

從 Cisco Meeting Server 2.9 升級至 3.0 (及更新版本) 的順利升級指南

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[有關升級的重要資訊](#)

[要考慮的事項摘要](#)

[授權](#)

[Webbridge \(WebRTC和CMA客戶端 \)](#)

[Web GUI更改](#)

[錄音機/串流器](#)

[Cisco Expressway注意事項](#)

[CMS邊緣](#)

[CMS \(Acano\) X系列](#)

[SIP邊緣](#)

[進一步資訊](#)

[授權-升級前檢查授權](#)

[確定升級後分配了PMP許可證的使用者數量](#)

[您是否有足夠的SMP許可證？](#)

[配置CMM](#)

[配置Webbridge \(WebRTC和CMA客戶端 \)](#)

[Web應用程式使用者空間建立許可權](#)

[聊天功能](#)

[WebRTC點對點呼叫](#)

[WebBridge設定發生顯著更改](#)

[從Web GUI中刪除了外部訪問部分](#)

[錄製或串流](#)

[錄製程式](#)

[串流器](#)

[Expressway注意事項](#)

[CMS邊緣](#)

簡介

本文檔介紹將運行版本2.9 (或更早版本) 的思科Meeting Server部署升級到3.0 (或更高版本) 所面臨的挑戰，以及如何處理這些挑戰以實現平穩升級過程。

移除的功能：XMPP已移除 (這會影響WebRTC)、中繼/負載平衡器、Webbridge

功能已更改：錄音機和流轉換器現在是SIP，Webbridge由Webbridge3替代

本檔案僅涵蓋升級前需要考慮的主題。它並未涵蓋3.X中的所有新功能。

必要條件

需求

思科建議您瞭解以下主題：

- CMS管理
- CMS升級
- 證書建立和簽名

這裡提到的所有內容都在各種檔案中進行了概述。如果您需要進一步明確功能，建議您隨時閱讀產品發行版本註釋，並參閱我們的程式設計指南和部署指南：[CMS安裝及設定指南](#)和[CMS產品發行版本註釋](#)。

採用元件

本文檔中的資訊基於思科Meeting Server。

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

本文檔旨在指導您是否已部署CMS 2.9.x (或更早版本)，無論是否單一部署或具有恢復能力，以及您計畫何時升級到CMS 3.0。本檔案中的資訊適用於所有CMS型號。



注意：X系列無法升級到CMS 3.0。您需要計畫儘快更換X系列伺服器。

有關升級的重要資訊

升級CMS的唯一支援方法是逐步升級。在撰寫本文時，CMS 3.5已經發佈。如果您使用的是CMS 2.9，則必須以階梯式方式升級(2.9 → 3.0 → 3.1 → 3.2 → 3.3 → 3.4 → 3.5 (請注意，升級程式自CMS 3.5起有變更，因此請仔細閱讀版本說明!!)

如果您未執行逐步升級，並且出現異常行為，TAC可能會請求降級並重新開始。

此外，從CMS 3.4開始，CMS必須使用智慧許可。不能升級到CMS 3.4或更高版本，仍使用傳統許可證。除非已設定智慧許可，否則請勿升級到CMS 3.4或更高版本。

要考慮的事項摘要

使用這些問題導航至與您自己的情況相關的部分。 每個考慮事項都指一個超連結，指向本文檔中更詳細的說明。

授權

在升級之前，您的伺服器上是否有足夠的個人多方(PMP)/共用多方(SMP)許可證？

在3.0中，即使使用者未登入，也會分配PMP許可證。例如，如果您已透過LDAP導入10000個使用者，但您只有100個PMP許可證，則一旦升級到3.0，就會使您不符合要求。對於此使用案例，請確保確實檢查已設定userProfile和/或系統/配置檔案的租戶，以檢視是否已設定值為true且具有hasLicense的userProfile。

如何在API上檢查userProfile並檢視您是否設定了hasLicense=true（表示PMP許可使用者），將在[本節中](#)更詳細地介紹。

當前cms.lic檔案中是否有PMP/SMP許可證？

由於許可證行為在3.0以後發生了變化，在執行升級之前，您必須確認是否具有足夠的PMP/SMP許可證。[本節](#)將對此進行更詳細的介紹。

您是否部署了思科Meeting Manager (CMM)？

CMS 3.0需要CMM 3.0，因為許可證的處理方式發生了變化。建議在您將環境升級到3.0之前部署CMM 2.9，因為您可以檢查過去90天許可證消耗的90天報告。[本節](#)將對此進行更詳細的介紹。

您是否擁有智慧許可？

CMS 3.0需要CMM 3.0，因為許可證的處理方式發生了變化。因此，如果您已經透過CMM使用智慧許可，請確保您的PMP和SMP許可證與集群關聯。

Webbridge（WebRTC和CMA客戶端）

是否在CMS 2.9中使用WebRTC？

Webbridge在CMS 3.0中發生了重大變化。有關從webbridge2遷移到webbridge3以及使用web app的指導，請參閱[本節](#)。

您的使用者是否使用CMA厚客戶端？

由於這些客戶端是基於XMPP的，因此在升級後無法再使用這些客戶端，因為XMPP伺服器已被刪除。如果這適用於您的使用案例，您可以在[本節](#)中找到更多資訊。

是否在WebRTC中使用聊天？

聊天功能在3.0版中從Web應用中刪除。在CMS 3.2中，聊天功能被重新引入，但它不是永續性的。在[本節](#)中可以找到有關此功能的詳細資訊。

您的使用者是否執行從WebRTC到裝置的點對點呼叫？

在CMS 3.0中，Web應用使用者無法再直接撥號到其他裝置。現在，您必須加入會議空間，並有許可權將參與者加入會議，以執行相同的動作。您可以在[本節](#)中找到有關此部件的詳細資訊。

您的使用者是否從WebRTC建立自己的coSpaces？

在3.0中，為了使Web應用使用者能夠從客戶端建立自己的空間，需要在API中建立coSpaceTemplate並將其分配給使用者。在LDAP匯入期間，此操作可以是手動或自動。CanCreateCoSpaces已從UserProfile中刪除。在[本節](#)中可以找到有關此功能的詳細資訊。

Web GUI更改

您是否在Web管理GUI中配置了WebBridge設定？

在3.0中，WebBridge設定將從GUI中刪除，因此您必須在API中配置WebBridge，並注意GUI中的當前設定，以便相應地在API中配置WebBridgeProfiles。您可以在[本節](#)中找到有關此更改的更多資訊。

您是否在Web管理GUI中配置了外部設定？

外部設定已從CMS 3.1的GUI中刪除。如果您在CMS 3.0或更舊的Web管理GUI（配置—>常規—>外部設定）中配置了Webbridge URL或IVR，則這些設定已從網頁中刪除，現在需要在API中進行配置。升級到3.1之前的設定不會增加到API，必須手動完成。您可以在[本節](#)中找到有關此更改的更多資訊。

錄音機/串流器

您目前是否使用任何CMS錄製器和/或串流器？

CMS記錄器和流處理器元件現在基於SIP，而不是基於XMPP。因此，在刪除XMPP時，需要在升級後對其進行調整。您可以在[本節](#)中找到有關此更改的更多資訊。

Cisco Expressway注意事項

如果您使用Expressway代理WebRTC，您當前的Cisco Expressway版本是什麼？

CMS 3.0需要Expressway 12.6或更高版本。[本節](#)中提供了有關WebRTC代理功能的詳細資訊。

CMS邊緣

您的環境中目前是否有CMS Edge？

CMS Edge在CMS 3.1上重新引入，具有更高的外部連線可擴充性。您可以在[本節](#)中找到有關此部件的詳細資訊。

CMS (Acano) X系列

您的環境中目前是否有x系列伺服器？

這些伺服器無法升級到CMS 3.0，您必須考慮儘快更換這些伺服器（在升級到3.0之前遷移到虛擬機器或CMS裝置）。您可以在[此連結](#)中找到有關這些伺服器的壽命終止通知。

SIP邊緣

當前您的環境中是否使用SIP Edge？

Sip Edge自CMS 3.0起已完全棄用。您需要使用Cisco Expressway將SIP呼叫引入您的CMS。請與您的思科客戶代表聯絡，瞭解如何為您的組織獲取Expressway。

進一步資訊

授權-升級前檢查授權

從2.x版本升級到3.0或更高版本時，許可證狀態不合規，是最具影響的問題。本節介紹如何確定平滑升級所需的PMP/SMP許可證數量。

在將部署升級到3.0之前，請部署CMM 2.9，並檢查Licenses 頁籤下的90天報告，以檢視許可證使用量是否一直低於您在CMS節點上分配的許可證數量：

Meetings		In compliance	
Shared Multiparty Plus	Allocated: 100, 90 day peak: 2	Personal Multiparty Plus	Allocated: 100, 90 day peak: 9

Recording or Streaming		In compliance	
Allocated	90 day peak	20	2

如果使用傳統許可（cms.lic檔案安裝在本地的CMS節點上），請檢查CMS許可證檔案以瞭解每個CMS節點上的個人和共用許可證數量（根據本處的景象，為100/100）（從每個callBridge節點透過WinSCP下載）。

```

],
"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": "10"
  }
}

```


許可證相關的問題，但如果您檢查了90天峰值，並且發現您使用的許可證多於可用許可證，則您仍可以升級到CMS 3.0，並使用CMM上的90天試用許可證對您的許可進行分類，或在升級之前採取行動。

Meetings		In compliance			
	Allocated	90 day peak			
Shared Multiparty Plus	100	2	Personal Multiparty Plus	Allocated	90 day peak
			100	9	

Recording or Streaming		In compliance	
	Allocated	90 day peak	
	20	2	

配置Webbridge (WebRTC和CMA客戶端)

CMS 3.0刪除了XMPP伺服器元件，從而刪除了WebBridge和使用CMA厚客戶端的能力。WebBridge3現在用於將Web應用使用者（以前稱為WebRTC使用者）連線到使用瀏覽器的會議。升級到3.0時，需要配置webbridge3。

 注意：升級到CMS 3.0後，CMA客戶端無法正常工作！

本影片確實會引導您完成有關如何建立webbridge 3證書的過程。

<https://video.cisco.com/detail/video/6232772471001?autoStart=true&q=cms>

在升級到3.0之前，客戶必須計畫如何配置Webbridge3。最重要的步驟在此重點介紹。

1. 您需要webbridge3的金鑰和證書鏈。如果證書包含運行webbridge3的所有CMS伺服器FQDN或IP地址作為備用主體名稱(SAN)/公用名(CN)，並且符合以下條件之一，則可以使用舊的webbridge證書：
 - a.證書沒有增強的金鑰用法（意味著它可以用作客戶端或伺服器）。
 - b.證書同時具有客戶端和伺服器身份驗證。HTTPS證書只需要伺服器身份驗證，而C2W證書需要伺服器和客戶端）。
2. 如果要為「webbridge3 https」證書建立新證書，建議進行公開簽名（以避免在使用Web應用時在客戶端上出現證書警告）。此同一證書可用於「webbridge3 c2w證書」，並且證書必須具有SAN/CN中Webbridge伺服器的FQDN。
3. CallBridge需要使用在webbridge3 c2w listen命令中配置的埠與新的webbridge3通訊。這可以是任何可用的連線埠，例如449。使用者需要確定Callbridge可以與此連線埠上的Webbridge3通訊，並在必要時預先進行任何防火牆變更。它不能與「webbridge https」用於偵聽的埠相同。

在CMS升級到3.0之前，建議使用「備份快照<伺服器名_日期>」進行備份，然後登入到Callbridge節點上的Webadmin頁面，以刪除所有XMPP設定和Webbridge設定。然後，連線到伺服器上的MMP，並透過SSH連線對具有xmpp和webbridge的所有核心伺服器執行以下步驟：

1. xmpp disable
2. xmpp reset
3. xmpp certs none
4. xmpp網域無
5. webbridge停用
6. webbridge未接聽
7. webbridge certs none
8. webbridge trust none

升級到3.0後，首先在以前運行webbridge的所有伺服器上配置webbridge3。您必須執行此操作，因為已經有DNS記錄指向這些伺服器，這樣，您就可以確保使用者傳送到Webbridge3時，它能夠準備處理請求。

Webbridge3配置 (透過SSH連線)

步驟 1. 配置webbridge3 http偵聽埠。

Webbridge3 https listen a : 443

步驟 2. 為瀏覽器連線的webbridge3配置證書。這是傳送到瀏覽器的證書，需要由公共證書頒發機構(CA)簽署，並且包含瀏覽器中用於使瀏覽器信任連線的FQDN。

Webbridge3 https certs wb3.key wb3trust.cer (這必須是信任鏈：建立一個在頂部具有終端實體的信任證書，然後按順序排列中繼CA，最後使用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
```

步驟 3. 配置用於偵聽callBridge到Webbridge (c2w)連線的埠。由於443用於webbridge3 https偵聽

埠，因此此配置必須是一個不同的可用埠，例如449。

Webbridge3 c2w 聆聽a : 449

4. 配置Webbridge傳送到Callbridge的c2w信任證書

Webbridge3 c2w certs wb3.key wb3trust.cer

5. 配置WB3用於信任callBridge證書的信任庫。這必須與Callbridge CA捆綁包上使用的證書相同（頂部必須是中間證書的捆綁包，末尾為根CA，後跟單回車）。

Webbridge3 c2w trust rootca.cer

6. 啟用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 (透過SSH連線)

步驟 1. 使用簽署webbridge3 c2w證書的CA證書/捆綁包配置callBridge信任。

Callbridge trust c2w rootca.cer

步驟 2. 重新啟動callBridge以使新信任生效。這將丟棄此特定callBridge上的所有呼叫，因此請謹慎使用此選項。

Callbridge重新啟動

用於連線WebBridge3的callBridge的API配置

1. 使用API中的POST建立新的WebBridge對象，並使用在Webbridge c2w介面白名單中配置的FQDN和埠為對象指定URL值（webbridge3配置中的步驟3）

c2w://webbridge.darmckin.local:449

此時，Webbridge3將再次運行，您可以作為訪客加入空間，或者如果之前導入了使用者，則他們必須能夠登入。

Web應用程式使用者空間建立許可權

您的使用者是否已經習慣了在WebRTC中建立自己的共用空間？從CMS 3.0開始，Web應用使用者無法建立自己的coSpace，除非他們擁有允許此功能的共用空間模板。

即使已指派coSpaceTemplate，這也不會建立其他人可以撥入的空間（無URI、無呼叫ID或密碼），但如果coSpace具有含'addParticipantAllowed'的callLegProfile，則他們可以從該空間撥出。

要具有可用於呼叫新空間的撥號字串，coSpaceTemplate必須具有accessMethodTemplate設定(請參閱2.9發行版本註釋-

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，建立coSpaceTemplate(s)，然後建立accessMethodTemplate(s)，並將coSpaceTemplate分配給ldapUserCoSpaceTemplateSources，或者您可以手動將coSpaceTemplate分配給api/v1/users中的使用者。

您可以建立和分配多個CoSpaceTemplates和accessMethodsTemplates。有關詳細資訊，請參閱CMS API指南(<https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-programming-reference-guides-list.html>)

The screenshot displays the API configuration interface for a CoSpaceTemplate. The top section shows the URL `/api/v1/coSpaceTemplates/b03dbf12-c480-487e-b4d8-955e491ff074` and related objects, including `/api/v1/coSpaceTemplates/b03dbf12-c480-487e-b4d8-955e491ff074/accessMethodTemplates`. Below this is a table view of the object configuration:

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

The bottom section shows the configuration form for the CoSpaceTemplate, with fields for name, description, callProfile, callLegProfile, and dialInSecurityProfile. A red arrow points from the `accessMethodTemplates` link in the top section to the configuration form for `/api/v1/coSpaceTemplates/b03dbf12-c480-487e-b4d8-955e491ff074/accessMethodTemplates`, which includes fields for name, uriGenerator, callLegProfile, generateUniqueCallId, and dialInSecurityProfile.

CoSpaceTemplate (API配置)

名稱：要賦予coSpaceTemplate的任何名稱。

說明：簡要說明（如果需要）。

callProfile：要使用白色callProfile透過此模板建立的任何空間？如果未提供，則使用在系統/配置檔案級別上設定的值。

callegProfile：您希望使用此模板建立的任何空間使用哪個callegProfile？如果未提供，則使用在系統/配置檔案級別上設定的值。

dialInSecurityProfile：您希望使用此模板建立的任何空間使用哪個dialInSecurityProfile？如果未提供，則使用在系統/配置檔案級別上設定的值。

AccessMethodTemplate (API配置)

名稱：要賦予coSpaceTemplate的任何名稱。

uriGenerator：用於為此訪問方法模板生成URI值的表達式；允許的字符集為「a」到「z」、「A」到「Z」、「0」到「9」、「。」、「-」、「_」和「\$」；如果不為空，則只能包含一個「\$」字元。此範例為\$.space，建立空間時，會使用使用者提供的名稱，並在其中附加「.space」。「Team Meeting」建立URL「Team.Meeting.space@domain」。

callLegProfile：您希望使用此模板建立的任何訪問方法使用哪個callegProfile？如果未提供，則使用已設定的CoSpaceTemplate級別，如果沒有，則使用系統/配置檔案級別中的設定。

generateUniqueCallId：是否為此訪問方法生成唯一數字ID，這將覆蓋cospace的全局數字ID。

dialInSecurityProfile：您希望使用此模板建立的任何訪問方法使用哪個dialInSecurityProfile？如果未提供，則使用已設定的CoSpaceTemplate級別，如果沒有，則使用系統/配置檔案級別中的設定。

聊天功能

CMS 3.0刪除了持續聊天功能，但在CMS 3.2中返回了非持續聊天空間。Web應用使用者可以使用Chat，但不會儲存在任何地方。安裝CMS 3.2後，Web應用使用者預設能夠在會議中相互傳送消息。這些消息僅在會議期間可用，並且只能看到加入後交換的消息。您無法晚加入並卷回檢視先前的訊息。

WebRTC點對點呼叫

在CMS 2.9.x上，WebRTC參與者能夠從他們的客戶端直接撥號到其他聯絡人。從CMS 3.0開始，這不再可行。現在，使用者必須登入並加入空間。從這裡，如果他們在callLegProfile(將addParticipants引數設定為True)中具有許可權，他們能夠增加其他聯絡人。這使CMS向參與者撥號，參與者在CMS的空間中會面。

WebBridge設定發生顯著更改

CMS 3.0和3.1已從GUI中刪除或重新定位了某些Webbridge設定，需要在API中進行配置以保持使用者的一致體驗。在3.x上，使用api/v1/webBridge和api/v1/webBridgeProfiles。

檢查您目前設定的專案，當您升級至3.0時，可以相應地在API中設定Webbridge和Webbridge設定檔。

The image displays three sequential screenshots of the CMS configuration interface, illustrating the changes to Web Bridge settings over time:

- CMS 2.9.x:** Shows a 'Web bridge settings' section (highlighted with a red box) containing fields for 'Guest account client URI', 'Guest account JID domain' (tp1ab2.local), 'Guest access via ID and passcode' (secure: require passcode to be supplied with ID), 'Guest access via hyperlinks' (allowed), 'User sign in' (allowed), and 'Joining scheduled Lync conferences by ID' (not allowed). Below this is an 'IVR' section with 'IVR numeric ID' (7772) and 'Joining scheduled Lync conferences by ID' (not allowed). A separate 'External access' section (also highlighted with a red box) includes 'Web Bridge URI' (https://14.49.25.94) and 'IVR telephone number'. A 'Submit' button is at the bottom.
- CMS 3.0:** Shows 'Lync Edge settings' (Server address, Username, Number of registrations), 'IVR' (IVR numeric ID: 7772, Joining scheduled Lync conferences by ID: not allowed), and the 'External access' section (Web Bridge URI: https://14.49.25.94, IVR telephone number). A 'Submit' button is at the bottom.
- CMS 3.1:** Shows 'Lync Edge settings' (Server address, Username, Number of registrations), 'IVR' (IVR numeric ID: 7772, Joining scheduled Lync conferences by ID: not allowed), and a 'Submit' button. The 'External access' section has been removed.

在3.0中，在GUI上刪除了Web網橋設定，然後在CMS 3.1中，外部訪問欄位也已刪除。

GUI中的Web網橋設定

- 訪客帳戶客戶端URI - callBridge使用此地址查詢webBridge。如果您在為WebRTC部署中有多个webBridge，則此欄位必須為空，並且您必須在api/v1/webbridge中具有唯一的URL，以用於callBridge需要連線的每個webBridge。刪除此欄位中的所有內容，並確保您已在API中配置了webBridge。
- 訪客帳戶Jid域 -在CMS 3.0中不再使用此欄位，您可以刪除此欄位。
- 訪客透過ID和密碼訪問- 在CMS 3.0中刪除且未替換。
- 訪客透過超連結訪問- 現在可在API的webBridgeProfiles下設定「AllowSecrets」中進行配置。

The image shows two screenshots of the CMS configuration interface for `/api/v1/webBridges`.

Top Screenshot (CMS 2.9.x): This interface includes the following fields:

- `url` (checkbox, text input, (URL))
- `resourceArchive` (checkbox, text input, (URL))
- `tenant` (checkbox, text input, Choose)
- `tenantGroup` (checkbox, text input, Choose)
- `idEntryMode` (checkbox, dropdown menu, <unset>)
- `allowWeblinkAccess` (checkbox, dropdown menu, <unset>)
- `showSignIn` (checkbox, dropdown menu, <unset>)
- `resolveCoSpaceCallIds` (checkbox, dropdown menu, <unset>)
- `resolveLyncConferenceIds` (checkbox, dropdown menu, <unset>)
- `callBridge` (checkbox, text input, Choose)
- `callBridgeGroup` (checkbox, text input, Choose)

Bottom Screenshot (CMS 3.0): This interface includes the following fields:

- `url` (checkbox, text input, (URL))
- `tenant` (checkbox, text input, Choose)
- `tenantGroup` (checkbox, text input, Choose)
- `callBridge` (checkbox, text input, Choose)
- `callBridgeGroup` (checkbox, text input, Choose)
- `webBridgeProfile` (checkbox, text input, Choose)

注意，在CMS 3.0中，已從api/v1/webBridge中刪除多個欄位。

- `resourceArchive` -現在位於webbridgeProfiles中。
- `idEntryMode` - 現在已棄用。
- `allowWeblinkAccess` -現在在webBridgeProfiles中為allowSecrets。
- `showSignIn` -現在以userPortalEnabled身份顯示在webBridgeProfiles中。
- `resolveCoSpaceCallIds`- 現在位於webbridgeProfiles中。
- `resolveLyncConferenceIDs` -現已位於webbridgeProfiles中。

The image shows the CMS configuration interface for `/api/v1/webBridgeProfiles` for CMS 3.0 onward. It includes the following fields:

- `name` (checkbox, text input)
- `resourceArchive` (checkbox, text input, (URL))
- `allowPasscodes` (checkbox, dropdown menu, <unset>)
- `allowSecrets` (checkbox, dropdown menu, <unset>)
- `userPortalEnabled` (checkbox, dropdown menu, <unset>)
- `allowUnauthenticatedGuests` (checkbox, dropdown menu, <unset>)
- `resolveCoSpaceCallIds` (checkbox, dropdown menu, <unset>)
- `resolveCoSpaceUris` (checkbox, dropdown menu, <unset>)

WebBridge配置檔案

- `resourceArchive` -如果使用自定義背景並且資源存檔儲存在Web伺服器上，請在此處輸入URL。
- `allowPasscodes` -如果為false，則使用者沒有作為訪客加入會議的選項。他們只能登入或使用包含空間資訊和金鑰的URL
- `allowSecrets` - 如果設定為false，則使用者不能使用URL(如

https://meet.company.com/meeting/040478?secret=gPDnucF8is4W1cS87_l.zw)加入空格。使用者需要使用<https://meet.company.com>，並輸入呼叫ID/會議ID/URI和PIN/密碼（如果已配置）。

- userPortalEnabled -如果設定為false，則web應用門戶登入頁不顯示登入選項。它僅顯示用於輸入呼叫ID/會議ID/URI和PIN/密碼（如果已配置）的欄位。
- allowUnauthenticatedGuests -如果設定為False，則訪客無法加入任何會議-即使具有包含會議ID和金鑰的完整URL也是如此。如果為False，則只有可以登入的使用者才可以加入會議。
範例. User2正在嘗試使用User1會議的URL。輸入URL後，User2必須登入才能繼續參加User1的會議。
- resolveCoSpaceCallIds -如果設定為False，則訪客只能透過使用URI和PIN/密碼（如果使用）來加入會議。不接受通話ID/會議ID/數字ID。
- resolveCoSpaceUri - 3個可能的設定：off、domainSuggestionDisabled和domainSuggestionEnabled。此webBridge是否接受coSpace和coSpace訪問方法SIP URI，以便允許訪問者加入cospace會議。


- 設定為「off」時，將停用透過URI加入。

- 如果設定為「domainSuggestionDisabled」，則會啟用透過URI加入，但URI的域不會自動完成或在使用此webBridgeProfile的webBridge上驗證。

- 如果設定為「domainSuggestionEnabled」，則透過URI加入的域已啟用，並且可以使用webBridgeProfile在webBridge上自動完成並驗證URI的域。

從Web GUI中刪除了外部訪問部分

在CMS 3.1中，外部存取區段已從Web GUI中移除。如果您在升級前已設定這些區段，則您需要在webbridgeProfiles下的API中重新設定。



External access

Web Bridge URI

IVR telephone number

首先，您需要按照上一節中的說明建立WebbridgeProfile。建立webbridgeProfile後，可以透過新建立的webBridgeProfile下的API中可用的連結建立IVR號碼和/或Web Bridge URI。



每個webBridgeProfile最多可建立32個IVR號碼或32個webbridgeAddresses

錄製或串流

CMS 2.9.x和更早版本上的錄製器和串流器元件是XMPP客戶端，而從CMS 3.0開始，它們基於SIP。現在允許使用API中的預設版面配置來變更錄製和串流的版面配置。此外，現在名稱標籤也會顯示在錄製/串流工作階段中。請參閱CMS 3.0發行版本註釋，瞭解錄製器/串流功能的更多資訊-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中配置了錄製器或串流器，則需要重新配置MMP和API中的設定，以便在升級後這些設定繼續運行。

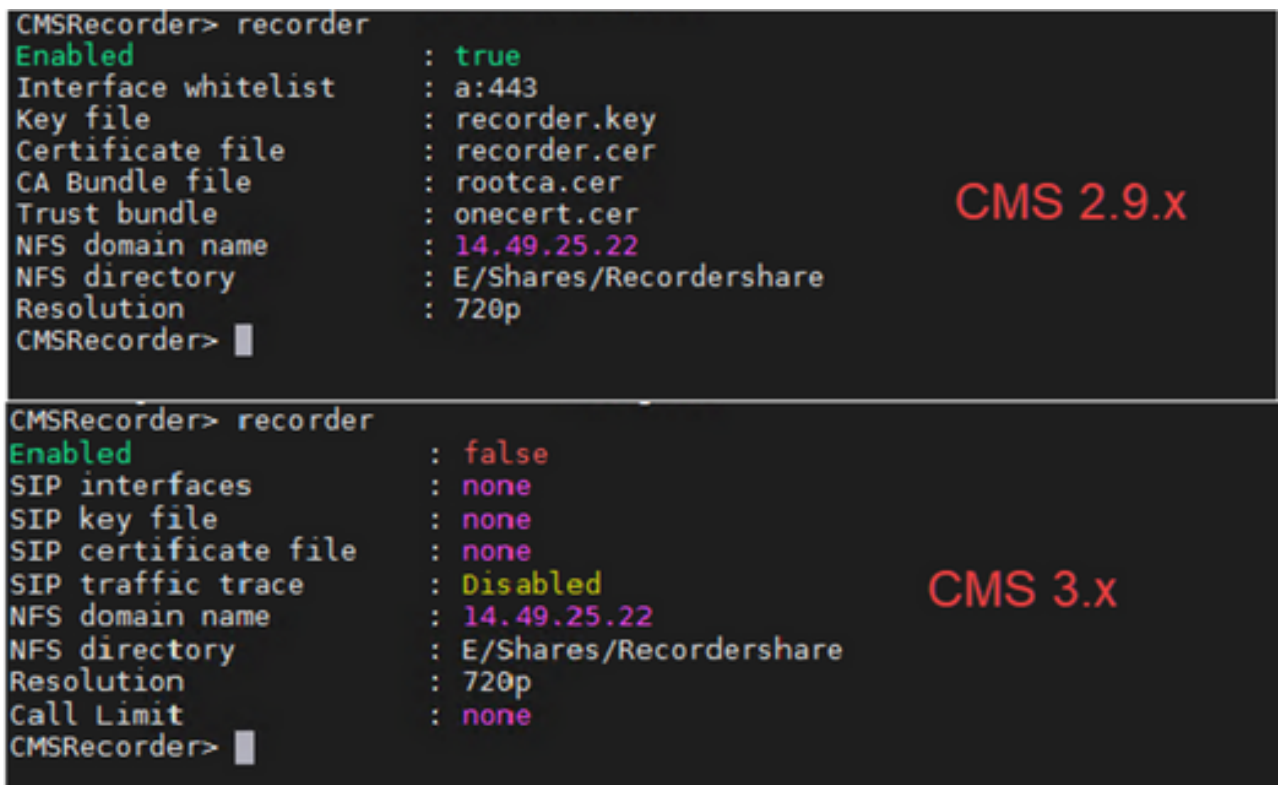
在CMS升級到3.0之前，建議使用「備份快照<伺服器名_日期>」進行備份，然後登入到Callbridge節點上的Webadmin頁面以刪除所有XMPP設定。然後，連線到伺服器上的MMP，並在所有透過SSH連線具有xmpp的核心伺服器上執行以下步驟：

1. xmpp disable
2. xmpp reset
3. xmpp certs none
4. xmpp網域無

錄製程式

MMP

下圖顯示了配置錄製器時在CMS 2.9.1上看到的配置示例，以及升級到3.0後的外觀。



```
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>

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>
```

升級之後，您必須重新設定錄製程式：

步驟 1.配置SIP偵聽介面。

錄製器sip監聽5060 5061 (SIP錄製器設定為監聽TCP和TLS的介面和埠)。如果不想使用TLS，您可以使用「錄製器sip偵聽5060無」)

步驟 2.設定當您使用TLS連線時，錄製器所使用的憑證。

recorder sip certs <key-file> <crt-file> [crt-bundle](如果沒有這些證書，tls服務不會在錄製器上啟動。記錄器使用crt捆綁包驗證callBridge證書。)

步驟 3.配置呼叫限制。

recorder limit <0-500|none>(設定伺服器可同時處理的記錄數限制。此表格位於我們的說明檔案中，錄製器限制必須與伺服器上的資源一致。)

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。這是callBridge在必須開始錄製時撥打的URI。此URI的域需要增加到出站規則表，並指向記錄器 (或呼叫控制) 作為要使用的SIP代理。

Object configuration	
recordingMode	automatic
sipRecorderUri	recorder@recorder.com

本圖顯示在Configuration > Outbound Calls中找到的出站規則上的錄製器元件的直接撥號。

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	14.49.17.246-6001		<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	14.49.17.246-6000	Streamer	<use local contact domain>	Standard SIP	Stop	0	Auto

本圖顯示透過呼叫控制(例如Cisco Unified Communications Manager (CUCM)或Expressway)對錄製器元件的呼叫。


Outbound calls

Filter

	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		<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		<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
					Standard SIP	Stop	0	Auto

CUCM (green arrow pointing to 14.49.17.229)

Expressway (red arrow pointing to 14.49.17.252)

 注意：如果您將錄製器配置為使用SIP TLS，並且呼叫失敗，請檢查MMP中的callBridge節點，以檢視是否啟用了TLS SIP驗證。MMP命令是「tls sip」。呼叫可能會失敗，因為記錄器憑證不受callBridge信任。要測試此功能，您可以使用「tls sip verify disable」在callBridge上停用此功能。

多重錄音機？

按照說明配置每個規則，並相應地調整出站規則。如果使用直接到記錄程式方法，請將現有出站到記錄程式規則更改為行為「繼續」，並在前一個出站規則下增加新的出站規則，優先順序比前一個出站規則低1。當第一個記錄器達到其呼叫限制時，它在此處將488 Unsuccessful命令傳送回callBridge，並且callBridge將移至下一個規則。

如果您要平衡記錄器的負載，請使用呼叫控制並調整呼叫控制路由，以便它能夠向多個記錄器發出呼叫。

串流器

MMP

從2.9.x升級到3.0後，需要重新配置流處理器。

步驟 1. 配置SIP偵聽介面。

流處理器sip監聽6000 6001 (SIP流處理器設定為監聽TCP和TLS的介面和埠)。如果您不想使用TLS，您可以使用「流處理器sip偵聽6000無」)

步驟 2. 配置使用TLS連線時流處理器使用的證書。

streamer sip certs <key-file> <crt-file> [crt-bundle] (如果沒有這些證書，tls服務不會在流處理器上啟動。流處理器使用crt捆綁來驗證callBridge證書。)

步驟 3. 配置呼叫限制

streamer limit <0-500|none>(設定伺服器可同時服務的流的數量限制。此表格位於我們的檔案中，串流器限制必須與伺服器上的資源一致。)

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。這是callBridge在必須啟動流式處理時撥打的URI。此URI的域需要增加到出站規則表，並指向流處理器（或呼叫控制）作為要使用的SIP代理。

[/api/v1/callProfiles/a7f80cbd-5c0b-4888-b3cb-5109408a1dec](#)

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

Table view XML view

Object configuration	
streamingMode	automatic
sipStreamerUri	stream@streamer.com

本圖顯示對Configuration > Outbound Calls上出站規則上的流處理器元件的直接撥號。

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		<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	Streamer	<use local contact domain>	Standard SIP	Stop	0	Auto
<input type="checkbox"/>					Standard SIP	Stop	0	Auto


本圖顯示透過呼叫控制(例如Cisco Unified Communications Manager (CUCM)或Expressway)對錄製器元件的呼叫。

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		<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		<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

Annotations: A green arrow points from the 'SIP proxy to use' column to the '14.49.17.229' value. A red arrow points from the 'SIP proxy to use' column to the '14.49.17.252' value. A blue 'CUCM' label is above the first two rows. A red 'Expressway' label is above the last two rows.

 注意：如果您將流處理器配置為使用SIP TLS，並且呼叫失敗，請檢查MMP中的callBridge節點，以檢視您是否啟用了TLS SIP驗證。MMP命令是「tls sip」。呼叫可能會失敗，因為callBridge不信任串流器憑證。要測試此功能，您可以使用「tls sip verify disable」在callBridge上停用此功能。

多重串流器？

按照說明配置每個規則，並相應地調整出站規則。如果您使用直接去串流器方法，請將現有的去話記錄器規則更改為行為「繼續」，並在上一個規則下增加新的去話規則，優先順序比第一個規則低1。當第一個流傳輸器達到其呼叫限制時，它在此處將488 Unreceptable傳送回callBridge，並且callBridge將移至下一個規則。

如果要對流處理器進行負載均衡，請使用呼叫控制並調整呼叫控制路由，以便它能夠向多個流處理器發出呼叫。

Expressway注意事項

如果您使用Cisco Expressway for Web Proxy，則必須確保Expressway在CMS升級之前至少運行了X12.6。CMS 3.0需要此許可證才能使Web代理正常運行並獲得支援。

與CMS 3.0配合使用時，Web應用參與者的容量已超過Expressway。對於大型OVA Expressway，預期容量為150個Full HD呼叫(1080p30)或200個其他型別呼叫（例如720p30）。您可以將Expressway集群（最多6個節點，其中4個用於擴展，2個用於冗餘，因此最多可達600個Full HD呼叫，或800個其他型別呼叫）來增加此容量。

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邊緣

CMS 3.1中重新引入了CMS Edge，因為它提供的容量比外部Web應用會話的Expressway更高。建議採用兩種配置。

小型邊緣規格

4 GB RAM、4個vCPU、1Gbps網路介面

此VM Edge規格具有足夠的電源以覆蓋單個CMS1000音訊和影片負載，即48 x 1080p、96 x 720p、192 x 480p和1000音訊呼叫。

對於部署，建議每個CMS1000有1個小型邊緣伺服器，或者每個CMS2000有4個小型邊緣伺服器。

大型邊緣規格

8 GB RAM、16個vCPU、10Gbps網路介面

此VM Edge規格具備足夠的電源以涵蓋單一CMS2000音訊和視訊容量，即350 x 1080p、700 x 720p、1000 x 480p和3000 x音訊呼叫。

對於部署，建議每個CMS2000或每個4個CMS1000有1個大型邊緣伺服器。

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

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）。