

# 配置Prime合作保證(PCA) -會議診斷

## 目錄

---

### [簡介](#)

### [必要條件](#)

#### [需求](#)

#### [採用元件](#)

### [背景資訊](#)

[將終端限制設定為每個OVA的有限可視性或完全可視性](#)

### [設定](#)

[案例 1. 影片終端註冊到Call Manager的會議](#)

[Cisco Unified Communications Manager設定](#)

[啟用HTTP](#)

[啟用SNMP](#)

[啟動CTI服務](#)

[為PCA CTI控制建立應用程式使用者 \( JTAPI使用者 \)](#)

[會議相關警報](#)

[會議相關報告](#)

[會議視訊測試呼叫](#)

[案例 2. 具有非Call Manager註冊端點的會議](#)

[會議相關警報](#)

[會議視訊測試呼叫](#)

### [驗證](#)

### [疑難排解](#)

---

## 簡介

本文檔介紹如何配置和設定Prime合作保證(PCA)中的會議診斷部署，以主動監控語音/視訊會議統計資訊。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- [Call Manager管理員登入](#)
- [PCA登入](#)
- [您的網真監控伺服器\(TMS\)](#)
- [核心/Expressway憑證 \( 如果適用 \)](#)

## 採用元件

本文檔中的資訊基於PCA版本11.x - 12.x。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

## 背景資訊

Cisco Prime Collaboration 11.x支援以下型別的可視性：

- 完全可視性-支援使用JTAPI/HTTP反饋和即時監控資訊（如會議統計資訊和會議資訊）進行呼叫檢測。
- 有限的可視性-使用JTAPI/HTTP反饋進行自動呼叫檢測，但不支援即時監控資訊（如會議統計資訊和會議資訊）。可視性有限的終端在會議拓撲中以半灰色的圖示表示。

Cisco Prime Collaboration 12.x支援以下型別的可視性：

- 完全可視性-支援使用JTAPI/HTTP反饋和即時監控資訊（如會議統計資訊和會議資訊）進行呼叫檢測。
- 無可視性-不支援使用JTAPI/HTTP反饋和即時監控資訊進行呼叫檢測。這些終端在「會議監控」頁面上以完全灰顯的圖示顯示。

### 將終端限制設定為每個OVA的有限可視性或完全可視性

- 小型開放式虛擬化存檔(OVA)最多可支援500個終端
- 中型OVA支援多達1000個終端
- 大型OVA支援多達1800個終端
- 超大型OVA支援多達2000個終端

有關會議和我們支援的會話的每個PCA支援的裝置清單如下面的表圖所示。

## 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 <i>intracluster</i> and <i>intercluster</i> sessions	Ad hoc,Scheduled	Point-to-point	Cisco TelePresence System 500, 1000, 3000, TX9000 Series.
Cisco Unified CM <i>intracluster</i> and <i>intercluster</i> sessions	Ad hoc,ScheduledStatic	Multipoint	Cisco TelePresence System 500, 1000, 3000, TX9000 Series, and CTMS.
Cisco VCS <i>intracluster</i> and <i>intercluster</i> 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 <i>intracluster</i> and <i>intercluster</i> sessions (with MCU)	Ad hoc,ScheduledPermanent (displayed as static)	Multipoint	Cisco C series, EX Series, Cisco MCU, Cisco MSE <sup>1</sup> , 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 <i>intracluster</i> and <i>intercluster</i> 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 <sup>2</sup>	Ad hoc	Point-to-pointMultipoint	<ul style="list-style-type: none"> <li>• Cisco C series, EX Series, Cisco MX series, Cisco MXP Series, Cisco IP Video Phone E20</li> <li>• Cisco TelePresence System 500, 1000, 3000, and TX9000 Series</li> <li>• Cisco TelePresence Server</li> <li>• IX 5000 series TelePresence endpoints</li> </ul>
Cisco Unified CM (8.6(1), 8.6(2), and 9.0) <i>intracluster</i> sessions <sup>3</sup>	Ad hoc	Point-to-point	<ul style="list-style-type: none"> <li>• Cisco C series, EX Series, Cisco MX series</li> <li>• Cisco TelePresence System 500, 1000, 3000, and TX9000 Series</li> <li>• IX 5000 series TelePresence endpoints</li> </ul>
Cisco Unified CM (8.6(1), 8.6(2), and 9.0) <i>intracluster</i> sessions	Ad hoc,Scheduled <b>Note</b> Scheduler must be CTS-Manager 1.7, 1.8, or 1.9.	Multipoint	<ul style="list-style-type: none"> <li>• Cisco C series, EX Series, Cisco MX series, Cisco IP Video Phone E20</li> <li>• Cisco TelePresence System 500, 1000, 3000, and TX9000 Series</li> <li>• CTMS 1.8 or Cisco TelePresence Server</li> </ul>
Sessions outside the enterprise firewall - Cisco VCS Expressway	Ad hocPermanent (displayed as static)	Point-to-point,Multipoint, Multisite	<ul style="list-style-type: none"> <li>• Cisco C series, EX Series, Cisco MX series, Cisco MXP Series, Cisco IP Video Phone E20</li> <li>• Cisco MCU or Cisco TelePresence Server</li> <li>• Cisco VCS Control and Cisco VCS Expressway</li> </ul>

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. <b>Note</b> 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 <a href="#">Supported Devices for Prime Collaboration Assurance</a> .
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 <b>Note</b> 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.

<sup>1</sup> The codian software must be running on Cisco MSE.

<sup>2</sup> This scenario is supported on CTS 1.7.4, and TC 4.1 to 7.0.

<sup>3</sup> 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.

## 設定

### 案例 1. 影片終端註冊到Call Manager的會議

步驟 1. 首先，您需要確保呼叫管理器處於「託管」狀態。

導航到資產>資產管理>管理憑據>為Call Manager集群建立配置檔案。



**注意：**請記住，每個憑據配置檔案都會對配置檔案中列出的每個ip使用相同的憑據。因此，如果您在同一個憑證配置檔案中列出Call Manager發佈伺服器和訂閱伺服器，它將使用這些相同的憑證來發現兩個IP地址。如果您的設定中確實存在導體，請首先發現該導體，然後發現Cisco Call Manager，如圖所示。

<input checked="" type="radio"/>	CUCM	ANY	10.201.196.222 ...
<input type="radio"/>	CUE	ANY	10.201.196.209
<input type="radio"/>	CUSP	SIPPROXY	10.201.160.42
<input type="radio"/>	Default	ANY	
<input type="radio"/>	JoeCUBE	ROUTER/VOICEGATEWAY	10.201.196.210

\* Indicates required fields

\*Profile Name:

Device Type:  (Optional)

\*IP Version:

\*Apply this credential to the given IP address:  ⓘ

---

▼ General SNMP Options

SNMP Timeout:  seconds

SNMP Retries:

SNMP Version:

步驟 2. 確保您已設定了超文本傳輸協定(HTTP)、簡單名稱管理協定(SNMP)和Java電話API (JTAPI)憑證

此外，您還必須在Call Manager Serviceability中啟用Cisco Computer Telephony Integration (CTI)服務。

## Cisco Unified Communications Manager設定

### 啟用HTTP

如果您要允許Cisco Prime Collaboration使用管理員憑證登入，則無需建立新使用者。或者，如果您要允許Cisco Prime合作管理器使用正確的憑證登入到Cisco Unified Communications Manager，您必須建立新的HTTP使用者組和Cisco Prime合作可用於通訊的相應使用者。

要建立使用者，請執行以下步驟：

步驟 1. 使用您的管理員帳戶登入到Cisco Unified CM管理Web介面。

步驟 2. 建立具有足夠許可權的使用者組。導航到使用者管理>使用者設定>訪問控制組，然後使用適當的名稱(在本例中為PC\_HTTP\_Users)建立新使用者組。現在，選擇Save。

步驟 3. 導航到使用者管理 > 使用者設定 > 訪問控制組，然後選擇查詢。尋找您定義的群組，然後按一下右邊的圖示。

步驟 4. 選取將角色指定給群組，然後選取下列角色：

- 標準AXL API訪問
- 標準CCM管理員使用者

- 標準可維護性管理

步驟 5. 按一下Save。

步驟 6. 從主選單導航到使用者管理>應用程式使用者>建立新使用者。

在「應用程式使用者組態」頁面上指定適當的密碼。您只能從Available Devices文本區域選擇特定型別的裝置，或允許Cisco Prime Collaboration監控所有裝置

步驟 7. 在許可權資訊部分中，選擇增加到使用者組，然後選擇在步驟1中建立的組。（例如，PC\_HTTP\_Users）。

步驟 8. 按一下「儲存」。頁面會重新整理，並顯示正確的許可權。

## 啟用SNMP

預設情況下，Cisco Unified Communications Manager中未啟用SNMP。

若要啟用SNMP：

步驟 1. 在Cisco Unified Communications Manager Web GUI中登入Cisco Unified Serviceabilityview。

步驟 2. 導航到工具>服務啟用。

步驟 3. 選擇Publisher Server。

步驟 4. 導航到效能>監控服務，然後選中Cisco Call Manager SNMP服務對應的覈取方塊。

步驟 5. 在螢幕底部選擇Save。

建立SNMP社群字串：

步驟 1. 登入Cisco Unified Serviceabilityview the Cisco Unified Communications Manager Web GUI。

步驟 2. 在Cisco Unified Serviceability檢視的主選單中，導航至SNMP > v1/v2c > Community String。

步驟 3. 選取伺服器，然後按一下「尋找」。

如果已經定義了社群字串，則社群字串名稱將顯示在搜尋結果中。

步驟 4. 按一下「新增」「新建」，在不顯示任何結果的情況下新增字串。

步驟 5. 指定所需的SNMP資訊並儲存配置。

---

 注意：僅需要SNMP只讀(RO)訪問。

---

## 啟動CTI服務

執行所需的Cisco Unified Communications Manager節點程式，最好在兩個節點上設定。

步驟 1. 登入到Cisco Unified Serviceability，該功能可在Cisco Unified Communications Manager圖形使用者介面中檢視。

步驟 2. 導航到工具>服務啟用。

步驟 3. 從下拉選單中選擇伺服器。

步驟 4. 在CM Services部分中，選中Cisco CTI Manager 覈取方塊。

步驟 5. 在螢幕頂部選擇Save

為PCA CTI控制建立應用程式使用者 ( JTAPI使用者 )

JTAPI用於從裝置檢索會話狀態資訊。您必須在呼叫處理器中為CTI控制建立具有接收終端上的JTAPI事件所需許可權的應用使用者。Prime合作管理多個呼叫處理器集群。必須確保群集ID是唯一的。建立一個新的應用使用者，以幫助Cisco Prime Collaboration獲取所需資訊。

要建立新的JTAPI應用程式使用者，請執行以下步驟：

步驟 1. 透過您的管理員帳戶登入到Cisco Unified CM管理Web介面。

步驟 2. 建立具有足夠許可權的使用者組。導航到使用者管理>使用者設定>訪問控制組，然後使用適當的名稱(在本例中為PC\_HTTP\_Users)建立新使用者組。現在，選擇Save。

步驟 3. 選擇User Management > User Settings > Access Control Group，然後按一下Find。尋找您定義的群組，並選取右邊的圖示。

步驟 4. 按一下「將角色指定給群組」並選取下列角色：


- 標準CTI允許呼叫監控
- 已啟用標準CTI
- 標準CTI允許控制支援互聯Xfer和conf的電話

步驟 5. 選取儲存。

步驟 6. 從主選單導航到使用者管理>應用程式使用者>建立新使用者。

在「應用程式使用者組態」頁面上指定適當的密碼。您可以從Available Devices文本區域選擇特定型別的裝置，或允許Cisco Prime Collaboration監控所有裝置。


---

 注意：密碼不能包含分號(;)或等於(=)。

---

步驟 7. 在許可權資訊部分，選擇增加到訪問控制組，然後選擇在步驟1中建立的組。(例如，PC\_HTTP\_Users)。

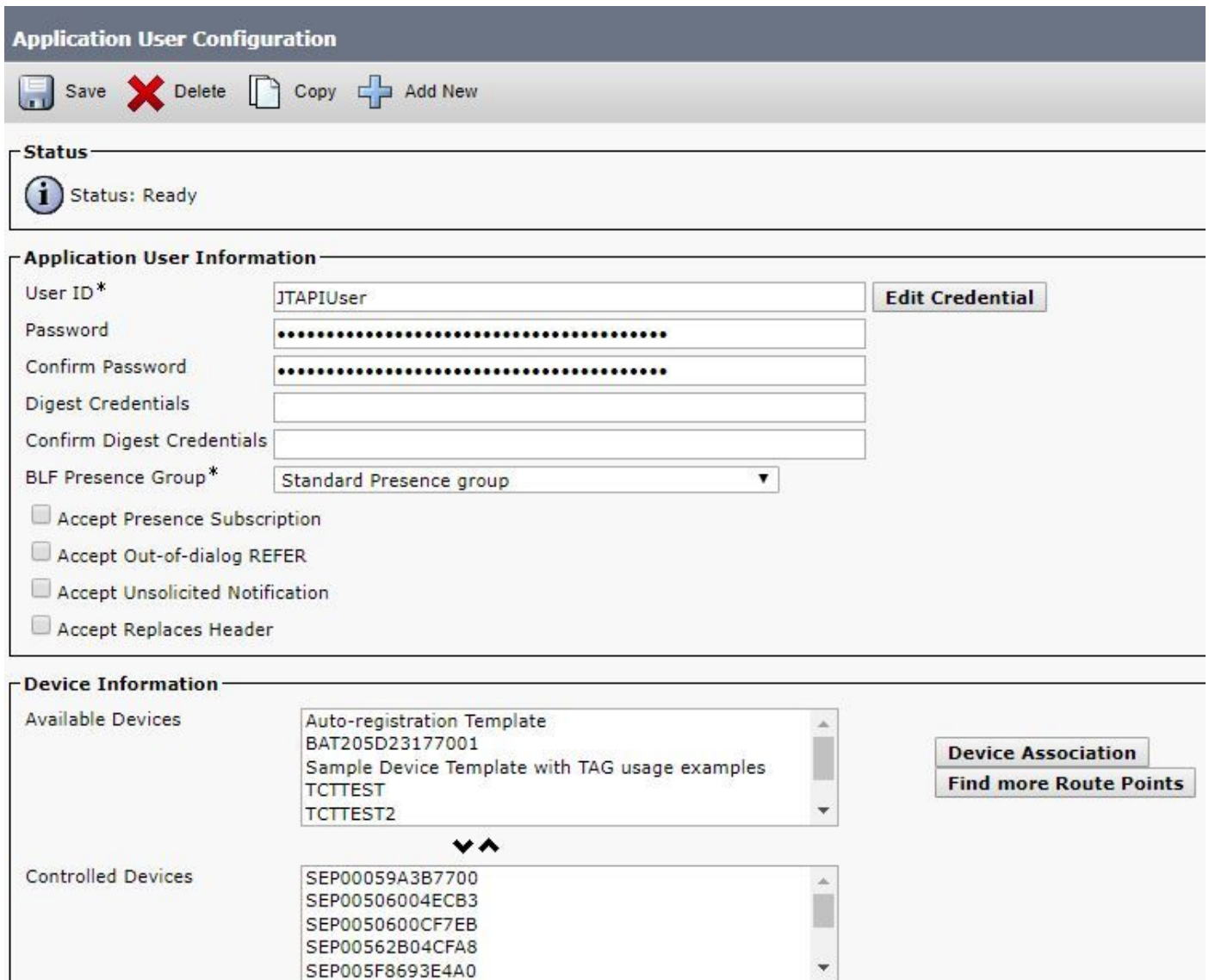
步驟 8. 按一下「儲存」。頁面會重新整理，並顯示正確的許可權。

 注意：如果在增加JTAPI使用者之前管理了Call Manager，請確保已將JTAPI使用者增加到Call Manager的憑據配置檔案中，然後重新搜尋該使用者。

從場景1繼續。步驟：

步驟 3. 導航到您建立的Call Manager JTAPI應用使用者，然後將支援的終端從可用裝置移動到受控裝置。

您可以透過裝置關聯功能執行此操作，如圖所示。



The screenshot displays the 'Application User Configuration' interface. At the top, there is a header bar with the title 'Application User Configuration' and a toolbar containing 'Save', 'Delete', 'Copy', and 'Add New' buttons. Below the header, the 'Status' section shows 'Status: Ready'. The main area is divided into two sections: 'Application User Information' and 'Device Information'. In the 'Application User Information' section, there are input fields for 'User ID\*' (containing 'JTAPIUser'), 'Password', 'Confirm Password', 'Digest Credentials', and 'Confirm Digest Credentials'. There is also a dropdown menu for 'BLF Presence Group\*' set to 'Standard Presence group'. Below these are several checkboxes for 'Accept Presence Subscription', 'Accept Out-of-dialog REFER', 'Accept Unsolicited Notification', and 'Accept Replaces Header'. An 'Edit Credential' button is located to the right of the User ID field. The 'Device Information' section features two scrollable lists: 'Available Devices' (containing 'Auto-registration Template', 'BAT205D23177001', 'Sample Device Template with TAG usage examples', 'TCITEST', and 'TCITEST2') and 'Controlled Devices' (containing 'SEP00059A3B7700', 'SEP00506004ECB3', 'SEP0050600CF7EB', 'SEP00562B04CFA8', and 'SEP005F8693E4A0'). A 'Device Association' button and a 'Find more Route Points' button are positioned to the right of the device lists.

如果返回到終端設定為每個OVA的有限可視性或完全可視性的限制，則可以驗證已增加到OVA大小的裝置數量。

在此螢幕中，您可以按裝置名稱、說明或目錄號進行過濾，以幫助您管理和過濾這些裝置，如圖所示。

請注意在步驟7中新增的這些裝置。



User Device Association				
	Select All		Clear All	
	Clear All In Search		Save Selected/Changes	
Remove All Associated				
User Device Association (1 - 14 of 14)				
Find User Device Association where Name <input type="text"/> begins with <input type="text"/> Find Clear Filter				
<input checked="" type="checkbox"/> Show the devices already associated with user				
<input type="checkbox"/>			Device Name	
<input checked="" type="checkbox"/>			SEP00059A3B7700	1000
<input checked="" type="checkbox"/>			SEP00506004ECB3	1011
<input checked="" type="checkbox"/>			SEP0050600CF7EB	1030
<input checked="" type="checkbox"/>			SEP00562B04CFA8	1003
<input checked="" type="checkbox"/>			SEP005F8693E4A0	1010
<input checked="" type="checkbox"/>			SEP7426ACEF09C7	1005
<input checked="" type="checkbox"/>			SEP7426ACF35AE7	1006
<input checked="" type="checkbox"/>			SEPD0C789141410	1007

請確定已為此JTAPI使用者新增正確的使用者角色：

- 標準CTI允許呼叫監控
- 已啟用標準CTI
- 標準CTI允許控制支援已連線Xfer和conf的電話，如圖所示。

### Permissions Information

Groups: JTAPIUser Add to Access Control Group Remove from Access Control Group

Roles: Standard CTI Allow Call Monitoring Standard CTI Allow Control of Phones supporting Conne Standard CTI Enabled View Details

有關每個PCA支援的裝置清單，有關會議和我們支援的會話，請返回到「背景資訊」部分。

注意：此外，請確保由CTI應用程式使用者控制的裝置在裝置資訊下選中「允許透過CTI控制裝置」覈取方塊，如下圖所示。



注意：在您繼續閱讀下面的內容之前，請務必注意：如果您將終端註冊到Call Manager並且將Call Manager與VCS/TMS整合，那麼您首先會發現VCS/TMS，然後最後會發現Call Manager。這樣，從庫存的角度來看，您的所有基礎設施都會對映到正確的位置。此外，當您發現VCS/TMS時，請確保將預設的Discover頁籤更改為TMS/VCS或呼叫管理器各自的裝置。

步驟 4. 接下來，在PCA中，選擇裝置發現並輸入您的呼叫管理器的IP地址，選中Auto-Configuration上的兩個覈取方塊，然後選擇Run Now，如下圖所示。

**Discover Devices**

Manage Credentials → Device Discovery

**ⓘ** Ensure creating Cluster information using "Manage TMS Cluster" UI before discovering TMS cluster. \* Indicates required field

Job Name: Discovery 2017-Oct-26 12:58:16 EDT

Check Device Accessibility

Discover: Communications Manager (UCM) Cluster and connected devices

\*IP Address: 10.201.196.222|10.201.196.221 ⓘ

Associate to Domain: Internal (Optional)

*If you have SIP trunks configured between the desired "Communications Manager" cluster and other "Communications Manager" clusters, please exclude all the Destination IPs of those SIP trunks in the Discovery Filter while triggering Logical Discovery.*

**▼ Auto-Configuration**

Add the Prime Collaboration server as a CDR Destination in the Unified CM servers ⓘ

Add the Prime Collaboration server as a Syslog Destination in the Unified CM servers ⓘ

**▶ Filters**

**▶ Advanced Filters**

Back Schedule Run Now

步驟 5. 在Call Manager處於Managed狀態後，繼續執行步驟6。

**✎** 注意：如果Call Manager未處於Managed狀態，大多數時間都是由HTTP或SNMP引起的，如果需要進一步的幫助，請建立TAC支援案例以使Call Manager處於Managed狀態。

步驟 6. 導航到資產>資產計畫>集群資料發現計畫，選擇立即運行。

**✎** 注意：這取決於您有多少已註冊/未註冊裝置。此過程可能需要幾分鐘到幾小時之間的任意時間。透過刷新頁面來全天檢查。此外，這會將Call Manager集群對映在一起，並檢索您的所有終端。完成之後，請繼續下一步。

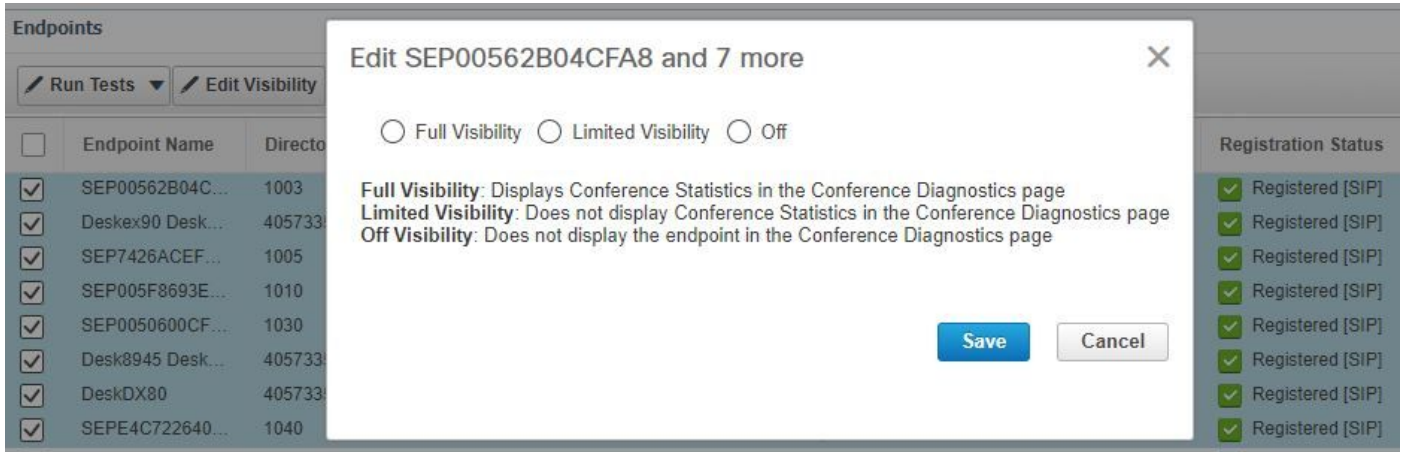
**✎** 注意：如果有任何端點希望獲得支援的會議統計資訊，則在PCA資產中務必提及。確保為報告和所有統計資訊妥善管理這些資訊，以顯示正確的資訊。

步驟 7. 導航到診斷>終端診斷。

要獲取會議終端的最新統計資訊，您需要將其可視性設定為系統允許的最高級別。


選擇您想要在會議診斷中監控的所有終端，然後按一下Edit Visibility，然後選擇Full Visibility，如下圖所示。

有限可視性只顯示拓撲中的裝置，但沒有統計資訊，並且它無法檢索與會議診斷相關的裝置的適用警報。

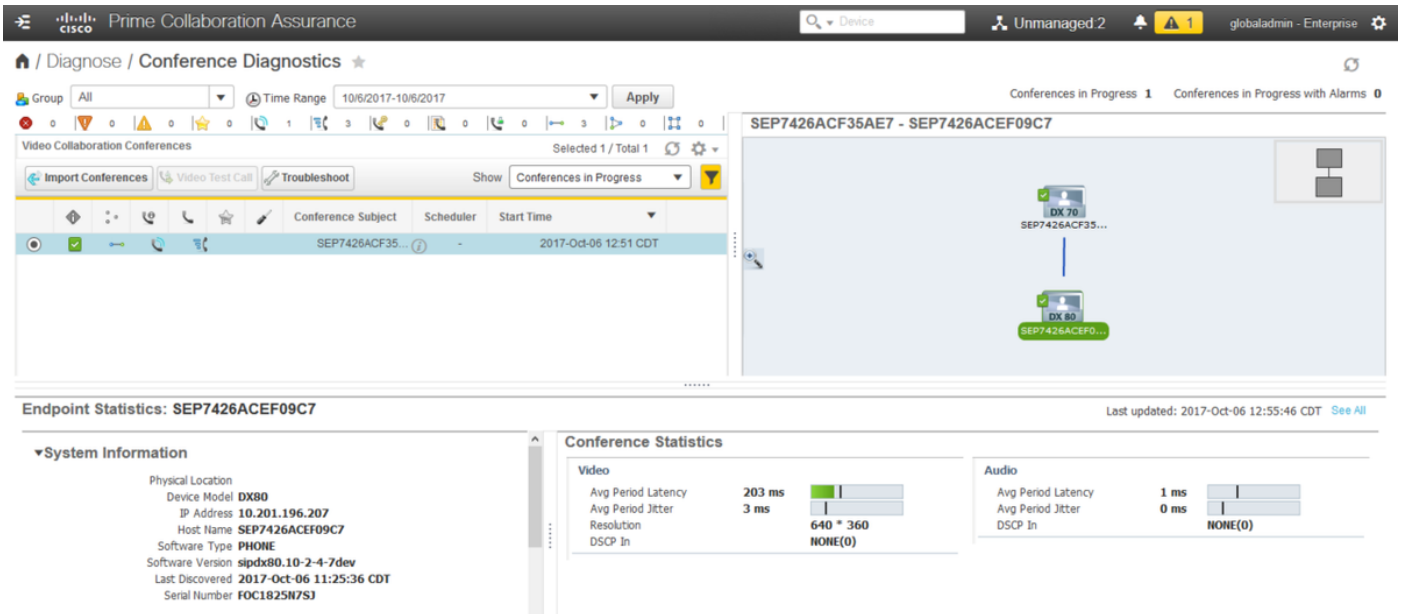


The following table lists the default and maximum visibility details for the endpoints:

Endpoint Type	Default Visibility	Maximum Visibility
<ul style="list-style-type: none"> <li>CTS 500, 1000, and 3000 Series</li> <li>Cisco Codec</li> <li>Cisco TelePresence SX20</li> <li>Cisco TelePresence MXP Series</li> <li>Cisco IP Video Phone E20</li> </ul>	Full	Full
<ul style="list-style-type: none"> <li>Cisco Jabber Video for TelePresence (Movi)</li> <li>Polycom</li> </ul>	Limited	Limited
Cisco Cius	Off	Full
Cisco IP Phones (89xx, 99xx)	Off	Full
Cisco Desktop Collaboration Experience DX650 and DX630	Off	Full
<ul style="list-style-type: none"> <li>Cisco SX80 and Cisco SX10</li> <li> <ul style="list-style-type: none"> <li>Cisco MX200 G2, Cisco MX300 G2, Cisco MX700, and Cisco MX800</li> </ul> </li> </ul>	Full	Full
Cisco DX70 and DX80	Off	Full
<b>MRA Endpoints:</b> <ul style="list-style-type: none"> <li>Cisco Jabber</li> <li>Cisco TelePresence MX Series</li> <li>Cisco TelePresence System EX Series</li> <li>Cisco TelePresence System SX Series</li> </ul>	Limited	Limited

 註：例如，如果您選擇10個終端並選擇「完全可視性」，則它會為每個裝置選擇最高級別的可視性支援。

步驟 8. 要進行測試，請導航到診斷>會議診斷，並顯示正在進行或已完成會議，如圖所示。



The screenshot displays the Cisco Prime Collaboration Assurance interface for Conference Diagnostics. The top navigation bar includes the Cisco logo, the product name, a search bar, and user information. The main content area is divided into several sections:

- Video Collaboration Conferences:** A table listing conferences with columns for Group, Time Range, and a list of conferences. One conference is selected.
- Endpoint Statistics: SEP7426ACEF09C7:** A detailed view of the selected conference, including a network diagram showing two endpoints (DX 70 and DX 80) connected to a central node.
- System Information:** A table of device details for the selected endpoint.

Property	Value
Physical Location	
Device Model	DX80
IP Address	10.201.196.207
Host Name	SEP7426ACEF09C7
Software Type	PHONE
Software Version	sipdx80.10-2-4-7dev
Last Discovered	2017-Oct-06 11:25:36 CDT
Serial Number	FOC1825N7S3
- Conference Statistics:** A summary of performance metrics for video and audio.

Metric	Value
Avg Period Latency (Video)	203 ms
Avg Period Jitter (Video)	3 ms
Resolution (Video)	640 * 360
DSCP In (Video)	NONE(0)
Avg Period Latency (Audio)	1 ms
Avg Period Jitter (Audio)	0 ms
DSCP In (Audio)	NONE(0)

在這些會議中，您可以檢視音訊和視訊呼叫的平均資料包丟失、延遲和抖動。

此外，獲取會話和所涉及裝置的拓撲。

目前，會議診斷程式根據DN提取資訊，如果您的環境已共用DN，PCA將檢索收到的第一個會議資訊。

## 會議相關警報

對於會議診斷，您可以接收任何會話的三個不同警報並設定其閾值：

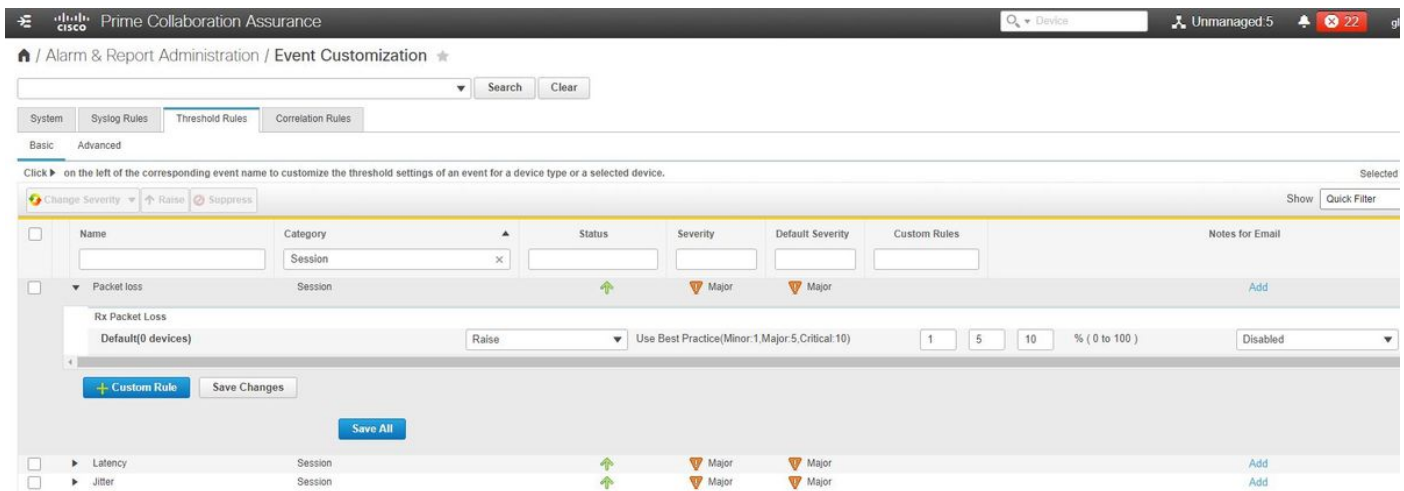
- 封包丟失
- 延遲
- 抖動

對於每種設定，您可以修改預設閾值，或定義您希望與此警報關聯的裝置。

步驟 1. 導航到 Alarm & Report Administration > Event Customization。

步驟 2. 選擇 Threshold Rules 並確保已選擇 Basic。

步驟 3. 向下捲動或按一下右側「Category Named Session」，如下圖所示。



步驟 4.選擇警報旁邊的下拉箭頭。您要修改並修改資料包丟失、抖動或延遲的次要、主要或關鍵百分比。

步驟 5.如果您想要驚豔，請將「提升」切換為「驚豔」。

步驟 6.如果要定義與警報關聯的終端，可以選擇Custom Rule。

步驟 7.然後，選擇要用於此警報的Device Type > Select All Devices或Selectable Devices，然後按一下Save。

## 會議相關報告

對於會議診斷報告，可以檢索和檢視。

有兩個報告：

- 會議報告
- Telepresence終端報告

對於「會議報告」，您可以根據需要檢視一至四週時間範圍內或自定義時間段內的所有會議清單。

步驟 1.導航到報告>會議報告，如圖所示。

The screenshot displays the Cisco Prime Collaboration Assurance interface for Conference Reports. The top navigation bar includes the Cisco logo, 'Prime Collaboration Assurance', a search bar, and 'Unmanaged: 5'. The main header shows 'Reports / Conference Reports' with two tabs: 'Conference Summary Report' (active) and 'Conference Detail Report'. On the left, a 'Device Group' tree shows 'ALL' selected under 'Endpoints'. The main area is titled 'All Conferences summary' and shows a table with columns: Endpoint Name, Local DNURI, IP Address, Number of Participations, Use (%), Scheduled Duration (min), Utilized Scheduled time (%), Average Conference Duration, and Longest Conference Duration. Below this, a section titled 'Participated Conferences of Endpoint: SEPC80084A8239 (1004)' shows a table with columns: Conference ID, Start Time, End Time, Duration (min), Scheduled Duration (min), Remote DNURI, Remote IP Address, Remote Device Type, Direction, Conference Type, Conference Status, Protocol, Call Termination, Security, and Resolution.

## 會議摘要報告

此報告提供您已選擇為有限/完全可視性的每個終端及其會議的檢視。

此處顯示的統計資料如下：

- 平均會議使用量
- 與會議相關的警報
- 平均丟包、抖動和延遲
- 最長的會議

這有助於您對語音/影片網路中存在的問題進行細緻的檢視，以確定哪些終端的問題最多。

此外，您還可以根據使用情況使用相應的頻寬。

## 會議詳細資訊報告頁籤

如果確實遇到會議的警報，您可以導航到會議詳細資訊報告頁籤。

選擇會議後，您可以對其進行細化，以查詢您可能有興趣的終端名稱、軟體版本和其他詳細資訊。

對於Telepresence Endpoint Reports，您可以按終端檢視：

- 此裝置擁有的會議數目
- 使用率百分比
- 終端型號
- 使用量

此外，您可以透過Change Utilization頁籤更改利用率引數，如下圖所示。

## Change Utilization Settings for Endpoint Model: DX70



Work Hours per Day	10	▼
Work Days per Week	5	▼

**Save** **Cancel**

這會設定該裝置的引數，以便系統從使用狀況得知要顯示的百分比。

「No Show Endpoint Summary Report」顯示未出席計畫會議的終端。

在此圖形中，您還可以檢視終端以及總計畫會議數，以及其中有多少會議已經舉行並且沒有節目。

### 會議視訊測試呼叫

您可以在兩個處於託管狀態的影片終端之間建立點對點影片測試呼叫，以測試您的網路。您可以檢視事件和警報、會話統計資訊、終端統計資訊以及與其他呼叫類似的統計資訊。此呼叫僅支援CTS、C和EX系列編解碼器。

此外，這還可用於驗證會議診斷的所有功能是否正常。

#### 必要條件

- E20編解碼器系列不支援此功能。
- 要使用此功能，必須為終端增加CLI憑證。
- 確保終端已註冊並為終端啟用JTAPI（如果終端已註冊到Unified CM）。
- 如果您在MSP模式下部署了Cisco Prime Collaboration，則影片測試呼叫功能不可用。

步驟 1. 導航到診斷>終端診斷。

步驟 2. 根據提及的必要條件選取兩個適用的端點。


步驟 3. 選擇Run Tests > Video Test Call。

步驟 4. 您可以將視訊測試呼叫排定為立即執行或依照重新發生的排程執行。

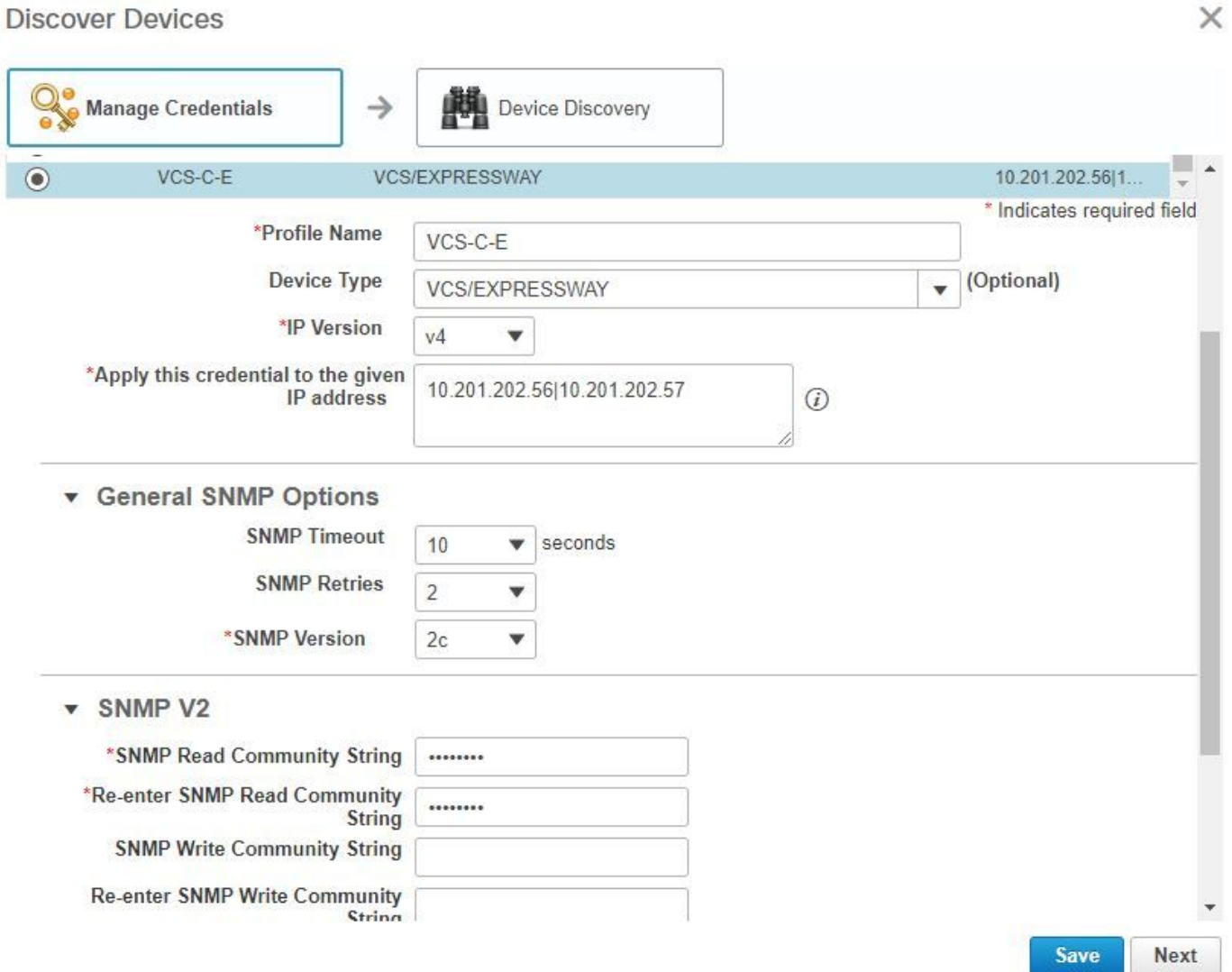
步驟 5. 然後，此影片測試呼叫將顯示在會議診斷螢幕中。

### 案例 2. 具有非Call Manager註冊端點的會議



步驟 1. 確保Telepresence Management Suite (TMS)和Video Communications Server (VCS)憑證可用。

 注意：在此場景中發現VCS/TMS時，發現過程非常重要。如果您的設定中確實有呼叫管理器，請先查詢指揮交換機，然後查詢Cisco Call Manager。

步驟 2. 導航到資產>資產管理>管理憑據> 選擇增加，然後輸入您的TMS資訊，同時為您的VCS建立單獨的憑據配置檔案，如圖所示。



Discover Devices ✕

 Manage Credentials →  Device Discovery

VCS-C-E VCS/EXPRESSWAY 10.201.202.56|1...

\*Profile Name  \* Indicates required field

Device Type  (Optional)

\*IP Version

\*Apply this credential to the given IP address  ⓘ

▼ General SNMP Options

SNMP Timeout  seconds

SNMP Retries

\*SNMP Version

▼ SNMP V2

\*SNMP Read Community String

\*Re-enter SNMP Read Community String

SNMP Write Community String

Re-enter SNMP Write Community String

步驟 3. 建立憑據配置檔案後，選擇Device Discovery，輸入ip addresses，然後在Discovery頁籤中選擇VCS並發現VCS裝置。並且，為TMS選擇TMS並輸入它的IP地址。按一下Run Now (如圖所示)。



## Discover Devices



**i** Ensure creating Cluster information using "Manage TMS Cluster" UI before discovering TMS cluster.

\* Indicates required field

Job Name

Check Device Accessibility

Discover

\*IP Address  **i**

Associate to Domain  (Optional)

*If you have SIP trunks configured between the desired "Communications Manager" cluster and other "Communications Manager" clusters, please exclude all the Destination IPs of those SIP trunks in the Discovery Filter while triggering Logical Discovery.*

### ► Filters

### ► Advanced Filters

### ▼ Schedule

Start Time  Date:

(yyyy/MM/dd hh:mm AM/PM)

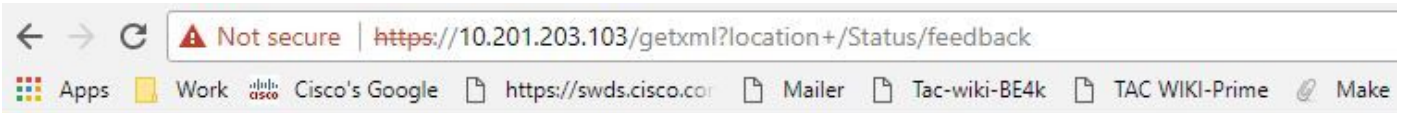
Recurrence  None  Hourly  Daily  Weekly  Monthly

步驟 4. 確保VCS和TMS處於託管狀態。

注意：如果VCS或TMS未處於Managed狀態，大多數時間都是由HTTP或SNMP引起的，如果需要進一步的幫助，請建立TAC案例以使VCS/TMS處於Managed狀態。


注意：使用此URL並在VCS處於「託管」狀態後使用適當的IP地址替換IP\_Address\_of\_VCS\_Server。PCA伺服器必須註冊為VCS的反饋伺服器，這樣可以確保在會議會話結束時，VCS發回PCA的資料沒有問題。

[https://<IP\\_Address\\_of\\_VCS\\_Server>/getxml?location+/Status/feedback](https://<IP_Address_of_VCS_Server>/getxml?location+/Status/feedback)時會請求http憑證，輸入後，您必須收到回應，如圖所示。




This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<Status xmlns="http://www.tandberg.no/XML/CUIL/1.0" product="TANDBERG VCS" version="X8.9">
  <SystemUnit item="1">
    <Product item="1">TANDBERG VCS</Product>
    <Uptime item="1">935228</Uptime>
    <SystemTime item="1">2017-10-27 16:50:05</SystemTime>
    <TimeZone item="1">US/Central</TimeZone>
    <LocalTime item="1">2017-10-27 11:50:05</LocalTime>
  <Software item="1">
    <Version item="1">X8.9</Version>
    <Build item="1">oak_v8.9.0_rc_2</Build>
    <Name item="1">s42700</Name>
    <ReleaseDate item="1">2016-11-24</ReleaseDate>
    <ReleaseKey item="1">5026834098101150</ReleaseKey>
  <Configuration item="1">
    <NonTraversalCalls item="1">750</NonTraversalCalls>
    <TraversalCalls item="1">100</TraversalCalls>
    <Registrations item="1">0</Registrations>
    <TPRoom item="1">50</TPRoom>
    <UserDevice item="1">50</UserDevice>
    <Expressway item="1">False</Expressway>
    <Encryption item="1">True</Encryption>
    <Interworking item="1">True</Interworking>
    <FindMe item="1">True</FindMe>
    <DeviceProvisioning item="1">True</DeviceProvisioning>
    <DualNetworkInterfaces item="1">False</DualNetworkInterfaces>
    <AdvancedAccountSecurity item="1">True</AdvancedAccountSecurity>
    <StarterPack item="1">False</StarterPack>
    <EnhancedOCSCollaboration item="1">False</EnhancedOCSCollaboration>
    <ExpresswaySeries item="1">True</ExpresswaySeries>
  </Configuration>
</SystemUnit>
</Status>
```

 注意：如果Prime Collaboration未通過HTTP反饋訂閱訂閱VCS，則在註冊的終端加入或離開會話，或向VCS註冊或取消註冊時，VCS不會通知它。在這種情況下，請根據需要將這些終端的可視性設定為完全或受限，並確保您的VCS處於「託管」狀態。

步驟 5. 導航到資產>資產計畫>集群資料發現計畫，選擇立即運行。

 注意：此過程可能需要一些時間，因為它在所有基礎設施裝置上執行此功能。因此，如果幾分鐘後仍未完成，請在1-2小時後重新檢查。超大型系統最多可能需要4個小時。如果有任何端點希望獲得支援的會議統計資訊，PCA資產中必須提及這一點，並且您還要確保這些端點受報告的管理，並且所有統計資訊都顯示正確的資訊。

有關會議及我們支援的會話方面根據PCA支援的裝置清單，請參閱背景資訊部分。


步驟 6. 導航到診斷>終端診斷。

要獲取會議端點的正確統計資訊，您需要將其可視性設定為系統允許的最高級別。

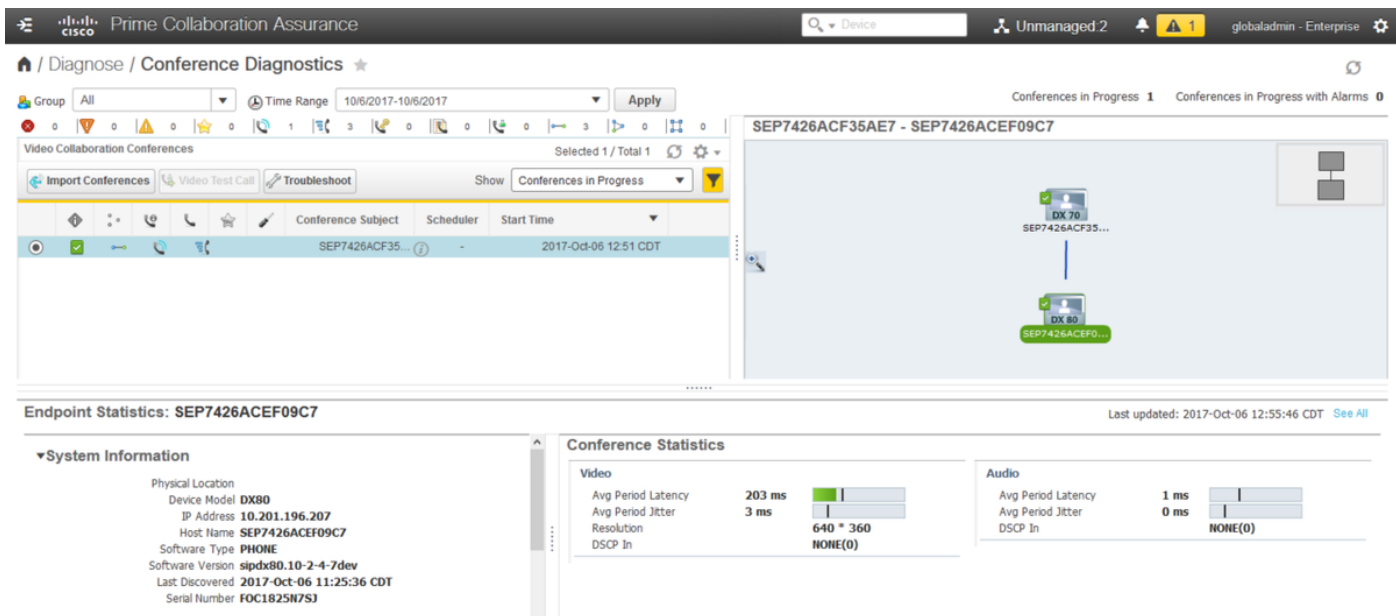
選擇您想要在會議診斷中監控的所有終端，然後按一下Edit Visibility，然後選擇最大可視性。

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

Endpoint Type	Default Visibility	Maximum Visibility
<ul style="list-style-type: none"><li>CTS 500, 1000, and 3000 Series</li><li>Cisco Codec</li><li>Cisco TelePresence SX20</li><li>Cisco TelePresence MXP Series</li><li>Cisco IP Video Phone E20</li></ul>	Full	Full
<ul style="list-style-type: none"><li>Cisco Jabber Video for TelePresence (Movi)</li><li>Polycom</li></ul>	Limited	Limited
Cisco Cius	Off	Full
Cisco IP Phones (89xx, 99xx)	Off	Full
Cisco Desktop Collaboration Experience DX650 and DX630	Off	Full
<ul style="list-style-type: none"><li>Cisco SX80 and Cisco SX10</li><li>Cisco MX200 G2, Cisco MX300 G2, Cisco MX700, and Cisco MX800</li></ul>	Full	Full
Cisco DX70 and DX80	Off	Full
MRA Endpoints: <ul style="list-style-type: none"><li>Cisco Jabber</li><li>Cisco TelePresence MX Series</li><li>Cisco TelePresence System EX Series</li><li>Cisco TelePresence System SX Series</li></ul>	Limited	Limited

 注意：如果您選擇（例如）10個終端並選擇「完全可視性」，則它會為每個裝置選擇最高級別的可視性支援。

步驟 7. 為了測試，n 導航到診斷>會議診斷，並且正在或已經完成會議，如下圖所示。



在這些會議中，您可以檢視音訊和視訊呼叫的平均資料包丟失、延遲和抖動。

此外，您還可獲得會話和所涉及裝置的拓撲。

## 會議相關警報

對於會議診斷，您可以接收三個不同的「警報」（任何會話）並設定其閾值：

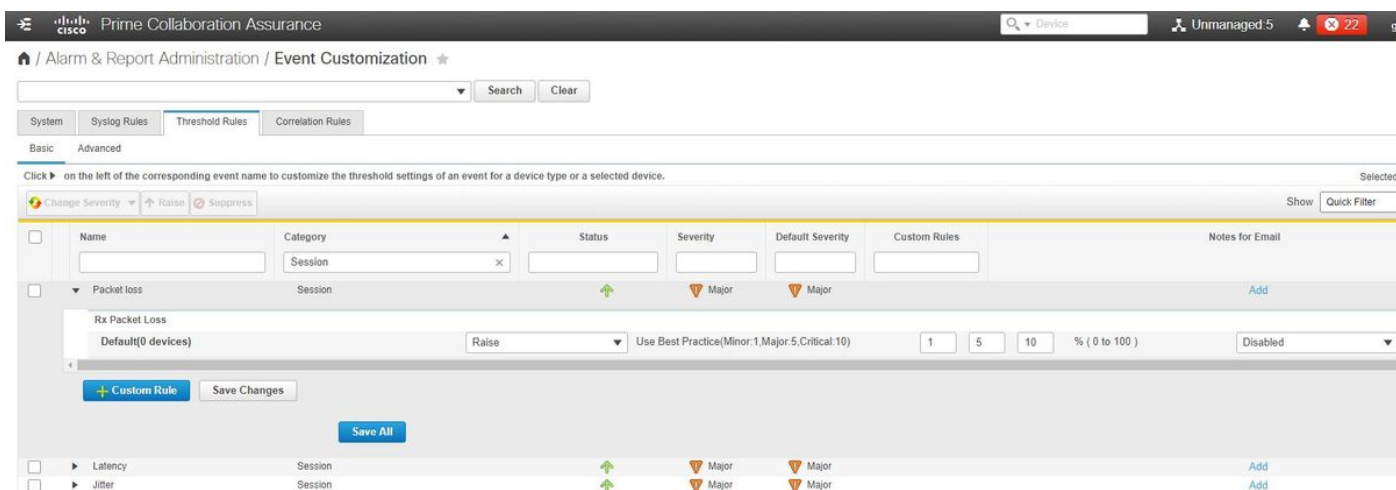
- 封包丟失
- 延遲
- 抖動

您可以修改預設閾值、完全停用該閾值或定義您希望與此警報關聯的裝置。

步驟 1. 導航到 Alarm & Report Administration > Event Customization.

步驟 2. 選擇 Threshold Rules 並確保已選擇 Basic.

步驟 3. 向下捲動或按一下右側「Category Named Session」，如下圖所示。



步驟 4.選擇要修改的警報旁的下拉箭頭，可以修改資料包丟失、抖動或延遲的次要、主要或嚴重百分比。

步驟 5.如果您要取樣，請將「提升」切換為「取樣」。

步驟 6.如果要定義與警報關聯的終端，請選擇Custom Rule。

步驟 7.接下來，選擇Device Type >，選擇All devices或Selectable devices，然後按一下儲存。

## 會議相關報告

對於會議診斷報告，可以檢索和檢視。

有兩個報告：

- 會議報告
- Telepresence終端報告

對於「會議報告」，您可以根據需要檢視一至四週時間範圍內或自定義時間段內的所有會議清單。

步驟 1.導航到報告>會議報告，如圖所示。

The screenshot shows the Cisco Prime Collaboration Assurance interface. The top navigation bar includes the Cisco logo, 'Prime Collaboration Assurance', a search bar, and user information 'globaladmin - Enterprise'. The main content area is titled 'Reports / Conference Reports' and has two tabs: 'Conference Summary Report' (selected) and 'Conference Detail Report'. On the left, there is a 'Device Group' sidebar with a tree view containing 'ALL', 'Endpoints', 'Infrastructure', 'Predefined', and 'User Defined'. The main area displays 'All Conferences summary' with a table of conference data. Below this, there is a section for 'Participated Conferences of Endpoint: SEPC80084A8239 (1004)' showing a detailed table of individual conference events.

Endpoint Name	Local DNURI	IP Address	Number of Partic...	Use (...)	Scheduled Duration (min)	Utilized Scheduled time (%)	Average Conferenc...	Longest Conferenc...
SEPC80084A8...	1004	10.201.196.198	2	3.33	N/A	N/A	2	3
SEPAC44F2100...	1001	10.201.196.199	2	3.23	N/A	N/A	2	3
SEP00562B04C...	1003	10.201.196.194	2	3.18	N/A	N/A	2	3
SEP0004F2E106...	1002	10.201.196.196	2	3.08	N/A	N/A	2	3
SEP7428ACF35...	1006	10.201.196.218	3	1.9	N/A	N/A	1	2
SEPD0C789141...	1007	10.201.196.197	3	1.65	N/A	N/A	1	2
SEP7428ACEF0...	1005	10.201.196.207	2	0.85	N/A	N/A	1	1
SEP005F893E4...	1010	10.201.196.205	1	0.57	N/A	N/A	1	1

Confere...	Start Time	End Time	Duration (m...	Scheduled Duration (...)	Remote DN...	Remote IP Addr...	Remote Device Type	Direction	Confere...	Conference St...	Proto...	Call Termination	Security	Resolution
8842987227	2017-Oct-10 10:33:26 EDT	2017-Oct-10 10:34:28 EDT	1.02	N/A	1001	10.201.196.199	PHONE		Ad hoc	Point-to-Point				
8842987222	2017-Oct-10 10:30:58 EDT	2017-Oct-10 10:33:17 EDT	2.32	N/A	1003	10.201.196.194	PHONE		Ad hoc	Point-to-Point				

## 會議摘要報告

此報告提供您已選擇為有限/完全可視性的每個終端及其會議的檢視。

此處顯示的統計資料如下：

- 平均會議使用量
- 與會議相關的警報
- 平均丟包、抖動和延遲
- 最長的會議

這有助於您對語音/影片網路中可能存在的問題進行細緻的檢視，以確定哪些終端存在最多的問題。

以及根據使用量利用您的頻寬

### 會議詳細資訊報告頁籤

如果確實遇到會議的警報，您可以導航到「會議詳細資訊報告」頁籤。

選擇會議後，您可以細化以查詢終端名稱、軟體版本以及您可能感興趣的其他詳細資訊。

對於Telepresence Endpoint Reports，您可以檢視每個終端的

- 此裝置擁有的會議數目
- 使用率百分比
- 終端型號
- 使用量

此外，您可以透過「更改利用率」頁籤更改「利用率引數」，如圖所示。

## Change Utilization Settings for Endpoint Model: DX70



Work Hours per Day	<input type="text" value="10"/>
Work Days per Week	<input type="text" value="5"/>
	<input type="button" value="Save"/> <input type="button" value="Cancel"/>

這會設定該裝置的引數，以便系統從使用狀況得知要顯示的百分比。

「No Show Endpoint Summary Report」顯示未出席計畫會議的終端。

在此圖形中，您可以檢視終端以及總計畫會議數，以及這些會議中有多少已發生且未顯示。

### 會議視訊測試呼叫

您可以在處於託管狀態的兩個影片終端之間建立點對點影片測試呼叫，以測試您的網路。您可以檢視事件和警報、會話統計資訊、終端統計資訊和網路拓撲。此呼叫僅支援CTS、C和EX系列編解碼器。

此外，這還可用於驗證會議診斷的所有功能是否正確。

#### 必要條件

- E20編解碼器系列不支援此功能。
- 要使用此功能，必須為終端增加CLI憑證。

- 確保終端已註冊並為終端啟用JTAPI ( 如果終端已註冊到Unified CM ) 。
- 如果您已在MSP模式下部署了Cisco Prime Collaboration，則影片測試呼叫功能不可用。

步驟 1. 導航到診斷>終端診斷。

步驟 2. 根據前提條件選擇兩個適用的端點。

步驟 3. 選擇Run Tests > Video Test Call。

步驟 4. 您可以將視訊測試呼叫排定為立即執行或依照重新發生的排程執行。

步驟 5. 然後，此影片測試呼叫將顯示在會議診斷螢幕中。

## 驗證

目前沒有適用於此組態的驗證程序。

## 疑難排解

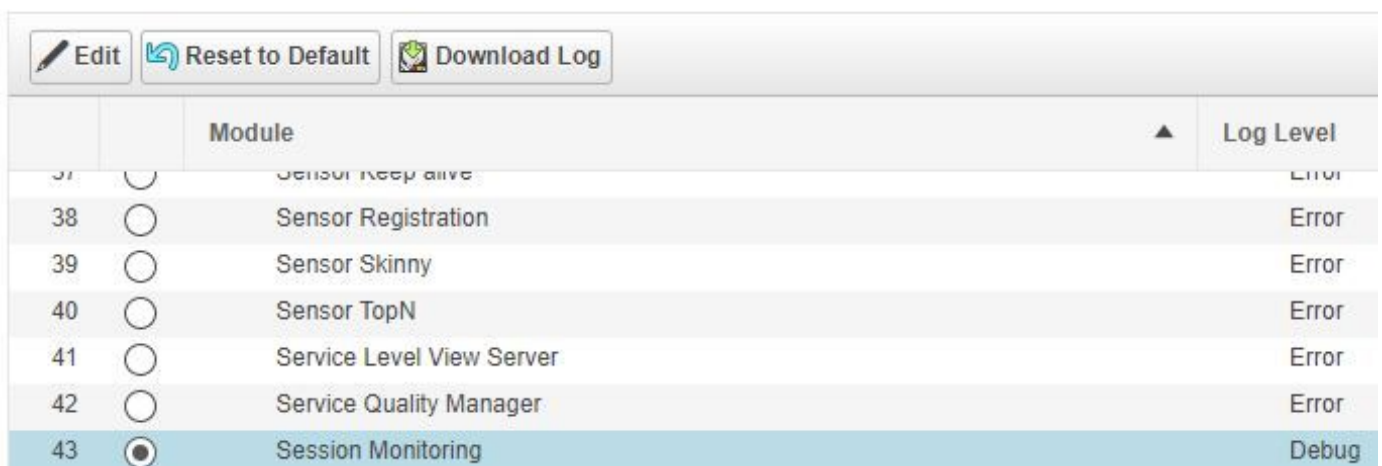
本節提供的資訊可用於對組態進行疑難排解。

用於故障排除的要收集的日誌

步驟 1. 導航到系統管理>日誌管理。

步驟 2. 向下滾動到模組，選擇Session Monitoring，然後選擇Edit，如下圖所示。

🏠 / System Administration / Log Management ★



		Module	▲	Log Level
37	<input type="radio"/>	Sensor Keep alive		Error
38	<input type="radio"/>	Sensor Registration		Error
39	<input type="radio"/>	Sensor Skinny		Error
40	<input type="radio"/>	Sensor TopN		Error
41	<input type="radio"/>	Service Level View Server		Error
42	<input type="radio"/>	Service Quality Manager		Error
43	<input checked="" type="radio"/>	Session Monitoring		Debug

步驟 3. 將日誌級別更改為debug，然後按一下Save。

步驟 4. 重現問題，然後返回Log Management螢幕。

步驟 5. 重現問題後，選擇Session Monitoring並選擇Download Log。

步驟 6. 下載後，解壓縮zip檔案。

步驟 7. 打開zip檔案並導航到有用的日誌的位置：

/opt/emms/emsam/log/SessionMon/

- CUCMJTAPI.log
- CUCMJTAPIDiag.log
- CSMTTracker
- CSMTTrackerDiag.log
- CSMTTrackerDataSource.log
- PostInitSessionMon.log



## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。