

配置Prime协作保证(PCA) -会议诊断

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[将终端的限制设置为每个OVA的有限或完全可视性](#)

[配置](#)

[场景 1.视频终端注册到Call Manager的会议](#)

[Cisco Unified Communications Manager设置](#)

[启用HTTP](#)

[启用 SNMP](#)

[启动CTI服务](#)

[为PCA CTI控制创建应用程序用户 \(JTAPI用户 \)](#)

[会议相关警报](#)

[会议相关报告](#)

[会议视频测试呼叫](#)

[场景 2 : 与非Call Manager注册终端的会议](#)

[会议相关警报](#)

[会议视频测试呼叫](#)

[验证](#)

[故障排除](#)

简介

本文档介绍如何在Prime协作保证(PCA)中配置和设置会议诊断部署，以主动监控语音/视频会议统计信息。

先决条件

要求

Cisco 建议您了解以下主题：

- Call Manager管理员登录
- PCA登录
- 您的网真监控服务器(TMS)
- 核心/Expressway凭证 (如果适用)

使用的组件

本文档中的信息基于PCA版本11.x - 12.x。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

Cisco Prime Collaboration 11.x支持以下类型的可视性：

- 完全可视性-支持使用JTAPI/HTTP反馈和实时监控信息（例如会议统计数据 and 会议信息）进行呼叫检测。
- 有限的可视性-使用JTAPI/HTTP反馈进行自动呼叫检测，但不支持实时监控信息（例如会议统计信息和会议信息）。可视性有限的终端在会议拓扑中以半暗图标表示。

Cisco Prime Collaboration 12.x支持以下类型的可视性：

- 完全可视性-支持使用JTAPI/HTTP反馈和实时监控信息（例如会议统计数据 and 会议信息）进行呼叫检测。
- 无可视性-不支持使用JTAPI/HTTP反馈和实时监控信息进行呼叫检测。这些终端在“会议监控”(Conference Monitoring)页面上以全灰色的图标显示。

将终端的限制设置为每个OVA的有限或完全可视性

- 小型开放式虚拟化存档(OVA)支持多达500个端点
- 中型OVA支持多达1000个终端
- 大型OVA支持多达1800个终端
- 超大型OVA支持多达2000个终端

每个PCA在会议和我们支持的会话方面支持的设备列表如此处的表图像所示。

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 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 <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 ²	Ad hoc	Point-to-pointMultipoint	<ul style="list-style-type: none"> • 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) <i>intracluster</i> sessions ³	Ad hoc	Point-to-point	<ul style="list-style-type: none"> • 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) <i>intracluster</i> sessions	Ad hoc,Scheduled Note Scheduler must be CTS-Manager 1.7, 1.8, or 1.9.	Multipoint	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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.

配置

场景 1. 视频终端注册到Call Manager的会议

步骤1: 首先，您需要确保呼叫管理器处于“托管”状态。

导航到资产>资产管理>管理凭证>为Call Manager集群创建配置文件。



注意：请记住，每个凭证配置文件均对配置文件中列出的每个ip使用相同的凭证。因此，如果您在同一凭证配置文件中列出Call Manager发布服务器和订用服务器，它将使用相同的凭证来发现这两个ip地址。如果您的设置中确实包含指挥交换机，请先找到指挥交换机，然后找到Cisco Call Manager，如图所示。

<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

第二步：确保您已设置超文本传输协议(HTTP)、简单名称管理协议(SNMP)和Java电话API (JTAPI)凭证

此外，您还必须在Call Manager Serviceability中启用思科计算机电话集成(CTI)服务。

Cisco Unified Communications Manager设置

启用HTTP

如果要允许Cisco Prime协作使用管理员凭证登录，则无需创建新用户。或者，如果要允许Cisco Prime协作管理器使用正确的凭证登录Cisco Unified Communications Manager，您必须创建新的HTTP用户组和Cisco Prime协作可用于通信的对应用户。

要创建用户，请执行以下步骤：

步骤1:使用您的管理员帐户登录Cisco Unified CM管理Web界面。

第二步：创建具有足够权限的用户组。导航到User Management > User Settings > Access Control Group并使用适当的名称PC_HTTP_Users创建新用户组。现在，选择Save。

第三步：导航到用户管理>用户设置>访问控制组，然后选择查找。找到您定义的组，然后点击右侧的图标。

第四步：选择将角色分配给组并选择以下角色：

- 标准AXL API访问
- 标准CCM管理员用户
- 标准适用性管理

第五步：Click Save.

第六步：从主菜单导航到用户管理>应用程序用户>创建新用户。

在Application User Configurationpage上指定合适的密码。您只能从Available Devices文本区域选择特定类型的设备，或允许Cisco Prime Collaboration监控所有设备

步骤 7.在Permission Information部分，选择Add to User Group并选择在步骤1中创建的组。（例如，PC_HTTP_Users）。

步骤 8单击保存。页面将会刷新，并显示正确的权限。

启用 SNMP

默认情况下，思科统一通信管理器中未启用SNMP。

要启用SNMP，请执行以下操作：

步骤1:在Cisco Unified Communications Manager Web GUI中登录Cisco Unified Serviceabilityview。

第二步：导航到工具>服务激活。

第三步：选择Publisher Server。

第四步：导航到性能>监控服务，选中Cisco Call Manager SNMP服务复选框。

第五步：在屏幕底部选择Save。

要创建SNMP社区字符串，请执行以下操作：

步骤1:登录到Cisco Unified Serviceabilityview the Cisco Unified Communications Manager Web GUI。

第二步：从Cisco Unified Serviceability视图的主菜单中，导航至SNMP > v1/v2c > Community String。

第三步：选择服务器并单击“查找”。

如果社区字符串已定义，社区字符串名称将显示在搜索结果中。

第四步：单击Add newto，在不显示任何结果的情况下添加新字符串。

第五步：指定所需的SNMP信息并保存配置。

 注意：仅需要SNMP只读(RO)访问权限。

启动CTI服务

对所需的Cisco Unified Communications Manager节点执行此过程，最好在两个节点上设置。

步骤1:登录到Cisco Unified Serviceability (可在Cisco Unified Communications Manager图形用户界面中查看)。

第二步：导航到工具>服务激活。

第三步：从下拉列表中选择服务器。

第四步：在CM Services部分，选中Cisco CTI Manager复选框。

第五步：选择屏幕顶部的Save

为PCA CTI控制创建应用程序用户 (JTAPI用户)

JTAPI用于从设备检索会话状态信息。必须在呼叫处理器中为CTI控制创建具有在终端上接收JTAPI事件所需权限的应用用户。Prime协作管理多个呼叫处理器集群。必须确保集群ID是唯一的。创建一个新的应用用户，以帮助Cisco Prime Collaboration获取所需信息。

要创建新的JTAPI应用用户，请执行以下步骤：

步骤1:通过您的管理员帐户登录到Cisco Unified CM管理Web界面。

第二步：创建具有足够权限的用户组。 导航到User Management > User Settings > Access Control Group并使用适当的名称PC_HTTP_Users创建新用户组。现在，选择Save。

第三步：选择User Management > User Settings > Access Control Group，然后单击Find。找到您定义的组，然后选择右侧的图标。


第四步：点击Assign Role to Group并选择以下角色：

- Standard CTI Allow Call Monitoring
- Standard CTI Enabled
- 标准 CTI 允许控制支持所连接的转接和会议的电话

第五步：选择保存(Save)。

第六步：从主菜单导航到用户管理>应用程序用户>创建新用户。

在Application User Configurationpage上指定合适的密码。您可以从Available Devices文本区域选择特定类型的设备，或允许Cisco Prime Collaboration监控所有设备。

 注意：密码不能包含分号(;)或等号(=)。

步骤 7.在权限信息部分，选择添加到访问控制组，然后选择在步骤1中创建的组。(例如，PC_HTTP_Users)。

步骤 8单击保存。页面将会刷新，并显示正确的权限。

 注意：如果在添加JTAPI用户之前管理了Call Manager，请确保已将JTAPI用户添加到Call Manager的凭证配置文件中，然后重新发现该用户。

接场景1。步骤:

第三步：导航到您创建的Call Manager JTAPI应用用户，然后将支持的终端从可用设备移动到受控设备。

您可以通过设备关联功能执行此操作，如图所示。

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 icons for 'Save', 'Delete', 'Copy', and 'Add New'. Below the header, the 'Status' section shows 'Status: Ready'. The 'Application User Information' section includes fields for 'User ID*' (JTAPIUser), 'Password', 'Confirm Password', 'Digest Credentials', 'Confirm Digest Credentials', and 'BLF Presence Group*' (Standard Presence group). There are also four checkboxes for 'Accept Presence Subscription', 'Accept Out-of-dialog REFER', 'Accept Unsolicited Notification', and 'Accept Replaces Header'. The 'Device Information' section features two lists: 'Available Devices' (Auto-registration Template, BAT205D23177001, Sample Device Template with TAG usage examples, TCTTEST, TCTTEST2) and 'Controlled Devices' (SEP00059A3B7700, SEP000506004ECB3, SEP00050600CF7EB, SEP000562B04CFA8, SEP0005F8693E4A0). Buttons for 'Edit Credential', 'Device Association', and 'Find more Route Points' are also visible.

如果回溯到设置为每个OVA的有限或完全可视性的终端限制，您可以验证已添加到OVA大小的设备数量。

在此屏幕中，您可以按设备名称、说明或目录编号进行过滤，以帮助您管理和过滤这些设备，如图所示。

在第7步添加设备时，注意这些设备会很有用。

User Device Association			
	Select All		Clear All
	Select All In Search		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

确保为此JTAPI用户添加正确的用户角色：

- Standard CTI Allow Call Monitoring
- Standard CTI Enabled
- 标准CTI允许控制支持已连接转接和会议的电话，如图所示。

Permissions Information

Groups: JTAPIUser [View Details](#)

Roles:

- Standard CTI Allow Call Monitoring
- Standard CTI Allow Control of Phones supporting Conne
- Standard CTI Enabled

[View Details](#)

有关每个PCA支持的设备列表（关于会议和我们支持的会话），请参阅“背景信息”部分。


注意：此外，请确保由CTI应用用户控制的设备在设备信息下选中了“允许从CTI控制设备”复选框（如图所示）。




注意：在您继续操作之前，请务必注意：如果您将终端注册到Call Manager并且Call Manager与VCS/TMS集成，则您首先会发现VCS/TMS，然后最后才发现Call Manager。这样，从资产角度看，您的所有基础设施都会映射到正确的位置。此外，当您发现VCS/TMS时，请确保将默认Discover选项卡更改为TMS/VCS或Call manager的相应设备。

第四步：然后在PCA中，选择Device Discovery并输入呼叫管理器的IP地址，选中Auto-Configuration上的两个复选框，然后选择Run Now（如图所示）。

Discover Devices ✕

 Manage Credentials

→

 Device Discovery

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.

▼ Auto-Configuration

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

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


▶ Filters


▶ Advanced Filters

第五步：当呼叫管理器处于托管状态后，继续执行步骤6。

 **注意：**如果Call Manager未处于托管状态，则大多数时间应归因于HTTP或SNMP；如果需要进一步的帮助，请打开TAC案例以使Call Manager处于托管状态。

第六步：导航到资产>资产计划>集群数据发现计划，选择立即运行。

 **注意：**这取决于您有多少已注册/未注册的设备。此过程可能需要几分钟到几小时之间的任何时间。通过刷新页面全天进行检查。此外，这会将Call Manager集群映射在一起并检索所有终端。完成之后，继续下一步。

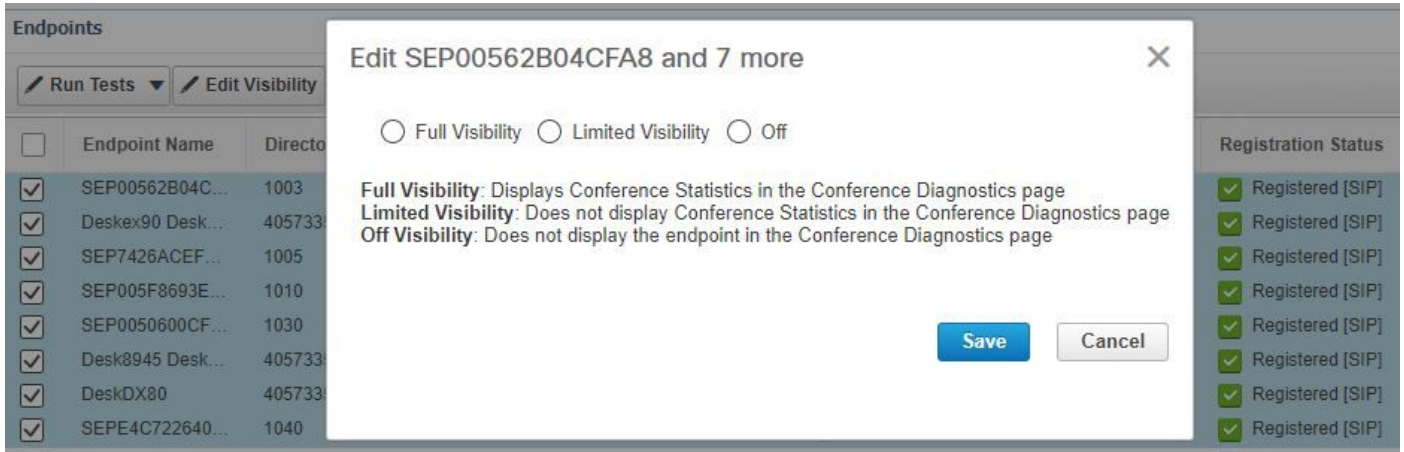
 **注意：**如果有任何终端您希望支持会议统计信息，请在PCA资产中提及该终端。确保妥善管理这些报告和所有统计信息，以显示正确的信息。

步骤 7. 导航到诊断>终端诊断。

要获取会议终端的最新统计信息，您需要将其可视性设置为系统允许的最高级别。


选择您要在会议诊断中监控的所有终端，然后点击编辑可视性，然后选择完全可视性（如图所示）。

有限可视性只显示拓扑中的设备，但没有统计信息，并且无法检索与会议诊断相关的设备的适用警报。

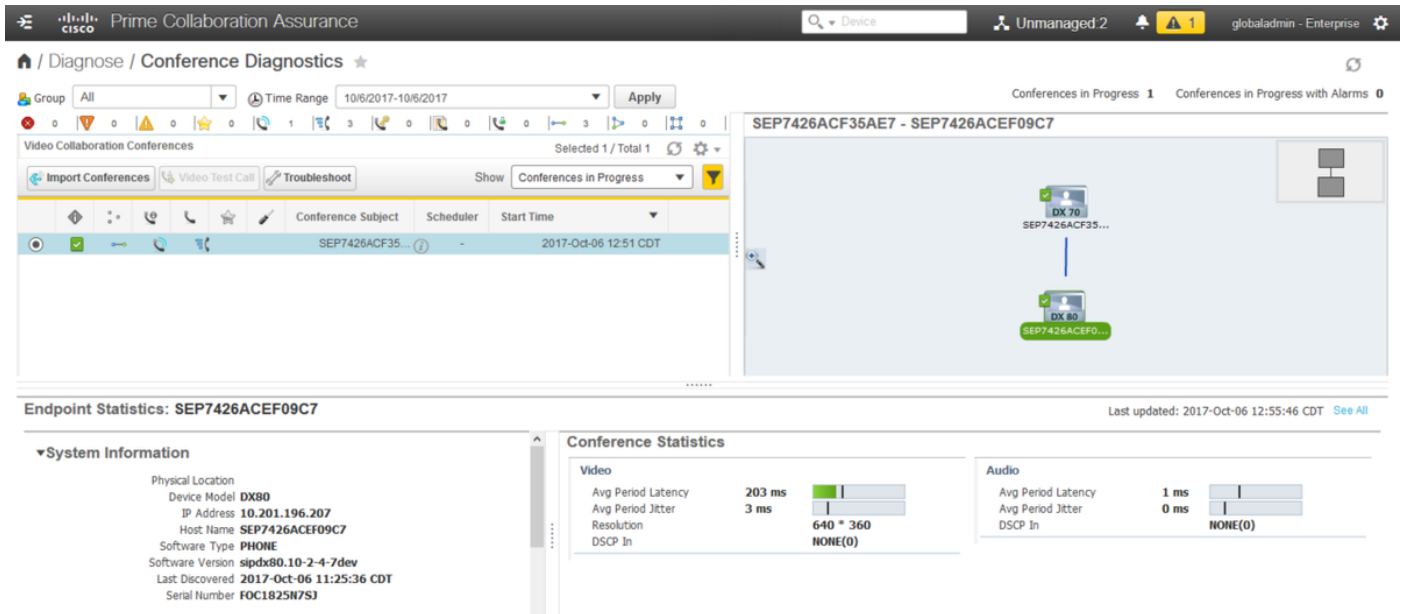


The following table lists the default and maximum visibility details for the endpoints:

Endpoint Type	Default Visibility	Maximum Visibility
<ul style="list-style-type: none"> CTS 500, 1000, and 3000 Series Cisco Codec Cisco TelePresence SX20 Cisco TelePresence MXP Series Cisco IP Video Phone E20 	Full	Full
<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> Cisco SX80 and Cisco SX10 <ul style="list-style-type: none"> Cisco MX200 G2, Cisco MX300 G2, Cisco MX700, and Cisco MX800 	Full	Full
Cisco DX70 and DX80	Off	Full
MRA Endpoints: <ul style="list-style-type: none"> Cisco Jabber Cisco TelePresence MX Series Cisco TelePresence System EX Series Cisco TelePresence System SX Series 	Limited	Limited

 注意：如果您选择（例如）10个终端并选择“完全可视性”(Full Visibility)，则它会为每个设备选择最高级别的可视性支持。

步骤 8要进行测试，请导航到诊断>会议诊断，并显示“会议进行中”或“已完成”，如图所示。



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 titled "Diagnose / Conference Diagnostics" and features a filter for "Conferences In Progress". A table lists conference details, with one entry selected. To the right, a network diagram shows two endpoints (DX 70 and DX 80) connected to a central hub. Below the diagram, "Endpoint Statistics" for SEP7426ACEF09C7 are shown, including system information and conference statistics for video and audio.

Category	Item	Value
System Information	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	FOC1825N7SJ	
Conference Statistics - Video	Avg Period Latency	203 ms
	Avg Period Jitter	3 ms
	Resolution	640 * 360
	DSCP In	NONE(0)
Conference Statistics - Audio	Avg Period Latency	1 ms
	Avg Period Jitter	0 ms
	DSCP In	NONE(0)

在这些会议中，您可以查看音频和视频呼叫的平均数据包丢失、延迟和抖动。

另外，获取会话和所涉设备的拓扑。

目前，会议诊断根据DN提取信息，如果您的环境已共享DN，PCA将检索它收到的用于会议的第一个信息。

会议相关警报

对于会议诊断，您可以接收任何会话的三个不同警报并设置其阈值：

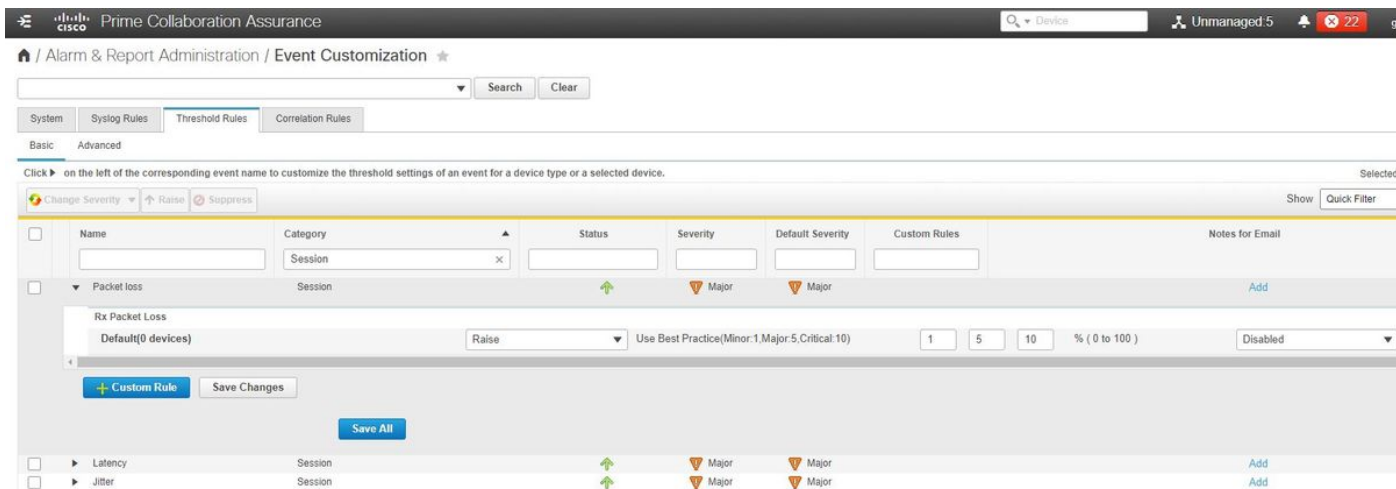
- 包丢失
- 延迟
- 抖动

对于其中每种，您可以修改默认阈值、超出该阈值或定义您要与此警报关联的设备。

步骤1:导航到警报和报告管理>事件自定义。

第二步：选择Threshold Rules并确保已选择Basic。

第三步：向下滚动或过滤至右侧的“Category Named Session”，如图所示。



第四步：选择警报旁边的下拉箭头。您需要修改，并且可以修改数据包丢失、抖动或延迟的次要百分比、主要百分比或重要百分比。

第五步：如果您想超频，请将Raise（提升）切换为Surpress（超频）。

第六步：如果要定义与警报关联的终端，可以选择Custom Rule。

步骤 7.然后，选择要用于此警报的设备类型>选择所有设备或可选设备，然后单击保存。

会议相关报告

对于会议诊断报告，可以检索和查看。

有两份报告：

- 会议报告
- 网真终端报告

对于会议报告，您可以根据需要查看一至四周时间范围内或自定义时间段内的所有会议列表。

步骤1:导航到报告>会议报告（如图所示）。

The screenshot shows the Cisco Prime Collaboration Assurance interface for Conference Reports. It is divided into two main sections:

All Conferences summary

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

Participated Conferences of Endpoint: SEPC80084A8239 (1004)

Confere...	Start Time	End Time	Duration (m...	Scheduled Duration (...)	Remote DN...	Remote IP Addr...	Remote Device Type	Direction	Conferenc...	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				

会议摘要报告

此报告提供您已选择作为有限/完全可视性的每个终端及其会议的视图。

此处显示的统计信息如下：

- 平均会议使用情况
- 与会议相关的警报
- 平均丢包、抖动和延迟
- 最长会议

这有助于您对语音/视频网络中存在的问题进行精细查看，以确定哪些终端的问题最多。

此外，您还可以根据使用情况相应地利用您的带宽。

会议详细信息报告选项卡

如果您确实遇到会议警报，可以导航到会议详细信息报告选项卡。

选择会议后，您可以对其进行细化，以查找您可能感兴趣的终端名称、软件版本和其他详细信息。

对于网真终端报告，您可以查看每个终端的：

- 此设备拥有的会议数
- 利用率百分比
- 终端型号
- 使用率

另外，您可以通过Change Utilization选项卡更改利用率参数，如图所示。

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"/>

这会设置该设备的参数，以便系统从使用情况了解要显示的百分比。

“No Show Endpoint Summary”报告显示错过计划会议的终端。

在此图中，您还可以查看终端、总排定会议数以及已经举行和没有举行的会议数。

会议视频测试呼叫

您可以在两个处于受管状态的视频终端之间创建点对点视频测试呼叫，以测试您的网络。您可以查看事件和警报、会话统计信息、终端统计信息以及与其他呼叫一样具有统计信息的网络拓扑。此呼叫仅支持CTS、C和EX系列编解码器。

此外，这还可用于验证会议诊断的所有功能是否正常。

先决条件

- E20编解码器系列不支持此功能。
- 要使用此功能，必须为终端添加CLI凭证。
- 确保终端已注册，且为终端启用JTAPI（如果终端已注册到Unified CM）。
- 如果您在MSP模式下部署了Cisco Prime Collaboration，则视频测试呼叫功能不可用。

步骤1:导航到诊断>终端诊断。

第二步：根据提及的前提条件选择两个适用的终端。

第三步：选择Run Tests > Video Test Call。

第四步：您可以安排视频测试呼叫立即运行或按照重新出现的计划运行。

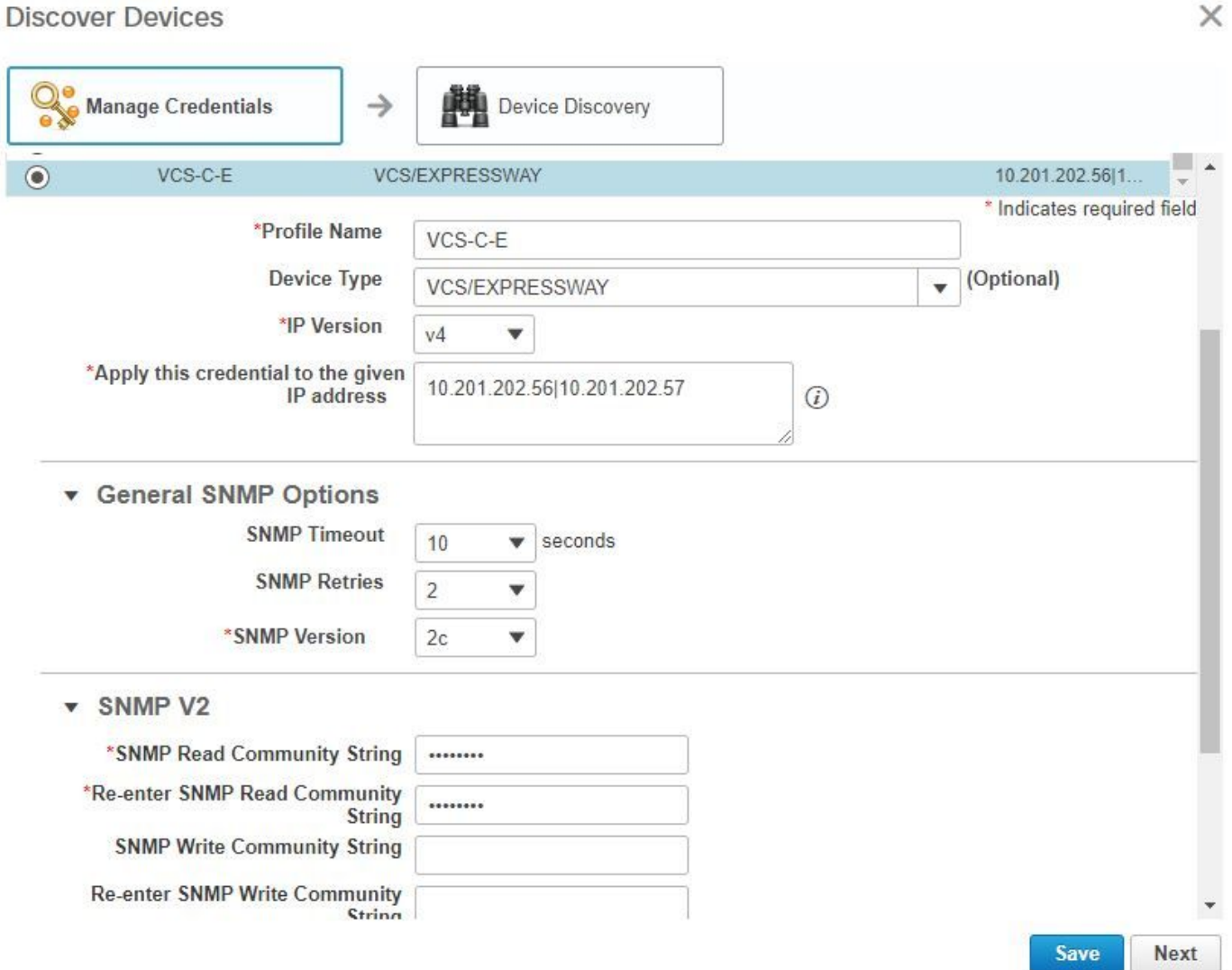
第五步：然后，此视频测试呼叫将显示在Conference Diagnostics（会议诊断）屏幕中。

场景 2：与非Call Manager注册终端的会议

步骤1:确保网真管理套件(TMS)和视频通信服务器(VCS)凭证可用。

 注意：在此场景中发现VCS/TMS时，发现过程非常重要。如果您的设置中确实存在呼叫管理器，请首先发现conductor，然后发现Cisco Call Manager。

第二步：导航到资产>资产管理>管理凭证>选择添加，然后输入TMS的信息，同时为您的VCS创建单独的凭证配置文件（如图所示）。



Discover Devices

Manage Credentials → Device Discovery

Profile Name	Device Type	IP Address
VCS-C-E	VCS/EXPRESSWAY	10.201.202.56 10.201.202.57

*Profile Name: VCS-C-E

Device Type: VCS/EXPRESSWAY (Optional)

*IP Version: v4

*Apply this credential to the given IP address: 10.201.202.56|10.201.202.57

General SNMP Options

SNMP Timeout: 10 seconds

SNMP Retries: 2

*SNMP Version: 2c

SNMP V2

*SNMP Read Community String:

*Re-enter SNMP Read Community String:

SNMP Write Community String:

Re-enter SNMP Write Community String:

Save Next

第三步：创建凭证配置文件后，选择Device Discovery，输入ip addresses，在Discovery选项卡中选择VCS并发现VCS设备。并且，为TMS选择TMS并输入其IP地址。单击Run Now（如图所示）。

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)

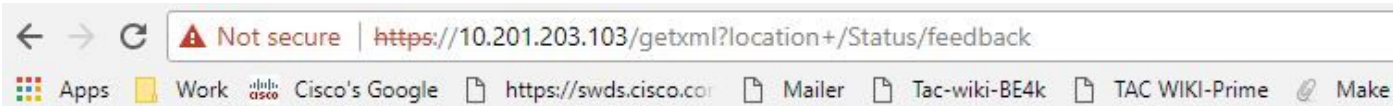
Recurrence None Hourly Daily Weekly Monthly

第四步：确保VCS和TMS处于托管状态。

注意：如果VCS或TMS未处于托管状态，大多数时间应归因于HTTP或SNMP；如果需要进一步的帮助，请打开TAC案例以使VCS/TMS处于托管状态。


注意：使用此URL并在VCS处于托管状态后用适当的IP地址替换IP_Address_of_VCS_Server。PCA服务器必须注册为VCS的反馈服务器，这可确保会议会话结束时数据不会出现VCS发回PCA的问题。

https://<IP_Address_of_VCS_Server>/getxml?location+/Status/feedback时会请求http凭证，输入后，您必须收到响应（如图所示）。




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未通过HTTP反馈订用订用VCS，则当注册终端加入或离开会话，或注册或注销VCS时，VCS不会向其发出通知。在这种情况下，请根据需要将这些终端的可视性设置为完全或受限，并确保您的VCS处于受管状态。

第五步：导航到资产>资产计划>集群数据发现计划，选择立即运行。

 注意：此过程可能需要一些时间，因为它会在所有基础设施设备上执行此功能。因此，如果几分钟后仍未完成，请在1-2小时后重新检查。超大型系统最多可能需要4小时。如果您希望支持任何终端的会议统计信息，并且还要确保这些报告以及显示正确信息的所有统计信息都受到管理，那么在PCA资产中提及这一点很重要。

有关会议及我们支持的会话中每个PCA支持的设备列表，请参阅“背景信息”部分。


第六步：导航到诊断>终端诊断。

要获取会议终端的正确统计信息，您需要将其可视性设置为系统允许的最高级别。

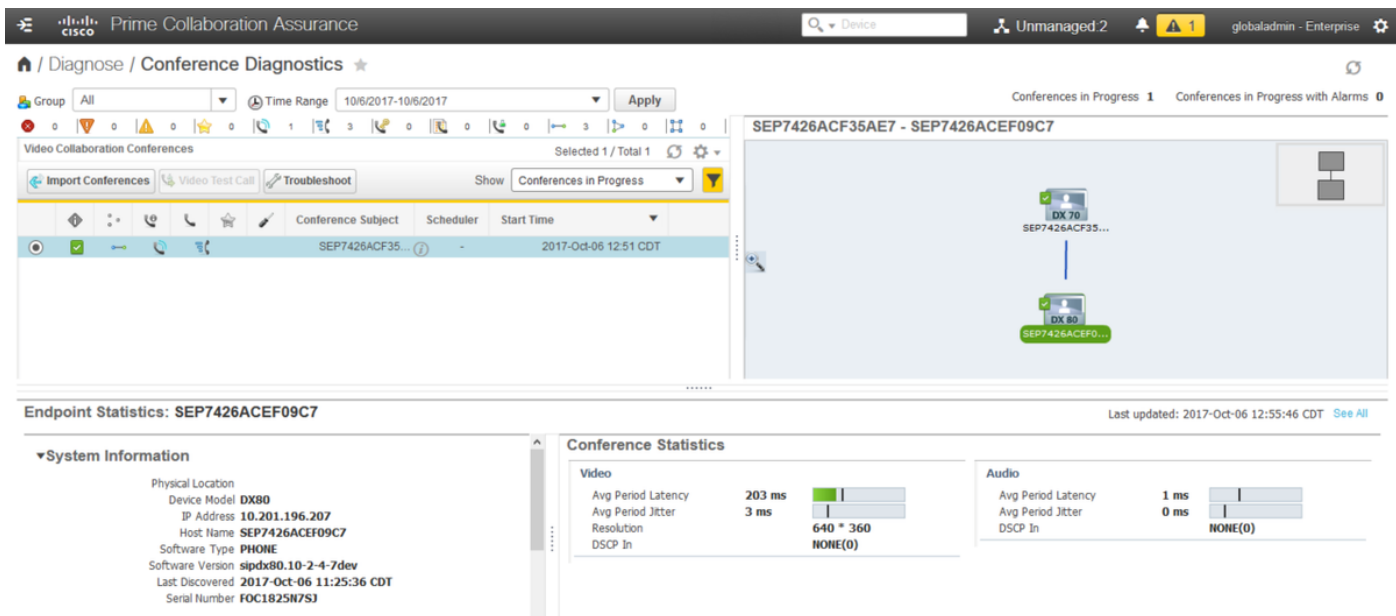
选择您要在会议诊断中监控的所有终端，然后单击编辑可视性，然后选择最大可视性。

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"> CTS 500, 1000, and 3000 Series Cisco Codec Cisco TelePresence SX20 Cisco TelePresence MXP Series Cisco IP Video Phone E20 	Full	Full
<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> Cisco SX80 and Cisco SX10 <ul style="list-style-type: none"> Cisco MX200 G2, Cisco MX300 G2, Cisco MX700, and Cisco MX800 	Full	Full
Cisco DX70 and DX80	Off	Full
MRA Endpoints: <ul style="list-style-type: none"> Cisco Jabber Cisco TelePresence MX Series Cisco TelePresence System EX Series Cisco TelePresence System SX Series 	Limited	Limited

 **注意：**如果您选择（例如）10个终端并选择“完全可视性”，则会选择每个设备的最高级别的可视性支持。

步骤 7.要进行测试，n导航至诊断>会议诊断，以及正在进行或完成的会议，如图所示。



在这些会议中，您可以查看音频和视频呼叫的平均数据包丢失、延迟和抖动。

此外，您还需要获得会话和所涉设备的拓扑。

会议相关警报

对于会议诊断，您可以在任何会话中收到三个不同的警报并设置其阈值：

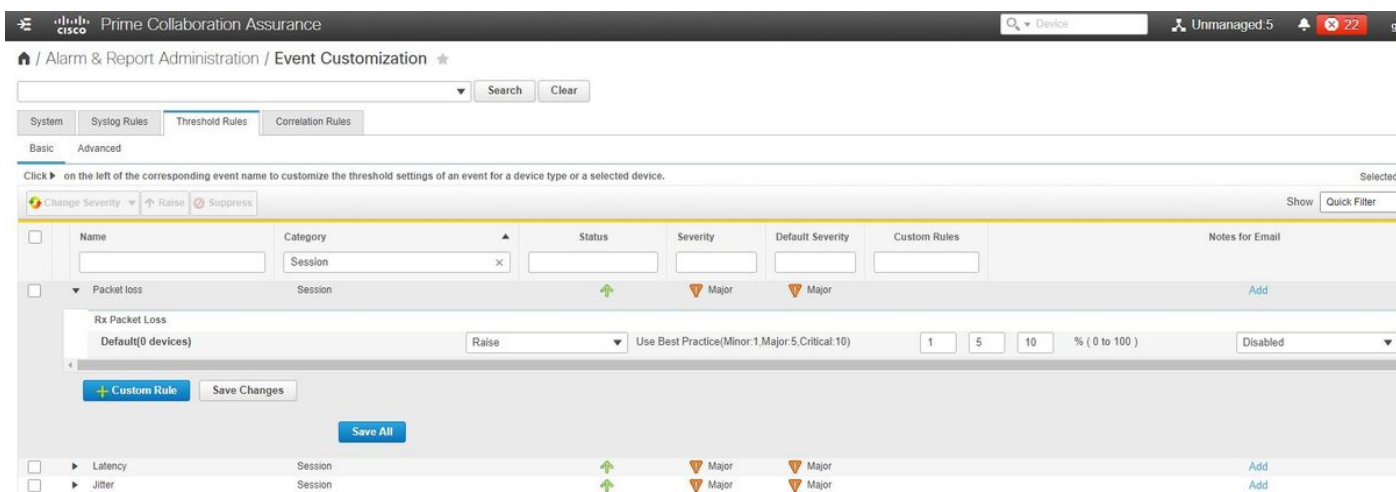
- 包丢失
- 延迟
- 抖动

其中每个选项都可以修改默认阈值、完全禁用该阈值或定义您要与此警报关联的设备。

步骤1:导航到报警和报告管理>事件自定义。

第二步：选择Threshold Rules并确保已选择Basic。

第三步：向下滚动或过滤至右侧的“Category Named Session”，如图所示。



第四步：选择要修改的警报旁边的下拉箭头，可以修改数据包丢失、抖动或延迟的次要、主要或关键百分比。

第五步：如果您想要超频，请将Raise（提升）切换为Surpress（超频）。

第六步：如果要定义与警报关联的终端，请选择Custom Rule。

步骤 7.然后，选择Device Type >，选择All devices或Selected devices，这是您想要的警报，然后单击Save。

会议相关报告

对于会议诊断报告，可以检索和查看。

有两份报告：

- 会议报告
- 网真终端报告

对于会议报告，您可以根据需要查看一至四周时间范围内或自定义时间段内的所有会议列表。

步骤1:导航到报告>会议报告（如图所示）。

The screenshot shows the Cisco Prime Collaboration Assurance interface. The main section is titled 'All Conferences summary' and displays a table with columns: Endpoint Name, Local DN/URI, IP Address, Number of Participations, Use (in minutes), Scheduled Duration (min), Utilized Scheduled time (%), Average Conference Duration, and Longest Conference Duration. The table lists several endpoints with their respective statistics.

Below the summary table, there is a section for 'Participated Conferences of Endpoint: SEPC80084AA8239 (1004)'. This section shows a detailed table with columns: Conference ID, Start Time, End Time, Duration (min), Scheduled Duration (min), Remote DN/URI, Remote IP Address, Remote Device Type, Direction, Conference Type, Conference Status, Protocol, Call Termination, Security, and Resolution. Two conferences are listed with their specific details.

会议摘要报告

此报告提供您已选择作为有限/完全可视性的每个终端及其会议的视图。

此处显示的统计信息如下：

- 平均会议使用情况
- 与会议相关的警报
- 平均丢包、抖动和延迟
- 最长会议

这有助于您对您的语音/视频网络内可能出现的问题进行精细查看，以确定哪些终端的问题最多。

并根据使用情况相应地利用您的带宽

会议详细信息报告选项卡

如果您确实遇到会议警报，可以导航到Conference Detail Report选项卡。

选择会议后，您可以细化以查找您可能感兴趣的终端名称、软件版本和其他详细信息。

对于网真终端报告，您可以查看每个终端的

- 此设备拥有的会议数
- 利用率百分比
- 终端型号
- 使用率

此外，您可以通过更改利用率选项卡更改利用率参数，如图所示。

Change Utilization Settings for Endpoint Model: DX70



Work Hours per Day

10

Work Days per Week

5

Save

Cancel

这会设置该设备的参数，以便系统从使用情况了解要显示的百分比。

“No Show Endpoint Summary”报告显示错过计划会议的终端。

在此图中，您可以查看终端、总排定会议数以及已经举行和没有举行的会议数。

会议视频测试呼叫

您可以在处于托管状态的两个视频终端之间创建点对点视频测试呼叫，以测试您的网络。您可以查看事件和警报、会话统计信息、终端统计信息和网络拓扑。此呼叫仅支持CTS、C和EX系列编解码器。

此外，这还可用于验证会议诊断的所有功能是否正确。

先决条件

- E20编解码器系列不支持此功能。

- 要使用此功能，必须为终端添加CLI凭证。
- 确保终端已注册，且为终端启用JTAPI（如果终端已注册到Unified CM）。
- 如果您在MSP模式下部署了Cisco Prime协作，则视频测试呼叫功能不可用。

步骤1:导航到诊断>终端诊断。

第二步：根据必备条件选择两个适用的终端。

第三步：选择Run Tests > Video Test Call。

第四步：您可以安排视频测试呼叫立即运行或按照重新出现的计划运行。

第五步：然后，此视频测试呼叫将显示在Conference Diagnostics（会议诊断）屏幕中。

验证

当前没有可用于此配置的验证过程。

故障排除

本部分提供了可用于对配置进行故障排除的信息。

用于故障排除的要收集的日志

步骤1:导航到系统管理>日志管理。

第二步：向下滚动到模块并选择Session Monitoring，然后选择Edit（如图所示）。

🏠 / System Administration / Log Management ★

<input type="button" value="Edit"/> <input type="button" value="Reset to Default"/> <input type="button" value="Download Log"/>			
		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

第三步：将日志级别更改为debug，然后单击Save。

第四步：重现问题，然后返回到Log Management屏幕。

第五步：重现问题后，选择Session Monitoring并选择Download Log。

第六步：下载后，解压缩zip文件。

步骤 7.打开zip文件并导航到位置以获取有用的日志：

/opt/emms/emsam/log/SessionMon/

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

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。