

# Leitfaden für ein reibungsloses Upgrade von Cisco Meeting Server 2.9 auf 3.0 (und höher)

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Wichtige Informationen zu Upgrades](#)

[Zusammenfassung der zu berücksichtigenden Aspekte](#)

[Lizenzen](#)

[Webbridge \(WebRTC und CMA-Client\)](#)

[Änderungen an der Web-Benutzeroberfläche](#)

[Rekorder/Streamer](#)

[Überlegungen zu Cisco Expressway](#)

[CMS-Edge](#)

[CMS X-Serie \(Acano\)](#)

[SIP-Edge](#)

[Weitere Informationen](#)

[Lizenzierung - Lizenzen vor dem Upgrade überprüfen](#)

[Bestimmen Sie, wie vielen Benutzern nach dem Upgrade eine PMP-Lizenz zugewiesen wird.](#)

[Verfügen Sie über ausreichend SMP-Lizenzen?](#)

[CMM konfigurieren](#)

[Konfigurieren von Webbridge \(WebRTC und CMA-Client\)](#)

[Berechtigungen zur Erstellung von Speicherplatz für Web-Anwendungen](#)

[Chat-Funktion](#)

[WebRTC Point-to-Point-Anrufe](#)

[Bemerkenswerte Änderungen der WebBridge-Einstellungen](#)

[Abschnitt für externen Zugriff von Web-GUI entfernt](#)

[Aufzeichnung oder Streaming](#)

[Rekorder](#)

[Streamer](#)

[Überlegungen zum Expressway](#)

[CMS-Edge](#)

## Einleitung

In diesem Dokument werden die Herausforderungen bei der Aktualisierung einer Cisco Meeting Server-Bereitstellung mit Version 2.9 (oder früher) auf 3.0 (oder höher) beschrieben. Außerdem wird erläutert, wie diese Herausforderungen im Hinblick auf einen reibungslosen Upgrade-Prozess bewältigt werden können.

**Funktionen entfernt:** XMPP wurde entfernt (betrifft WebRTC), Trunks/Load Balancer, Webbridge

**Neue Funktionen:** Rekorder und Streamer sind jetzt SIP, und webbridge wird durch webbridge3 ersetzt

In diesem Dokument werden nur Themen behandelt, die Sie vor dem Upgrade berücksichtigen müssen. Sie deckt nicht alle neuen Funktionen ab, die in 3.x verfügbar sind.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- CMS Administration
- CMS-Upgrades
- Erstellung und Signierung von Zertifikaten

Alles, was hier erwähnt wird, ist in verschiedenen Dokumenten beschrieben. Es ist immer ratsam, die Produktveröffentlichungshinweise zu lesen und sich in unseren Programmierhandbüchern und Bereitstellungsleitfäden zu informieren, wenn Sie weitere Informationen zu den Funktionen benötigen: [CMS Installations- und Konfigurationsleitfäden](#) und [CMS Produktveröffentlichungshinweise](#) .

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Meeting Server.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

## Hintergrundinformationen

Dieses Dokument dient als Leitfaden für den Fall, dass Sie bereits über eine CMS 2.9.x-Bereitstellung (oder eine frühere Version) verfügen, unabhängig davon, ob es sich um eine kombinierte oder ausfallsichere Bereitstellung handelt und Sie ein Upgrade auf CMS 3.0 planen. Die Informationen in diesem Dokument beziehen sich auf alle CMS-Modelle.

**Anmerkung:** X-series kann nicht auf CMS 3.0 aufgerüstet werden. Sie müssen Ihren X-series Server so schnell wie möglich austauschen.

## Wichtige Informationen zu Upgrades

Das Upgrade von CMS kann nur schrittweise erfolgen. Zum Zeitpunkt der Erstellung dieses Dokuments wurde CMS 3.5 veröffentlicht. Wenn Sie auf CMS 2.9 sind, müssen Sie ein schrittweises Upgrade durchführen (2.9 → 3.0 → 3.1 → 3.2 → 3.3 → 3.4 → 3.5 (Der

Aktualisierungsprozess für Notizen hat Änderungen gegenüber CMS 3.5, lesen Sie daher die Versionshinweise sorgfältig!!)

Wenn Sie kein schrittweises Upgrade durchführen und ungewöhnliches Verhalten feststellen, kann das TAC ein Downgrade und einen Neustart von Ihnen verlangen.

Ab CMS 3.4 MUSS CMS außerdem Smart Licensing verwenden. Sie können kein Upgrade auf CMS 3.4 oder höher durchführen und weiterhin herkömmliche Lizenzen verwenden. Führen Sie erst dann ein Upgrade auf CMS 3.4 oder höher durch, wenn Sie Smart Licensing eingerichtet haben.

## Zusammenfassung der zu berücksichtigenden Aspekte

Navigieren Sie mithilfe dieser Fragen zu den Abschnitten, die Ihre eigene Situation betreffen. Jede Überlegung bezieht sich auf einen Hyperlink zu einer detaillierteren Beschreibung in diesem Dokument.

### Lizenzen

#### **Verfügen Sie vor dem Upgrade über ausreichend Personal MultiParty (PMP)-/Shared MultiParty (SMP)-Lizenzen auf Ihren Servern?**

In Version 3.0 werden die PMP-Lizenzen zugewiesen, auch wenn der Benutzer nicht angemeldet ist. Wenn Sie beispielsweise 10000 Benutzer über LDAP importiert haben, aber nur über 100 PMP-Lizenzen verfügen, wird die Compliance dadurch beeinträchtigt, sobald Sie ein Upgrade auf 3.0 durchführen. Überprüfen Sie in diesem Anwendungsfall auf jeden Fall, ob Tenants mit userProfile und/oder System/Profilen festlegt, ob userProfile mit hasLicense mit dem Wert true festgelegt ist.

In [diesem Abschnitt](#) wird detaillierter beschrieben, wie Sie das Benutzerprofil auf der API überprüfen und feststellen, ob hasLicense=true set (d. h. lizenzierte PMP-Benutzer) vorhanden ist.

#### **Verfügen Sie über PMP/SMP-Lizenzen in Ihrer aktuellen Datei "cms.lic"?**

Aufgrund eines geänderten Lizenzverhaltens ab Version 3.0 müssen Sie vor dem Upgrade überprüfen, ob Sie über genügend PMP/SMP-Lizenzen verfügen. Dies wird in [diesem Abschnitt](#) ausführlicher beschrieben.

#### **Ist Cisco Meeting Manager (CMM) bei Ihnen im Einsatz?**

CMS 3.0 erfordert CMM 3.0 aufgrund von Änderungen im Umgang mit Lizenzen. Es wird empfohlen, CMM 2.9 bereitzustellen, bevor Sie ein Upgrade Ihrer Umgebung auf 3.0 durchführen, da Sie Ihren 90-Tage-Bericht zur Lizenznutzung für die letzten 90 Tage überprüfen können. Dies wird in [diesem Abschnitt](#) ausführlicher beschrieben.

#### **Verfügen Sie über Smart Licensing?**

CMS 3.0 erfordert CMM 3.0 aufgrund von Änderungen im Umgang mit Lizenzen. Wenn Sie Smart Licensing bereits über CMM verwenden, stellen Sie sicher, dass Ihrem Cluster PMP- und SMP-Lizenzen zugeordnet sind.

## Webbridge (WebRTC und CMA-Client)

### Verwenden Sie WebRTC in CMS 2.9?

Webbridge hat sich in CMS 3.0 deutlich verändert. Für Hinweise zur Migration von webbridge2 zu webbridge3 und zur Verwendung der Web-App finden Sie die Informationen in [diesem Abschnitt](#).

### Verwenden Ihre Benutzer den CMA-Thick-Client?

Da diese Clients auf XMPP basieren, können diese Clients nach dem Upgrade nicht mehr verwendet werden, da der XMPP-Server entfernt wurde. Wenn dies auf Ihren Anwendungsfall zutrifft, finden Sie weitere Informationen in [diesem Abschnitt](#).

### Verwenden Sie Chat in WebRTC?

Die Chat-Funktion wurde in 3.0 aus der Web-App entfernt. In CMS 3.2 wird der Chat wieder eingeführt, aber er ist nicht persistent. Weitere Informationen zu dieser Funktion finden Sie in [diesem Abschnitt](#).

### Führen Ihre Benutzer Point-to-Point-Anrufe von WebRTC an Geräte durch?

In CMS 3.0 kann ein Web-App-Benutzer nicht mehr direkt ein anderes Gerät anwählen. Jetzt müssen Sie einem Meeting-Bereich beitreten und die Berechtigung haben, dem Meeting Teilnehmer hinzuzufügen, die die gleiche Aktion ausführen. Weitere Informationen zu diesem Teil finden Sie in [diesem Abschnitt](#).

### Erstellen Ihre Benutzer ihre eigenen CoSpaces über WebRTC?

In Version 3.0 muss eine coSpaceTemplate in API erstellt und dem Benutzer zugewiesen werden, damit Web-App-Benutzer ihre eigenen Bereiche vom Client erstellen können. Dies kann manuell oder automatisch während des LDAP-Imports erfolgen. CanCreateCoSpaces wird aus UserProfile entfernt. Weitere Informationen zu dieser Funktion finden Sie in [diesem Abschnitt](#).

## Änderungen an der Web-Benutzeroberfläche

### Sind die WebBridge-Einstellungen in der Web-Admin-GUI konfiguriert?

Die WebBridge-Einstellungen werden in 3.0 aus der GUI entfernt. Sie müssen daher die WebBridges in der API konfigurieren und sich die aktuellen Einstellungen in der GUI notieren, damit Sie die WebBridgeProfiles in der API entsprechend konfigurieren können. Weitere Informationen zu dieser Änderung finden Sie in [diesem Abschnitt](#).

### Haben Sie in der grafischen Benutzeroberfläche für den Webadministrator externe Einstellungen konfiguriert?

Die externen Einstellungen wurden in CMS 3.1 aus der GUI entfernt. Wenn Sie Webbridge URL oder IVR in Ihrem CMS 3.0 oder einer älteren Web-Admin-GUI (Konfiguration → Allgemein → Externe Einstellungen) konfiguriert haben, wurden diese von der Webseite entfernt und müssen nun in der API konfiguriert werden. Die vorherigen Einstellungen vor dem Upgrade auf 3.1 werden NICHT zur API hinzugefügt und müssen manuell vorgenommen werden. Weitere Informationen zu dieser Änderung finden Sie in [diesem Abschnitt](#).

## Rekorder/Streamer

### Verwenden Sie derzeit CMS-Rekorder und/oder Streamer?

Die CMS Recorder- und Streamer-Komponente ist jetzt SIP- statt XMPP-basiert. Wenn XMPP entfernt wird, müssen diese daher nach dem Upgrade angepasst werden. Weitere Informationen zu dieser Änderung finden Sie in [diesem Abschnitt](#).

## Überlegungen zu Cisco Expressway

### Welche ist Ihre aktuelle Cisco Expressway-Version, wenn Sie Expressway als Proxy für WebRTC verwenden?

CMS 3.0 erfordert Expressway 12.6 oder neuer. Weitere Informationen zu dieser WebRTC-Proxy-Funktion finden Sie in [diesem Abschnitt](#).

## CMS-Edge

### Verfügen Sie derzeit über einen CMS Edge in Ihrer Umgebung?

CMS Edge wird in CMS 3.1 wieder eingeführt und bietet eine höhere Skalierbarkeit für externe Verbindungen. Weitere Informationen zu diesem Teil finden Sie in [diesem Abschnitt](#).

## CMS X-Serie (Acano)

### Verfügen Sie derzeit über Server der x-Serie in Ihrer Umgebung?

Diese Server können nicht auf CMS 3.0 aufgerüstet werden, und Sie müssen diese bald ersetzen (vor dem Upgrade auf 3.0 auf eine virtuelle Maschine oder eine CMS-Appliance umstellen). Den End-of-Life-Hinweis zu diesen Servern finden Sie unter [diesem Link](#).

## SIP-Edge

### Verwenden Sie derzeit SIP Edge in Ihrer Umgebung?

Sip Edge ist seit CMS 3.0 vollständig veraltet. Sie benötigen Cisco Expressway, um SIP-Anrufe in Ihr CMS zu integrieren. Wenden Sie sich an Ihren Cisco Kundenbetreuer, um mehr über Expressways für Ihre Organisation zu erfahren.

## Weitere Informationen

### Lizenzierung - Lizenzen vor dem Upgrade überprüfen

Der Status einer nicht konformen Lizenz ist das schwerwiegendste Problem, wenn Sie von einer Version 2.x auf Version 3.0 oder höher aktualisieren. In diesem Abschnitt wird beschrieben, wie Sie die Anzahl der PMP/SMP-Lizenzen bestimmen, die Sie für ein reibungsloses Upgrade benötigen.

Bevor Sie Ihre Bereitstellung auf 3.0 aktualisieren, stellen Sie CMM 2.9 bereit, und überprüfen Sie

den **90-Tage-Bericht** unter der Registerkarte "**Lizenzen**", um festzustellen, ob die Lizenznutzung unter dem aktuell zugewiesenen Lizenzbetrag auf den CMS-Knoten geblieben ist:

The screenshot shows the Cisco Meeting Management interface for the 'Licenses' section. The cluster is 'CMS VM Cluster'. A 'Download 90 day report' button is highlighted with a red box. The 'Meetings' section is 'In compliance' and shows the following data:

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

The 'Recording or Streaming' section is also 'In compliance' and shows the following data:

Category	Allocated	90 day peak
Recording or Streaming	20	2

Wenn Sie die herkömmliche Lizenzierung verwenden (die Datei cms.lic wird lokal auf Ihren CMS-Knoten installiert), überprüfen Sie in der CMS-Lizenzdatei die Anzahl der persönlichen und gemeinsam genutzten Lizenzen (100/100 wie hier abgebildet) auf jedem der CMS-Knoten (über WinSCP von jedem callBridge-Knoten herunterladen).

```

},
"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"
  }
}

```

Wenn Sie bereits Smart Licensing verwenden, überprüfen Sie, wie viele PMP/SMP-Lizenzen den CMS-Servern im Cisco Software Smart Portal zugewiesen sind.

Öffnen Sie den 90-Tage-Bericht (Zip-Datei heißt *license-data.zip*) und die Datei *daily-peaks.csv*.

Search Results in Downloads > license-data

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

Sortieren Sie in Excel die PMP-Spalte nach Z bis A, um die höheren Werte nach oben zu erhalten, und führen Sie dann die gleichen Werte für die SMP-Spalte aus. Sind die in dieser Datei



angezeigten Werte niedriger als die in der CMS-Lizenzdatei verfügbaren Lizenzen? Wenn ja, dann sind Sie in Ordnung und vollständig in Übereinstimmung. Wenn dies nicht der Fall ist, werden Warnungen und/oder Fehler generiert, wie in Abbildung 6 in Abschnitt 1.7.3 des [CMS-Bereitstellungsleitfadens](#) angegeben, zu denen Sie weitere Informationen finden können, wie auch in Abschnitt 1.7.4 beschrieben.

Wie im Beispiel-Image gezeigt, wurden in den letzten 90 Tagen 2,1667 SMP-Lizenzen verwendet, während PMP-Lizenzen nicht zu Spitzenzeiten vergeben wurden. In der Datei "cms.lic" wurden 100 Einheiten jedes Lizenztyps angegeben, sodass diese Konfiguration vollständig konform ist. Daher gibt es keine Probleme mit der Lizenzierung, wenn dieses Setup auf CMS 3.0 aktualisiert wird. Es kann jedoch weiterhin ein Problem geben, wenn auf dem Setup 10.000 Benutzer über LDAP importiert worden wären. Wie damals haben Sie nur 100 PMP-Lizenzen, aber Sie weisen 10000 zu (mit userProfile mit hasLicense auf True gesetzt), sodass Sie in diesem Fall nicht konform sind, sobald Sie auf 3.0 aktualisieren. Weitere Informationen hierzu finden Sie im nächsten Abschnitt.

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

**Bestimmen Sie, wie vielen Benutzern nach dem Upgrade eine PMP-Lizenz zugewiesen wird.**

Allen Benutzern, die importiert werden und ein **userProfile** mit **hasLicense=true** verwenden, wird in CMS 3.0 automatisch eine PMP-Lizenz zugewiesen.

Überprüfen Sie in der API, wie viele Benutzerprofile vorhanden sind, und prüfen Sie, ob einer dieser Profile "hasLicense=true" festgelegt hat. Wenn dies der Fall ist, müssen Sie überprüfen, wo diese userProfile zugewiesen sind.

Die Benutzerprofile können auf einer der folgenden Ebenen zugewiesen werden:

1. LDAP-Quellen
2. Tenants
3. System/Profile



Überprüfen Sie alle 3 Speicherorte auf zugewiesene Benutzerprofile, die über License=true verfügen.

## 1. LDAP-Quellen/Tenants

Für jede LDAP-Quelle, die einen Tenant oder ein userProfile verwendet, wird Benutzern, die mit dieser LDAP-Quelle importiert werden, eine PMP-Lizenz zugewiesen, wenn der Parameter hasLicense auf True festgelegt ist. Wenn ein Tenant vorhanden ist, müssen Sie auf die Tenant-ID klicken, um festzustellen, ob ihm ein userProfile zugewiesen ist, und dann überprüfen, ob dieses userProfile mit 'hasLicense=true' konfiguriert ist. Wenn es keinen Tenant gibt, aber ein userProfile-Satz vorhanden ist, klicken Sie darauf, um zu sehen, ob es 'hasLicense=true' enthält. Wenn eine der beiden Methoden 'hasLicense=true' hat, können Sie überprüfen, wie viele Benutzer importiert wurden, indem Sie eine GET-Funktion für 'api/v1/users' und eine Filterung für die Domäne ausführen, die für die jidMapping-Funktion auf der ldapmapping verwendet wird, die der ldapSource zugeordnet ist.

**Anmerkung:** Dies kann in anderen Situationen komplexer sein, in denen Sie dies mit den von Ihnen erstellten Active Directory-Zuordnungen und -Filtern überprüfen müssen.

Schritt 1: Suchen Sie die Zuordnungs-ID aus der ldapSource.

Schritt 2. Suchen Sie ldapMappings, um jidMapping zu finden.

Schritt 3. Suche in api/v1/users nach der Domain, die in der jidMapping verwendet wird.

Schritt 4: Addieren Sie die Benutzer aus jeder LDAP-Quelle. So viele LDAP-importierte Benutzer benötigen PMP-Lizenzen.

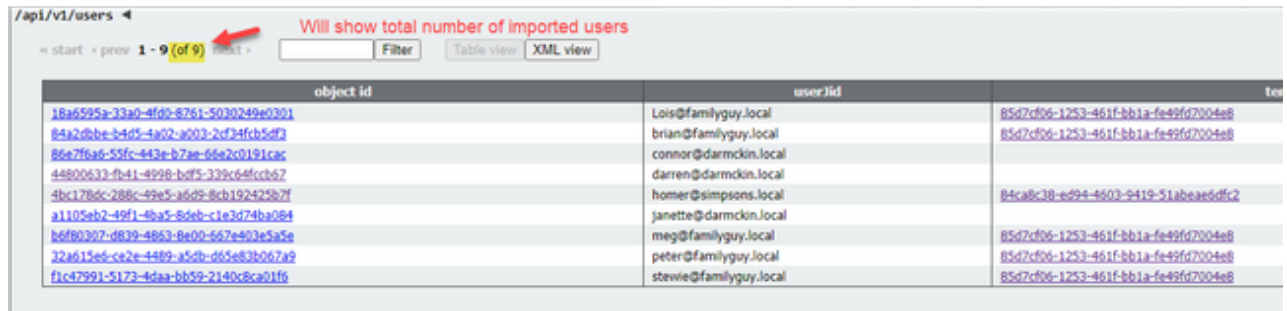
The screenshot shows a web interface with three main sections:

- LDAP Source Configuration:** A table with columns 'name', 'server', 'mapping', 'tenant', and 'baseDn'. The 'mapping' field contains the ID '5fc6f57a-1e31-4717-abcd-4875f14b2db8'. A red '1' is placed over the 'ldapSource' link in the 'Related objects' section.
- LDAP Mappings:** A table with columns 'object id' and 'jidMapping'. The 'jidMapping' field contains '\$SAMAccountNames@simpsons.local'. A red '2' is placed over the 'ldapMappings' link.
- Users:** A table with columns 'object id' and 'userJid'. The 'userJid' field contains 'simpsons'. A red '3' is placed over the 'users' link.

## 2. System/Profile

Wenn ein userProfile auf System-/Profilebene festgelegt ist und userProfile den Wert "hasLicense=true" aufweist, wird jedem in CMS importierten Benutzer beim Upgrade des Servers eine PMP-Lizenz zugewiesen. Wenn Sie 10.000 Benutzer importiert haben, aber nur 100 PMPs haben, führt dies dazu, dass Sie bei einem Upgrade auf CMS 3.0 die Compliance nicht mehr erfüllen und eine 30-Sekunden-Bildschirmmeldung und Audio-Eingabeaufforderung zu Beginn der Anrufe angezeigt werden.

Wenn das Benutzerprofil auf Systemebene angibt, dass Benutzer einen PMP erhalten sollen, rufen Sie `api/v1/users` auf, um die Gesamtzahl der Benutzer anzuzeigen:



Will show total number of imported users

object id	userJid	user
18a6595a-33a0-4fd0-8761-5030249e0301	Lois@familyguy.local	85d7c06-1253-461f-bb1a-fe49fd7004e8
85a2d8be-34d5-4a02-a003-2cf2f8cb50f2	brian@familyguy.local	85d7c06-1253-461f-bb1a-fe49fd7004e8
86e2f6a6-55fc-443e-b7ae-66e20191cac	connor@damckin.local	
44800633-fb41-4998-bdf5-339c64fcc657	darren@damckin.local	
4bc178dc-288c-49e5-ad09-8cb192425b7f	homer@simpsons.local	84ca8c38-ed94-4603-9419-51abea6dffc2
a1105eb2-49f1-4ba5-8deb-c1e3d74ba084	janette@damckin.local	
b6f80307-d839-4863-8e00-667e403e5a5e	meg@familyguy.local	85d7c06-1253-461f-bb1a-fe49fd7004e8
32a615e6-ce2e-4489-a5db-d65e83b067a9	peter@familyguy.local	85d7c06-1253-461f-bb1a-fe49fd7004e8
ffc47991-5173-4daa-bb59-2140c8ca01f5	stewie@familyguy.local	85d7c06-1253-461f-bb1a-fe49fd7004e8

Wenn Sie zuvor alle Benutzer aus Ihrem LDAP importiert haben, aber jetzt feststellen, dass Sie nur eine bestimmte Teilmenge aus dieser Liste benötigen, erstellen Sie einen besseren Filter in Ihrem LDAP-Quellcode, sodass nur die Benutzer importiert werden, denen Sie PMP-Lizenzen zuweisen möchten. Überprüfen Sie Ihren Filter auf `ldapSource` und führen Sie dann eine neue LDAP-Synchronisierung in `api/v1/ldapsync` durch. Dies führt dazu, dass nur die gewünschten Benutzer importiert und alle anderen aus diesem vorherigen Import entfernt werden.

**Anmerkung:** Wenn Sie dies richtig machen und der neue Import nur unerwünschte Benutzer entfernt, verbleibende Benutzer `coSpace CallIDs` und Geheimnisse nicht ändern, aber wenn Sie einen Fehler machen, kann dies dazu führen, dass alle `CallIDs` und Geheimnisse ändern. Erstellen Sie eine Sicherung Ihrer Datenbanknoten, bevor Sie dies versuchen, wenn Sie sich darum sorgen!

## Verfügen Sie über ausreichend SMP-Lizenzen?

Wenn Sie Ihre täglichen Spitzenwerte aus dem CMM 90 Day Report betrachtet haben, haben Sie bereits genug SMP-Lizenzen, um Ihre Spitzenwerte abzudecken? SMP-Lizenzen werden verwendet, wenn dem Meeting-Veranstalter keine PMP-Lizenz zugewiesen wurde (entweder als CoSpace-Veranstalter/Ad-hoc-Meeting/TMS-geplantes Meeting). Wenn Sie absichtlich SMP verwenden und genug haben, um Ihre Spitzenzeiten abzudecken, dann ist das alles in Ordnung. Wenn Sie den 90-Tage-Peak für SMP überprüfen und nicht klar ist, warum diese verbraucht werden, sind hier einige Dinge zu überprüfen.

1. Ad-hoc-Anrufe (von CUCM eskaliert) verwenden eine SMP-Lizenz, wenn das zum Zusammenführen verwendete Gerät nicht einem Benutzer zugeordnet ist, dem in CMS über das Benutzerprofil eine PMP-Lizenz zugewiesen wurde. CUCM stellt die GUID des Benutzers bereit, der das Meeting eskaliert. Wenn diese GUID einem von Meeting Server importierten LDAP-Benutzer mit zugewiesener PMP-Lizenz entspricht, wird die Lizenz dieses Benutzers verwendet.
2. Wenn einem CoSpace-Besitzer keine PMP-Lizenz zugewiesen wurde, verwenden Anrufe an diese CoSpaces eine SMP-Lizenz.
3. Wenn das Meeting in TMS-Version 15.6 oder höher geplant wurde, wird der Meeting-Veranstalter an das CMS gesendet. Wenn diesem Benutzer keine PMP-Lizenz zugewiesen wurde, verwendet dieses Meeting eine SMP-Lizenz.

## CMM konfigurieren

Ab CMS 3.0 wird CMM 3.0 benötigt, damit CMS ordnungsgemäß funktioniert. CMM ist für die

Lizenzierung von CMS verantwortlich. Wenn Sie also ein Upgrade von CMS auf 3.0 planen, benötigen Sie einen CMM-Server. Es wird empfohlen, CMM 2.9 in CMS 2.9 bereitzustellen, damit Sie vor dem Upgrade Ihre Lizenznutzung überprüfen können.

CMM überprüft alle hinzugefügten CallBridges auf SMP- und PMP-Lizenzen sowie auf die CallBridge-Lizenz. Dabei wird die Nummer verwendet, die auf den verschiedenen Geräten im Cluster am höchsten ist.

Wenn z. B. CMS1 über 20 PMP- und 10 SMP-Lizenzen verfügt und CMS2 über 40 PMP- und 5 SMP-Lizenzen in herkömmlicher Lizenzierung verfügt, meldet das CMM, dass Sie 40 PMP- und 10 SMP-Lizenzen verwenden müssen.

Wenn Sie mehr PMP-Lizenzen als importierte Benutzer besitzen, haben Sie keine Probleme im Zusammenhang mit PMP- (oder SMP-) Lizenzen, aber wenn Sie diesen 90-Tage-Peak überprüfen und feststellen, dass Sie mehr als verfügbar verwendet haben, können Sie dennoch auf CMS 3.0 aktualisieren und die 90-Tage-Testlizenz auf CMM verwenden, um die Dinge mit Ihrer Lizenz zu regeln, oder vor dem Upgrade Maßnahmen ergreifen.

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

Recording or Streaming	
Allocated	90 day peak
20	2

## Konfigurieren von Webbridge (WebRTC und CMA-Client)

CMS 3.0 entfernt die XMPP-Serverkomponente und damit WebBridge und die Möglichkeit, den CMA-Thick-Client zu verwenden. WebBridge3 wird heute verwendet, um Web-App-Benutzer (ehemals WebRTC-Benutzer) über den Browser mit Meetings zu verbinden. Wenn Sie auf 3.0 aktualisieren, müssen Sie webbridge3 konfigurieren.

**Anmerkung:** CMA-Thick-Client funktioniert nach dem Upgrade auf CMS 3.0 nicht!

In diesem Video erfahren Sie, wie Sie die webbridge 3-Zertifikate erstellen.

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

Vor dem Upgrade auf 3.0 müssen Kunden planen, wie sie Webbridge3 konfigurieren. Die wichtigsten Schritte sind hier aufgeführt.

1. Sie benötigen einen Schlüssel und eine Zertifikatskette für webbridge3. Das alte Webbridge-Zertifikat kann verwendet werden, wenn das Zertifikat alle FQDNs oder IP-Adressen des CMS-Servers als Subject Alternative Name (SAN)/Common Name (CN) enthält, auf denen webbridge3 ausgeführt wird, und wenn eine der folgenden Bedingungen erfüllt ist:

antwort: Das Zertifikat weist keine erweiterte Schlüsselverwendung auf (d. h. es kann entweder als Client oder Server verwendet werden).

b. Das Zertifikat weist sowohl Client- als auch Serverauthentifizierung auf. Das HTTP-Zertifikat benötigt nur die Serverauthentifizierung, während das C2W-Zertifikat sowohl den Server als auch den Client erfordert.)

2. Wenn Sie ein neues Zertifikat für das "**webbridge3 https**"-Zertifikat erstellen möchten, wird empfohlen, es öffentlich zu signieren (um Zertifikatswarnungen auf dem Client bei Verwendung der Web-App zu vermeiden). Das gleiche Zertifikat kann für das "webbridge3 c2w-Zertifikat" verwendet werden, und das Zertifikat muss den FQDN der Webbridge-Server im SAN/CN aufweisen.
3. CallBridges müssen mit der neuen webbridge3 über einen Port kommunizieren, der im Befehl **webbridge3 c2w listen** konfiguriert ist. Dies kann ein beliebiger verfügbarer Port sein, z. B. 449. Benutzer müssen sicher sein, dass die Callbridges mit webbridge3 an diesem Port kommunizieren können und dass ggf. im Voraus Änderungen an der Firewall vorgenommen werden. Es kann sich nicht um denselben Port handeln, den "webbridge https" zum Abhören verwendet.

Vor dem CMS-Upgrade auf Version 3.0 wird empfohlen, ein Backup mit 'backup snapshot <servername\_date>' durchzuführen und sich dann bei der webadmin-Seite auf Ihren callbridge-Knoten anzumelden, um alle XMPP-Einstellungen und Webbridge-Einstellungen zu entfernen. Stellen Sie dann eine Verbindung mit dem MMP auf Ihren Servern her, und führen Sie diese Schritte auf allen Core-Servern aus, die über xmpp und webbridge über eine SSH-Verbindung verfügen:

1. **xmpp deaktivieren**
2. **xmpp zurücksetzen**
3. **xmpp certs none**
4. **XMPP-Domäne keine**
5. **Webbridge-Deaktivierung**
6. **Webbridge nicht hören**
7. **Webbridge-Zertifikate keine**
8. **Webbridge-Vertrauenswürdigkeit keine**

Sobald Sie ein Upgrade auf 3.0 durchgeführt haben, beginnen Sie mit der Konfiguration von webbridge3 auf allen Servern, auf denen zuvor webbridge ausgeführt wurde. Sie müssen dies tun, da es bereits DNS-Einträge gibt, die auf diese Server verweisen. Auf diese Weise stellen Sie sicher, dass ein Benutzer, der an eine webbridge3 gesendet wird, bereit ist, die Anfrage zu bearbeiten.

### Webbridge3-Konfiguration (über alle SSH-Verbindungen)

Schritt 1: Konfigurieren des HTTP-Überwachungsports webbridge3

### **Webbridge3 HTTPS-Übertragung:443**

Schritt 2: Konfigurieren Sie Zertifikate für Webbridge3 für Browser-Verbindungen. Dieses Zertifikat wird an Browser gesendet und muss von einer öffentlichen Zertifizierungsstelle signiert werden. Es enthält den FQDN, der im Browser verwendet wird, damit der Browser der Verbindung vertrauen kann.

**Webbridge3 https certs wb3.key wb3trust.cer** (Dies muss eine Vertrauenskette sein: ein Vertrauenszertifikat erstellen, in dem die Endeinheit an der Spitze steht, gefolgt von den zwischengeschalteten Zertifizierungsstellen, und mit RootCA abschließen).

```
-----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
```

Schritt 3: Konfigurieren Sie den Port so, dass er CallBridge-to-Webbridge-Verbindungen (c2w) abhört. Da 443 für den Webbridge3 HTTPS-Listen-Port verwendet wird, muss diese Konfiguration ein anderer, verfügbarer Port sein, z. B. 449.

#### **Webbridge3 c2w abhören:449**

4. Konfigurieren Sie Zertifikate, die Webbridge an callbridge für die c2w-Vertrauensstellung sendet.

#### **Webbridge3 c2w-Zertifikate wb3.key wb3trust.cer**

5. Konfigurieren Sie den Vertrauensspeicher, den WB3 verwendet, um dem callBridge-Zertifikat zu vertrauen. Dies muss mit dem Zertifikat übereinstimmen, das für das Callbridge-CA-Paket verwendet wird (und muss ein Paket von Zwischenzertifikaten darüber und eine Root-CA am Ende gefolgt von einem einzelnen Wagenrücklauf sein).

#### **Webbridge3 c2w - Vertrauen auf rootca.cer**

6. Aktivieren Sie webbridge3

#### **Webbridge3 aktivieren**

```
Usage:
webbridge3
webbridge3 restart
6 webbridge3 enable
webbridge3 disable
1 webbridge3 https listen <interface:port whitelist>
2 webbridge3 https certs <key-file> <cert-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> <cert-fullchain-file>
webbridge3 c2w certs none
5 webbridge3 c2w trust <cert-bundle>
webbridge3 c2w trust none
webbridge3 options <space-separated options>
webbridge3 options none
webbridge3 status
```

## CallBridge-Konfigurationsänderungen (über alle SSH-Verbindungen)

Schritt 1: Konfigurieren Sie die callBridge-Vertrauensstellung mit dem Zertifizierungsstellenzertifikat/Bündel, das das webbridge3 c2w-Zertifikat signiert hat.

**Callbridge trust c2w rootca.cer**

Schritt 2: Starten Sie die callBridge neu, damit die neue Vertrauensstellung wirksam wird. Dadurch werden alle Anrufe für diese spezielle callBridge-Klasse fallen gelassen. Verwenden Sie diese daher mit Vorsicht.

**Callbridge-Neustart**

## API-Konfiguration für CallBridges zur Verbindung mit WebBridge3

1. Erstellen Sie ein neues WebBridge-Objekt mithilfe von POST in der API, und geben Sie ihm einen URL-Wert mithilfe von FQDN und einem auf der Webbridge c2w-Schnittstelle konfigurierten Port (Whitelist) (Schritt 3 in der Webbridge3-Konfiguration).

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

An diesem Punkt funktioniert Webbridge3 wieder, und Sie können Leerzeichen als Gast beitreten, oder wenn Sie zuvor Benutzer importiert haben, müssen diese sich anmelden können.

## **Berechtigungen zur Erstellung von Speicherplatz für Web-Anwendungen**

Sind Ihre Benutzer daran gewöhnt, ihre eigenen Räume in WebRTC zu erstellen? Ab CMS 3.0 können Web-App-Benutzer keine eigenen CoSpaces erstellen, es sei denn, ihnen wurde eine CoSpace-Vorlage zugewiesen, die dies ermöglicht.

Selbst wenn eine coSpaceTemplate zugewiesen ist, wird dadurch kein Raum geschaffen, in den sich andere einwählen können (kein URI, keine Anruf-ID oder kein Passcode). Wenn der coSpace jedoch ein callLegProfile mit "addParticipantAllowed" hat, können sie sich aus dem Raum heraus einwählen.



Damit Wählzeichenfolgen zum Aufrufen in den neuen Space verwendet werden können, muss coSpaceTemplate über eine accessMethodTemplate-Konfiguration verfügen (siehe 2.9 Release Notes -

[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)).

Erstellen Sie in der API coSpaceTemplate(s), und erstellen Sie dann accessMethodTemplate(s), und weisen Sie die coSpaceTemplate den ldapUserCoSpaceTemplateSources zu. Alternativ können Sie einem Benutzer in api/v1/users manuell eine coSpaceTemplate zuweisen.

Sie können mehrere CoSpace-Vorlagen und accessMethodsTemplates erstellen und zuweisen. Weitere Informationen finden Sie im CMS API-Leitfaden (<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 shows the configuration for a specific CoSpaceTemplate and a list of associated accessMethodTemplates.

**CoSpaceTemplate Configuration:**

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

**AccessMethodTemplates Configuration:**

Field	Value	Required
name	First CoSpaceTemplate	present
description		
callProfile	008e1aa7-0079-4d65-b6ae-fb218bd2e6b4	present
callLegProfile	ef583b0e-a6fe-49cf-bece-b557332a76bf	present
dialInSecurityProfile		

The interface includes a 'Modify' button for the accessMethodTemplates configuration.

## CoSpaceTemplate (API-Konfiguration)

**Name:** Beliebiger Name, den Sie der coSpaceTemplate zuweisen möchten.

**Beschreibung:** Kurze Beschreibung, falls gewünscht.

**Anrufprofil:** White callProfile Möchten Sie alle mit dieser Vorlage erstellten Leerzeichen verwenden? Wird diese Angabe nicht gemacht, wird die auf System-/Profilebene festgelegte Konfiguration verwendet.

**calllegProfil:** Welches calllegProfile soll von mit dieser Vorlage erstellten Leerzeichen verwendet werden? Wird diese Angabe nicht gemacht, wird die auf System-/Profilebene festgelegte Konfiguration verwendet.

**dialInSecurityProfile:** Welches dialInSecurityProfile soll mit dieser Vorlage erstellte Leerzeichen verwenden? Wird diese Angabe nicht gemacht, wird die auf System-/Profilebene festgelegte Konfiguration verwendet.



Konfiguration verwendet.

### **AccessMethodTemplate (API-Konfiguration)**

**Name:** Beliebiger Name, den Sie der coSpaceTemplate zuweisen möchten.

**uriGenerator:** Der Ausdruck, der zum Generieren von URI-Werten für diese Zugriffsmethodenvorlage verwendet werden soll. Die zulässigen Zeichen sind 'a' bis 'z', 'A' bis 'Z', '0' bis '9', '!', '-', '\_' und '\$'; wenn nicht leer, muss es genau ein "\$" Zeichen enthalten. Ein Beispiel hierfür ist \$.space, das den vom Benutzer beim Erstellen des Leerzeichens angegebenen Namen verwendet und ".space" daran anhängt. "Team Meeting" erstellt die URL "Team.Meeting.space@domain".

**callLegProfile:** Welches calllegProfile soll von mit dieser Vorlage erstellten accessMethods verwendet werden? Wenn dies nicht angegeben ist, wird die CoSpaceTemplate-Ebene verwendet. Wenn keine CoSpaceTemplate-Ebene angegeben ist, wird die Ebene des Systems bzw. Profils verwendet.

**GenerateUniqueCallId:** Legt fest, ob für diese Zugriffsmethode eine eindeutige numerische ID generiert werden soll, die die globale ID für den Cospace überschreibt.

**dialInSecurityProfile:** Welches dialInSecurityProfile soll von den mit dieser Vorlage erstellten Zugriffsmethoden verwendet werden? Wenn dies nicht angegeben ist, wird die CoSpaceTemplate-Ebene verwendet. Wenn keine CoSpaceTemplate-Ebene angegeben ist, wird die Ebene des Systems bzw. Profils verwendet.

## **Chat-Funktion**

In CMS 3.0 wurde die persistente Chat-Funktion entfernt, in CMS 3.2 wurde jedoch der nicht persistente Chat innerhalb von Leerzeichen zurückgegeben. Der Chat steht Benutzern von Web-Anwendungen zur Verfügung und wird nirgendwo gespeichert. Nach der Installation von CMS 3.2 können sich Web-App-Benutzer während Meetings standardmäßig gegenseitig Nachrichten senden. Diese Nachrichten sind nur während des Meetings verfügbar, und es werden nur Nachrichten angezeigt, die nach dem Beitritt ausgetauscht werden. Sie können nicht zu spät teilnehmen und einen Bildlauf zurück durchführen, um vorherige Nachrichten zu sehen.

## **WebRTC Point-to-Point-Anrufe**

In CMS 2.9.x konnten WebRTC-Teilnehmer direkt von ihrem Client aus andere Kontakte anrufen. Ab CMS 3.0 ist dies nicht mehr möglich. Jetzt müssen sich Benutzer anmelden und einem Space beitreten. Von dort aus können sie, wenn sie über die Berechtigung im callLegProfile (**addParticipants**-Parameter auf True festgelegt) verfügen, weitere Kontakte hinzufügen. Dadurch wählt sich das CMS beim Teilnehmer aus und trifft sich auf einem Platz im CMS.

## **Bemerkenswerte Änderungen der WebBridge-Einstellungen**

CMS 3.0 und 3.1 haben einige der Webbridge-Einstellungen aus der GUI entfernt oder verschoben und müssen in der API konfiguriert werden, um eine konsistente Benutzererfahrung zu gewährleisten. Verwenden Sie unter 3.x **api/v1/webBridges** und **api/v1/webBridgeProfiles**.

Prüfen Sie, was Sie derzeit konfiguriert haben, sodass Sie beim Upgrade auf 3.0 die Webbridge-

und Webbridge-Profile in der API entsprechend konfigurieren können.

The image displays three screenshots of the CMS configuration interface, illustrating the changes in Web Bridge and External Access 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 visible.
- 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 is still present with 'Web Bridge URI' (https://14.49.25.94) and 'IVR telephone number'. A 'Submit' button is visible.
- 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). The 'External access' section has been removed. A 'Submit' button is visible.

In 3.0 wurden **Web Bridge Einstellungen** auf der GUI entfernt, in CMS 3.1 wurden auch die **External Access** Felder entfernt.

### Web-Bridge-Einstellungen in der GUI

- **Guest Account Client URI** - Diese wurde von callBridge verwendet, um die webBridge zu finden. Wenn Sie mehrere webBridges in Ihrer Bereitstellung für WebRTC verwendet haben, muss dieses Feld bereits leer sein, und Sie müssen eindeutige URLs in api/v1/webbridges für jede webBridge haben, mit der die callBridge eine Verbindung herstellen muss. Löschen Sie alle Angaben in diesem Feld, und stellen Sie sicher, dass die webBridges in der API konfiguriert sind.
- **Gastkonto Jid Domain** - wird in CMS 3.0 nicht mehr verwendet und kann gelöscht werden.
- **Gastzugriff über ID und Passcode** - entfernt und nicht in CMS 3.0 ersetzt.

- **Gastzugriff über Hyper Links** - jetzt konfigurierbar unter webBridgeProfiles in API in der Einstellung "AllowSecrets".

The image shows two screenshots of the CMS API configuration interface for webBridges. The top screenshot is for CMS 2.9.x and shows fields for url, resourceArchive, tenant, tenantGroup, idEntryMode, allowWeblinkAccess, showSignIn, resolveCoSpaceCallIds, callBridge, and callBridgeGroup. The bottom screenshot is for CMS 3.0 and shows fields for url, tenant, tenantGroup, callBridge, callBridgeGroup, and webBridgeProfile. The 'Create' button is visible at the bottom of both forms.

Beachten Sie, dass in CMS 3.0 mehrere Felder aus api/v1/webBridges entfernt wurden.

- **resourceArchive** - jetzt in webbridgeProfiles.
- **idEntryMode** - jetzt veraltet.
- **allowWeblinkAccess** - jetzt in webBridgeProfiles als allowSecrets.
- **showSignIn** - jetzt in webBridgeProfiles als userPortalEnabled.
- **resolutCoSpaceCallIds**- jetzt in webbridgeProfiles.
- **ResolveLyncConferenceIDs** - jetzt in webbridgeProfiles.

The image shows a screenshot of the CMS API configuration interface for webBridgeProfiles. The form is titled "/api/v1/webBridgeProfiles" and includes fields for name, resourceArchive, allowPasscodes, allowSecrets, userPortalEnabled, allowUnauthenticatedGuests, resolveCoSpaceCallIds, and resolveCoSpaceUris. The "Create" button is at the bottom. The text "CMS 3.0 onward" is displayed in red on the right side.

## WebBridge-Profil

- **resourceArchive** - Wenn Sie benutzerdefinierte Hintergründe verwenden und Ihr Ressourcenarchiv auf einem Webserver gespeichert ist, geben Sie die URL hier ein.
- **allowPasscodes**: Bei "false" können Benutzer nicht als Gäste an Meetings teilnehmen. Sie können sich nur anmelden oder eine URL verwenden, die die Space-Informationen und den geheimen Schlüssel enthält.
- **allowSecrets** - Wenn dieser Wert auf false festgelegt ist, können Benutzer Leerzeichen nicht

über eine URL wie

[https://meet.company.com/meeting/040478?secret=gPDnucF8is4W1cS87\\_l.zw\\_beiitreten](https://meet.company.com/meeting/040478?secret=gPDnucF8is4W1cS87_l.zw_beiitreten). Die Benutzer müssen "https://meet.company.com" verwenden und, falls konfiguriert, die Anruf-ID/Meeting-ID/URI und die PIN/den Passcode eingeben.

- **userPortalEnabled** - Wenn dieser Wert auf false festgelegt ist, wird die Option zum Anmelden nicht auf der Landing Page des Web-App-Portals angezeigt. Es werden nur die Felder zur Eingabe von Anruf-ID/Meeting-ID/URI und PIN/Passcode angezeigt, wenn diese konfiguriert wurden.
- **allowUnAuthenticatedGuests** - Bei der Einstellung False können Gäste keinem Meeting beitreten - auch nicht mit der vollständigen URL, die die Meeting-ID und den Schlüssel enthält. Bei False können nur Benutzer, die sich anmelden können, an einem Meeting teilnehmen. Beispiel. User2 versucht, die URL für das Meeting von User1 zu verwenden. Nach Eingabe der URL muss sich User2 anmelden, um mit dem Meeting von User1 fortzufahren.
- **resolutCoSpaceCallIds** - Wenn diese Eigenschaft auf False festgelegt ist, können Gäste nur an Meetings teilnehmen, indem sie den URI und die PIN/den Passcode eingeben, wenn sie verwendet werden. Anruf-ID/Meeting-ID/numerische ID werden nicht akzeptiert.
- **resolutCoSpaceUris** - 3 mögliche Einstellungen: off, domainSuggestionDisabled und domainSuggestionEnabled. Legt fest, ob diese webBridge CoSpace- und CoSpace-Zugriffsmethoden SIP-URIs akzeptiert, um Besuchern die Teilnahme an Cospace-Meetings zu ermöglichen.

- Wenn 'off' gesetzt ist, wird der Beitritt durch URI deaktiviert.

- Wenn 'domainSuggestionDisabled' als Wert festgelegt ist, ist der Join über URI aktiviert, aber die Domäne des URI wird auf webBridges mit diesem webBridgeProfile nicht automatisch vervollständigt oder verifiziert.

- Wenn 'domainSuggestionEnabled' als Join durch URI festgelegt ist, ist der URI aktiviert, und die Domäne des URI kann mithilfe dieses webBridgeProfile automatisch vervollständigt und auf webBridges überprüft werden.

## Abschnitt für externen Zugriff von Web-GUI entfernt

In CMS 3.1 wurde der Bereich für den externen Zugriff aus der Web-GUI entfernt. Wenn Sie diese vor dem Upgrade konfiguriert haben, müssen Sie sie in der API unter webbridgeProfiles neu konfigurieren.



External access

Web Bridge URI

IVR telephone number

Zunächst müssen Sie ein webbridgeProfile erstellen, wie im vorherigen Abschnitt beschrieben. Nachdem Sie ein webbridgeProfile erstellt haben, können Sie eine IVR-Nummer und/oder einen Web Bridge URI über die in der API unter dem neu erstellten webBridgeProfile verfügbaren Links erstellen.

« return to object list

/api/v1/webBridgeProfiles/04dd26d0-777e-4dc5-8f0c-74b3887a1743

Related objects: </api/v1/webBridgeProfiles>

</api/v1/webBridgeProfiles/04dd26d0-777e-4dc5-8f0c-74b3887a1743/ivrNumbers>

</api/v1/webBridgeProfiles/04dd26d0-777e-4dc5-8f0c-74b3887a1743/webBridgeAddresses>

Sie können bis zu 32 IVR-Nummern oder 32 Webbridge-Adressen pro WebBridge-Profil erstellen.

## Aufzeichnung oder Streaming

Die Recorder- und Streamer-Komponente in CMS 2.9.x und früheren Versionen waren XMPP-Clients, und von CMS 3.0 sind sie SIP-basiert. Dadurch können jetzt Layouts für Aufzeichnungen und Streaming mit dem Standardlayout in der API geändert werden. Außerdem werden jetzt Namensschilder in der Aufnahme-/Streaming-Sitzung angezeigt. Weitere Informationen zu den Recorder-/Streaming-Funktionen finden Sie in den Versionshinweisen zu CMS 3.0 unter [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).

Wenn Sie Rekorder oder Streamer in 2.9.x konfiguriert haben, müssen Sie die Einstellungen in MMP und API neu konfigurieren, damit diese nach dem Upgrade weiterhin funktionieren.

Vor dem CMS-Upgrade auf Version 3.0 wird empfohlen, ein Backup mit 'backup snapshot <servername\_date>' durchzuführen und sich dann bei der webadmin-Seite auf Ihren callbridge-Knoten anzumelden, um alle XMPP-Einstellungen zu entfernen. Stellen Sie dann eine Verbindung mit dem MMP auf Ihren Servern her, und führen Sie die folgenden Schritte auf allen Core-Servern aus, die über eine SSH-Verbindung mit xmpp verbunden sind:

1. xmpp deaktivieren
2. xmpp zurücksetzen
3. xmpp certs none
4. XMPP-Domäne keine

### Rekorder

### MMP

Die Abbildungen zeigen ein Beispiel der Konfigurationen, die in CMS 2.9.1 bei der Konfiguration des Recorders beobachtet wurden, und wie es unmittelbar nach dem Upgrade auf 3.0 aussieht.

```
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>
```

CMS 2.9.x

CMS 3.x

Nach dem Upgrade müssen Sie den Rekorder neu konfigurieren:

Schritt 1: Konfigurieren Sie die SIP-Überwachungsschnittstelle.

**rekorder sip listen a 5060 5061** (Die Schnittstelle und die Ports, auf denen der SIP-Recorder für das respektvolle Überwachen von TCP und TLS eingerichtet ist. Wenn Sie TLS nicht verwenden möchten, können Sie "**rekorder sip listen a 5060 none**" verwenden.)

Schritt 2: Konfigurieren Sie die Zertifikate, die der Rekorder verwendet, wenn Sie eine TLS-Verbindung verwenden.

**rekorder sip certs <key-file> <crt-file> [crt-bundle]** (Ohne diese Zertifikate startet der tls-Dienst nicht auf dem Recorder. Der Recorder verwendet das crt-Bundle, um das callBridge-Zertifikat zu verifizieren.)

Schritt 3: Konfigurieren Sie das Anruflimit.

**rekorder limit <0-500|none>** (Legt die Grenze für die Anzahl gleichzeitiger Aufzeichnungen fest, die der Server bereitstellen kann. Diese Tabelle finden Sie in unserer Dokumentation. Die Rekorder-Grenze muss mit den Ressourcen auf dem Server übereinstimmen.)



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

Bei api/v1/callProfiles müssen Sie den **sipRecorderUri** konfigurieren. Dies ist der URI, den CallBridge wählt, wenn eine Aufzeichnung gestartet werden muss. Die Domäne dieses URIs muss zur Tabelle der ausgehenden Regeln hinzugefügt werden und auf den Rekorder (oder die Anrufsteuerung) als zu verwendenden SIP-Proxy verweisen.

Object configuration	
recordingMode	automatic
sipRecorderUri	recorder@recorder.com

Diese Abbildung zeigt eine Direktdurchwahl zur Rekorder-Komponente in den Regeln für ausgehende Anrufe unter **Konfiguration > Ausgehende Anrufe**.

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

Diese Abbildung zeigt einen Anruf an die Rekorderkomponente über eine Anrufsteuerung (wie z.B. Cisco Unified Communications Manager (CUCM) oder 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

**Anmerkung:** Wenn Sie den Rekorder für die Verwendung von SIP TLS konfiguriert haben und wenn Anrufe fehlschlagen, überprüfen Sie Ihren callBridge-Knoten in MMP, um festzustellen, ob die TLS SIP-Verifizierung aktiviert ist. Der MMP-Befehl lautet **'tls sip'**. Anrufe können fehlschlagen, weil das Rekordzertifikat von callBridge nicht vertrauenswürdig ist. Sie können dies testen, indem Sie dies auf der callBridge mit **'tls sip verify disable'** deaktivieren.



## Mehrere Rekorder?

Konfigurieren Sie die einzelnen Regeln wie beschrieben, und passen Sie die Regeln für ausgehende Anrufe entsprechend an. Wenn Sie eine Direct To Recorder-Methode verwenden, ändern Sie die vorhandene Regel für ausgehende Anrufe in Recorder in das Verhalten "Continue" (Weiter), und fügen Sie eine neue Regel für ausgehende Anrufe unterhalb der vorherigen mit einer niedrigeren Priorität als der ersten hinzu. Wenn der erste Recorder sein Anruflimit erreicht hat, sendet er eine 488 Unaccept (Unannehmbar) zurück an callBridge, und callBridge geht zur nächsten Regel über.

Wenn Sie den Lastenausgleich für die Rekorder vornehmen möchten, verwenden Sie eine Anrufsteuerung, und passen Sie die Anrufsteuerungsweiterleitung an, sodass mehrere Rekorder angerufen werden können.

## **Streamer**

### MMP

Nach dem Upgrade von 2.9.x auf 3.0 müssen Sie Streamer neu konfigurieren.

Schritt 1: Konfigurieren Sie die SIP-Überwachungsschnittstelle.

**streamer sip listen a 6000 6001** (Die Schnittstelle und die Ports, auf denen der SIP-Streamer eingerichtet ist, um TCP und TLS zu überwachen. Wenn Sie TLS nicht verwenden möchten, können Sie "**streamer sip listen a 6000 none**" verwenden.)

Schritt 2: Konfigurieren Sie die Zertifikate, die der Streamer verwendet, wenn Sie eine TLS-Verbindung verwenden.

**streamer sip certs <key-file> <cert-file> [crt-bundle]** (Ohne diese Zertifikate startet der tls-Dienst nicht auf dem streamer. Der Streamer verwendet das crt-Paket, um das callBridge-Zertifikat zu verifizieren.)

Schritt 3: Konfigurieren des Anruflimits

**streamer limit <0-500|none>** (Legt den Grenzwert für die Anzahl gleichzeitiger Streams fest, die der Server bedienen kann. Diese Tabelle finden Sie in unserer Dokumentation, und die Streamer-Grenze muss mit den Ressourcen auf dem Server übereinstimmen.)

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

Bei `api/v1/callProfiles` müssen Sie `sipStreamUri` konfigurieren. Dies ist der URI, den callBridge wählt, wenn das Streaming gestartet werden muss. Die Domäne dieses URIs muss zur Tabelle der ausgehenden Regeln hinzugefügt werden und auf den Streamer (oder die Anrufsteuerung) als zu verwendender SIP-Proxy verweisen.

`/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>sipStreamerUri</code>	<code>stream@streamer.com</code>

Diese Abbildung zeigt eine Direktdurchwahl zur Streamer-Komponente in den Regeln für ausgehende Anrufe unter **Konfiguration > Ausgehende Anrufe**.

Outbound calls

Filter

	Domain	SIP proxy to use	Local contact domain	Local from domain	Trunk type	Behavior	Priority	Encryption
<input type="checkbox"/>	recorder.com	14.49.17.246:5061		<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	14.49.17.246:6000		<use local contact domain>	Standard SIP	Stop	0	Auto
<input type="checkbox"/>					Standard SIP	Stop	0	Auto

Recorder

Streamer

Diese Abbildung zeigt einen Anruf an die Recorderkomponente über eine Anrufsteuerung (wie z.B. Cisco Unified Communications Manager (CUCM) oder Expressway).

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

*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 'Streamer.com' row. A blue 'CUCM' label is above the 'Local contact domain' column. A red 'Expressway' label is above the 'Streamer.com' row.*

**Anmerkung:** Wenn Sie den Streamer so konfiguriert haben, dass er SIP-TLS verwendet, und wenn Anrufe fehlschlagen, überprüfen Sie Ihren callBridge-Knoten in MMP, um festzustellen, ob die TLS-SIP-Verifizierung aktiviert ist. Der MMP-Befehl lautet **'tls sip'**. Anrufe können fehlschlagen, weil das Streamer-Zertifikat von callBridge nicht als vertrauenswürdig eingestuft wird. Sie können dies testen, indem Sie dies auf der callBridge mit **'tls sip verify disable'** deaktivieren.

### Mehrere Streamer?

Konfigurieren Sie die einzelnen Regeln wie beschrieben, und passen Sie die Regeln für ausgehende Anrufe entsprechend an. Wenn Sie eine Methode für das direkte Aufzeichnen verwenden, ändern Sie die vorhandene Regel für das ausgehende Aufzeichnen in das Verhalten "Continue" (Fortfahren), und fügen Sie eine neue Regel für das ausgehende Aufzeichnen unterhalb der vorherigen hinzu, deren Priorität um eins kleiner als die erste ist. Wenn der erste Streamer sein Anruflimit erreicht hat, sendet er eine 488 Unaccept (Unannehmbar) an callBridge zurück, und callBridge geht zur nächsten Regel über.

Wenn Sie den Lastenausgleich für Ihre Streamer vornehmen möchten, verwenden Sie eine Anrufsteuerung, und passen Sie die Anrufsteuerungsweiterleitung so an, dass Anrufe an mehrere Streamer weitergeleitet werden können.

### Überlegungen zum Expressway

Wenn Sie Cisco Expressway für Webproxy verwenden, müssen Sie sicherstellen, dass Ihr Expressway mindestens X12.6 vor dem CMS-Upgrade ausgeführt wird. Dies ist in CMS 3.0 erforderlich, damit der Webproxy funktioniert und unterstützt wird.

Die Kapazität für Web-App-Teilnehmer hat sich gegenüber Expressways bei Verwendung mit CMS 3.0 erhöht. Für einen großen OVA-Expressway wird eine Kapazität von 150 Full-HD-Anrufen (1080p30) oder 200 Anrufen anderer Art (z. B. 720p30) erwartet. Sie können diese Kapazität durch Clustering von Expressways auf bis zu 6 Knoten erhöhen (wobei 4 für Skalierung und 2 für Redundanz verwendet wird, sodass maximal 600 Full HD-Anrufe oder 800 Anrufe anderer Art möglich sind).

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-Edge

CMS Edge wird in CMS 3.1 wieder eingeführt, da es höhere Kapazitäten als der Expressway für externe Web-App-Sitzungen bietet. Es gibt zwei empfohlene Konfigurationen.

### Small Edge-Spezifikationen

4 GB RAM, 4 vCPUs, **1 Gbit/s** Netzwerkschnittstelle

Diese VM Edge-Spezifikation verfügt über eine ausreichende Leistung, um eine einzelne CMS1000-Audio- und Video-Lastkapazität von 48 x 1080p, 96 x 720p, 192 x 480p und 1000 Audio-Anrufen abzudecken.

Für die Bereitstellung wird ein Small Edge-Server pro CMS1000 oder vier Small Edge-Server pro CMS2000 empfohlen.

### Spezifikationen für große Ränder

8 GB RAM, 16 vCPUs, **10 Gbit/s** Netzwerkschnittstelle

Diese VM-Edge-Spezifikation verfügt über eine ausreichende Leistung, um eine einzelne CMS2000-Audio- und Videokapazität von 350 x 1080p, 700 x 720p, 1000 x 480p und 3000 x Audioanrufe abzudecken.

Für die Bereitstellung wird ein großer Edge-Server pro CMS2000 oder vier CMS1000 empfohlen.

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

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.