

# Conseils pour une mise à niveau en douceur de Cisco Meeting Server 2.9 vers 3.0 (et versions ultérieures)

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Informations importantes sur les mises à niveau](#)

[Résumé des éléments à prendre en compte](#)

[Licences](#)

[Webbridge \(client WebRTC et CMA\)](#)

[Modifications de la GUI Web](#)

[Enregistreurs / Flux](#)

[Considérations relatives à Cisco Expressway](#)

[Périphérie CMS](#)

[Série X CMS \(Acano\)](#)

[Périphérie SIP](#)

[Informations complémentaires](#)

[Licences - Vérifier les licences avant la mise à niveau](#)

[Déterminer le nombre d'utilisateurs auxquels une licence PMP est attribuée une fois la mise à niveau effectuée](#)

[Disposez-vous de suffisamment de licences SMP ?](#)

[Configurer CMM](#)

[Configurer Webbridge \(client WebRTC et CMA\)](#)

[Autorisations de création d'espace utilisateur Web app](#)

[Fonction de conversation](#)

[Appels point à point WebRTC](#)

[Modifications notables des paramètres webBridge](#)

[Section Accès externe supprimée de l'interface utilisateur graphique Web](#)

[Enregistrement ou diffusion en continu](#)

[Enregistreur](#)

[Diffuseur](#)

[Contrepartie Expressway](#)

[Périphérie CMS](#)

---

## Introduction

Ce document décrit les défis de la mise à niveau d'un déploiement de Cisco Meeting Server exécutant la version 2.9 (ou antérieure) vers la version 3.0 (ou ultérieure) et comment les gérer pour un processus de mise à niveau fluide.

Fonctionnalités supprimées : XMPP a été supprimé (ce qui affecte WebRTC), agrégations/équilibres de charge, webbridge

Fonctionnalités modifiées : les enregistreurs et les streamers sont désormais SIP et webbridge est remplacé par webbridge3

Ce document couvre uniquement les rubriques à prendre en compte avant la mise à niveau. Il ne couvre pas toutes les nouvelles fonctionnalités disponibles dans 3.X.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- administration CMS
- Mises à niveau CMS
- Création et signature de certificats

Tout ce qui est mentionné ici est décrit dans divers documents. Il est toujours conseillé de lire les notes de version du produit et de vous reporter à nos guides de programmation et de déploiement si vous avez besoin de plus de précisions sur les fonctionnalités : [Guides d'installation et de configuration de CMS](#) et [Notes de version du produit CMS](#) .

### Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Meeting Server.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Informations générales

Ce document a pour but de vous guider si vous disposez déjà d'un déploiement CMS 2.9.x (ou antérieur), qu'il soit unique, combiné ou résilient, et quand vous prévoyez de mettre à niveau vers CMS 3.0. Les informations contenues dans ce document concernent tous les modèles de CMS.

---

 Remarque : la série X ne peut pas être mise à niveau vers CMS 3.0. Vous devez prévoir de remplacer vos serveurs de la gamme X dès que possible.

---

# Informations importantes sur les mises à niveau

La seule méthode prise en charge pour mettre à niveau CMS est une mise à niveau par étapes. Au moment de la rédaction de ce document, CMS 3.5 a été publié. Si vous utilisez CMS 2.9, vous devez effectuer la mise à niveau par étapes (2.9 → 3.0 → 3.1 → 3.2 → 3.3 → 3.4 → 3.5) (Notez que le processus de mise à niveau a été modifié à partir de CMS 3.5, lisez donc attentivement les notes de version!!)

Si vous n'effectuez pas de mise à niveau progressive et que vous rencontrez un comportement inhabituel, le TAC peut vous demander de procéder à une mise à niveau vers une version antérieure et de recommencer.

En outre, à partir de la version 3.4 de CMS, CMS DOIT utiliser Smart Licensing. Vous ne pouvez pas effectuer de mise à niveau vers CMS 3.4 ou version ultérieure et continuer à utiliser des licences traditionnelles. Ne mettez pas à niveau vers CMS 3.4 ou version ultérieure à moins d'avoir configuré Smart Licensing.

## Résumé des éléments à prendre en compte

Utilisez ces questions pour accéder aux sections relatives à votre propre situation. Chaque considération fait référence à un hyperlien vers une description plus détaillée présentée dans ce document.

### Licences

Disposez-vous de suffisamment de licences Personal MultiParty (PMP) / Shared MultiParty (SMP) sur vos serveurs avant la mise à niveau ?

Dans la version 3.0, les licences PMP sont attribuées, même si l'utilisateur n'est pas connecté. Par exemple, si vous avez importé 10000 utilisateurs via LDAP, mais que vous n'avez que 100 licences PMP, cela vous met hors de conformité dès que vous effectuez la mise à niveau vers la version 3.0. Pour cet exemple d'utilisation, assurez-vous de vérifier les locataires qui ont userProfile défini et/ou system/profiles pour voir si un userProfile avec hasLicense avec une valeur true est défini.

La vérification du profil utilisateur sur l'API et la vérification de la configuration de hasLicense=true (qui signifie les utilisateurs disposant d'une licence PMP) sont décrites plus en détail dans [cette section](#).

Votre fichier cms.lic actuel contient-il des licences PMP/SMP ?

En raison d'un changement de comportement de licence à partir de la version 3.0, vous devez confirmer si vous disposez de suffisamment de licences PMP/SMP avant d'effectuer la mise à niveau. Ceci est décrit plus en détail dans [cette section](#).

Avez-vous déployé Cisco Meeting Manager (CMM) ?

CMS 3.0 nécessite CMM 3.0 en raison des modifications apportées au mode de gestion des licences. Il est recommandé de déployer CMM 2.9 avant d'effectuer une mise à niveau de votre environnement vers la version 3.0, car vous pouvez consulter votre rapport de 90 jours pour connaître la consommation de licence des 90 derniers jours. Ceci est décrit plus en détail dans [cette section](#).

#### Disposez-vous de licences Smart ?

CMS 3.0 nécessite CMM 3.0 en raison des modifications apportées au mode de gestion des licences. Par conséquent, si vous utilisez déjà Smart Licensing via CMM, assurez-vous que des licences PMP et SMP sont associées à votre cluster.

#### Webbridge (client WebRTC et CMA)

##### Utilisez-vous WebRTC dans CMS 2.9 ?

Webbridge a considérablement changé dans CMS 3.0. Pour obtenir des conseils sur la migration de webbridge2 vers webbridge3 et sur l'utilisation de l'application Web, reportez-vous à la [présente section](#).

##### Vos utilisateurs utilisent-ils le client CMA épais ?

Comme ces clients sont basés sur XMPP, ces clients ne peuvent plus être utilisés après la mise à niveau car le serveur XMPP a été supprimé. Si cela s'applique à votre cas d'utilisation, vous trouverez plus d'informations dans [cette section](#).

##### Utilisez-vous la fonction de conversation dans WebRTC ?

La fonctionnalité de conversation est supprimée de l'application Web dans la version 3.0. Dans CMS 3.2, la conversation est réintroduite, mais elle n'est pas persistante. Vous trouverez plus d'informations sur cette fonctionnalité dans [cette section](#).

##### Vos utilisateurs effectuent-ils des appels point à point à partir de WebRTC vers des périphériques ?

Dans CMS 3.0, un utilisateur d'application Web ne peut plus composer directement un numéro sur un autre appareil. Vous devez à présent vous connecter à un espace de téléconférence et être autorisé à ajouter des participants à la téléconférence pour effectuer la même action. Vous trouverez plus d'informations sur cette partie dans [cette section](#).

##### Vos utilisateurs créent-ils leurs propres coSpaces à partir de WebRTC ?

Dans la version 3.0, pour que les utilisateurs d'applications Web puissent créer leurs propres espaces à partir du client, un coSpaceTemplate doit être créé dans l'API et attribué à l'utilisateur. Cette opération peut être manuelle ou automatique pendant l'importation LDAP. CanCreateCoSpaces est supprimé de UserProfile. Vous trouverez plus d'informations sur cette fonctionnalité dans [cette section](#).

#### Modifications de la GUI Web

## Les paramètres webBridge sont-ils configurés dans l'interface utilisateur graphique de l'administrateur Web ?

Les paramètres webBridge sont supprimés de l'interface utilisateur graphique dans la version 3.0. Vous devez donc configurer les webbridge dans l'API et noter vos paramètres actuels dans l'interface utilisateur graphique afin de pouvoir configurer les webBridgeProfiles dans l'API en conséquence. Vous trouverez plus d'informations sur cette modification dans [cette section](#).

## Les paramètres externes sont-ils configurés dans l'interface utilisateur graphique de l'administrateur Web ?

Les paramètres externes ont été supprimés de l'interface utilisateur graphique dans CMS 3.1. Si l'URL de Webbridge ou l'IVR sont configurés dans votre interface utilisateur graphique d'administration Web CMS 3.0 ou antérieure (Configuration —> Général —> Paramètres externes), ils ont été supprimés de la page Web et doivent maintenant être configurés dans l'API. Les paramètres précédents avant la mise à niveau vers 3.1 ne sont PAS ajoutés à l'API et doivent être effectués manuellement. Vous trouverez plus d'informations sur cette modification dans [cette section](#).

## Enregistreurs / Flux

### Utilisez-vous actuellement un ou plusieurs enregistreurs CMS et/ou un ou plusieurs streamers ?

L'enregistreur CMS et le composant streamer sont désormais basés sur SIP au lieu de XMPP. Par conséquent, comme le XMPP est en cours de suppression, ceux-ci doivent être modifiés après la mise à niveau. Vous trouverez plus d'informations sur cette modification dans [cette section](#).

## Considérations relatives à Cisco Expressway

### Quelle est votre version actuelle de Cisco Expressway si vous utilisez Expressway pour créer un proxy WebRTC ?

CMS 3.0 requiert Expressway 12.6 ou version ultérieure. Vous trouverez plus d'informations sur cette fonctionnalité de proxy WebRTC dans [cette section](#).

## Périphérie CMS

### Votre environnement comporte-t-il actuellement un CMS Edge ?

CMS Edge est réintroduit sur CMS 3.1 avec une évolutivité supérieure pour les connexions externes. Vous trouverez plus d'informations sur cette partie dans [cette section](#).

## Série X CMS (Acano)

### Votre environnement comporte-t-il actuellement des serveurs x-series ?

Ces serveurs ne peuvent pas être mis à niveau vers CMS 3.0 et vous devez envisager de les remplacer bientôt (passez à une machine virtuelle ou à un appareil CMS avant de procéder à la

mise à niveau vers la version 3.0). Vous trouverez l'avis de fin de vie de ces serveurs dans [ce lien](#).

## Périphérie SIP

### Utilisez-vous actuellement SIP Edge dans votre environnement ?

Sip Edge est totalement déconseillé depuis CMS 3.0. Vous devez utiliser Cisco Expressway pour passer des appels SIP dans votre CMS. Contactez votre représentant Cisco pour savoir comment obtenir Expressway pour votre organisation.

## Informations complémentaires

### Licences - Vérifier les licences avant la mise à niveau

L'état de la licence non conforme est le problème le plus important lorsque vous effectuez une mise à niveau vers la version 3.0 ou supérieure à partir d'une version 2.x. Cette section décrit comment déterminer le nombre de licences PMP/SMP dont vous avez besoin pour une mise à niveau en douceur.

Avant de mettre à niveau votre déploiement vers la version 3.0, déployez CMM 2.9 et vérifiez le rapport de 90 jours sous l'onglet Licences pour voir si l'utilisation de la licence est restée en deçà de la quantité de licence actuellement allouée sur les noeuds CMS :

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

Allocated	90 day peak
20	2

Si vous utilisez la licence traditionnelle (le fichier cms.lic est installé localement sur vos noeuds CMS), vérifiez le fichier de licence CMS pour les quantités de licences personnelles et partagées (100 / 100 selon l'image ici) sur chacun des noeuds CMS (téléchargement via WinSCP depuis chaque noeud callBridge).

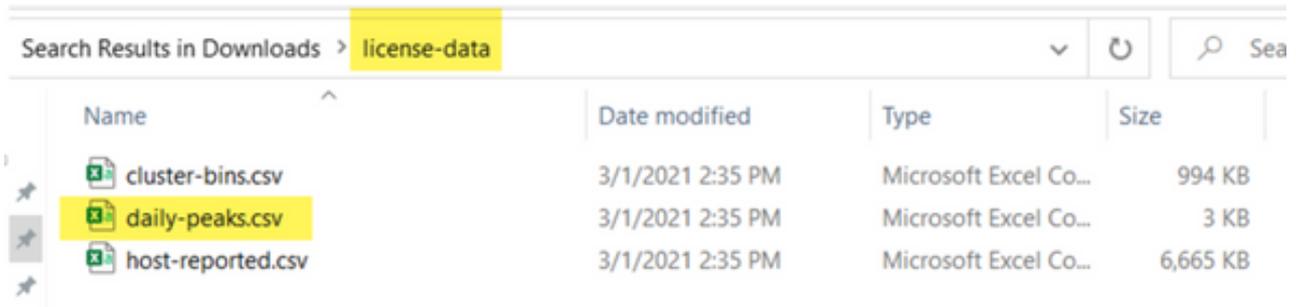
```

],
"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"
  }
}

```

, vérifiez combien de licences PMP/SMP sont attribuées dans le portail Cisco Software Smart pour les serveurs CMS.

Ouvrez le rapport de 90 jours (le fichier Zip est nommé license-data.zip) et ouvrez le fichier nommé daily-peaks.csv.



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

Dans Excel, triez la colonne PMP par Z à A pour obtenir les valeurs les plus élevées vers le haut, puis effectuez la même opération pour la colonne SMP. Les valeurs que vous voyez dans ce fichier sont-elles inférieures aux licences disponibles dans le fichier de licence CMS ? Si oui, alors vous êtes bien et entièrement en conformité. Si ce n'est pas le cas, alors cela crée des avertissements et/ou des erreurs comme indiqué sur la Figure 6 sur la section 1.7.3 du [guide de déploiement CMS](#) pour lequel vous pouvez trouver plus d'informations ainsi que sur la section 1.7.4.

Selon l'image, par exemple, 2 167 licences SMP ont été utilisées et aucune licence PMP n'a été utilisée au cours des 90 derniers jours. Le fichier cms.lic indiquait 100 unités de chaque type de licence, ce qui rend cette configuration entièrement conforme. Par conséquent, il n'y a aucun problème de licence lorsque cette configuration effectue une mise à niveau vers CMS 3.0. Cependant, il peut toujours y avoir un problème lorsque, dans la configuration, 10 000 utilisateurs via LDAP auraient été importés. Comme alors vous avez seulement 100 licences PMP, mais vous allouez 10000 (avec userProfile avec hasLicense défini sur True) donc dans ce cas vous êtes hors de conformité dès que vous mettez à niveau vers 3.0. Pour en savoir plus, consultez la section suivante.

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

Déterminer le nombre d'utilisateurs auxquels une licence PMP est attribuée une fois la mise à niveau effectuée

Tous les utilisateurs qui sont importés et qui utilisent un userProfile avec hasLicense=true se voient automatiquement attribuer une licence PMP dans CMS 3.0.

Dans l'API, vérifiez le nombre de profils utilisateur dont vous disposez et vérifiez si l'un d'entre eux a « hasLicense=true » défini. Si c'est le cas, vous devez vérifier où ces profils utilisateur sont attribués.

Les profils utilisateur peuvent être affectés à l'un des niveaux suivants :

1. SourcesLDAP
2. Locataires
3. Système/profils

Vérifiez les 3 emplacements pour les profils utilisateur attribués qui ont hasLicense=true.

1. Sources/Locataires Ldap

Pour chaque ldapSource qui utilise un service partagé ou un userProfile, les utilisateurs importés avec ce ldapSource se voient attribuer une licence PMP lorsque le paramètre hasLicense a la

valeur True. S'il y a un service partagé, vous devez cliquer sur l'ID du service partagé pour voir si un profil utilisateur lui est attribué, puis vérifier si ce profil utilisateur est configuré avec 'hasLicense=true'. S'il n'y a pas de locataire, mais qu'il y a un profil utilisateur défini, cliquez dessus pour voir s'il a 'hasLicense=true'. Si l'une ou l'autre des méthodes a 'hasLicense=true', vous pouvez vérifier combien d'utilisateurs ont été importés en effectuant une GET pour 'api/v1/users' et en filtrant pour le domaine utilisé pour le jidMapping sur le ldapmapping associé à ldapSource par exemple.

 Remarque : cette opération peut être plus complexe dans d'autres situations, auquel cas vous devez la vérifier à l'aide des mappages et des filtres Active Directory que vous avez créés.

Étape 1. Recherchez l'ID de mappage dans ldapSource.

Étape 2. Recherchez ldapMappings pour trouver jidMapping.

Étape 3. Recherchez dans api/v1/users le domaine utilisé dans le jidMapping.

Étape 4. Ajoutez les utilisateurs trouvés dans chaque source ldap. Il s'agit du nombre d'utilisateurs LDAP importés qui ont besoin de licences PMP.

/api/v1/ldapSources/9ec2c58e-38e5-4b11-af64-d6ac28e62387

Related objects: [/api/v1/ldapSources](#) **1** ldapSource

Table view XML view

Object configuration	
name	3472667-4075-4816-8fcb-fe8e10fb4fb
server	3472667-4075-4816-8fcb-fe8e10fb4fb
mapping	5fca838-e911-4717-a0cd-4879f14b2db8
tenant	8fca838-e911-4717-a0cd-4879f14b2db8
baseDn	DC=amckin,DC=local

/api/v1/ldapMappings **2** ldapMappings

= start < prev **1 - 3** (of 3) next > Create new Table view XML view

object id	jidMapping
1f62059f-5d31-486c-9fc1-a2bc162a8ff4	\$\$AMAccountName\$\$@damckin.local
5fca838-e911-4717-a0cd-4879f14b2db8	\$\$AMAccountName\$\$@simpsons.local
cf609fa7-b668-4c4e-9264-c5d9275ed6b3	\$\$AMAccountName\$\$@familyguy.local

/api/v1/users **3** users

= start < prev **1 - 4** (of 4) next > simpsons Filter Table view XML view

object id	userid
2e2ef242-1b0c-4695-8da3-10e354603689	bart@simpsons.local
b285eb07-9895-4788-9977-008c3d2f1013	homer@simpsons.local
68599e67-1936-4269-b5a2-3e821f920d07	lisa@simpsons.local
0acedee-98ef-4305-b339-98310860ba99	marge@simpsons.local

## 2. Système/Profils

Si un userProfile est défini au niveau du système/profils, et que ce userProfile a "hasLicense=true" alors tout utilisateur importé dans CMS se verra attribuer une licence PMP lors de la mise à niveau du serveur. Si vous avez importé 10 000 utilisateurs, mais que vous n'avez que 100 PMP, vous êtes en situation de non-conformité lorsque vous effectuez la mise à niveau vers CMS 3.0. Un message de 30 secondes s'affiche à l'écran et une invite audio s'affiche au début des appels.

Si le profil utilisateur au niveau du système indique que les utilisateurs doivent obtenir un PMP, accédez à api/v1/users pour voir combien d'utilisateurs il y a au total :

/api/v1/users ◀ Will show total number of imported users

start < prev 1 - 9 (of 9) next > Filter Table view XML view

object id	userJid	...
<a href="#">18a6595a-33a0-4fd0-8761-5030249e0301</a>	Lois@familyguy.local	85d7c06-1253-461f-bb1a-fe49fd7004e8
<a href="#">84a2d8be-b4d5-4a02-a003-2cf34fcb5df3</a>	brian@familyguy.local	85d7c06-1253-461f-bb1a-fe49fd7004e8
<a href="#">86e7f8a6-55fc-443e-b7ae-66e2c0191cac</a>	connor@darcmkin.local	
<a href="#">44800633-fb41-4998-bdf5-339c64fccb67</a>	darren@darcmkin.local	
<a href="#">4bc178dc-288c-49e5-a6d9-8cb192425b7f</a>	homer@simpsons.local	84ca8c38-ed94-4603-9419-51abaa6dfc2
<a href="#">a1105eb2-49f1-4ba5-8deb-c1e3d74ba084</a>	janette@darcmkin.local	
<a href="#">b6f80307-d839-4863-8e00-667e403a5a5e</a>	meg@familyguy.local	85d7c06-1253-461f-bb1a-fe49fd7004e8
<a href="#">32a615e6-ce2e-4489-a5db-d65e83b067a9</a>	peter@familyguy.local	85d7c06-1253-461f-bb1a-fe49fd7004e8
<a href="#">f1c47991-5173-4daa-bb59-2140c8ca01f6</a>	stewie@familyguy.local	85d7c06-1253-461f-bb1a-fe49fd7004e8

Si vous aviez précédemment importé tous les utilisateurs de votre ldap, mais réalisez maintenant que vous avez seulement besoin d'un certain sous-ensemble de cette liste, créez un meilleur filtre dans votre ldapSource afin qu'il importe seulement les utilisateurs auxquels vous voulez attribuer des licences PMP. Modifiez votre filtre sur ldapSource, puis effectuez une nouvelle synchronisation LDAP dans api/v1/ldapsync. Seuls les utilisateurs souhaités sont importés et tous les autres utilisateurs de cette importation précédente sont supprimés.

 Remarque : si vous effectuez cette opération correctement et que la nouvelle importation ne supprime que les utilisateurs indésirables, les identifiants d'appel et les secrets coSpace restants ne changent pas, mais si vous faites une erreur, cela peut entraîner la modification de tous les identifiants d'appel et les secrets. Effectuez une sauvegarde de vos noeuds de base de données avant d'essayer ceci si cela vous inquiète !

Disposez-vous de suffisamment de licences SMP ?

Lorsque vous avez examiné vos pics quotidiens du rapport CMM 90 Day, disposez-vous déjà de suffisamment de licences SMP pour couvrir votre pic ? Les licences SMP sont utilisées lorsque le propriétaire de la téléconférence n'a pas reçu de licence PMP (soit en tant que coSpace owner / ad-hoc meeting / TMS scheduled meeting). Si vous utilisez intentionnellement le protocole SMP et que vous avez suffisamment d'informations pour couvrir vos heures de pointe, alors tout va bien. Si vous vérifiez le pic de 90 jours pour le protocole SMP et que vous ne savez pas pourquoi ces informations sont consommées, voici quelques éléments à vérifier.

1. Les appels ad hoc (transmis depuis CUCM) utilisent une licence SMP si le périphérique utilisé pour la fusion n'est pas associé à un utilisateur auquel une licence PMP a été attribuée dans CMS via le profil utilisateur. CUCM fournit le GUID de l'utilisateur qui fait remonter la téléconférence. Si ce GUID correspond à un utilisateur LDAP importé par Meeting Server auquel une licence PMP a été attribuée, la licence de cet utilisateur est utilisée.
2. Si aucune licence PMP n'a été attribuée à un propriétaire coSpace, les appels destinés à ces coSpaces utilisent une licence SMP.
3. Si la téléconférence a été réservée dans TMS version 15.6 ou ultérieure, le propriétaire de la téléconférence est envoyé à CMS et si aucune licence PMP n'a été attribuée à cet utilisateur, cette téléconférence utilise une licence SMP.

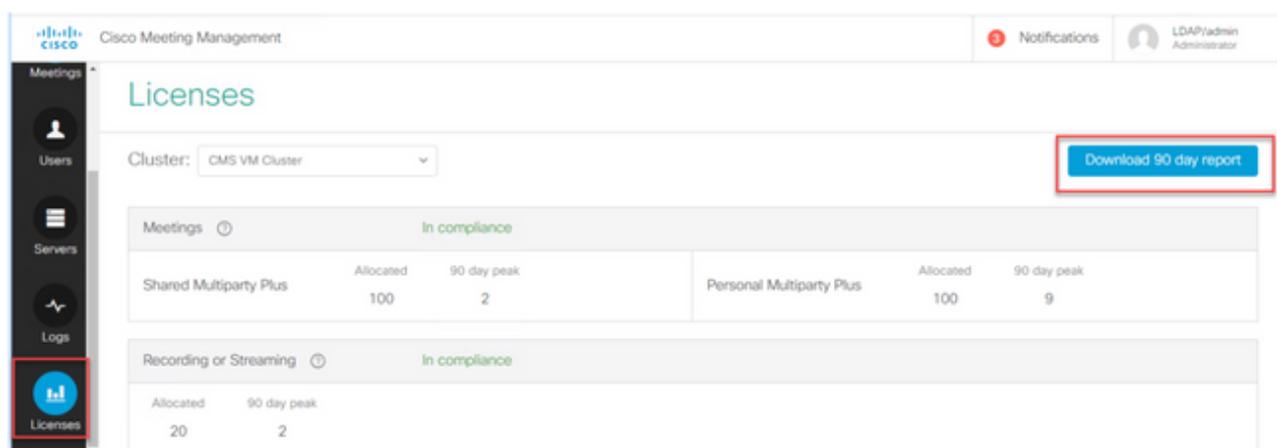
Configurer CMM

À partir de CMS 3.0, CMM 3.0 est nécessaire au bon fonctionnement de CMS. CMM est responsable de la gestion des licences de CMS. Par conséquent, si vous envisagez de mettre à niveau CMS vers la version 3.0, vous devez disposer d'un serveur CMS. Il est recommandé de déployer CMS 2.9 pendant que vous êtes sur CMS 2.9 afin de vérifier la consommation de votre licence avant de procéder à la mise à niveau.

CMM vérifie toutes les licences callBridges ajoutées pour les licences SMP et PMP et la licence callBridge. Il utilise le nombre le plus élevé parmi les différents périphériques du cluster.

Par exemple, si CMS1 dispose de 20 licences PMP et 10 licences SMP et que CMS2 dispose de 40 licences PMP et 5 licences SMP dans le cadre d'une licence traditionnelle, le CMS signale que vous avez 40 licences PMP et 10 licences SMP à utiliser.

Si vous avez plus de licences PMP que d'utilisateurs importés, vous n'avez aucun problème lié aux licences PMP (ou SMP), mais si vous vérifiez ce pic de 90 jours et que vous constatez que vous avez utilisé plus de licences disponibles, vous pouvez toujours effectuer une mise à niveau vers CMS 3.0 et utiliser la licence d'essai de 90 jours sur CMM pour trier les choses avec votre licence, ou prendre des mesures avant la mise à niveau.



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

Recording or Streaming		In compliance	
Allocated	90 day peak		
20	2		

## Configurer Webbridge (client WebRTC et CMA)

CMS 3.0 supprime le composant serveur XMPP et, avec cela, WebBridge et la possibilité d'utiliser le client CMA épais. WebBridge3 est désormais utilisé pour connecter des utilisateurs d'applications Web (anciennement appelés utilisateurs WebRTC) à des téléconférences à l'aide du navigateur. Lorsque vous effectuez une mise à niveau vers la version 3.0, vous devez configurer webbridge3.

 Remarque : le client CMA épais ne fonctionne pas après la mise à niveau vers CMS 3.0 !

Cette vidéo vous guide tout au long du processus de création des certificats de webbridge 3.

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

Avant la mise à niveau vers la version 3.0, les clients doivent planifier la configuration de Webbridge3. Les étapes les plus importantes sont soulignées ici.

1. Vous avez besoin d'une clé et d'une chaîne de certificats pour webbridge3. L'ancien certificat de pont Web peut être utilisé si le certificat contient tous les noms de domaine complets (FQDN) ou adresses IP du serveur CMS en tant que nom alternatif de sujet (SAN)/ nom commun (CN) qui exécutent webbridge3, et si l'un de ces éléments est satisfait :

a. Le certificat n'a pas d'utilisation améliorée de la clé (ce qui signifie qu'il peut être utilisé comme client ou serveur).

b. Le certificat comporte l'authentification client et l'authentification serveur. Le certificat HTTP nécessite uniquement l'authentification du serveur, alors que le certificat C2W nécessite à la fois le serveur et le client).

2. Si vous voulez créer un nouveau certificat pour le certificat "webbridge3 https", il est recommandé d'être signé publiquement (pour éviter les avertissements de certificat sur le client lors de l'utilisation de l'application web). Ce même certificat peut être utilisé pour le « certificat c2w webbridge3 », et le certificat doit avoir le nom de domaine complet des serveurs webbridge dans le SAN/CN.

3. CallBridges doit communiquer avec le nouveau pont Web3 à l'aide d'un port configuré dans la commande webbridge3 c2w listen. Il peut s'agir de n'importe quel port disponible, par exemple 449. Les utilisateurs doivent s'assurer que les ponts d'appel peuvent communiquer avec webbridge3 sur ce port et que les modifications du pare-feu sont effectuées à l'avance, si nécessaire. Il ne peut pas s'agir du même port utilisé par « webbridge https » pour écouter.

Avant la mise à niveau de CMS vers la version 3.0, il est recommandé d'effectuer une sauvegarde à l'aide de « backup snapshot <servername\_date> », puis de se connecter à la page webadmin de vos noeuds de pont d'appel pour supprimer tous les paramètres XMPP et les paramètres Webbridge. Connectez-vous ensuite au MMP sur vos serveurs, et effectuez ces étapes sur tous les serveurs Core qui ont xmpp et webbridge sur une connexion SSH :

1. xmpp disable
2. réinitialisation xmpp
3. xmpp certs none
4. xmpp domain none
5. webbridge désactiver
6. webbridge listen none
7. certs webbridge aucun
8. confiance webbridge aucune

Une fois que vous avez effectué la mise à niveau vers la version 3.0, commencez par configurer webbridge3 sur tous les serveurs qui exécutaient précédemment webbridge. Vous devez effectuer cette opération car il existe déjà des enregistrements DNS qui pointent vers ces serveurs. Ainsi, vous vous assurez que si un utilisateur est envoyé à un pont Web3, il est prêt à traiter la demande.

Configuration de Webbridge3 (sur toute la connexion SSH)

Étape 1. Configurez le port d'écoute http de webbridge3.

Webbridge3 https listen a:443

Étape 2. Configurez des certificats pour webbridge3 pour les connexions de navigateur. Il s'agit du certificat envoyé aux navigateurs et qui doit être signé par une autorité de certification publique et contenant le nom de domaine complet (FQDN) utilisé dans le navigateur pour que le navigateur puisse approuver la connexion.

Webbridge3 https certs wb3.key wb3trust.cer (Il doit s'agir d'une chaîne d'approbation : créez un certificat d'approbation avec une entité de fin au-dessus, suivi des autorités de certification intermédiaires dans l'ordre, pour terminer avec 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
```

Étape 3. Configurez le port à utiliser pour écouter les connexions callBridge vers webbridge (c2w). Puisque 443 est utilisé pour le port d'écoute https de webbridge3, cette configuration doit être un port différent, disponible comme par exemple 449.

Webbridge3 c2w listen a:449

4. Configurez les certificats que webbridge envoie à callbridge pour l'approbation c2w

Webbridge3 c2w certs wb3.key wb3trust.cer

5. Configurez le magasin de confiance que WB3 utilise pour faire confiance au certificat callBridge. Ce certificat doit être le même que celui utilisé sur le groupe CA de la passerelle d'appels (et il doit s'agir d'un groupe de certificats intermédiaires au-dessus, et d'une CA racine à la fin, suivie d'un retour chariot unique).

Webbridge3 c2w trust rootca.cer

6. Activer le pont Web3

## 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
```

### Modifications de la configuration de CallBridge (sur toute la connexion SSH)

Étape 1. Configurez la confiance callBridge avec le certificat/bundle CA qui a signé le certificat c2w webbridge3.

```
Callbridge trust c2w rootca.cer
```

Étape 2. Redémarrez callBridge pour que la nouvelle approbation prenne effet. Tous les appels sur ce callBridge particulier sont abandonnés. Utilisez-le avec prudence.

Redémarrage de Callbridge

### Configuration API pour la connexion de callBridges à webBridge3

1. Créez un nouvel objet webBridge à l'aide de POST dans l'API et attribuez-lui une valeur d'URL à l'aide du nom de domaine complet et du port configuré sur la liste blanche d'interface c2w de webbridge (étape 3 de la configuration de webbridge3)

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

À ce stade, Webbridge3 fonctionne à nouveau et vous pouvez joindre des espaces en tant qu'invités. Si vous avez déjà importé des utilisateurs, ils doivent être en mesure de se connecter.

### Autorisations de création d'espace utilisateur Web app

Vos utilisateurs sont-ils habitués à pouvoir créer leurs propres espaces dans WebRTC ? Depuis CMS 3.0, les utilisateurs d'applications web ne peuvent pas créer leurs propres coSpaces à moins qu'un modèle de coSpace leur soit attribué pour cela.

Même si un coSpaceTemplate est attribué, cela ne crée pas un espace auquel les autres utilisateurs peuvent accéder par numérotation (pas d'URI, pas d'ID d'appel ou de code secret),

mais si le coSpace a un callLegProfile avec « addParticipantAllowed », ils peuvent passer des appels à partir de l'espace.

Pour que les chaînes de numérotation puissent être utilisées pour appeler dans le nouvel espace, le coSpaceTemplate doit disposer d'une configuration accessMethodTemplate (voir les notes de version 2.9 -

[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)).

Dans l'API, créez un ou plusieurs modèles coSpaceTemplate, puis créez un ou plusieurs modèles accessMethodTemplate et attribuez le modèle coSpaceTemplate aux sources ldapUserCoSpaceTemplateSources. Vous pouvez également attribuer manuellement un modèle coSpaceTemplate à un utilisateur dans api/v1/users.

Vous pouvez créer et attribuer plusieurs CoSpaceTemplates et accessMethodsTemplates. Pour plus d'informations, consultez le guide de l'API CMS

(<https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-programming-reference-guides-list.html>)

The screenshot displays the API interface for managing CoSpaceTemplates. It is divided into three main sections:

- Top Section:** Shows the API endpoint `/api/v1/coSpaceTemplates/b03dbf12-c480-487e-b4d8-955e491ff074`. Below it, a table view shows the object configuration for the selected CoSpaceTemplate:

Object configuration	
name	First CoSpaceTemplate
callProfile	008e1aa7-0079-4d65-b6ae-fb218bd2e6b4
callLegProfile	ef583b0e-a6fe-49cf-bece-b557332a76bf
numAccessMethodTemplates	2
- Middle Section:** Shows the configuration form for the CoSpaceTemplate. Fields include:
  - name: First CoSpaceTemplate (present)
  - description: (empty)
  - callProfile: 008e1aa7-0079-4d65-b6ae-fb218bd2e6b4 (present)
  - callLegProfile: ef583b0e-a6fe-49cf-bece-b557332a76bf (present)
  - dialInSecurityProfile: (empty)A "Modify" button is located at the bottom of this form.
- Bottom Section:** Shows the configuration form for an accessMethodTemplate. Fields include:
  - name: (empty)
  - uriGenerator: (empty)
  - callLegProfile: (empty) (Choose)
  - generateUniqueCallId: <unset> (dropdown)
  - dialInSecurityProfile: (empty) (Choose)A "Create" button is located at the bottom of this form.

A red arrow points from the `accessMethodTemplates` link in the top section to the bottom section, indicating the relationship between the two.

### CoSpaceTemplate (configuration de l'API)

Nom : tout nom que vous souhaitez donner au coSpaceTemplate.

Description : Brève description si nécessaire.

callProfile : White callProfile voulez-vous que les espaces créés avec ce modèle soient utilisés ? S'il n'est pas fourni, il utilise ce qui est défini au niveau du système/profil.

calllegProfile : Quel calllegProfile voulez-vous utiliser pour les espaces créés avec ce modèle ? S'il n'est pas fourni, il utilise ce qui est défini au niveau du système/profil.

dialInSecurityProfile : quel dialInSecurityProfile voulez-vous que les espaces créés avec ce modèle utilisent ? S'il n'est pas fourni, il utilise ce qui est défini au niveau du système/profil.

### AccessMethodTemplate (configuration de l'API)

Nom : tout nom que vous souhaitez donner au coSpaceTemplate.

uriGenerator : expression à utiliser pour générer des valeurs URI pour ce modèle de méthode d'accès ; le jeu de caractères autorisé est 'a' à 'z', 'A' à 'Z', '0' à '9', '.', '-', '\_' et '\$' ; s'il n'est pas vide, il doit contenir exactement un caractère '\$'. Par exemple, \$.space utilise le nom fourni par l'utilisateur lors de la création de l'espace et y ajoute ".space". « Team Meeting » crée l'URL « Team.Meeting.space@domain ».

callLegProfile : quel calllegProfile voulez-vous que les accessMethods créés avec ce modèle utilisent ? S'il n'est pas fourni, il utilise ce qui est défini au niveau CoSpaceTemplate et s'il n'y en a pas, utilisez ce qui est au niveau système/profil.

generateUniqueCallId : indique si un ID numérique unique doit être généré pour cette méthode d'accès qui remplace l'ID global pour le coespace.

dialInSecurityProfile : quel dialInSecurityProfile voulez-vous que les méthodes d'accès créées avec ce modèle utilisent ? S'il n'est pas fourni, il utilise ce qui est défini au niveau CoSpaceTemplate et s'il n'y en a pas, utilisez ce qui est au niveau système/profil.

## Fonction de conversation

CMS 3.0 a supprimé la fonction de conversation persistante, mais dans CMS 3.2, la conversation non persistante dans les espaces a été renvoyée. La discussion est disponible pour les utilisateurs d'applications Web et n'est stockée nulle part. Une fois CMS 3.2 installé, les utilisateurs de l'application Web peuvent par défaut s'envoyer des messages pendant les téléconférences. Ces messages ne sont disponibles que pendant la téléconférence et seuls les messages échangés après l'adhésion sont visibles. Vous ne pouvez pas vous joindre en retard et revenir en arrière pour afficher les messages précédents.

## Appels point à point WebRTC

Sur CMS 2.9.x, les participants WebRTC ont pu appeler directement leurs clients vers d'autres contacts. À partir de CMS 3.0, cela n'est plus possible. Désormais, les utilisateurs doivent se connecter et rejoindre un espace. À partir de là, s'ils ont l'autorisation dans callLegProfile (le paramètre addParticipants a la valeur True), ils peuvent ajouter d'autres contacts. CMS se connecte alors par numérotation au participant et se rencontre sur un espace dans CMS.

## Modifications notables des paramètres webBridge

CMS 3.0 et 3.1 a supprimé ou déplacé certains paramètres du pont Web de l'interface utilisateur

graphique et ils doivent être configurés dans l'API pour garantir une expérience homogène aux utilisateurs. Sur 3.x, utilisez `api/v1/webBridges` et `api/v1/webBridgeProfiles`.

Vérifiez ce que vous avez actuellement configuré afin que lorsque vous effectuez la mise à niveau vers la version 3.0, vous puissiez configurer les profils `webbridge` et `webbridge` dans l'API en conséquence.

The image displays three screenshots of the CMS interface, illustrating the changes in web bridge settings across different versions:

- CMS 2.9.x:** Shows the 'Web bridge settings' section with 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). The 'External access' section includes 'Web Bridge URI' (https://14.49.25.94) and 'IVR telephone number'. A 'Submit' button is present.
- CMS 3.0:** Shows the 'Lync Edge settings' section with fields for 'Server address', 'Username', and 'Number of registrations'. The 'IVR' section includes 'IVR numeric ID' (7772) and 'Joining scheduled Lync conferences by ID' (not allowed). The 'External access' section includes 'Web Bridge URI' (https://14.49.25.94) and 'IVR telephone number'. A 'Submit' button is present.
- CMS 3.1:** Shows the 'Lync Edge settings' section with fields for 'Server address', 'Username', and 'Number of registrations'. The 'IVR' section includes 'IVR numeric ID' (7772) and 'Joining scheduled Lync conferences by ID' (not allowed). A 'Submit' button is present.

Dans la version 3.0, les paramètres du pont Web ont été supprimés sur l'interface graphique utilisateur, puis dans CMS 3.1, les champs d'accès externe ont également été supprimés.

#### Paramètres du pont Web dans l'interface utilisateur graphique

- URI du client du compte invité - il a été utilisé par `callBridge` pour trouver le `webBridge`. Si votre déploiement de `WebRTC` comportait plusieurs ponts Web, ce champ doit déjà être vide

et vous devez disposer d'URL uniques dans api/v1/webbridge pour chaque pont Web auquel CallBridge doit se connecter. Supprimez tout ce qui se trouve dans ce champ et assurez-vous que webBridges est configuré dans l'API.

- Domaine Jid du compte invité - il n'est plus utilisé dans CMS 3.0 et vous pouvez le supprimer.
- Accès invité via ID et code - supprimé et non remplacé dans CMS 3.0.
- Accès invité via les hyperliens - désormais configurable sous webBridgeProfiles dans l'API dans le paramètre « AllowSecrets ».

The image displays two screenshots of the configuration interface for web bridges in different versions of CMS. The top screenshot, labeled 'CMS 2.9.x', shows the following fields: url (URL), resourceArchive (URL), tenant (Choose), tenantGroup (Choose), idEntryMode (<unset>), allowWeblinkAccess (<unset>), showSignIn (<unset>), resolveCoSpaceCallIds (<unset>), resolveLyncConferenceIds (<unset>), callBridge (Choose), and callBridgeGroup (Choose). The bottom screenshot, labeled 'CMS 3.0', shows the following fields: url (URL), tenant (Choose), tenantGroup (Choose), callBridge (Choose), callBridgeGroup (Choose), and webBridgeProfile (Choose). Both screenshots include a 'Create' button at the bottom.

Notez que dans CMS 3.0, plusieurs champs ont été supprimés de api/v1/webBridges.

- resourceArchive - maintenant dans webbridgeProfiles.
- idEntryMode - désormais déconseillé.
- allowWeblinkAccess - maintenant dans webBridgeProfiles comme allowSecrets.
- showSignIn - maintenant dans webBridgeProfiles comme userPortalEnabled.
- solveCoSpaceCallIds- maintenant dans webbridgeProfiles.
- solveLyncConferenceIDs - maintenant dans webbridgeProfiles.

The screenshot shows a web form for configuring web bridge profiles. The title is "/api/v1/webBridgeProfiles". The form contains the following fields:

- name: text input field
- resourceArchive: text input field with "(URL)" label
- allowPasscodes: checkbox and dropdown menu (set to "<unset>")
- allowSecrets: checkbox and dropdown menu (set to "<unset>")
- userPortalEnabled: checkbox and dropdown menu (set to "<unset>")
- allowUnauthenticatedGuests: checkbox and dropdown menu (set to "<unset>")
- resolveCoSpaceCallIds: checkbox and dropdown menu (set to "<unset>")
- resolveCoSpaceUris: checkbox and dropdown menu (set to "<unset>")

A "Create" button is located at the bottom center. A red text overlay "CMS 3.0 onward" is positioned on the right side of the form.

## ProfilWebBridge

- resourceArchive - si vous utilisez des arrière-plans personnalisés et que votre archive de ressources est stockée sur un serveur Web, entrez l'URL ici.
- allowPasscodes : si la valeur est false, les utilisateurs n'ont pas la possibilité de participer aux téléconférences en tant qu'invités. Ils peuvent uniquement se connecter ou utiliser une URL contenant les informations d'espace et le secret
- allowSecrets - Si cette valeur est false, les utilisateurs ne peuvent pas joindre des espaces à l'aide d'une URL telle que [https://meet.company.com/meeting/040478?secret=gPDnucF8is4W1cS87\\_l.zw](https://meet.company.com/meeting/040478?secret=gPDnucF8is4W1cS87_l.zw). Les utilisateurs doivent utiliser <https://meet.company.com> et entrer l'ID d'appel/ID de téléconférence/URI et le PIN/code secret si l'un d'eux est configuré.
- userPortalEnabled - si la valeur est false, la page d'accueil du portail d'applications web n'affiche pas l'option de connexion. Il n'affiche les champs permettant de saisir l'ID d'appel/ID de téléconférence/URI et le PIN/code secret que si l'un d'eux est configuré.
- allowUnauthenticatedGuest - si la valeur est False, les invités ne peuvent pas se joindre à une téléconférence, même avec l'URL complète qui contient l'ID et le secret de la téléconférence. Lorsque la valeur est False, seuls les utilisateurs qui peuvent se connecter peuvent participer à une téléconférence. Exemple . L'utilisateur2 tente d'utiliser l'URL de la téléconférence de l'utilisateur1. Après avoir saisi l'URL, l'utilisateur 2 doit se connecter pour continuer la téléconférence de l'utilisateur 1.
- solveCoSpaceCallIds - si la valeur est False, les invités ne peuvent rejoindre les téléconférences qu'en saisissant l'URI et le code PIN/mot de passe s'ils sont utilisés. L'ID d'appel/ID de téléconférence/ID numérique n'est pas accepté.
- solveCoSpaceUris - 3 paramètres possibles : off, domainSuggestionDisabled et domainSuggestionEnabled. Indique si ce WebBridge accepte les URI SIP coSpace et coSpace accessMethod pour permettre aux visiteurs de participer aux réunions cospace.

- Lorsque l'option 'off' join by URI est désactivée.

- Lorsque la valeur 'domainSuggestionDisabled' est activée, la jointure par URI est activée, mais le domaine de l'URI n'est pas complété automatiquement ou vérifié sur webBridges à l'aide de ce webBridgeProfile.

- Lorsque la valeur 'domainSuggestionEnabled' est activée, la jointure par URI est activée et le domaine de l'URI peut être complété automatiquement et vérifié sur webBridges à l'aide de ce webBridgeProfile.

## Section Accès externe supprimée de l'interface utilisateur graphique Web

Dans CMS 3.1, la section Accès externe a été supprimée de l'interface utilisateur graphique Web. Si vous les aviez configurées avant la mise à niveau, vous devez les reconfigurer dans l'API sous `webbridgeProfiles`.



External access

Web Bridge URI

IVR telephone number

Tout d'abord, vous devez créer un `webbridgeProfile` comme décrit dans la section précédente. Une fois que vous avez créé un `webbridgeProfile`, vous pouvez créer un numéro IVR et/ou un URI de pont Web via les liens disponibles dans l'API sous le `webBridgeProfile` nouvellement créé.



Vous pouvez créer jusqu'à 32 numéros IVR ou 32 adresses de pont Web par profil de pont Web

## Enregistrement ou diffusion en continu

L'enregistreur et le composant streamer sur CMS 2.9.x et versions antérieures étaient des clients XMPP, et à partir de CMS 3.0, ils sont basés sur SIP. Cela permet désormais de modifier les dispositions des enregistrements et de la diffusion en continu à l'aide de la disposition par défaut dans l'API. En outre, les étiquettes de nom sont désormais affichées dans la session d'enregistrement/de diffusion en continu. Consultez les notes de version de CMS 3.0 pour plus d'informations sur les fonctionnalités d'enregistrement/de diffusion en continu -

[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).

Si vous avez configuré l'enregistreur ou le streamer dans 2.9.x, vous devez reconfigurer les paramètres dans MMP et API afin que ceux-ci continuent à fonctionner après la mise à niveau.

Avant la mise à niveau de CMS vers la version 3.0, il est recommandé d'effectuer une sauvegarde à l'aide de « `backup snapshot <servername_date>` », puis de se connecter à la page `webadmin` de vos nœuds `callbridge` pour supprimer tous les paramètres XMPP. Connectez-vous ensuite au MMP sur vos serveurs et effectuez les étapes suivantes sur tous les serveurs Core disposant de `xmpp` sur une connexion SSH :

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

Enregistreur

## MMP

Les figures montrent un exemple des configurations vues sur CMS 2.9.1 lorsque l'enregistreur a été configuré, et comment il se présente immédiatement après la mise à niveau vers la version 3.0.

```
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>
```

Après la mise à niveau, vous devez reconfigurer l'enregistreur :

Étape 1. Configurez l'interface d'écoute SIP.

enregistreur sip listen a 5060 5061 (interface et ports que l'enregistreur SIP est configuré pour écouter pour TCP et TLS, respectivement. Si vous ne voulez pas utiliser TLS, vous pouvez utiliser 'enregistreur sip listen a 5060 none')

Étape 2. Configurez les certificats utilisés par l'enregistreur si vous utilisez une connexion TLS.

recorder sip certs <key-file> <crt-file> [crt-bundle] (sans ces certificats, le service tls ne démarre pas sur l'enregistreur. L'enregistreur utilise l'ensemble crt pour vérifier le certificat callBridge.)

Étape 3. Configurez la limite d'appels.

recorder limit <0-500|none> (Définit la limite du nombre d'enregistrements simultanés que le

serveur peut servir. Ce tableau figure dans notre documentation et la limite d'enregistrement doit être alignée sur les ressources du serveur.)

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

Sur `api/v1/callProfiles`, vous devez configurer `sipRecorderUri`. Il s'agit de l'URI que `callBridge` compose lorsqu'il doit démarrer un enregistrement. Le domaine de cet URI doit être ajouté à votre table de règles sortantes et pointer vers l'enregistreur (ou le contrôle d'appel) en tant que proxy SIP à utiliser.

Object configuration	
<code>recordingMode</code>	<code>automatic</code>
<code>sipRecorderUri</code>	<code>recorder@recorder.com</code>

Cette figure illustre une numérotation directe vers le composant Enregistreur sur les règles sortantes trouvées dans Configuration > Appels sortants.

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

Cette figure illustre un appel au composant d'enregistrement via un contrôle d'appel (comme par exemple Cisco Unified Communications Manager (CUCM) ou Expressway).

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		<use local contact domain>	Standard SIP	Stop	0	Auto
<input type="checkbox"/> streamer.com	14.49.17.252	Expressway	<use local contact domain>	Standard SIP	Stop	0	Auto

---

 Remarque : si vous avez configuré l'enregistreur pour utiliser le protocole SIP TLS et si les appels échouent, vérifiez votre noeud callBridge dans MMP pour voir si la vérification du protocole SIP TLS est activée. La commande MMP est 'tls sip'. Les appels peuvent échouer car le certificat de l'enregistreur n'est pas approuvé par callBridge. Vous pouvez le tester en le désactivant sur callBridge à l'aide de 'tls sip verify disable'.

---

### Plusieurs enregistreurs ?

Configurez chacune d'elles comme expliqué et ajustez vos règles sortantes en conséquence. Si vous utilisez une méthode d'enregistrement direct, changez la règle sortante existante en comportement « Continuer » et ajoutez une nouvelle règle sortante sous la précédente avec une priorité inférieure de un à la première. Lorsque le premier enregistreur a atteint sa limite d'appels, il renvoie un message 488 Unacceptable ici à callBridge et callBridge passe à la règle suivante.

Si vous souhaitez équilibrer la charge de vos enregistreurs, utilisez un contrôle d'appel et ajustez le routage de votre contrôle d'appel afin qu'il puisse passer des appels vers plusieurs enregistreurs.

Diffuseur

### MMP

Après la mise à niveau de 2.9.x vers 3.0, vous devez reconfigurer streamer.

Étape 1. Configurez l'interface d'écoute SIP.

streamer sip listen a 6000 6001 (interface et ports que le streamer SIP est configuré pour écouter pour TCP et TLS, respectivement. Si vous ne voulez pas utiliser TLS, vous pouvez utiliser 'streamer sip listen a 6000 none')

Étape 2. Configurez les certificats que le streamer utilise si vous utilisez une connexion TLS.

streamer sip certs <key-file> <crt-file> [crt-bundle] (Sans ces certificats, le service tls ne démarre pas sur le streamer. Le streamer utilise le paquet crt pour vérifier le certificat callBridge.)

Étape 3. Configurer la limite d'appels

streamer limit <0-500|none> (Définit la limite du nombre de flux simultanés que le serveur peut servir. Ce tableau figure dans notre documentation et la limite du streamer doit correspondre aux ressources sur le serveur.)

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

Sur `api/v1/callProfiles`, vous devez configurer `sipStreamUri`. Il s'agit de l'URI que le pont d'appel compose lorsqu'il doit commencer la diffusion en continu. Le domaine de cet URI doit être ajouté à votre table de règles sortantes et pointer vers le streamer (ou le contrôle d'appel) en tant que proxy SIP à utiliser.

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

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

Table view XML view

Object configuration	
<code>streamingMode</code>	<code>automatic</code>
<code>sipStreamUri</code>	<code>stream@streamer.com</code>

Cette figure illustre une numérotation directe vers le composant streamer sur les règles sortantes trouvées dans Configuration > Appels sortants.

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
					Standard SIP	Stop	0	Auto

Cette figure illustre un appel au composant d'enregistrement via un contrôle d'appel (comme par exemple Cisco Unified Communications Manager (CUCM) ou Expressway).

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
					Standard SIP	Stop	0	Auto

*Annotations: A green arrow points from the 'SIP proxy to use' column to the 'Local contact domain' column. A red arrow points from the 'SIP proxy to use' column to the 'SIP proxy to use' column. A blue 'CUCM' stamp is over the 'Local contact domain' column. A red 'Expressway' stamp is over the 'SIP proxy to use' column.*

 Remarque : si vous avez configuré le streamer pour utiliser SIP TLS et si les appels échouent, vérifiez votre noeud callBridge dans MMP pour voir si la vérification SIP TLS est activée. La commande MMP est 'tls sip'. Les appels peuvent échouer car le certificat du streamer n'est pas approuvé par callBridge. Vous pouvez le tester en le désactivant sur callBridge à l'aide de 'tls sip verify disable'.

### Diffuseurs multiples ?

Configurez chacune d'elles comme expliqué et ajustez vos règles sortantes en conséquence. Si vous utilisez une méthode de diffusion directe en continu, changez la règle sortante vers enregistreur existante en comportement « Continuer » et ajoutez une nouvelle règle sortante sous la précédente avec une priorité inférieure de un à la première. Lorsque le premier streamer a atteint sa limite d'appels, il renvoie un message 488 Unacceptable ici à callBridge, et callBridge passe à la règle suivante.

Si vous souhaitez équilibrer la charge de vos streamers, utilisez un contrôle d'appel et ajustez le routage de votre contrôle d'appel afin qu'il puisse passer des appels vers plusieurs streamers.

### Contrepartie Expressway

Si vous utilisez Cisco Expressway pour Web Proxy, vous devez vous assurer que votre Expressway exécute au moins X12.6 avant la mise à niveau de CMS. Ceci est requis par CMS 3.0 pour que le proxy web fonctionne et soit pris en charge.

La capacité des participants aux applications Web a augmenté par rapport à Expressways lorsqu'il est utilisé avec CMS 3.0. Pour un grand Expressway OVA, la capacité attendue est de 150 appels Full HD (1080p30) ou 200 appels de type Autre (par exemple 720p30). Vous pouvez augmenter cette capacité en mettant en grappe Expressway, jusqu'à 6 noeuds (4 étant utilisés pour l'évolutivité et 2 pour la redondance, jusqu'à un maximum de 600 appels Full HD ou 800 appels de type Autre).

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

### Périphérie CMS

CMS Edge est réintroduit dans CMS 3.1 car il offre des capacités supérieures à l'Expressway pour les sessions d'applications Web externes. Deux configurations sont recommandées.

#### Spécifications de périphérie réduite

4 Go de RAM, 4 processeurs virtuels, 1 Gbit/s d'interface réseau

Cette spécification VM Edge est suffisamment puissante pour couvrir une seule capacité de charge audio et vidéo du CMS1000, soit 48 x 1080p, 96 x 720p, 192 x 480p et 1000 appels audio.

Pour le déploiement, il est recommandé d'avoir 1 petit serveur de périphérie par CMS1000 ou 4 petits serveurs de périphérie par CMS2000.

#### Spécifications de périphérie large

8 Go de RAM, 16 processeurs virtuels, interface réseau 10 Gbit/s

Cette spécification VM Edge est suffisamment puissante pour couvrir une seule capacité audio et vidéo du CMS2000, soit 350 x 1080p, 700 x 720p, 1000 x 480p et 3000 x appels audio.

Pour le déploiement, il est recommandé d'avoir 1 grand serveur de périphérie par CMS2000 ou 4 CMS1000.

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

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.