

# 从 Cisco Meeting Server 2.9 平稳升级至 3.0 ( 及更高版本 ) 指南

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[有关升级的重要信息](#)

[要考虑的事项摘要](#)

[许可证](#)

[Webbridge \( WebRTC和CMA客户端 \)](#)

[Web GUI更改](#)

[记录器/流转换器](#)

[Cisco Expressway注意事项](#)

[CMS边缘](#)

[CMS\(Acano\)X系列](#)

[SIP边缘](#)

[更多信息](#)

[许可 — 升级前检查许可证](#)

[确定升级后分配给PMP许可证的用户数量](#)

[您是否有足够的SMP许可证？](#)

[配置CMM](#)

[配置Webbridge \( WebRTC和CMA客户端 \)](#)

[Web应用用户空间创建权限](#)

[聊天功能](#)

[WebRTC点对点呼叫](#)

[值得注意的WebBridge设置更改](#)

[从Web GUI中删除的外部访问部分](#)

[录制或流](#)

[记录器](#)

[流处理器](#)

[Expressway注意事项](#)

[CMS边缘](#)

## 简介

本文档介绍将运行版本2.9 ( 或更早版本 ) 的思科会议服务器部署升级到3.0 ( 或更高版本 ) 所面临的挑战，以及如何处理这些挑战以实现平稳升级过程。

**删除的功能:**删除了XMPP ( 这会影响WebRTC )、中继/负载均衡器、Webbridge

**更改的功能:**记录器和流处理器现在是SIP，webbridge替换为webbridge3

本文档仅介绍在升级之前需要考虑的主题。它不包括3.X中的所有新功能。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- CMS管理
- CMS升级
- 证书创建和签名

这里提到的所有内容在各种文件中都有介绍。如果您需要进一步阐明功能：[CMS安装和配置指南](#)和CMS产品版本说明，请务必阅读产品版本说明并参阅编程指南和部署指南。

### 使用的组件

本文档中的信息基于思科会议服务器。

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 背景信息

本文档旨在指导您是否已部署CMS 2.9.x（或更低版本），无论是否合并了单个部署，还是具有恢复能力，以及您计划升级到CMS 3.0的时间。本文档中的信息涉及所有CMS型号。

**注意：**X系列无法升级到CMS 3.0。您需要计划尽快更换X系列服务器。

## 有关升级的重要信息

唯一支持的CMS升级方法是逐步升级。在撰写本文时，CMS 3.5已经发布。如果您在CMS 2.9上，则必须以阶梯式方式升级(2.9 → 3.0 → 3.1 → 3.2 → 3.3 → 3.4 → 3.5(注意，升级过程自CMS 3.5起已更改，请仔细阅读发行说明!!))

如果您不执行逐步升级，并且遇到异常行为，TAC可能会请求降级并重新开始。

此外，从CMS 3.4开始，CMS必须使用智能许可。您不能升级到CMS 3.4或更高版本，但仍使用传统许可证。请勿升级到CMS 3.4或更高版本，除非您已设置智能许可。

## 要考虑的事项摘要

使用这些问题导航至与您自己的情况相关的部分。每个注意事项都指向本文档中提供的更详细描述[的超链接](#)。

## 许可证

### 升级前，您的服务器上是否有足够的个人多方(PMP)/共享多方(SMP)许可证？

在3.0中，即使用户未登录，也会分配PMP许可证。例如，如果您已通过LDAP导入了10000个用户，但您只有100个PMP许可证，则一旦升级到3.0，就会使您不符合要求。对于此使用案例，请确保确实检查已设置userProfile和/或系统/配置文件的租户，以查看是否设置了值为true的hasLicense的userProfile。

如何检查API上的userProfile并查看您是否设置了hasLicense=true（即PMP许可用户），本节将详细介绍[介绍](#)。

### 您当前的cms.lic文件中是否有PMP/SMP许可证？

由于许可证行为在3.0之后发生更改，您必须在执行升级之前确认是否具有足够的PMP/SMP许可证。本节将对此进行更详细[介绍](#)。

### 您是否部署了思科会议管理器(CMM)？

CMS 3.0需要CMM 3.0，因为处理许可证的方式发生了变化。建议先部署CMM 2.9，然后再执行环境升级到3.0的过程，因为您可以查看90天报告，了解过去90天的许可证使用情况。本节将对此进行更详细[介绍](#)。

### 您是否有智能许可？

CMS 3.0需要CMM 3.0，因为处理许可证的方式发生了变化。因此，如果您已经通过CMM使用智能许可，请确保您有与集群关联的PMP和SMP许可证。

## Webbridge（WebRTC和CMA客户端）

### 您是否在CMS 2.9中使用WebRTC？

Webbridge在CMS 3.0中发生了重大变化。有关从webbridge2迁移到webbridge3以及使用Web应用的指导，请参阅本[部分](#)。

### 您的用户是否使用CMA客户端？

由于这些客户端是基于XMPP的，因此升级后无法再使用这些客户端，因为XMPP服务器已被删除。如果这适用于您的使用案例，您可以在此部分找到更[多信息](#)。

### 您是否在WebRTC中使用聊天？

聊天功能在3.0中从Web应用中删除。在CMS 3.2中，聊天功能重新引入，但并非持久性。您可以在此部分找到有关此功能的[更多信息](#)。

### 您的用户是否执行从WebRTC到设备的点对点呼叫？

在CMS 3.0中，Web应用用户不能再直接拨打其他设备。现在，您必须加入会议空间，并且拥有向会议添加参与者的权限，才能执行相同的操作。您可以在此部分找到有关此部件的[更多信息](#)。

### 您的用户是否从WebRTC创建自己的coSpaces？

在3.0中，为了使Web应用用户能够从客户端创建自己的空间，需要在API中创建coSpaceTemplate并将其分配给用户。在LDAP导入期间，可以手动或自动执行此操作。CanCreateCoSpaces已从UserProfile中删除。您可以在此部分找到有关此功能的[更多信息](#)。

## Web GUI更改

### 您在Web管理GUI中是否配置了WebBridge设置？

WebBridge设置将从3.0版的GUI中删除，因此您必须在API中配置WebBridge并注意GUI中的当前设置，以便在API中相应地配置WebBridgeProfiles。您可以在此部分找到有关此更改的[详细信息](#)。

### 您在Web管理员GUI中是否配置了外部设置？

外部设置已从CMS 3.1中的GUI中删除。如果您在CMS 3.0或更早的Web管理GUI(Configuration —> General —> External Settings)中配置了Webbridge URL或IVR，则这些内容已从网页中删除，现在需要在API中进行配置。升级到3.1之前的设置不会添加到API，必须手动完成。您可以在此部分找到有关此更改的[详细信息](#)。

## 记录器/流转换器

### 您当前是否使用任何CMS录制器和/或流转换器？

CMS记录器和流处理器组件现在基于SIP而不是基于XMPP。因此，在删除XMPP时，这些需要在升级后调整。您可以在此部分找到有关此更改的[详细信息](#)。

## Cisco Expressway注意事项

### 如果您使用Expressway代理WebRTC，您当前的Cisco Expressway版本是什么？

CMS 3.0需要Expressway 12.6或更高版本。您可以在此部分找到有关此WebRTC代理功能的[详细信息](#)。

## CMS边缘

### 您的环境中当前是否有CMS Edge？

CMS Edge在CMS 3.1上重新引入，具有更高的外部连接可扩展性。您可以在此部分找到有关此部件的[更多信息](#)。

## CMS(Acano)X系列

### 您的环境中当前是否有x系列服务器？

这些服务器无法升级到CMS 3.0，您必须考虑尽快更换这些服务器（在升级到3.0之前迁移到虚拟机或CMS设备）。您可以在此链接中找到有关这些服务器的寿命终止[通知](#)。

## SIP边缘

### 您当前是否在环境中使用SIP Edge？

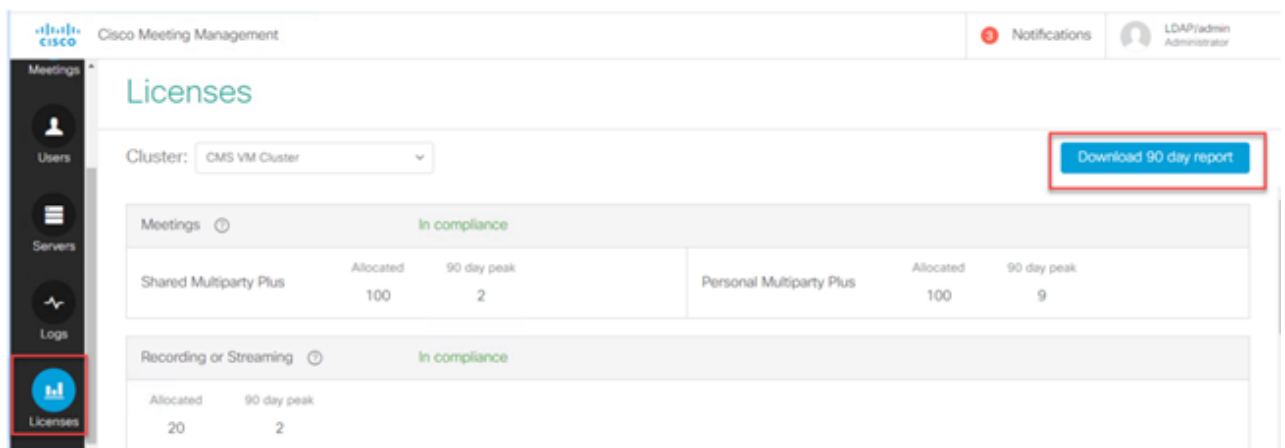
从CMS 3.0开始，Sip边缘已完全弃用。 您需要使用Cisco Expressway将SIP呼叫引入您的CMS。 请与您的思科客户代表联系，了解如何为您的组织获取Expressway。

## 更多信息

### 许可 — 升级前检查许可证

从2.x版本升级到3.0或更高版本时，合规性许可证状态是最具影响的问题。本节介绍如何确定平稳升级所需的PMP/SMP许可证数量。

在将部署升级到3.0之前，部署CMM 2.9并检查许可证选项卡下的**90天报告**，以查看许可证使用量是否保持在CMS节点上当前分配的许可证数量之下：



Shared Multiparty Plus		Personal Multiparty Plus	
Allocated	90 day peak	Allocated	90 day peak
100	2	100	9

Recording or Streaming	
Allocated	90 day peak
20	2

如果您使用 Traditional licensing ( cms.lic文件本地安装在您的CMS节点上 )，请检查CMS许可证文件，了解每个CMS节点上的个人和共享许可证数量 ( 100/100，如图所示 ) ( 从每个callBridge节点通过WinSCP下载 )。

```

},
"issued_to": "Darren McKinnon - TAC",
"notes": "Darren McKinnon - TAC",
"features":
{
  "callbridge":
  {
    "expiry": "2100-Jan-03"
  },
  "webbridge3":
  {
    "expiry": "2100-Jan-03"
  },
  "customizations":
  {
    "expiry": "2100-Jan-03"
  },
  "recording":
  {
    "expiry": "2100-Jan-03",
    "limit": "10"
  },
  "personal":
  {
    "expiry": "2100-Jan-03",
    "limit": "100"
  },
  "shared":
  {
    "expiry": "2100-Jan-03",
    "limit": "100"
  },
  "streaming":
  {
    "expiry": "2100-Jan-03",
    "limit": "100"
  }
}

```

如果您已经使用智能许可，请检查思科软件智能门户中为CMS服务器分配了多少个PMP/SMP许可证。

打开90天报告(Zip文件名为*license-data.zip*)，然后打开名为*daily-peaks.csv*的文件。

Name	Date modified	Type	Size
cluster-bins.csv	3/1/2021 2:35 PM	Microsoft Excel Co...	994 KB
daily-peaks.csv	3/1/2021 2:35 PM	Microsoft Excel Co...	3 KB
host-reported.csv	3/1/2021 2:35 PM	Microsoft Excel Co...	6,665 KB

在Excel上，按Z到A对PMP列进行排序，将较高的值放在顶部，然后对SMP列执行相同的操作。您在此文件中看到的值是否低于CMS许可证文件中可用的许可证？如果是，则表明您正常且完全合

规。如果不是，则会如[CMS部署指南](#)第1.7.3节中的图6所示创建警告和/或错误，有关更多信息，请参阅第1.7.4节。

根据示例，在过去90天内的高峰期有2.1667个SMP许可证被使用，没有PMP许可证。cms.lic文件指示每种许可证类型有100个单元，因此此设置完全兼容。因此，当此设置升级到CMS 3.0时，许可没有问题。但是，如果在设置时通过LDAP导入了10,000个用户，则仍可能有问题。此时您只有100个PMP许可证，但是您分配了10000（将hasLicense设置为True的userProfile），因此在这种情况下，一旦升级到3.0，您即不符合要求。有关更多信息，请参阅下一节。

date	pmp	smp	rec/str
12/10/2020	0	2.166666667	0
12/3/2020	0	2	0
1/7/2021	0	2	0
1/8/2021	0	2	0
1/14/2021	0	2	0
1/15/2021	0	2	0
1/26/2021	0	2	0
1/27/2021	0	2	0
2/19/2021	0	2	0
2/20/2021	0	2	0
1/11/2021	0	1.333333333	0
12/9/2020	0	1.166666667	0
1/12/2021	0	1.166666667	0
1/21/2021	0	1.166666667	0
2/8/2021	0	1.166666667	0
2/25/2021	0	1.166666667	0

## 确定升级后分配给PMP许可证的用户数量

在CMS 3.0中，所有导入并使用hasLicense=true的userProfile的用户都会自动分配一个PMP许可证。

在API中，检查您有多少个userProfiles，并检查其中是否设置了“hasLicense=true”。如果是，您需要检查这些userProfiles的分配位置。

用户配置文件可以在以下任何级别分配：

1. LdapSources
2. 租户
3. 系统/配置文件

检查所有3个位置，查找具有License=true的已分配用户配置文件。

### 1. Ldap源/租户

对于使用租户或userProfile的每个ldapSource，当hasLicense参数设置为True时，将为使用该ldapSource导入的用户分配PMP许可证。如果存在租户，您需要点击租户ID以查看它是否已分配了userProfile，然后检查该userProfile是否配置了“hasLicense=true”。如果没有租户，但存在userProfile集，请单击它查看它是否具有“hasLicense=true”。如果任一方式具有

“hasLicense=true”，则可以通过对“api/v1/users”执行GET并过滤用于IdapSource关联的Idapmapping上的jidMapping的域来验证导入了多少个用户。

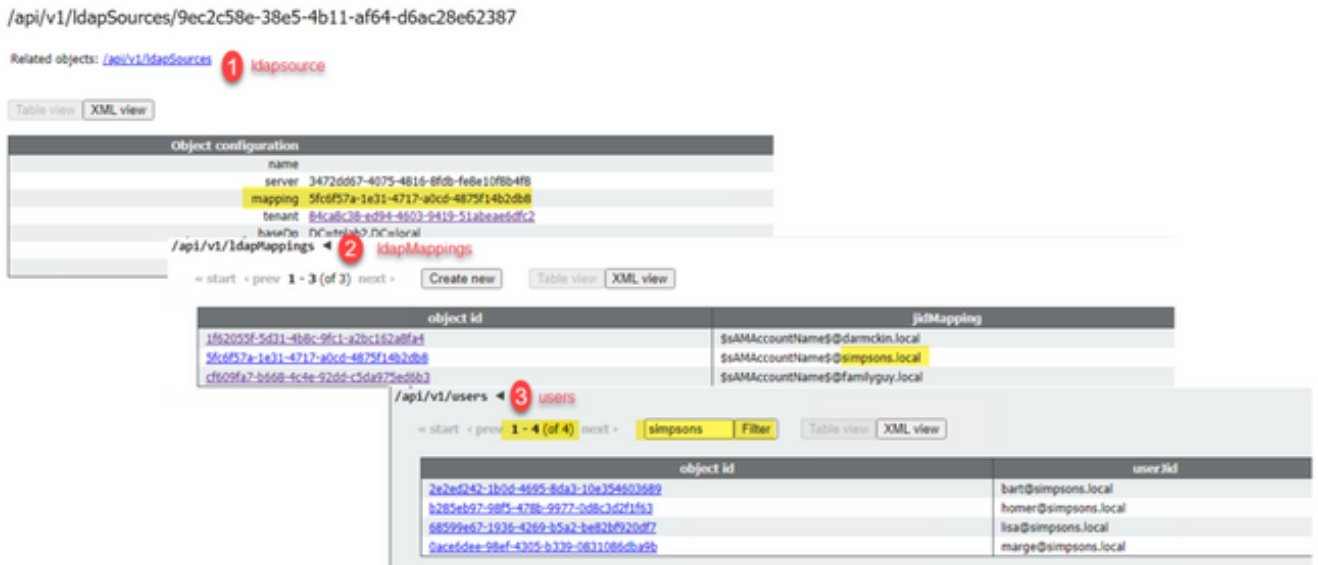
**注意：**在其他情况下，这会更复杂，在这种情况下，您需要使用您创建的ActiveDirectory映射和过滤器进行检查。

步骤1.从IdapSource查找映射ID。

步骤2.查找IdapMappings以查找jidMapping。

步骤3.在api/v1/users中搜索jidMapping中使用的域。

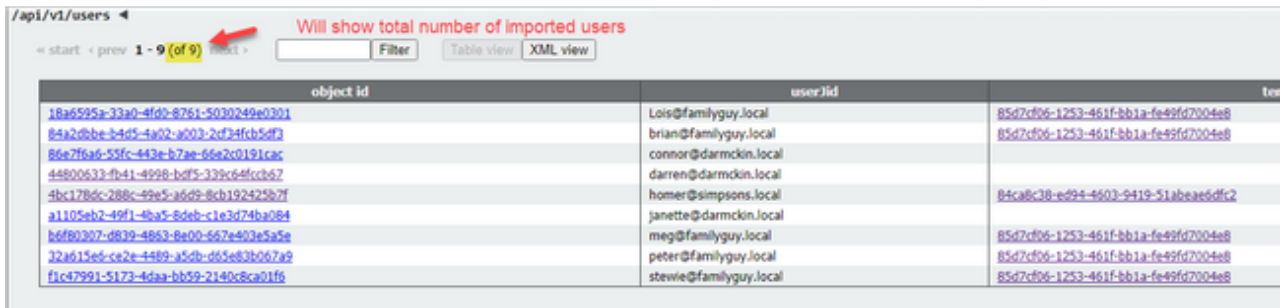
步骤4.添加从每个IdapSource找到的用户。 这是需要PMP许可证的LDAP导入用户的数量。



## 2.系统/配置文件

如果在系统/配置文件级别设置了userProfile，并且该userProfile为“hasLicense=true”，则在升级服务器时，任何导入到CMS的用户都将分配一个PMP许可证。如果您导入了10,000个用户，但只有100个PMP，则这会导致您在升级到CMS 3.0时不合规，并可能导致30秒的屏幕消息和呼叫开始时音频提示出现。

如果系统级别的userProfile指示用户要获取PMP，请转到api/v1/users查看总用户数：



如果您以前从Idap导入过所有用户，但现在意识到您只需要该列表中的某个子集，请在IdapSource中创建更好的过滤器，使其仅导入要为其分配PMP许可证的用户。在IdapSource上修改过滤器，然后在api/v1/ldapsync中执行新的LDAP同步。这会导致仅导入您所需的用户，并且会删除以前导入的所有其他用户。



**注意：**如果正确执行此操作，并且新导入仅删除不需要的用户，则其余用户的coSpace CallID和机密不会更改，但如果您犯了错误，则可能导致所有callId和机密更改。如果您对此感到担忧，请在尝试此操作之前备份数据库节点！

## 您是否有足够的SMP许可证？

当您查看CMM 90天报告中的每日峰值时，您是否有足够的SMP许可证来覆盖峰值时间？当会议的所有者尚未分配PMP许可证（作为coSpace所有者/临时会议/TMS安排的会议）时，使用SMP许可证。如果您有意使用SMP，并且拥有足够的容量来覆盖高峰时间，则一切正常。如果您查看了SMP的90天峰值并且不清楚为什么会消耗它们，以下是一些需要检查的内容。

- 1.临时呼叫（从CUCM升级）使用SMP许可证，如果用于合并的设备未与通过userProfile在CMS中分配了PMP许可证的用户相关联。CUCM提供升级会议的用户GUID。如果GUID对应于已导入会议服务器并具有已分配PMP许可证的LDAP用户，则使用该用户的许可证。
- 2.如果coSpace所有者尚未分配PMP许可证，则对这些特定coSpace的呼叫将使用SMP许可证。
- 3.如果在TMS 15.6版或更高版本中安排了会议，则会议所有者被发送到CMS；如果该用户未分配到PMP许可证，则该会议使用SMP许可证。

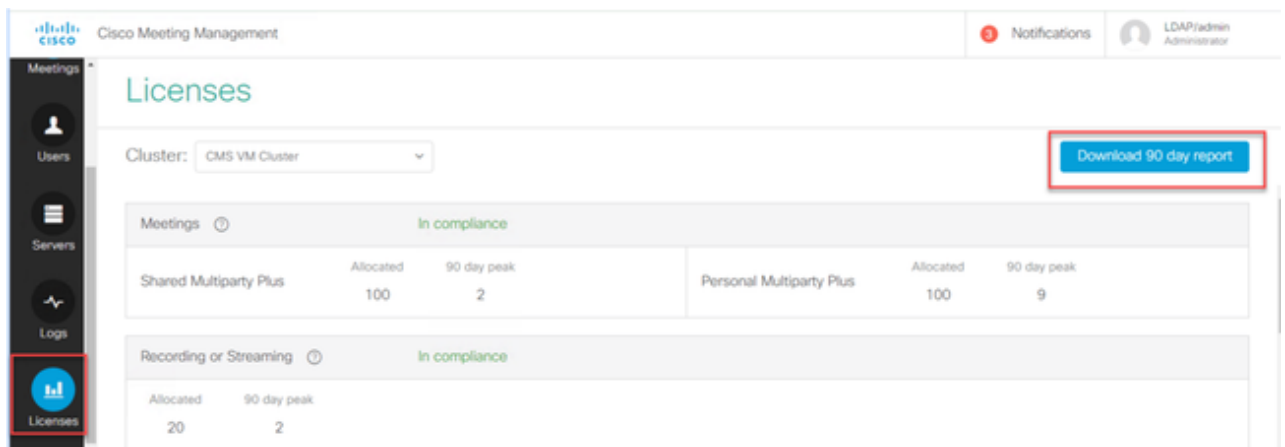
## 配置CMM

从CMS 3.0开始，CMS正常运行需要CMM 3.0。CMM负责CMS的许可，因此，如果您计划将CMS升级到3.0，您必须拥有CMM服务器。建议您在部署CMS 2.9时部署CMM 2.9，以便您在升级之前检查许可证使用情况。

CMM检查所有添加的callBridge的SMP和PMP许可证以及callBridge许可证。它使用的数字是集群内各种设备之间最高的。

例如，如果CMS1拥有20个PMP和10个SMP许可证，而CMS2拥有40个PMP和5个SMP许可证，则在传统许可中，CMM报告您有40个PMP和10个SMP许可证可以使用。

如果您拥有的PMP许可证比导入的用户多，则您没有任何与PMP（或SMP）许可证相关的问题，但是如果您检查了90天峰值，发现您使用的许可证多于可用许可证，您仍然可以升级到CMS 3.0并使用CMM上的90天试用许可证来根据您的许可进行分类，或者在升级之前采取措施。



Category	Compliance	Allocated	90 day peak
Meetings	In compliance		
Shared Multiparty Plus		100	2
Personal Multiparty Plus		100	9
Recording or Streaming	In compliance		
Allocated		20	2

## 配置Webbridge（WebRTC和CMA客户端）

CMS 3.0删除XMPP服务器组件，并随之删除WebBridge和使用CMA胖客户端的能力。WebBridge3现在用于使用浏览器将Web应用用户（以前称为WebRTC用户）连接到会议。升级到3.0时，需要配置webbridge3。

**注意：**升级到CMS 3.0后，CMA胖客户端无法正常工作！

此视频确实会引导您完成有关如何创建webbridge 3证书的过程。

<https://video.cisco.com/video/6232772471001>

在升级到3.0之前，客户必须计划如何配置Webbridge3。此处重点说明了最重要的步骤。

1.您确实需要webbridge3的密钥和证书链。如果证书包含运行webbridge3的所有CMS服务器FQDN或IP地址作为主题备用名称(SAN)/公用名称(CN)，并且满足以下任一条件，则可以使用旧webbridge证书：

a.证书没有增强型密钥使用（这意味着它可以用作客户端或服务器）。

b.证书同时具有客户端身份验证和服务器身份验证。HTTPs证书实际上只需要服务器身份验证，而C2W证书需要服务器和客户端）。

2.如果要为“webbridge3 https”证书创建新证书，建议对其进行公开签名（以避免在使用Web应用时在客户端上出现证书警告）。此证书可用于“webbridge3 c2w证书”，并且证书必须具有SAN/CN中Webbridge服务器的FQDN。

3. CallBridge需要使用在webbridge3 c2w listen命令中配置的端口与新的webbridge3进行通信。这可以是任何可用端口，例如449。用户需要确保callbridge可以与此端口上的webbridge3通信，并在必要时提前更改防火墙。它不能与“webbridge https”用于侦听的端口相同。

在CMS升级到3.0之前，建议使用“backup snapshot <servername\_date>”进行备份，然后登录callbridge节点上的webadmin页面，以删除所有XMPP设置和Webbridge设置。然后连接到服务器上的MMP，并通过SSH连接对具有xmpp和webbridge的所有核心服务器执行以下步骤：

1. xmpp disable
2. xmpp reset
3. xmpp certs none
4. xmpp domain none
5. webbridge disable
6. webbridge listen none
7. webbridge certs none
8. webbridge trust none

升级到3.0后，首先在以前运行webbridge的所有服务器上配置webbridge3。您必须执行此操作，因为已经存在指向这些服务器的DNS记录，因此，您可以这样确保如果用户被发送到webbridge3，它将准备好处理请求。

### Webbridge3配置（全部通过SSH连接）

步骤1.配置webbridge3 http侦听端口。

**Webbridge3 https listen a:443**

步骤2.为浏览器连接配置webbridge3的证书。这是发送到浏览器的证书，需要由公共证书颁发机构(CA)签名，其中包含浏览器中用于浏览器信任连接的FQDN。

**Webbridge3 https certs wb3.key wb3trust.cer**(这必须是信任链：创建一个信任证书，该证书顶部具有终端实体，然后按顺序排列中间CA，最后使用RootCA)。

```
-----BEGIN CERTIFICATE-----
Entity cert ← wb3/cb cert
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Intermediate cert
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
root cert
-----END CERTIFICATE-----
single carriage return at end
```

步骤3.配置用于监听callBridge到Webbridge(c2w)连接的端口。由于443用于webbridge3 https侦听端口，此配置必须是一个不同的可用端口，例如449。

**Webbridge3 c2w listen a:449**

4.配置webbridge发送到callbridge的c2w信任证书

**Webbridge3 c2w certs wb3.key wb3trust.cer**

5.配置WB3用于信任callBridge证书的信任存储。这必须与Callbridge CA捆绑包中使用的证书相同（并且必须是中间证书的捆绑包，中间证书位于顶部，根CA位于末尾，后跟单回车符）。

**Webbridge3 c2w trust rootca.cer**

6.启用webbridge3

**Webbridge3 enable**

```
Usage:
webbridge3
webbridge3 restart
6 webbridge3 enable
webbridge3 disable
1 webbridge3 https listen <interface:port whitelist>
2 webbridge3 https certs <key-file> <crt-fullchain-file>
webbridge3 https certs none
webbridge3 http-redirect (enable [port]|disable)
3 webbridge3 c2w listen <interface:port whitelist>
4 webbridge3 c2w certs <key-file> <crt-fullchain-file>
webbridge3 c2w certs none
5 webbridge3 c2w trust <crt-bundle>
webbridge3 c2w trust none
webbridge3 options <space-separated options>
webbridge3 options none
webbridge3 status
```

## CallBridge配置更改 (全部通过SSH连接)

步骤1.使用签署webbridge3 c2w证书的CA证书/捆绑配置callBridge信任。

**Callbridge trust c2w rootca.cer**

步骤2.重新启动callBridge以使新信任生效。 这将丢弃此特定callBridge上的所有呼叫，因此请谨慎使用此选项。

**Callbridge restart**

## 用于连接webBridge3的callBridge的API配置

1.使用API中的POST创建新的webBridge对象，并使用在webbridge c2w接口白名单中配置的FQDN和端口为其提供URL值 ( webbridge3配置中的步骤3 )

**c2w://webbridge.darmckin.local:449**

此时，Webbridge3会再次运行，您可以作为访客加入空间，或者如果以前导入过用户，他们必须能够登录。

## **Web应用用户空间创建权限**

您的用户是否习惯了在WebRTC中创建自己的空间？ 从CMS 3.0开始，Web应用用户无法创建自己的coSpaces，除非他们分配了允许此的共享空间模板。

即使分配了coSpaceTemplate，这也不会创建其他人可以拨入的空间 ( 无URI、无呼叫ID或密码 )，但是如果coSpace具有带“addParticipantAllowed”的callLegProfile，则他们可以从该空间拨出。

为了具有可用于呼叫新空间的拨号字符串，coSpaceTemplate必须具有accessMethodTemplate设置(请参阅2.9版本说明 —

[https://www.cisco.com/c/dam/en/us/td/docs/conferencing/ciscoMeetingServer/Release\\_Notes/Version-2-9/Cisco-Meeting-Server-Release-Notes-2-9-6.pdf](https://www.cisco.com/c/dam/en/us/td/docs/conferencing/ciscoMeetingServer/Release_Notes/Version-2-9/Cisco-Meeting-Server-Release-Notes-2-9-6.pdf))。

在API中，创建coSpaceTemplate，然后创建accessMethodTemplate，并将coSpaceTemplate分配给ldapUserCoSpaceTemplateSources，或者您可以手动将coSpaceTemplate分配给api/v1/users中的用户。

您可以创建和分配多个CoSpaceTemplates和accessMethodsTemplates。 有关详细信息，请参阅CMS API指南(<https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-programming-reference-guides-list.html>)

The screenshot displays two API configuration pages. The top page is for a CoSpaceTemplate with the following configuration:

Object configuration	
name	First CoSpaceTemplate
callProfile	008e1aa7-0079-4d65-b6ae-fb218bd2e6b4
callLegProfile	ef583b0e-a6fe-49cf-bece-b557332a76bf
numAccessMethodTemplates	2

The bottom page is for an AccessMethodTemplate with the following configuration:

name	<input type="text" value="First CoSpaceTemplate"/>	- present
description	<input type="text"/>	
callProfile	<input type="text" value="008e1aa7-0079-4d65-b6ae-fb218bd2e6b4"/>	Choose - present
callLegProfile	<input type="text" value="ef583b0e-a6fe-49cf-bece-b557332a76bf"/>	Choose - present
dialInSecurityProfile	<input type="text"/>	Choose

A red arrow points from the URL of the AccessMethodTemplate page to the URL of the CoSpaceTemplate page.

## CoSpaceTemplate ( API配置 )

**名称：**要为coSpaceTemplate指定的任何名称。

**描述:**简要说明（如果需要）。

**callProfile:** White callProfile是否希望使用此模板创建的任何空间？如果未提供，则使用在系统/配置文件级别设置的内容。

**calllegProfile:**您希望使用此模板创建的任何空间使用哪个calllegProfile？如果未提供，则使用在系统/配置文件级别设置的内容。

**dialInSecurityProfile:**您希望使用此模板创建的任何空格使用哪个dialInSecurityProfile?如果未提供，则使用在系统/配置文件级别设置的内容。

## AccessMethodTemplate ( API配置 )

**名称：**要为coSpaceTemplate指定的任何名称。

**uriGenerator:** 用于为此访问方法模板生成URI值的表达式；允许的字符集为'a'到'z'、'A'到'Z'、'0'到'9'、'!'、'-'、'\_'和'\$';如果非空，则它必须正好包含一个“\$”字符。例如，\$.space在创建空间时使用用户提供的名称并添加“.space”。“团队会议”创建url“Team.Meeting.space@domain”。

**callLegProfile:**您希望使用此模板创建的任何accessMethods使用哪个calllegProfile？如果未提供，则使用设置的CoSpaceTemplate级别；如果没有，则使用系统/配置文件级别中的内容。

**generateUniqueCallId:**是否为此访问方法生成唯一数字ID，这会覆盖余空间的全局数字ID。

**dialInSecurityProfile:**您希望使用此模板创建的任何访问方法使用哪个dialInSecurityProfile?如果未提供，则使用设置的CoSpaceTemplate级别；如果没有，则使用系统/配置文件级别中的内容。

## 聊天功能

CMS 3.0删除了持续聊天功能，但在CMS 3.2中，返回了空间内的非持续聊天。 Web应用用户可以使用“聊天”，但不会存储在任何地方。 安装CMS 3.2后，Web应用用户默认能够在会议期间相互发送消息。 这些消息仅在会议期间可用，并且只能看到加入后交换的消息。您不能延迟加入并回滚以查看以前的消息。

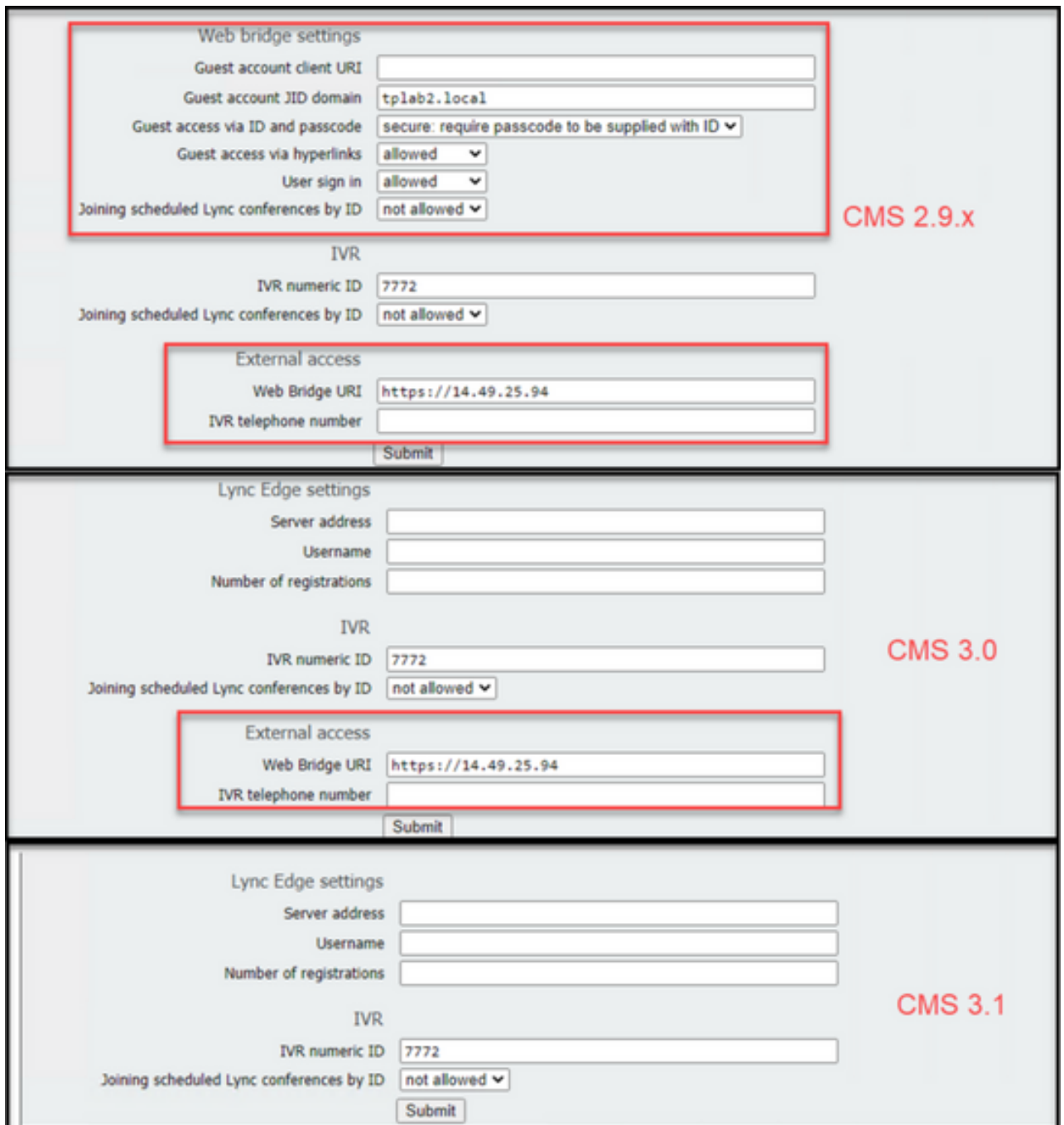
## WebRTC点对点呼叫

在CMS 2.9.x上，WebRTC参与者可以从其客户端直接拨打其他联系人。 从CMS 3.0开始，这不再可能。现在用户必须登录并加入空间。如果他们在该callLegProfile中拥有权限(**addParticipants**参数设置为True)，则他们能够添加其他联系人。 这会使CMS向参与者拨号，并且参与者在CMS的空间上会面。

## 值得注意的WebBridge设置更改

CMS 3.0和3.1已经从GUI中删除或重新定位了某些Webbridge设置，需要在API中进行配置以保持用户的一致体验。 在3.x上，使用api/v1/webBridge和api/v1/webBridgeProfiles。

检查您当前已配置的内容，这样在升级到3.0时，您可以相应地在API中配置webbridge和webbridge配置文件。



在3.0中，Web bridge settings在GUI上删除，然后在CMS 3.1中，External access字段也删除。

### GUI中的Web网桥设置

- 访客帐户客户端URI - callBridge已使用此地址查找webBridge。如果您在为WebRTC部署中有多个WebBridge，则此字段必须为空，并且对于callBridge需要连接的每个WebBridge，必须在api/v1/webbridge中具有唯一的URL。请删除此字段中的内容，并确保在API中配置了WebBridge。
- 访客帐户Jid域 — 在CMS 3.0中不再使用它，您可以删除它。
- 访客通过ID和密码访问 — 已在CMS 3.0中删除且未替换。
- 通过超链接访问访客 — 现在可在API中的webBridgeProfiles下设置“AllowSecrets”中进行配置。

请注意，在CMS 3.0中，已从api/v1/webBridge中删除了多个字段。

- **resourceArchive** — 现在位于webbridgeProfiles中。
- **idEntryMode** — 现已弃用。
- **allowWeblinkAccess** — 现在在webBridgeProfiles中作为allowSecrets。
- **showSignIn** — 现在以userPortalEnabled身份登录webBridgeProfiles。
- **resolveCoSpaceCallIds** — 现在位于webbridgeProfiles中。
- **resolveLyncConferenceIDs** — 现在位于webbridgeProfiles中。

### WebBridgeProfile

- **resourceArchive** — 如果您使用自定义背景并且资源存档存储在Web服务器上，请在此处输入URL。
- **allowPasscodes** — 如果为false，则用户无权选择作为来宾加入会议。他们只能登录或使用包含空间信息和密钥的URL
- **allowSecrets** — 如果设置为false，则用户无法使用URL(例如 [https://meet.company.com/meeting/040478?secret=gPDnucF8is4W1cS87\\_l.zw](https://meet.company.com/meeting/040478?secret=gPDnucF8is4W1cS87_l.zw))加入空格。用户需要使用<https://meet.company.com>，并输入呼叫ID/会议ID/URI和PIN/密码（如果已配置）。



- **userPortalEnabled** — 如果设置为false，则web应用门户登录页面不显示登录选项。它仅显示用于输入呼叫ID/会议ID/URI和PIN/密码的字段（如果已配置）。
- **allowUnauthenticatedGuests** — 如果设置为False，则访客无法加入任何会议 — 即使包含会议ID和密钥的完整URL也是如此。如果为False，则只有可以登录的用户才能加入会议。示例。User2正在尝试使用User1会议的URL。输入URL后，User2必须登录才能继续参加用户1的会议。
- **resolveCoSpaceCallIds** — 如果设置为False，则访客只能通过输入URI和PIN/密码（如果使用）来加入会议。不接受呼叫ID/会议ID/数字ID。
- **resolveCoSpaceUris** - 3个可能的设置：off、domainSuggestionDisabled和domainSuggestionEnabled。此webBridge是否接受coSpace和coSpace访问方法SIP URI，以便允许访问者加入共享空间会议。

— 当设置为“off”时，通过URI加入被禁用。

— 当设置为“domainSuggestionDisabled”时，通过URI加入已启用，但URI的域未自动完成或使用此webBridgeProfile在webBridge上验证。

— 如果设置为“domainSuggestionEnabled”，则通过URI加入已启用，并且可以使用此webBridgeProfile在webBridge上自动完成并验证URI的域。

## 从Web GUI中删除的外部访问部分

在CMS 3.1中，已从Web GUI中删除外部访问部分。如果在升级之前已配置了这些配置文件，则您需要在webbridgeProfiles下的API中重新配置它们。

External access

Web Bridge URI

IVR telephone number

首先，您需要创建webbridgeProfile，如上一节所述。一旦您创建了webbridgeProfile，您就可以通过新创建的webBridgeProfile下的API中的可用链接创建IVR号码和/或Web Bridge URI。



每个webBridgeProfile最多可创建32个IVR号码或32个webbridgeAddresses

## 录制或流

CMS 2.9.x及更早版本上的录制器和流处理器组件是XMPP客户端，从CMS 3.0中，它们基于SIP。现在允许使用API中的默认布局更改录制和流传输的布局。此外，现在名称标签显示在录制/流会话中。有关录制器/流传输功能的详细信息，请参阅CMS 3.0版本说明。

[https://www.cisco.com/c/dam/en/us/td/docs/conferencing/ciscoMeetingServer/Release\\_Notes/Version-3-0/Cisco-Meeting-Server-Release-Notes-3-0.pdf](https://www.cisco.com/c/dam/en/us/td/docs/conferencing/ciscoMeetingServer/Release_Notes/Version-3-0/Cisco-Meeting-Server-Release-Notes-3-0.pdf)。

如果您在2.9.x中配置了录制器或流转换器，则需要重新配置MMP和API中的设置，以便在升级后继续使用这些设置。

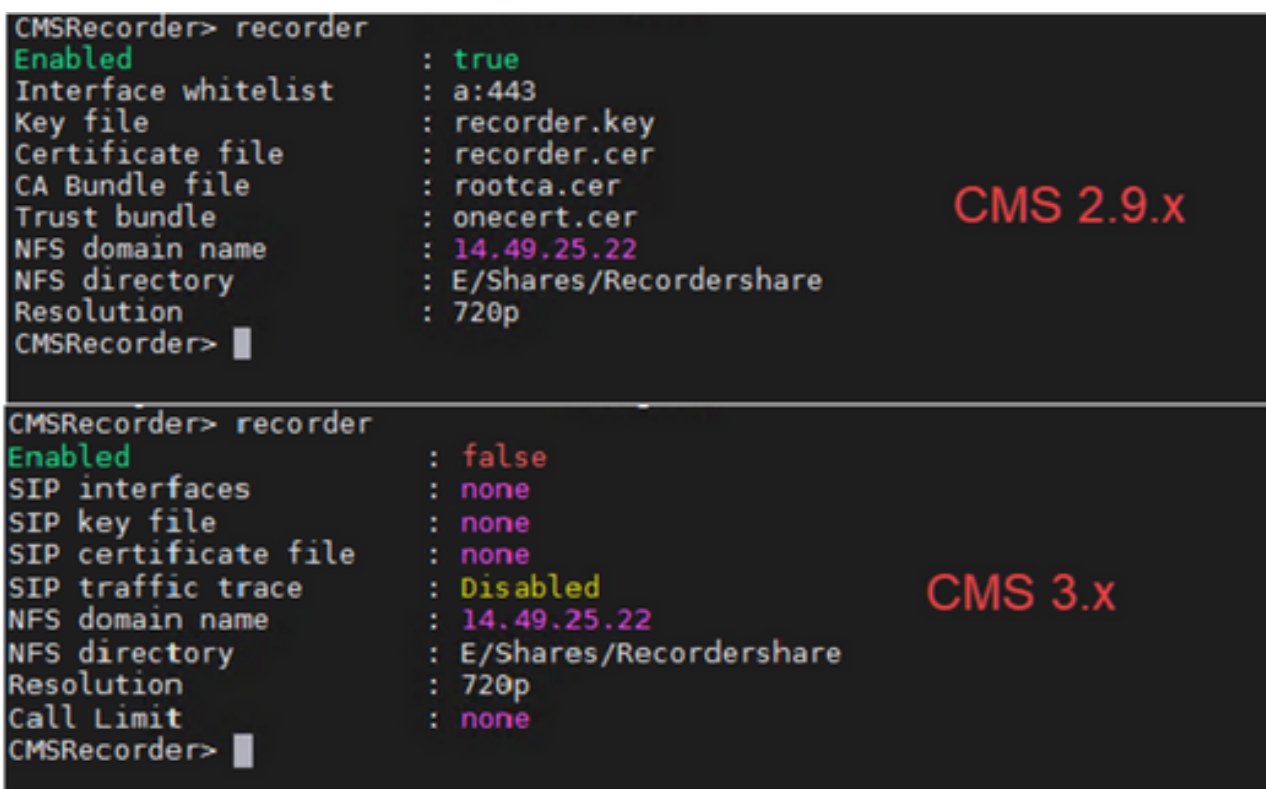
在CMS升级到3.0之前，建议使用“backup snapshot <servername\_date>”进行备份，然后登录callbridge节点上的webadmin页面以删除所有XMPP设置。然后连接到服务器上的MMP，并在通过SSH连接具有xmpp的所有核心服务器上执行以下步骤：

1. xmpp disable
2. xmpp reset
3. xmpp certs none
4. xmpp domain none

## 记录器

### MMP

图中显示了配置记录器时在CMS 2.9.1上看到的配置示例，以及升级到3.0后其外观如何。



```
CMSRecorder> recorder
Enabled                : true
Interface whitelist    : a:443
Key file                : recorder.key
Certificate file       : recorder.cer
CA Bundle file        : rootca.cer
Trust bundle          : onecert.cer
NFS domain name       : 14.49.25.22
NFS directory         : E/Shares/Recordershare
Resolution            : 720p
CMSRecorder> █
```

CMS 2.9.x

```
CMSRecorder> recorder
Enabled                : false
SIP interfaces        : none
SIP key file          : none
SIP certificate file  : none
SIP traffic trace     : Disabled
NFS domain name       : 14.49.25.22
NFS directory         : E/Shares/Recordershare
Resolution            : 720p
Call Limit            : none
CMSRecorder> █
```

CMS 3.x

升级后，您必须重新配置录制器：

步骤1.配置SIP侦听接口。

**recorder sip listen a 5060 5061**(SIP记录器设置为侦听TCP和TLS的接口和端口)。如果不想使用TLS，可以使用“**recorder sip listen a 5060 none**”)

步骤2.配置使用TLS连接的记录器使用的证书。

**recorder sip certs <key-file> <crt-file> [crt-bundle]**(如果没有这些证书，tls服务不会在录制器上启动)

。记录器使用crt-bundle验证callBridge证书。)

步骤3.配置呼叫限制。

recorder limit <0-500|none>(设置服务器可同时提供的记录数限制。该表在我们的文档中，记录器限制必须与服务器上的资源一致。)

Table 6: Internal SIP recorder performance and resource usage

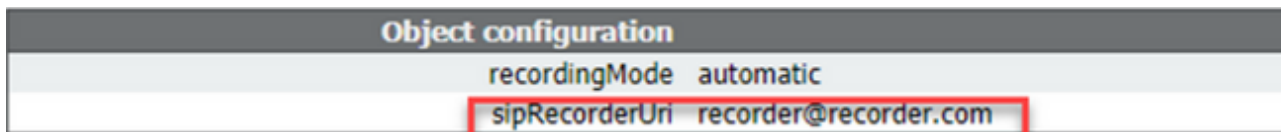
Recording Setting	Recordings per vCPU	RAM required per recording	Disk budget per hour	Maximum concurrent recording
720p	2	0.5GB	1GB	40
1080p	1	1GB	2GB	20
audio	16	100MB	150MB	100

Key point to note (applies to new internal recorder component only):

- Performance scales linearly adding vCPUs up to the number of host physical cores.

## API

在api/v1/callProfiles上，您需要配置sipRecorderUri。这是callBridge在必须开始录制时拨打的URI。此URI的域需要添加到出站规则表，并指向记录器（或呼叫控制）作为要使用的SIP代理。



此图显示了直接拨号到Configuration > Outbound Calls中找到的出站规则上的录制器组件。

The image shows a table of Outbound calls. The 'SIP proxy to use' column contains IP addresses. A red arrow points from the word 'Recorder' to the IP 14.49.17.246-5061. A green arrow points from the word 'Streamer' to the IP 14.49.17.246-6000.

Domain	SIP proxy to use	Local contact domain	Local from domain	Trunk type	Behavior	Priority	Encryption
recorder.com	14.49.17.246-5061		<use local contact domain>	Standard SIP	Continue	1	Encrypted
streamer.com	14.49.17.246-6000		<use local contact domain>	Standard SIP	Continue	1	Encrypted
recorder.com	14.49.17.246		<use local contact domain>	Standard SIP	Stop	0	Auto
streamer.com	14.49.17.246-6000		<use local contact domain>	Standard SIP	Stop	0	Auto

此图显示通过呼叫控制(例如Cisco Unified Communications Manager(CUCM)或Expressway)对录制器组件的呼叫。

The image shows a table of Outbound calls. The 'SIP proxy to use' column contains IP addresses. A green arrow points from the word 'CUCM' to the IP 14.49.17.229. A red arrow points from the word 'Expressway' to the IP 14.49.17.252.

Domain	SIP proxy to use	Local contact domain	Local from domain	Trunk type	Behavior	Priority	Encryption
recorder.com	14.49.17.229		<use local contact domain>	Standard SIP	Continue	1	Encrypted
streamer.com	14.49.17.229		<use local contact domain>	Standard SIP	Continue	1	Encrypted
recorder.com	14.49.17.252		<use local contact domain>	Standard SIP	Stop	0	Auto
streamer.com	14.49.17.252		<use local contact domain>	Standard SIP	Stop	0	Auto

注意：如果将录制器配置为使用SIP TLS，并且呼叫失败，请检查MMP中的callBridge节点，以查看是否启用了TLS SIP验证。MMP命令为“tls sip”。呼叫可能会失败，因为callBridge不信任录制器证书。您可以通过使用“tls sip verify disable”在callBridge上禁用此命

令来测试它。

## 多个记录器？

按照说明配置每个出站规则，并相应地调整出站规则。 如果使用直接记录器方法，请将现有的出站记录器规则更改为行为“继续”，并在前一个出站规则下添加新的出站规则，优先级比第一个出站规则低。 当第一个记录器达到其呼叫限制时，它会在此处将488 Unreceptable发送回callBridge，而callBridge将移至下一个规则。

如果要对记录器进行负载均衡，请使用呼叫控制并调整呼叫控制路由，以便它能够向多个记录器发出呼叫。

## 流处理器

### MMP

从2.9.x升级到3.0后，需要重新配置streamer。

步骤1.配置SIP侦听接口。

**streamer sip listen a 6000 6001**(SIP流处理器设置为侦听TCP和TLS的接口和端口)。 如果不想使用TLS，可以使用“**streamer sip listen a 6000 none**”)

步骤2.配置使用TLS连接的流处理器使用的证书。

**streamer sip certs <key-file> <crt-file> [crt-bundle]**(如果没有这些证书，tls服务不会在streamer上启动。流转换器使用crt-bundle验证callBridge证书。)

步骤3.配置呼叫限制

**streamer limit <0-500|none>**(设置服务器可同时处理的流数限制。该表在我们的文档中，流转换器限制必须与服务器上的资源一致。)

Table 7: Internal SIP streamer recommended specifications

Number of vCPUs	RAM	Number of 720p streams	Number of 1080p streams	Number of audio-only streams
4	4GB	50	37	100
4	8GB	100	75	200
8	8GB	200	150	200

Key points to note (applies to both new internal recorder and streamer components):

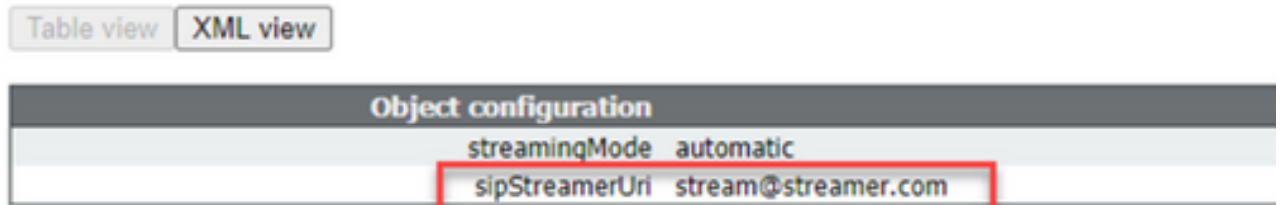
- Number of vCPUs should not oversubscribe the number of physical cores.
- Maximum number of 720p streams supported is 200 regardless of adding more vCPUs
- Maximum number of 1080p streams supported is 150 regardless of adding more vCPUs.
- Maximum number of audio-only streams supported is 200 regardless of adding more vCPUs.

## API

在/api/v1/callProfiles上，您需要配置sipStreamUri。这是callBridge在必须开始流传输时拨打的URI。此URI的域需要添加到您的出站规则表，并指向流转换器（或呼叫控制）作为要使用的SIP代理。

/api/v1/callProfiles/a7f80cbd-5c0b-4888-b3cb-5109408a1dec

Related objects: [/api/v1/callProfiles](#)



此图显示了直接拨号到Configuration > Outbound Calls中找到的出站规则上的流转换器组件。

Outbound calls

Filter  Submit

	Domain	SIP proxy to use	Local contact domain	Local from domain	Trunk type	Behavior	Priority	Encryption
<input type="checkbox"/>	recorder.com	14.49.17.246:5061	Recorder	<use local contact domain>	Standard SIP	Continue	1	Encrypted
<input type="checkbox"/>	streamer.com	14.49.17.246:5001	Streamer	<use local contact domain>	Standard SIP	Continue	1	Encrypted
<input type="checkbox"/>	recorder.com	14.49.17.246		<use local contact domain>	Standard SIP	Stop	0	Auto
<input type="checkbox"/>	streamer.com	14.49.17.246:5000		<use local contact domain>	Standard SIP	Stop	0	Auto
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Standard SIP	Stop	0	Auto

此图显示通过呼叫控制(例如Cisco Unified Communications Manager(CUCM)或Expressway)对录制器组件的呼叫。

Outbound calls

Filter  Submit

	Domain	SIP proxy to use	Local contact domain	Local from domain	Trunk type	Behavior	Priority	Encryption
<input type="checkbox"/>	recorder.com	14.49.17.229	CUCM	<use local contact domain>	Standard SIP	Continue	1	Encrypted
<input type="checkbox"/>	streamer.com	14.49.17.229		<use local contact domain>	Standard SIP	Continue	1	Encrypted
<input type="checkbox"/>	recorder.com	14.49.17.252	Expressway	<use local contact domain>	Standard SIP	Stop	0	Auto
<input type="checkbox"/>	streamer.com	14.49.17.252		<use local contact domain>	Standard SIP	Stop	0	Auto
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Standard SIP	Stop	0	Auto

**注意：**如果将流处理器配置为使用SIP TLS，并且呼叫失败，请检查MMP中的callBridge节点，以查看是否启用了TLS SIP验证。MMP命令为“tls sip”。呼叫可能会失败，因为callBridge不信任流处理器证书。您可以通过使用“tls sip verify disable”在callBridge上禁用此命令来测试它。

### 多个流处理器？

按照说明配置每个出站规则，并相应地调整出站规则。如果使用直接到流转换器方法，请将现有的出站记录器规则更改为行为“继续”，并在前一个出站规则下添加新的出站规则，优先级比第一个出站规则低。当第一个流处理器达到其呼叫限制时，它会将488 Unreceptable发送回到callBridge，并且callBridge会移至下一个规则。

如果要对数据流进行负载均衡，请使用呼叫控制并调整呼叫控制路由，以便它能够向多个数据流发出呼叫。

### Expressway注意事项

如果您使用用于Web代理的Cisco Expressway，则必须确保Expressway在CMS升级之前至少运行X12.6。CMS 3.0要求此步骤才能使Web代理运行并受支持。

与CMS 3.0配合使用时，Web应用参与者的容量比Expressway有所增加。对于大型OVA Expressway，预期容量为150个全高清呼叫(1080p30)或200个其他类型呼叫(例如720p30)。您可以通过将Expressway集群(最多6个节点，其中4个用于扩展，2个用于冗余，因此最多可以进行600个全高清呼叫或800个其他类型呼叫)来增加此容量。

Table 3: Cisco Meeting Server web app call capacities – external calling

Setup	Call Type	CE1200 Platform	Large OVA Expressway
Cisco Expressway Pair (X12.6 or later)	Full HD	150	150
	Other	200	200

## CMS边缘

CMS Edge在CMS 3.1中重新引入，因为它提供的容量比外部Web应用会话的Expressway更高。建议配置有两种。

### 小型边缘规格

4 GB RAM、4个vCPU、1Gbps网络接口

此VM Edge规格具有足够的电源以覆盖单个CMS1000音频和视频负载容量，即48 x 1080p、96 x 720p、192 x 480p和1000音频呼叫。

对于部署，建议每个CMS1000有1台小型边缘服务器，或者每个CMS2000有4台小型边缘服务器。

### 大型边缘规格

8 GB RAM、16个vCPU、10Gbps网络接口

此VM Edge规格具有足够的电源来支持单个CMS2000音频和视频功能，即350 x 1080p、700 x 720p、1000 x 480p和3000 x 音频呼叫。

对于部署，建议每个CMS2000或每个4 CMS1000有1个大型边缘服务器。

Type of Calls	1 x 4 vCPU VM call capacity	1 x 16 vCPU VM call capacity
Full HD calls, 1080p30 video	100	350
HD calls, 720p30 video	175	700
SD calls, 448p30 video	250	1000
Audio Calls (G.711)	850	3000

## 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）。