Call Managers se encuentren en estado Managed, vaya al paso 6.

Nota: Si el Call Manager no está en un estado administrado, la mayor parte del tiempo se debe a HTTP o SNMP; si se necesita más ayuda, abra un caso TAC para que el Call Manager se encuentre en un estado administrado.

Paso 6. Navegue hasta Inventario > Programación de inventario > Programación de detección de datos de clúster y seleccione Ejecutar ahora.

Nota: Esto depende de la cantidad de dispositivos registrados/no registrados que tenga. Este proceso puede tardar desde unos minutos hasta unas horas. Realice una comprobación durante todo el día actualizando la página. Además, asigna el clúster de Call Manager y recupera todos los puntos finales. Una vez finalizado, continúe con el siguiente paso.

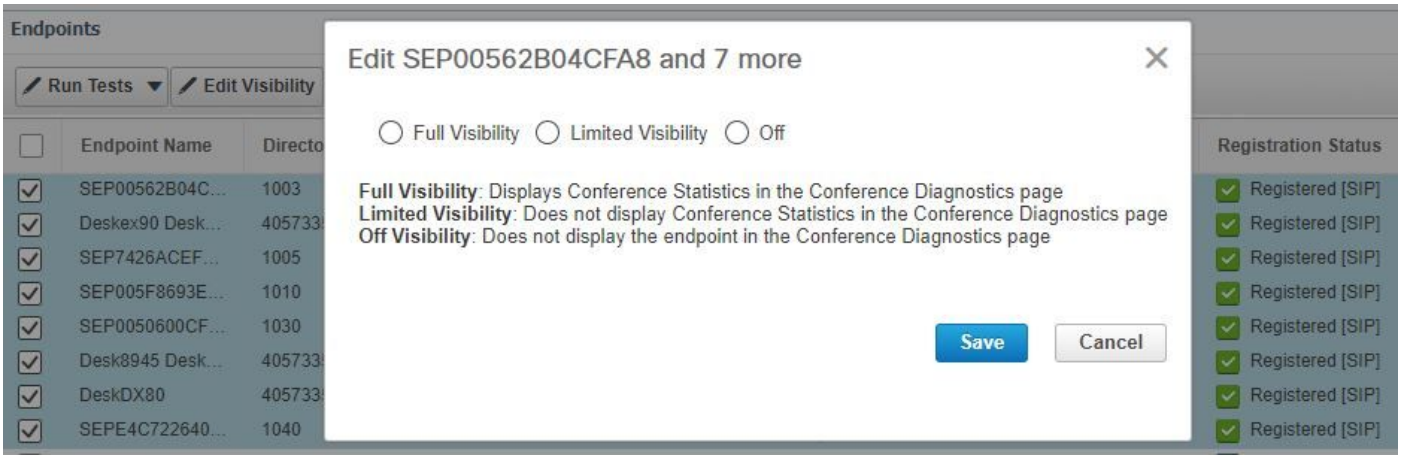
Nota: Es importante mencionar en el inventario de PCA si hay algún terminal en el que desee tener estadísticas de conferencia compatibles. Asegúrese de que se administran correctamente para los informes y todas las estadísticas, para mostrar la información correcta.

Paso 7. Vaya a Diagnose > Endpoint Diagnostics.

Para obtener estadísticas actualizadas de los terminales de conferencia, debe establecer su visibilidad en el nivel más alto posible que permita el sistema.

Seleccione todos los terminales que desee supervisar en el diagnóstico de conferencia, haga clic en Editar visibilidad y, a continuación, seleccione Visibilidad completa como se muestra en la imagen.

La visibilidad limitada solo muestra el dispositivo dentro de la topología, pero no muestra estadísticas y no puede recuperar las alarmas aplicables para los dispositivos relacionados con los diagnósticos de conferencia.

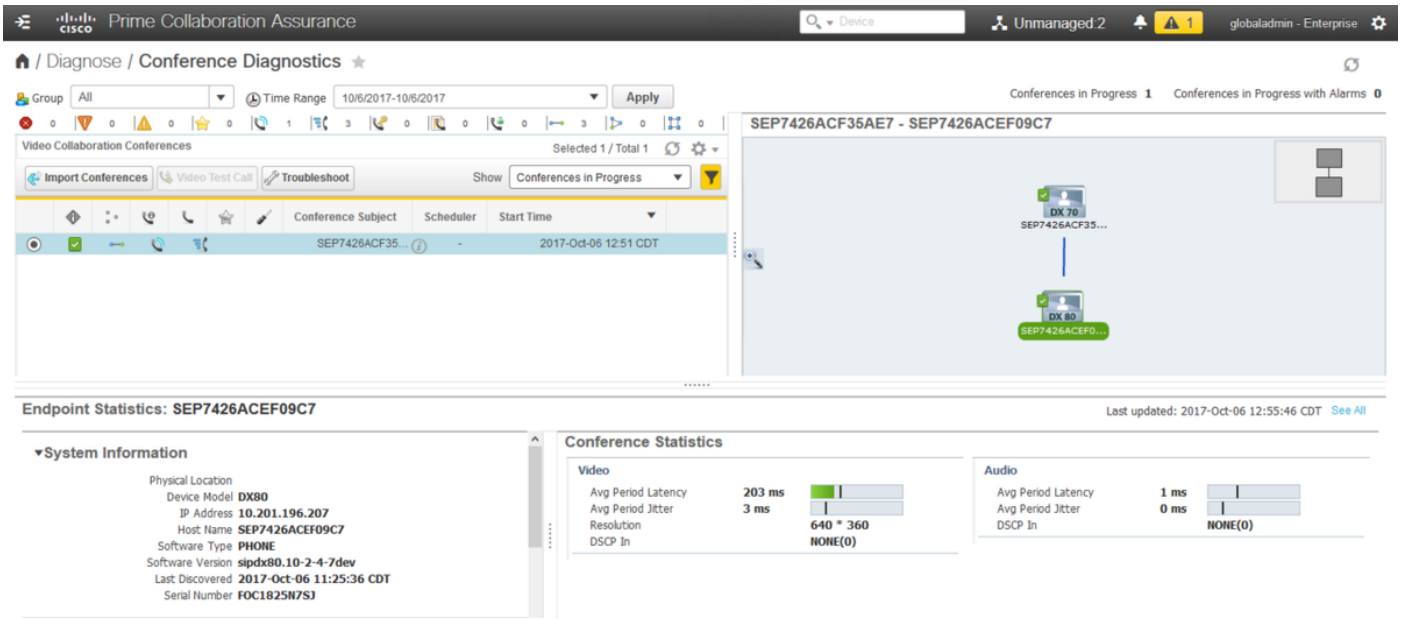


The following table lists the default and maximum visibility details for the endpoints:

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

Nota: si selecciona, por ejemplo, 10 terminales y selecciona Visibilidad completa, se selecciona el nivel más alto de visibilidad compatible con cada dispositivo.

Paso 8. Para probar, navegue hasta Diagnosis > Diagnóstico de conferencia y una conferencia en curso o completada muestra, como se muestra en la imagen.



En estas conferencias podrá ver la pérdida media de paquetes, la latencia y la fluctuación de las llamadas de audio y vídeo.

Además, obtenga una topología de la Sesión y los dispositivos involucrados.

Actualmente, el diagnóstico de conferencia extrae la información basándose en el DN y, si su entorno ha compartido DN, PCA recupera el primero que recibe para la conferencia.

Alarmas relacionadas con la conferencia

Para los diagnósticos de conferencia, puede recibir tres alarmas diferentes para cualquier sesión y establecer sus umbrales:

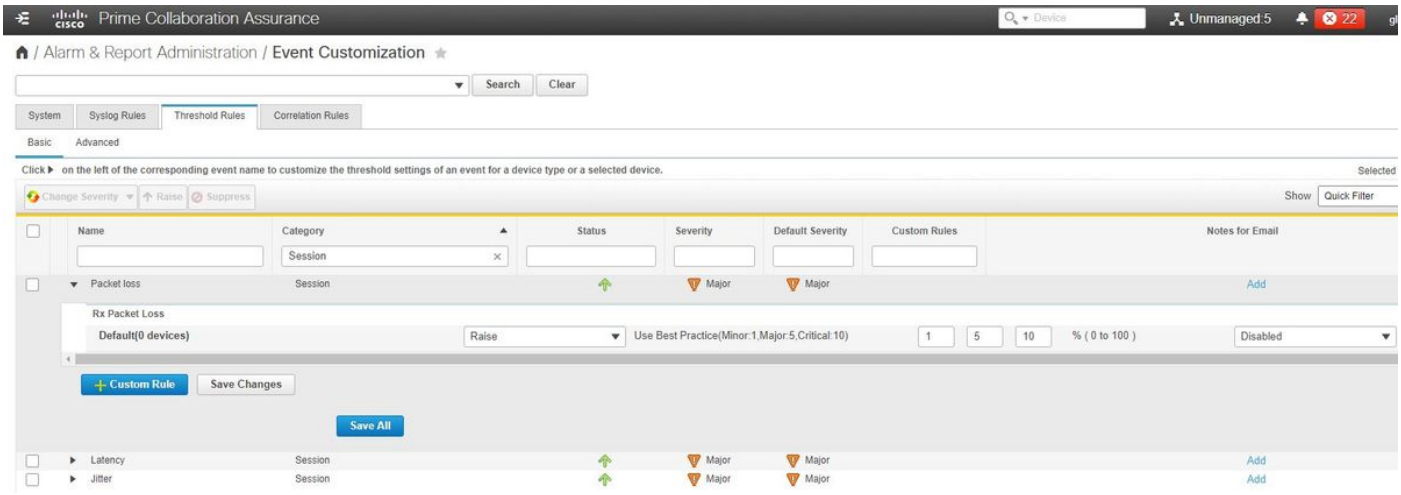
- Pérdida del paquete
- Latencia
- Fluctuación

Para cada uno de ellos, puede modificar el umbral predeterminado, suprimirlo o definir qué dispositivos desea asociar a esta alarma.

Paso 1. Navegue hasta Administración de alarmas e informes > Personalización de eventos.

Paso 2. Seleccione Threshold Rules y asegúrese de que ha seleccionado Basic.

Paso 3. Desplácese hacia abajo o filtre hacia la derecha para la sesión con nombre de categoría, como se muestra en la imagen.



Paso 4. Seleccione la flecha desplegable junto a la alarma. Desea modificar y puede modificar los porcentajes de pérdida de paquetes, fluctuación o latencia menores, mayores o críticos.

Paso 5. Si desea suprimir, cambie la opción Subir a Suprimir.

Paso 6. Si desea definir los puntos finales asociados a la alarma, puede seleccionar Regla personalizada.

Paso 7. A continuación, seleccione el Tipo de dispositivo > Seleccionar todos los dispositivos o Dispositivos seleccionables que desee para esta alarma y haga clic en Guardar.

Informes de conferencia relacionados

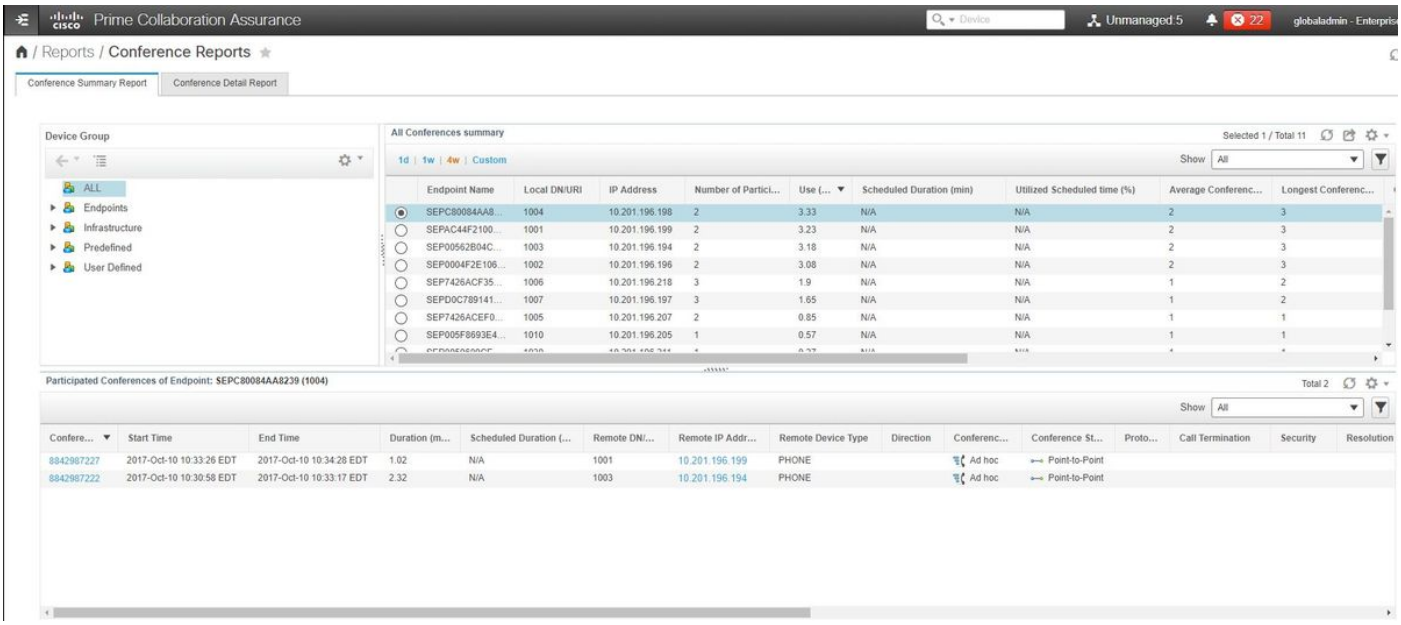
Para los diagnósticos de conferencia, se pueden recuperar y visualizar los informes.

Hay dos informes:

- Informes de conferencia
- Informes de terminales de Telepresence

En el caso de los informes de conferencia, puede ver una lista de todas las conferencias dentro de un período de tiempo de una a cuatro semanas o un período de tiempo personalizado, según sea necesario.

Paso 1. Navegue hasta Informes > Informes de conferencia como se muestra en la imagen.



Informes de resumen de conferencia

Estos informes ofrecen una vista de todos los terminales que ha seleccionado como de visibilidad completa/limitada y sus conferencias.

Las estadísticas que se muestran aquí son:

- Uso medio de conferencias
- Alarmas relacionadas con la conferencia
- Promedio de pérdida, fluctuación y latencia de paquetes
- Conferencia más larga

Esto puede ayudarle a obtener una visión granular de los problemas que puede tener en su red de voz/vídeo para determinar qué terminales tienen más problemas.

Además, puede utilizar su ancho de banda en correspondencia por uso.

Ficha Informe detallado de conferencia

Si detecta una alarma para una conferencia, puede navegar a la pestaña Informe de detalles de la conferencia.

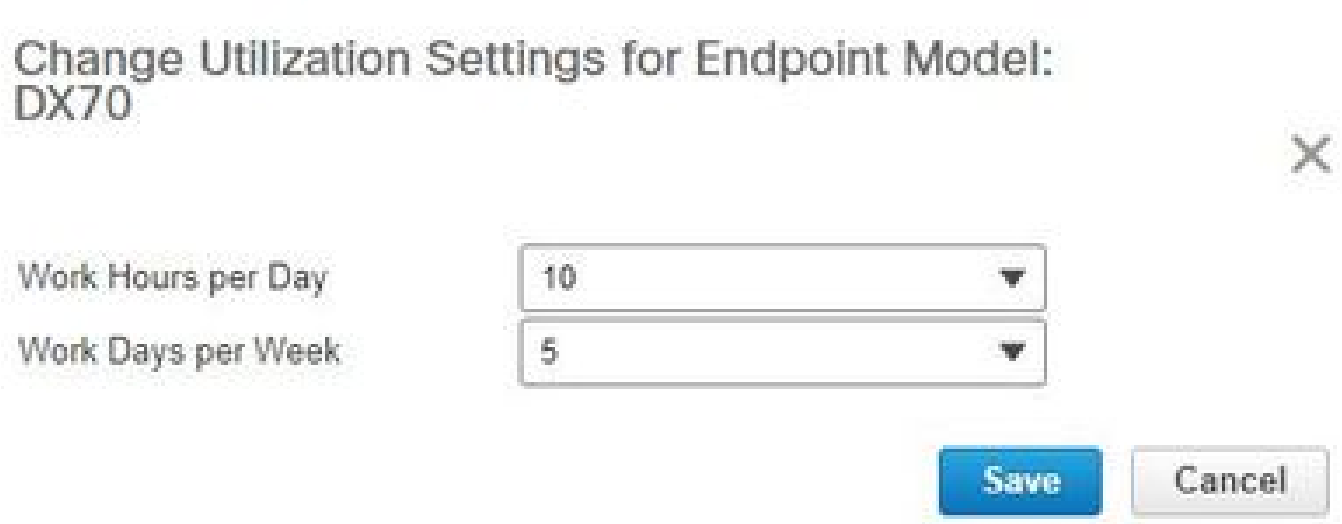
Una vez seleccionada la conferencia, puede refinarla para encontrar el nombre del terminal, la versión del software y otros detalles que le puedan interesar.

En el caso de los informes de terminales de Telepresence, puede ver por terminal:

- Número de conferencias que tuvo este dispositivo
- Porcentaje de utilización
- Modelo de terminal
- Uso

Además, puede cambiar los parámetros de utilización en la ficha Change Utilization, como se

muestra en la imagen.



De este modo, se establecen los parámetros del dispositivo para que el sistema sepa por el uso qué porcentaje mostrar.

El informe de resumen de terminal no mostrado muestra los terminales que no pudieron asistir a las conferencias programadas.

Dentro de este gráfico, también puede ver el punto final y cuántas conferencias programadas totales y cuántas de estas se produjeron y no se mostraron.

Llamada de prueba de vídeo de conferencia

Puede crear llamadas de prueba de vídeo punto a punto entre dos terminales de vídeo en estado administrado para probar la red. Puede ver eventos y alarmas, estadísticas de sesiones, estadísticas de terminales y topología de red con estadísticas como otras llamadas. Sólo se admiten los códecs de las series CTS, C y EX para esta llamada.

Además, se puede utilizar para validar que todo funciona correctamente con los diagnósticos de conferencia.

Prerequisites

- Esta característica no se admite en la serie de códecs E20.
- Para utilizar esta función, se deben agregar credenciales CLI para los terminales.
- Asegúrese de que los terminales estén registrados y de que JTAPI esté habilitado para los terminales (si están registrados en Unified CM).
- La función de llamada de prueba de vídeo no está disponible si ha implementado Cisco Prime Collaboration en modo MSP.

Paso 1. Vaya a Diagnose > Endpoint Diagnostics.

Paso 2. Seleccione dos terminales aplicables según los requisitos previos mencionados.

Paso 3. Seleccione Ejecutar pruebas > Llamada de prueba de vídeo.

Paso 4. Puede programar la videollamada de prueba para que se ejecute ahora o para que se repita.

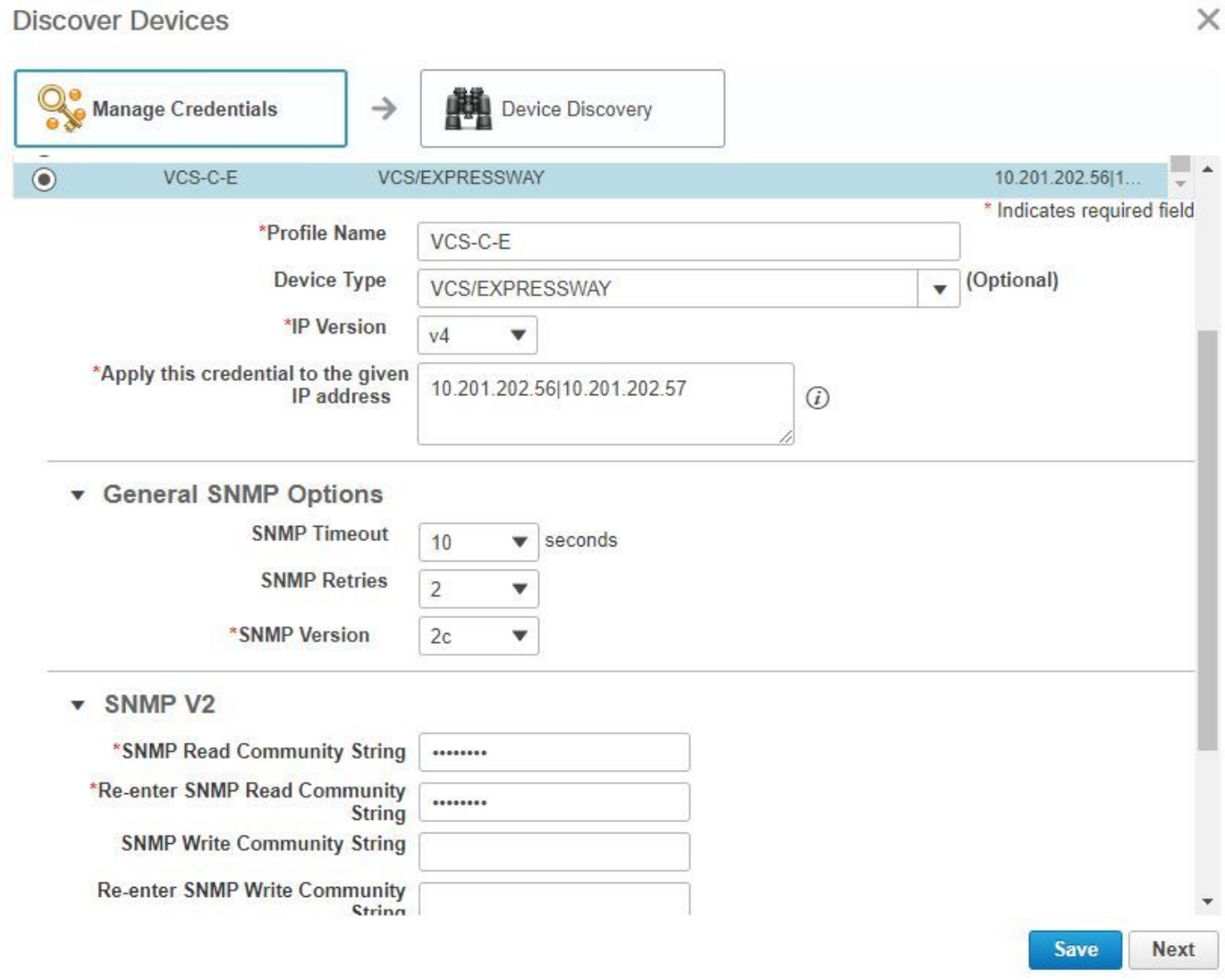
Paso 5. Esta llamada de prueba de vídeo se muestra a continuación en la pantalla Diagnóstico de conferencia.

Situación hipotética 2. Conferencia con terminales no registrados de Call Manager

Paso 1. Asegúrese de que las credenciales de Telepresence Management Suite (TMS) y Video Communications Server (VCS) estén disponibles.

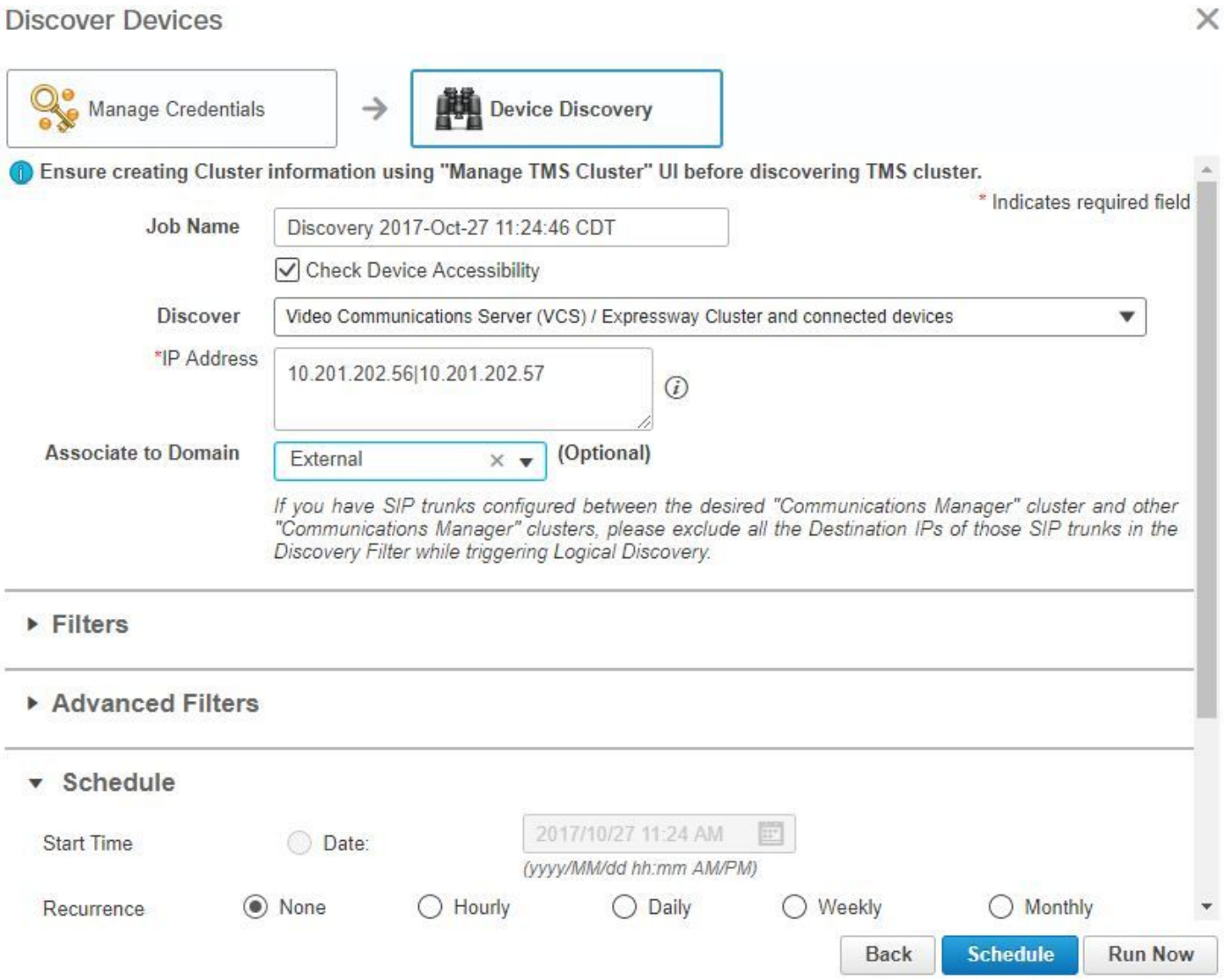
Nota: Cuando descubra su VCS/TMS en esta situación, el proceso de detección es importante. Si tiene un administrador de llamadas en la configuración, descubra primero el conductor y luego el administrador de llamadas de Cisco.

Paso 2. Navegue hasta Inventario > Administración de inventario > Administrar credenciales > Seleccione Agregar y luego ingrese la información para su TMS, mientras crea un perfil de credenciales separado para sus VCS como se muestra en la imagen.



Paso 3. Una vez creado el perfil de credenciales, seleccione Device Discovery, ingrese las

direcciones IP y en la pestaña Discovery, seleccione VCS y descubra los dispositivos VCS. También, seleccione TMS para el TMS e ingrese su dirección IP. Haga clic en Run Now como se muestra en la imagen.



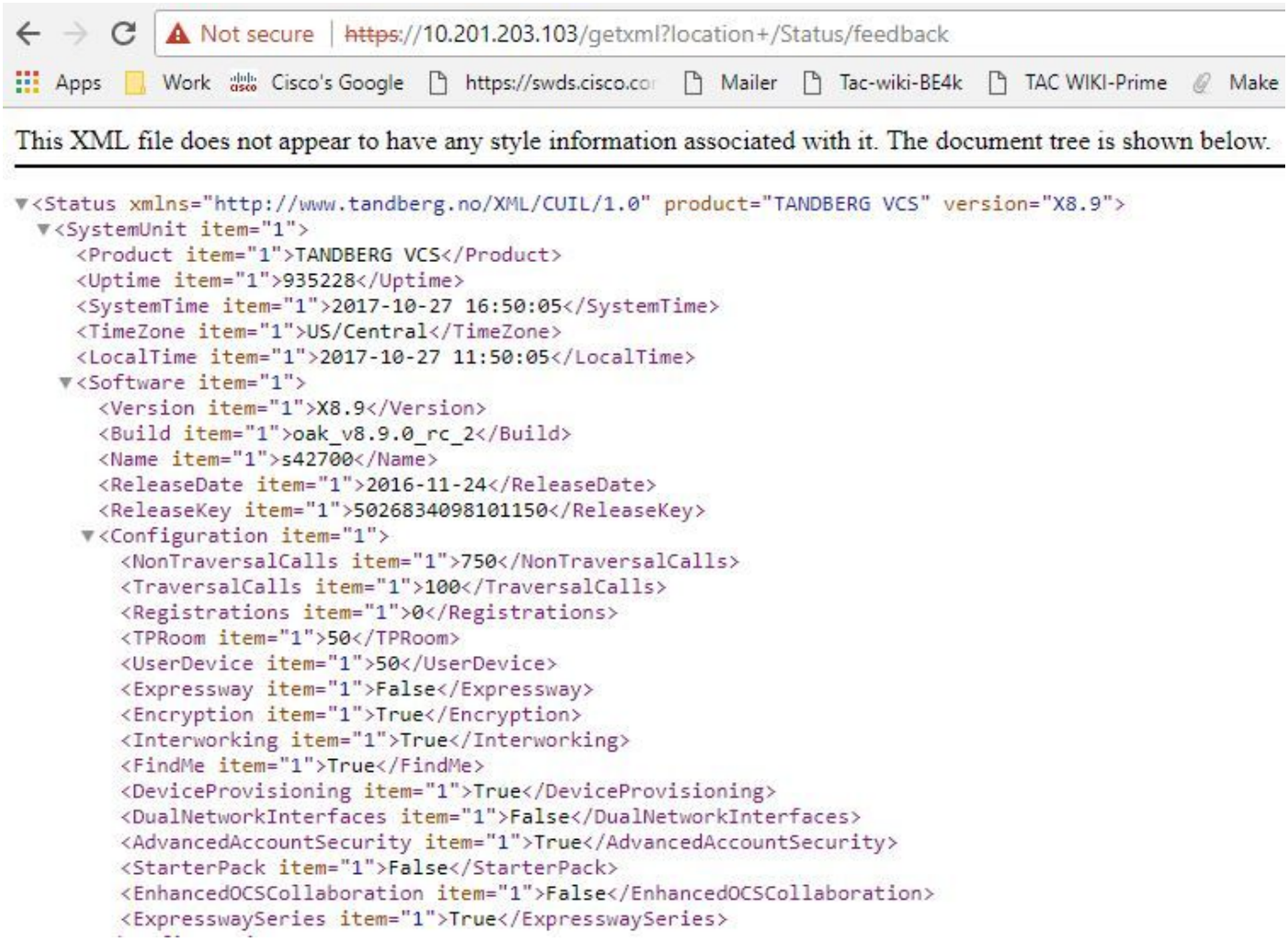
Paso 4. Asegúrese de que VCS y TMS se encuentran en estado Administrado.

Nota: Si el VCS o TMS no se encuentra en un estado administrado, la mayor parte del tiempo se debe a HTTP o SNMP; si se necesita más ayuda, abra un caso TAC para poner el VCS/TMS en un estado administrado.

Nota: Utilice esta dirección URL y sustituya la dirección IP _of_VCS_Server por la dirección IP adecuada una vez que el VCS se encuentre en estado Administrado. El servidor PCA debe estar registrado como servidor de comentarios para VCS, lo que garantiza que cuando finalice una sesión de conferencia no haya ningún problema con los datos que el VCS envía de vuelta al PCA.

https://<IP_Address_of_VCS_Server>/getxml?location+/Status/feedback , se solicitan las credenciales http y una vez ingresadas, debe recibir una respuesta como se muestra en la

imagen.



Nota: si Prime Collaboration no está suscrito a VCS a través de la suscripción de comentarios HTTP, VCS no debe notificarlo cuando un terminal registrado se una a una sesión o la abandona, ni registra o cancela el registro en VCS. En este caso, establezca la visibilidad de esos terminales en completa o limitada según sea necesario y asegúrese de que el VCS se encuentra en un estado administrado.

Paso 5. Navegue hasta Inventario > Programación de inventario > Programación de detección de datos de clúster y seleccione Ejecutar ahora.

Nota: Este proceso puede tardar un tiempo, ya que realiza esta función en todos los dispositivos de infraestructura. Por lo tanto, si no se completa después de unos minutos, vuelva a comprobarlo después de 1-2 horas. Los sistemas muy grandes pueden tardar hasta 4 horas. Es importante mencionar en el inventario de PCA si hay algún terminal en el que desee tener estadísticas de conferencia compatibles y que también se asegure de que estas también se gestionan para los informes y todas las estadísticas para mostrar la información adecuada.

Para obtener una lista de los dispositivos compatibles según PCA en lo que respecta a las

conferencias y nuestras sesiones compatibles, consulte la sección Información general.

Paso 6. Vaya a Diagnose > Endpoint Diagnostics.

Para obtener estadísticas correctas de los terminales de conferencia, debe establecer su visibilidad en el nivel más alto posible permitido por el sistema.

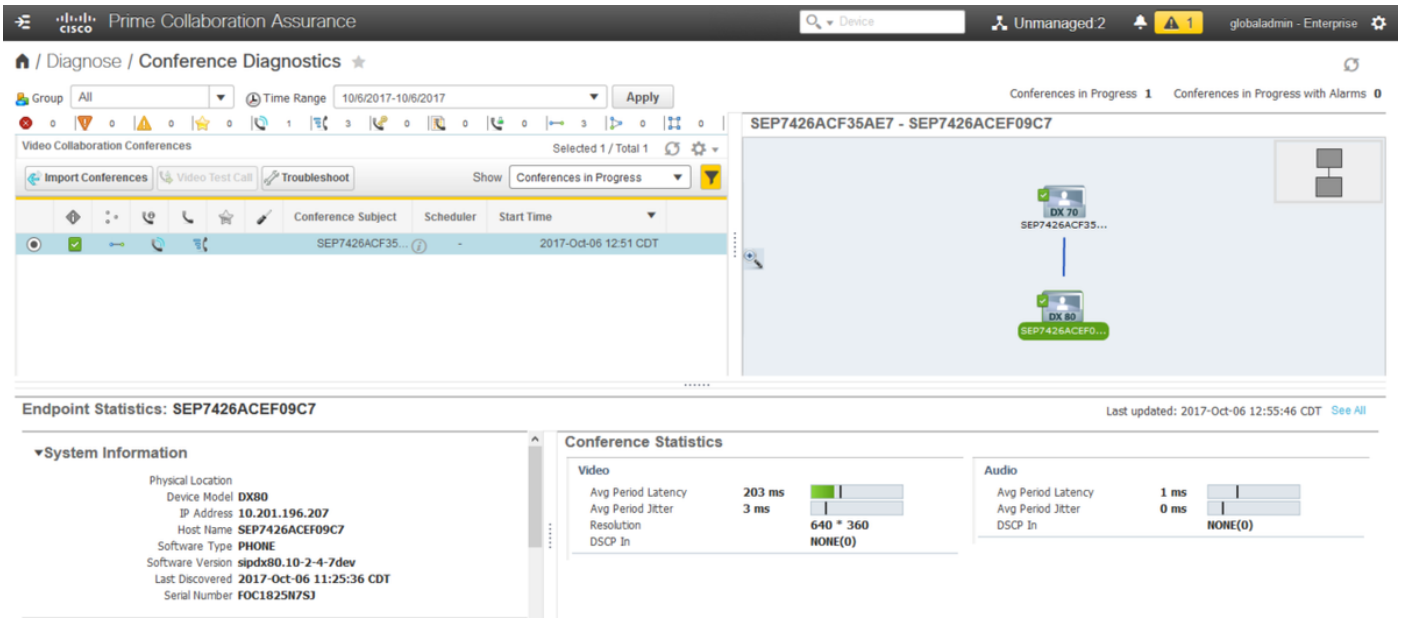
Seleccione todos los terminales que desee supervisar en el diagnóstico de conferencia, haga clic en Editar visibilidad y, a continuación, seleccione la visibilidad máxima.

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

Nota: Si selecciona, por ejemplo, 10 terminales y selecciona Visibilidad completa, se selecciona el nivel más alto de visibilidad compatible con cada dispositivo.

Paso 7. Para probar, nNavegue hasta Diagnose > Conference Diagnostics y una conferencia en curso o completada es como se muestra en la imagen.



En estas conferencias podrá ver la pérdida media de paquetes, la latencia y la fluctuación de las llamadas de audio y vídeo.

Además, se obtiene una topología de la sesión y de los dispositivos involucrados.

Alarmas relacionadas con la conferencia

Para el diagnóstico de conferencias, puede recibir tres alarmas diferentes en cualquier sesión y establecer sus umbrales:

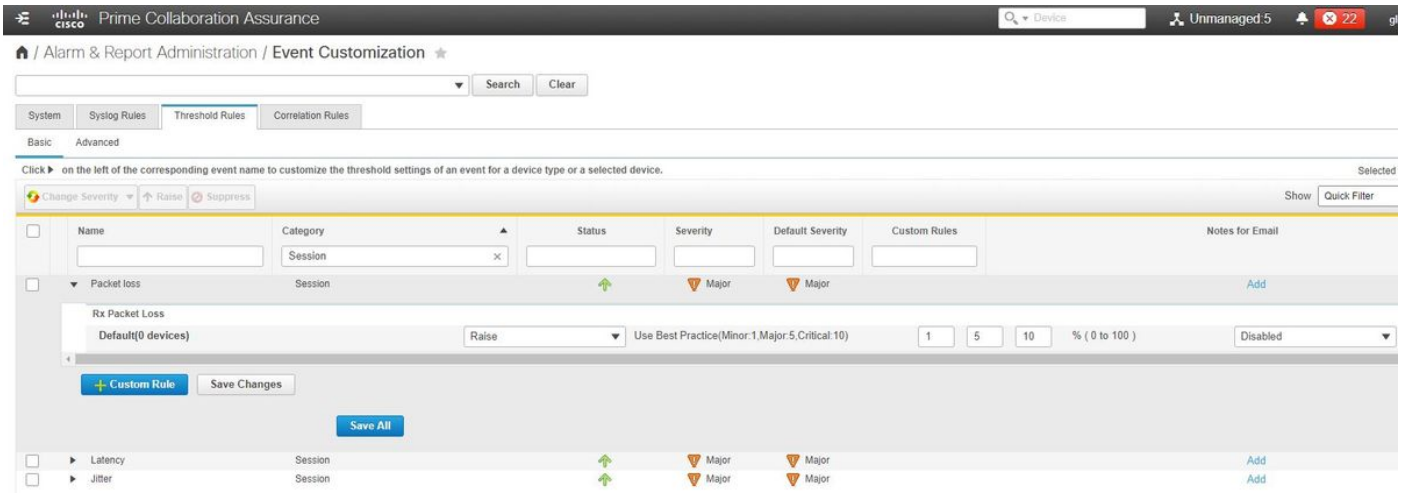
- Pérdida del paquete
- Latencia
- Fluctuación

Cada una de ellas puede modificar el umbral predeterminado, desactivarlo por completo o definir qué dispositivos desea asociar a esta alarma.

Paso 1. Navegue hasta Administración de alarmas e informes >Personalización de eventos.

Paso 2. Seleccione Threshold Rules y asegúrese de que ha seleccionado Basic.

Paso 3. Desplácese hacia abajo o filtre hacia la derecha para la sesión con nombre de categoría, como se muestra en la imagen.



Paso 4. Seleccione la flecha desplegable junto a la alarma que desea modificar y puede modificar los porcentajes menor, mayor o crítico para pérdida de paquetes, fluctuación o latencia.

Paso 5. Si desea superponerlo, cambie la opción Subir a Suprimir.

Paso 6. Si desea definir los puntos finales asociados a la alarma, seleccione Regla personalizada.

Paso 7. A continuación, seleccione Tipo de dispositivo > Seleccione Todos los dispositivos o Dispositivos seleccionables que desee para esta alarma y haga clic en Guardar.

Informes de conferencia relacionados

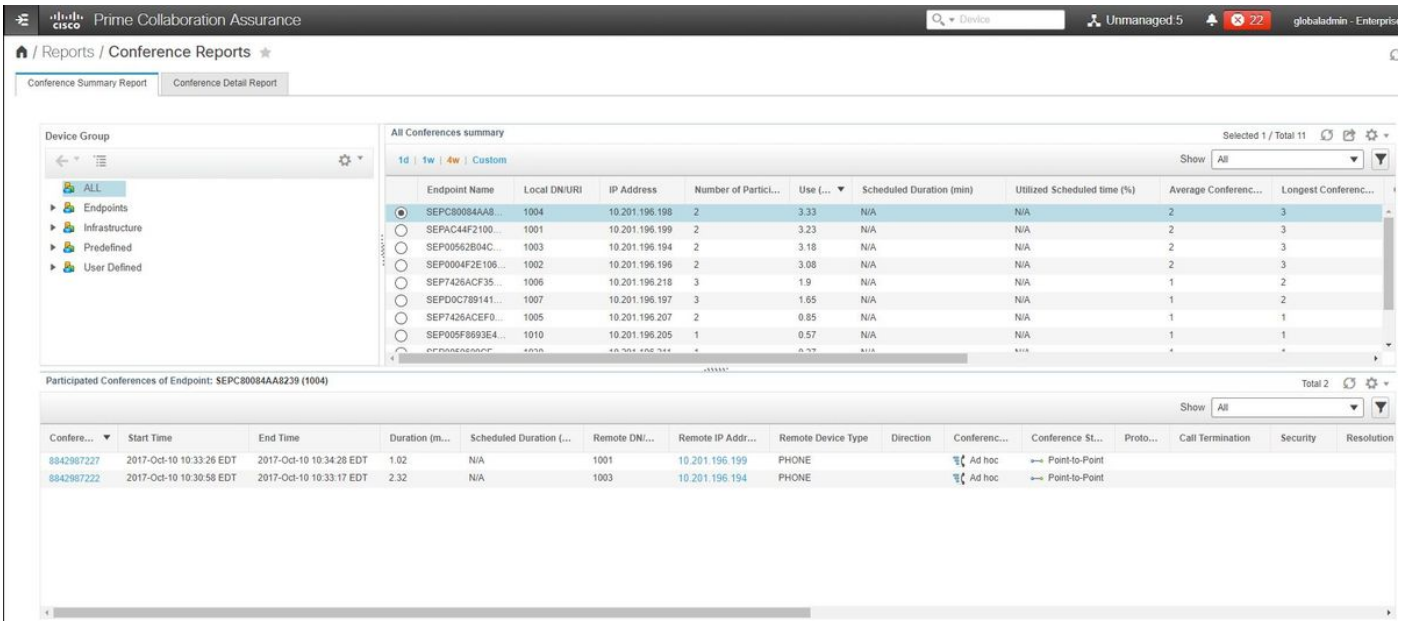
Para los diagnósticos de conferencia, se pueden recuperar y visualizar los informes.

Hay dos informes:

- Informes de conferencia
- Informes de terminales de Telepresence

En el caso de los informes de conferencia, puede ver una lista de todas las conferencias dentro de un período de tiempo de una a cuatro semanas o un período de tiempo personalizado, según sea necesario.

Paso 1. Vaya a Report > Conference Reports como se muestra en la imagen.



Informes de resumen de conferencia

Estos informes ofrecen una vista de todos los terminales que ha seleccionado como visibilidad limitada/completa y sus conferencias.

Las estadísticas que se muestran aquí son:

- Uso medio de conferencias
- Alarmas relacionadas con la conferencia
- Promedio de pérdida, fluctuación y latencia de paquetes
- Conferencia más larga

Esto puede ayudarle a obtener una visión granular de los problemas que puede tener en su red de voz/vídeo para determinar qué terminales tienen más problemas.

Así como utilizar su ancho de banda en correspondencia por uso

Ficha Informe detallado de conferencia

Si detecta una alarma para una conferencia, puede navegar a la pestaña Informe de detalles de la conferencia.

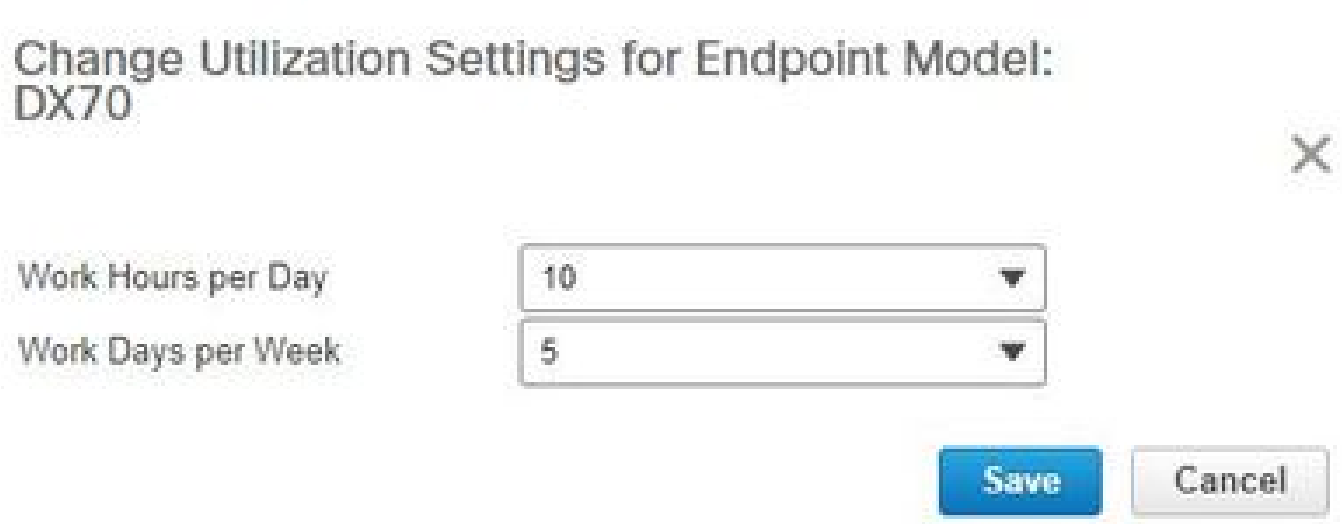
Una vez que haya seleccionado la conferencia, puede precisar el nombre del terminal, la versión del software y otros detalles que le puedan interesar.

En el caso de los informes de terminales de Telepresence, puede ver por terminal el

- Número de conferencias que tuvo este dispositivo
- Porcentaje de utilización
- Modelo de terminal
- Uso

Además, puede cambiar los parámetros de utilización en la ficha Change Utilization (Cambiar

utilización), como se muestra en la imagen.



De este modo, se establecen los parámetros del dispositivo para que el sistema sepa por el uso qué porcentaje mostrar.

El informe de resumen de terminal no mostrado muestra los terminales que no pudieron asistir a las conferencias programadas.

En este gráfico, puede ver el terminal y cuántas conferencias programadas totales y cuántas de ellas se produjeron y no se mostraron.

Llamada de prueba de vídeo de conferencia

Puede crear llamadas de prueba de vídeo punto a punto entre dos terminales de vídeo que se encuentran en un estado administrado para probar la red. Puede ver eventos y alarmas, estadísticas de sesiones, estadísticas de terminales y topología de red. Sólo se admiten los códecs de las series CTS, C y EX para esta llamada.

Además, se puede utilizar para validar que todas las funciones son correctas con los diagnósticos de conferencia.

Prerequisites

- Esta característica no se admite en la serie de códecs E20.
- Para utilizar esta función, se deben agregar credenciales CLI para los terminales.
- Asegúrese de que los terminales estén registrados y de que JTAPI esté habilitado para los terminales (si están registrados en Unified CM).
- La función de llamada de prueba de vídeo no está disponible si ha implementado Cisco Prime Collaboration en modo MSP.

Paso 1. Vaya a Diagnose > Endpoint Diagnostics.

Paso 2. Seleccione dos extremos aplicables según los requisitos previos.

Paso 3. Seleccione Ejecutar pruebas > Llamada de prueba de vídeo.

Paso 4. Puede programar la videollamada de prueba para que se ejecute ahora o para que se repita.

Paso 5. Esta llamada de prueba de vídeo se muestra a continuación en la pantalla Diagnóstico de conferencia.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

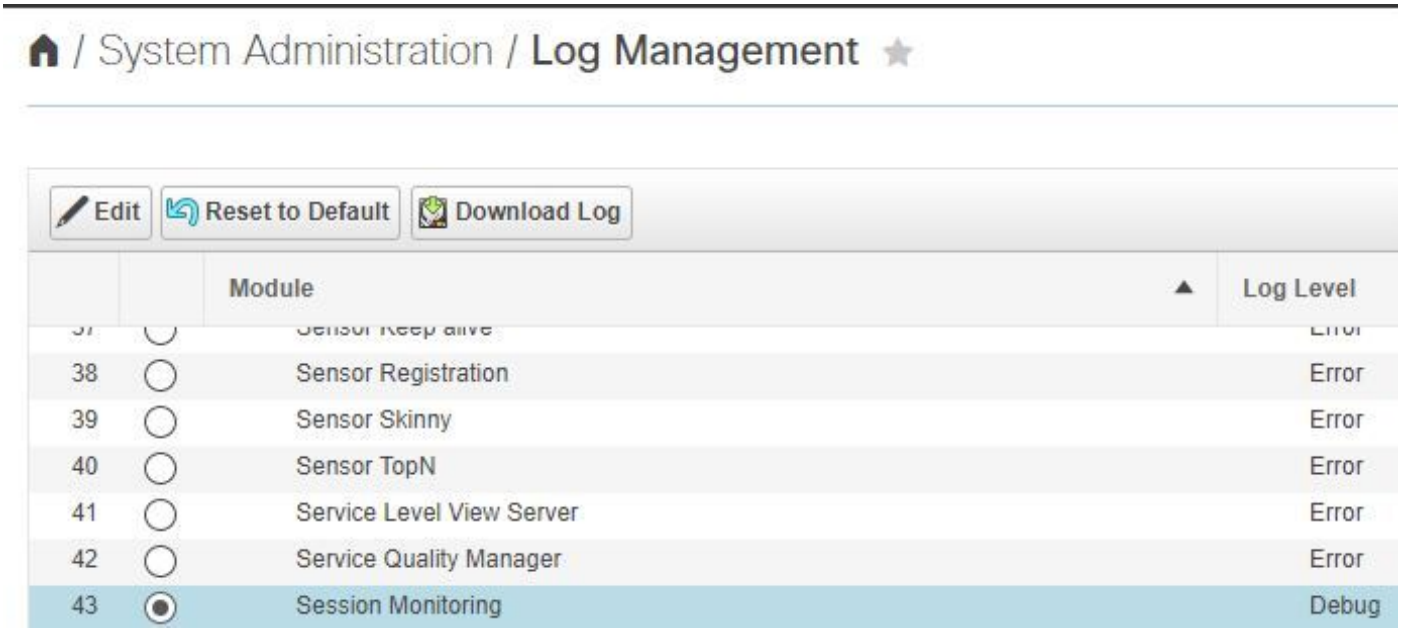
Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Registros que se recopilarán para solucionar problemas

Paso 1. Vaya a Administración del sistema > Administración de registro.

Paso 2. Desplácese hacia abajo hasta el módulo, seleccione Session Monitoring y seleccione Edit como se muestra en la imagen.



Paso 3. Cambie el nivel de registro a debug y haga clic en Save.

Paso 4. Reproduzca el problema y vuelva a la pantalla Log Management (Gestión de registros).

Paso 5. Después de reproducir el problema, seleccione Session Monitoring y Download Log.

Paso 6. Después de descargar, extraiga el archivo zip.

Paso 7. Abra el archivo zip y navegue hasta las ubicaciones para obtener registros útiles:

/opt/emms/emsam/log/SessionMon/

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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).