

Diretrizes de uma atualização simples do Cisco Meeting Server 2.9 para a versão 3.0 (e em diante)

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Informações importantes sobre atualizações](#)

[Resumo dos itens a serem considerados](#)

[Licenças](#)

[Webbridge \(cliente WebRTC e CMA\)](#)

[Alterações na GUI da Web](#)

[Gravadores/Streamers](#)

[Considerações sobre o Cisco Expressway](#)

[CMS Edge](#)

[CMS \(Aceno\) X-Series](#)

[Borda SIP](#)

[Mais informações](#)

[Licenciamento - Verificar licenças antes da atualização](#)

[Determine a quantos usuários é atribuída uma licença PMP após a atualização](#)

[Você tem licenças SMP suficientes?](#)

[Configurar CMM](#)

[Configurar Webbridge \(WebRTC e cliente CMA\)](#)

[Permissões de criação de espaço do usuário do aplicativo Web](#)

[Função de bate-papo](#)

[Chamadas ponto a ponto WebRTC](#)

[Alterações notáveis nas configurações do webBridge](#)

[Seção Acesso Externo removida da GUI Web](#)

[Gravação ou transmissão](#)

[Gravador](#)

[Streamer](#)

[Consideração do Expressway](#)

[CMS Edge](#)

Introduction

Este documento descreve os desafios de atualizar uma implantação do Cisco Meeting Server executando a versão 2.9 (ou anterior) para a versão 3.0 (ou posterior) e como lidar com eles para um processo de atualização tranquilo.

Recursos removidos: O XMPP foi removido (o que afeta o WebRTC), troncos/balancedores de carga, webbridge

Recursos alterados: Os gravadores e otimizadores agora são SIP e o webbridge é substituído pelo webbridge3

Este documento abrange apenas os tópicos que você precisa considerar antes de atualizar. Ele não cobre todos os novos recursos disponíveis no 3.X.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- administração de CMS
- Atualizações do CMS
- Criação e assinatura de certificado

Tudo o que aqui se refere está descrito em vários documentos. É sempre aconselhável ler as notas de versão do produto e consultar nossos guias de programação e guias de implantação se precisar de mais esclarecimentos sobre os recursos: [Guias de instalação e configuração do CMS](#) e [Notas de versão do produto do CMS](#).

Componentes Utilizados

As informações neste documento são baseadas no 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Este documento tem como objetivo orientar caso você já tenha uma implantação do CMS 2.9.x (ou anterior), independentemente de ser única, combinada ou resiliente, e quando planeja atualizar para o CMS 3.0. As informações neste documento pertencem a todos os modelos de CMS.

Note: O X-series não pode ser atualizado para o CMS 3.0. Você precisa planejar substituir seus servidores X-series o mais rápido possível.

Informações importantes sobre atualizações

O único método suportado para atualizar o CMS é uma atualização em etapas. No momento em que este documento foi escrito, o CMS 3.5 foi lançado. Se você estiver no CMS 2.9, deverá fazer o upgrade em etapas (2.9 → 3.0 → 3.1 → 3.2 → 3.3 → 3.4 → 3.5 (Observe que o processo de upgrade tem alterações a partir do CMS 3.5, portanto, leia as notas de versão com

atenção!!)

Se você não executar uma atualização em etapas e estiver tendo um comportamento incomum, o TAC poderá solicitar que você faça o downgrade e comece novamente.

Além disso, a partir do CMS 3.4, o CMS DEVE usar o Smart Licensing. Você não pode atualizar para o CMS 3.4 ou mais recente e ainda usar licenças tradicionais. Não atualize para o CMS 3.4 ou posterior, a menos que você tenha configurado o Smart Licensing.

Resumo dos itens a serem considerados

Use essas perguntas para navegar para as seções que pertencem à sua própria situação. Cada consideração se refere a um hiperlink para uma descrição mais detalhada apresentada neste documento.

Licenças

Você tem licenças suficientes de Personal MultiParty (PMP) / Shared MultiParty (SMP) em seus servidores antes da atualização?

No 3.0, as licenças PMP são alocadas, mesmo que o usuário não esteja conectado. Por exemplo, se você importou usuários 10000 por meio do LDAP, mas tem apenas 100 licenças PMP, isso o coloca fora de conformidade assim que você faz o upgrade para a versão 3.0. Para este caso de uso, verifique se há locatários com userProfile definido e/ou sistema/perfis para ver se um userProfile com hasLicense com um valor de true está definido.

Como verificar o userProfile na API e ver se você tem o conjunto de licenças=verdadeiro (significando usuários com licença PMP), é abordado em mais detalhes [nesta seção](#).

Você tem licenças PMP/SMP em seu arquivo cms.lic atual?

Devido a uma mudança no comportamento da licença no 3.0 em diante, você deve confirmar se tem licenças PMP/SMP suficientes antes de executar a atualização. Isso é descrito em mais detalhes [nesta seção](#).

Você tem o Cisco Meeting Manager (CMM) implantado?

O CMS 3.0 requer o CMM 3.0 devido a alterações na forma como as licenças são tratadas. É recomendável implantar o CMM 2.9 antes de executar uma atualização do seu ambiente para a versão 3.0, pois você pode verificar o consumo de licença do seu relatório de 90 dias nos últimos 90 dias. Isso é descrito em mais detalhes [nesta seção](#).

Você tem Smart Licensing?

O CMS 3.0 requer o CMM 3.0 devido a alterações na forma como as licenças são tratadas. Portanto, se você já estiver usando o Smart Licensing através do CMM, certifique-se de ter licenças PMP e SMP associadas ao seu cluster.

Webbridge (cliente WebRTC e CMA)

Você usa WebRTC no CMS 2.9?

O Webbridge mudou significativamente no CMS 3.0. Para obter orientação sobre a migração de webbridge2 para webbridge3 e o uso do aplicativo Web, as informações são encontradas [nesta seção](#).

Seus usuários usam o thick client CMA?

Como esses clientes são baseados em XMPP, eles não poderão mais ser usados após a atualização, pois o servidor XMPP foi removido. Se isso se aplicar ao seu caso de uso, você poderá encontrar mais informações [nesta seção](#).

Você usa Bate-papo em WebRTC?

A funcionalidade de bate-papo é removida do aplicativo Web no 3.0. No CMS 3.2, o bate-papo é reintroduzido, mas não é persistente. Você pode encontrar mais informações sobre este recurso [nesta seção](#).

Seus usuários realizam chamadas Point to Point do WebRTC para dispositivos?

No CMS 3.0, um usuário do aplicativo Web não pode mais discar diretamente para outro dispositivo. Agora você deve ingressar em um espaço de reunião e ter permissão para adicionar participantes à reunião para executar a mesma ação. Você pode encontrar mais informações sobre esta parte [nesta seção](#).

Seus usuários criam seus próprios coSpaces a partir do WebRTC?

No 3.0, para que os usuários do aplicativo Web possam criar seus próprios espaços a partir do cliente, um coSpaceTemplate precisa ser criado na API e atribuído ao usuário. Pode ser manual ou automático durante a importação LDAP. CanCreateCoSpaces é removido de UserProfile. Você pode encontrar mais informações sobre este recurso [nesta seção](#).

Alterações na GUI da Web

Você tem as configurações do WebBridge definidas na GUI do administrador da Web?

As configurações do webBridge são removidas da GUI no 3.0, portanto você deve configurar as webbridges na API e observar quais são suas configurações atuais na GUI para que você possa configurar os webBridgeProfiles na API de acordo. Você pode encontrar mais informações sobre essa alteração [nesta seção](#).

Você tem configurações externas configuradas na GUI do administrador da Web?

As configurações externas foram removidas da GUI no CMS 3.1. Se você tiver o URL do Webbridge ou o IVR configurado no CMS 3.0 ou uma GUI do administrador da Web mais antiga (Configuração —> Geral —> Configurações externas), eles foram removidos da página da Web e agora precisam ser configurados na API. As configurações anteriores à atualização para 3.1 NÃO são adicionadas à API e devem ser feitas manualmente. Você pode encontrar mais informações sobre essa alteração [nesta seção](#).

Gravadores/Streamers

Você usa algum gravador CMS e/ou dinamizador?

O gravador CMS e o componente de stream agora são baseados em SIP em vez de em XMPP. Portanto, como o XMPP está sendo removido, eles precisam ser ajustados após a atualização. Você pode encontrar mais informações sobre essa alteração [nesta seção](#).

Considerações sobre o Cisco Expressway

Qual é a sua versão atual do Cisco Expressway se você estiver usando Expressway para proxy WebRTC?

O CMS 3.0 requer Expressway 12.6 ou mais recente. Você pode encontrar mais informações sobre este recurso de proxy WebRTC [nesta seção](#).

CMS Edge

Você tem atualmente uma borda CMS em seu ambiente?

O CMS Edge é reintroduzido no CMS 3.1 com maior escalabilidade para conexões externas. Você pode encontrar mais informações sobre esta parte [nesta seção](#).

CMS (Acano) X-Series

Atualmente, você tem servidores x-series em seu ambiente?

Esses servidores não podem ser atualizados para o CMS 3.0 e você deve estar procurando substituí-los em breve (mude para uma máquina virtual ou dispositivo CMS antes de atualizar para a versão 3.0). Você pode encontrar o aviso de fim da vida útil sobre esses servidores [neste link](#).

Borda SIP

Você usa atualmente o SIP Edge em seu ambiente?

O Sip Edge foi totalmente substituído a partir do CMS 3.0. Você precisa usar o Cisco Expressway para trazer chamadas SIP para o seu CMS. Entre em contato com seu representante de conta da Cisco para saber como obter o Expressways para sua empresa.

Mais informações

Licenciamento - Verificar licenças antes da atualização

O status de licença fora de conformidade é o problema mais impactante quando você atualiza para a versão 3.0 ou superior a partir de uma versão 2.x. Esta seção descreve como determinar a quantidade de licenças PMP/SMP necessárias para uma atualização tranquila.

Antes de atualizar sua implantação para a versão 3.0, implante o CMM 2.9 e verifique o **relatório de 90 dias** na guia **Licenças** para ver se o uso da licença permaneceu sob a quantidade de licença alocada atual nos nós do CMS:

Cisco Meeting Management

Notifications LDAP/admin Administrator

Licenses

Cluster: CMS VM Cluster [Download 90 day report](#)

Meetings		In compliance			
	Allocated	90 day peak		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		

Se você usa o licenciamento tradicional (o arquivo cms.lic é instalado localmente nos nós do CMS), verifique o arquivo de licença do CMS para as quantidades de licenças pessoais e compartilhadas (100 / 100 conforme a imagem aqui) em cada um dos nós do CMS (baixe através do WinSCP de cada nó callBridge).

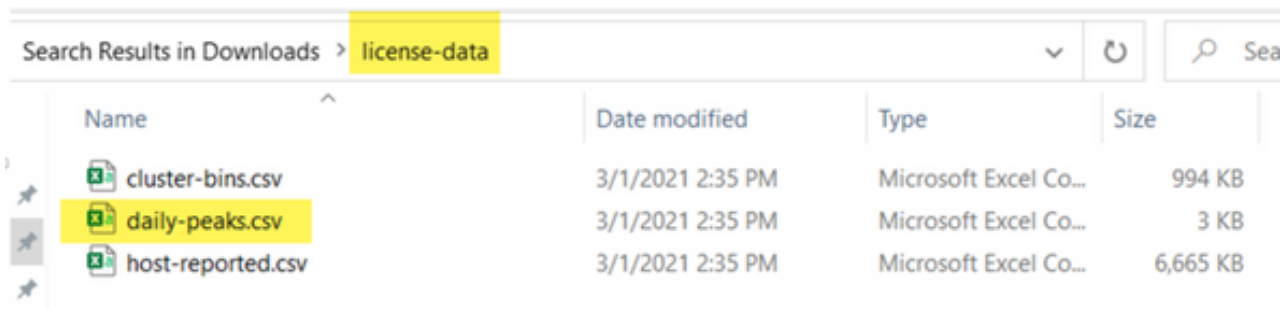
```

],
"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"
  }
}

```

Se você já usa o [Smart Licensing](#), verifique quantas licenças PMP/SMP estão atribuídas no Cisco Software Smart Portal para os servidores CMS.

Abra o relatório de 90 dias (o arquivo Zip é chamado *license-data.zip*) e abra o arquivo *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

No Excel, classifique a coluna PMP por Z a A para obter os valores mais altos para o topo e, em seguida, execute o mesmo para a coluna SMP. Os valores exibidos nesse arquivo são inferiores às licenças disponíveis no arquivo de licença do CMS? Em caso afirmativo, você está bem e totalmente em conformidade. Caso contrário, isso criará avisos e/ou erros, conforme indicado na Figura 6 na seção 1.7.3 do [guia de implantação do CMS](#), para o qual você pode encontrar mais informações também na seção 1.7.4.

De acordo com a imagem, por exemplo, foram usadas 2.1667 licenças de SMP e nenhuma licença de PMP durante o pico dos últimos 90 dias. O arquivo cms.lic indicou 100 unidades de cada tipo de licença, portanto, esta configuração é totalmente compatível. Portanto, não há problemas com o licenciamento quando essa configuração é atualizada para o CMS 3.0. No entanto, ainda pode haver um problema quando na configuração 10.000 usuários por meio do LDAP teriam sido importados. Como então você tem apenas 100 licenças PMP, mas você aloca 10000 (com userProfile com hasLicense definido como True) para que neste caso você esteja fora de conformidade assim que você atualizar para 3.0. Mais sobre isso na próxima seção.

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

Determine a quantos usuários é atribuída uma licença PMP após a atualização

Todos os usuários importados e que usam um **userProfile** com **hasLicense=true** recebem automaticamente uma licença PMP no CMS 3.0.

Na API, verifique quantos **userProfiles** você tem e se algum deles tem "hasLicense=true" definido. Em caso afirmativo, é necessário verificar onde esses **userProfiles** estão atribuídos.

Os perfis de usuário podem ser atribuídos em qualquer um destes níveis:

1. FontesLDAP
2. Locatários
3. Sistema/perfis

Verifique todos os 3 locais para **userProfiles** atribuídos que tenham **hasLicense=true**.

1. Fontes Ldap/Locatários

Para cada **ldapSource** que esteja usando um espaço ou um **userProfile**, os usuários importados com esse **ldapSource** receberão uma licença PMP quando o parâmetro **hasLicense** estiver definido como **True**. Se houver um espaço, clique na ID do espaço para ver se ele tem um **userProfile** atribuído e verifique se esse **userProfile** está configurado com 'hasLicense=true'. Se não houver nenhum espaço, mas houver um **userProfile** definido, clique nele para ver se ele tem 'hasLicense=true'. Se ambas as maneiras tiverem 'hasLicense=true', você poderá verificar quantos usuários foram importados executando **GET** para 'api/v1/users' e filtrando para o domínio usado para **jidMapping** no **ldapmapping** associado ao **ldapSource**, por exemplo.

Note: Isso pode ser mais complexo em outras situações em que você precisa verificar isso com os mapeamentos e filtros do **Active Directory** criados.

Etapa 1. Localize o ID de mapeamento a partir do **ldapSource**.

Etapa 2. Pesquise **ldapMappings** para localizar **jidMapping**.

Etapa 3. Procure em **api/v1/users** pelo domínio usado em **jidMapping**.

Etapa 4. Adicione os usuários encontrados em cada **ldapSource**. Veja quantos usuários **LDAP** importados precisam de licenças PMP.

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

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

Table view XML view

Object configuration	
name	
server	3472dd67-4075-4816-8fdb-fe8e10f8b4f8
mapping	5fcd57a-1e31-4717-a0cd-4875f14b2db8
tenant	8fca8c38-ed94-4603-9419-51abeae6dfc2
haveTo	DarcmckinLocal

/api/v1/ldapMappings 2 ldapMappings

= start < prev 1 - 3 (of 3) next >

Create new Table view XML view

object id	ldapMapping
186205f-5d31-488c-96c1-a2bc162a8fa4	\$SAMAAccountNames@darcmckin.local
5fcd57a-1e31-4717-a0cd-4875f14b2db8	\$SAMAAccountNames@simpsons.local
cf609fa7-b668-4c4e-92d6-c5d975e0bb7	\$SAMAAccountNames@familyguy.local

/api/v1/users 3 users

= start < prev 1 - 4 (of 4) next >

simpsons Filter Table view XML view

object id	user/id
2e2ed242-1b0d-4695-8da3-10e354603689	bart@simpsons.local
b285eb97-98f5-478b-9977-0d8c3d2f1b3	homer@simpsons.local
68599e67-1936-4269-35a2-3e81b920df7	lisa@simpsons.local
face6dee-98ef-4305-b339-0831085db496	marge@simpsons.local

2. Sistema/Perfis

Se um userProfile for definido no nível do sistema/perfis e esse userProfile tiver "hasLicense=true", qualquer usuário importado para o CMS receberá uma licença PMP quando o servidor for atualizado. Se você importou 10.000 usuários, mas só tem 100 PMPs, isso resulta em falta de conformidade quando você faz o upgrade para o CMS 3.0, e pode fazer com que uma mensagem na tela de 30 segundos seja exibida e o prompt de áudio no início das chamadas.

Se userProfile no nível do sistema indicar que os usuários devem obter um PMP, vá para /api/v1/users para ver quantos usuários há no total:

/api/v1/users 9 (of 9)

Will show total number of imported users

= start < prev 1 - 9 (of 9) next >

Filter Table view XML view

object id	user/id	ten
18a6595a-33a0-4fd0-8761-5030249e0301	Lois@familyguy.local	85d7cd06-1253-461f-bb1a-fe49fd7004e8
84a2dbbe-34d5-4a02-a003-2cf34fb5d9f3	brian@familyguy.local	85d7cd06-1253-461f-bb1a-fe49fd7004e8
86e2f6a6-55fc-443e-b7ae-66a200191cac	connor@darcmckin.local	
44800633-fb41-4998-b0f5-339c64fcb657	darren@darcmckin.local	
dbcc178dc-288c-99e5-a6d9-8cb192425b7f	homer@simpsons.local	8fca8c38-ed94-4603-9419-51abeae6dfc2
a1105eb2-49f1-4ba5-8deb-c1e3d74ba084	janette@darcmckin.local	
b6f80307-d879-4863-8e00-667e403e5a2e	meg@familyguy.local	85d7cd06-1253-461f-bb1a-fe49fd7004e8
32a615ee-ca2e-4489-a5db-d65e83b067a9	peter@familyguy.local	85d7cd06-1253-461f-bb1a-fe49fd7004e8
fic47991-5173-4daa-bb59-2140c8ca01f6	stewie@familyguy.local	85d7cd06-1253-461f-bb1a-fe49fd7004e8

Se você já importou todos os usuários do ldap, mas agora percebeu que precisa apenas de um determinado subconjunto dessa lista, crie um filtro melhor no ldapSource para que ele importe apenas os usuários aos quais deseja receber licenças PMP. Revise seu filtro em ldapSource e execute uma nova sincronização LDAP em /api/v1/ldapsync. Isso faz com que apenas os usuários desejados sejam importados e todos os outros usuários dessa importação anterior removidos.

Note: Se você fizer isso corretamente e a nova importação apenas remover usuários indesejados, os usuários restantes coSpace CallIDs e os segredos não serão alterados, mas se você cometer um erro, isso poderá resultar na alteração de todos os callIDs e segredos. Faça um backup dos nós do banco de dados antes de tentar isso, se estiver preocupado com isso!

Você tem licenças SMP suficientes?

Ao observar os picos diários do Relatório de 90 dias do CMM, você já tem licenças SMP

suficientes para cobrir o pico? As licenças SMP são usadas quando o proprietário da reunião não recebeu uma licença PMP (como proprietário do coSpace / reunião ad-hoc / reunião agendada do TMS). Se você estiver usando o SMP intencionalmente e tiver o suficiente para cobrir os horários de pico, tudo estará OK. Se você verificar o pico de 90 dias para SMP e não estiver claro por que eles são consumidos, veja algumas coisas a serem verificadas.

1. As chamadas ad hoc (conforme escaladas do CUCM) usam uma licença SMP se o dispositivo usado para mesclar não estiver associado a um usuário que recebeu uma licença PMP no CMS através do perfil do usuário. O CUCM fornece o GUID do usuário que está escalando a reunião. Se essa GUID corresponder a um usuário LDAP importado do servidor da reunião com uma licença PMP atribuída, a licença desse usuário será usada.

2. Se um proprietário do coSpace não tiver recebido uma licença PMP, as chamadas para esses coSpaces específicos usarão uma licença SMP.

3. Se a reunião tiver sido agendada no TMS versão 15.6 ou mais recente, o proprietário da reunião será enviado ao CMS e, se esse usuário não tiver recebido uma licença PMP, essa reunião usará uma licença SMP.

Configurar CMM

A partir do CMS 3.0, o CMM 3.0 é necessário para que o CMS funcione corretamente. O CMM é responsável pelo licenciamento do CMS, portanto, se você planeja atualizar o CMS para 3.0, deverá ter um servidor CMM. É recomendável implantar o CMM 2.9 enquanto você estiver no CMS 2.9 para que possa verificar o consumo de licença antes da atualização.

O CMM verifica todas as callBridges adicionadas para licenças SMP e PMP e para a licença callBridge. Ele usa o número mais alto entre os vários dispositivos dentro do cluster.

Por exemplo, se o CMS1 tiver 20 licenças PMP e 10 licenças SMP e o CMS2 tiver 40 licenças PMP e 5 licenças SMP no licenciamento tradicional, o CMM informará que você tem 40 licenças PMP e 10 licenças SMP para usar.

Se você tiver mais licenças de PMP do que usuários importados, não terá problemas relacionados às licenças de PMP (ou SMP), mas se verificar o pico de 90 dias e descobrir que usou mais do que o disponível, você ainda poderá atualizar para o CMS 3.0 e usar a licença de avaliação de 90 dias no CMM para resolver os problemas com o seu licenciamento ou agir antes da atualização.

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

Recording or Streaming		In compliance	
Allocated	90 day peak	20	2

Configurar Webbridge (WebRTC e cliente CMA)

O CMS 3.0 remove o componente de servidor XMPP e, com isso, remove o webBridge e a capacidade de usar o cliente thick CMA. O WebBridge3 é o que é usado agora para conectar usuários de aplicativos Web (antes chamados de usuários WebRTC) a reuniões usando o navegador. Ao atualizar para a versão 3.0, você precisa configurar o webbridge3.

Note: O cliente thick CMA não funciona após a atualização para o CMS 3.0!

Este vídeo o orienta durante o processo de criação dos certificados webbridge 3.

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

Antes da atualização para a versão 3.0, os clientes devem planejar como configurar o Webbridge3. As etapas mais importantes estão destacadas aqui.

1. Você precisa de uma cadeia de chaves e certificados para webbridge3. O certificado webbridge antigo pode ser usado se o certificado contiver todos os FQDNs do servidor CMS ou endereços IP como Nome Alternativo do Assunto (SAN)/Nome Comum (CN) que estejam executando o webbridge3 e se qualquer um destes for atendido:

a. O certificado não tem Uso Avançado de Chave (o que significa que pode ser usado como Cliente ou servidor).

b. O certificado tem autenticação de cliente e de servidor. O certificado HTTP só precisa realmente de Autenticação de Servidor, enquanto o certificado C2W requer servidor e cliente).

2. Se você quiser criar um novo certificado para o certificado "**webbridge3 https**", é recomendável que ele seja assinado publicamente (para evitar avisos de certificado no cliente ao usar o aplicativo Web). Esse mesmo certificado pode ser usado para o "certificado webbridge3 c2w", e o certificado deve ter o FQDN dos servidores webbridge em SAN/CN.

3. As CallBridges precisam se comunicar com a nova webbridge3 usando uma porta configurada no comando **webbridge3 c2w listen**. Pode ser qualquer porta disponível, como 449. Os usuários precisam ter certeza de que as callbridges podem se comunicar com webbridge3 nessa porta e ter todas as alterações de firewall feitas antecipadamente, se necessário. Não pode ser a mesma porta usada por "webbridge https" para escutar.

Antes da atualização do CMS para a versão 3.0, é recomendável fazer um backup usando 'backup snapshot <servername_date>' e depois fazer login na página webadmin em seus nós callbridge para remover todas as Configurações XMPP e Configurações Webbridge. Em seguida, conecte-se ao MMP em seus servidores e execute estas etapas em todos os servidores centrais que possuem xmpp e webbridge em uma conexão SSH:

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

Depois de atualizar para a versão 3.0, comece configurando webbridge3 em todos os servidores que executavam webbridge anteriormente. Você deve fazer isso porque já existem registros DNS lá fora que apontam para esses servidores, portanto, dessa forma, você garante que, se um usuário for enviado para um webbridge3, ele estará preparado para lidar com a solicitação.

Configuração Webbridge3 (toda a conexão SSH)

Etapa 1. Configurar a porta de escuta http webbridge3.

Webbridge3 https ouça a:443

Etapa 2. Configurar certificados para webbridge3 para conexões do navegador. Este é o certificado enviado aos navegadores e precisa ser assinado por uma CA (Autoridade de Certificação) pública e que contém o FQDN usado no navegador para que o navegador confie na conexão.

Webbridge3 https certs wb3.key wb3trust.cer (Isso precisa ser uma cadeia de confiança: criar um certificado de confiança que tenha uma entidade final no topo, seguido por CAs Intermediárias em ordem, terminando com 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
```

Etapa 3. Configure a porta a ser usada para escutar as conexões callBridge para webbridge (c2w). Como 443 é usado para a porta de escuta https webbridge3, essa configuração deve ser uma porta disponível diferente, como por exemplo 449.

Webbridge3 c2w ouvir a:449

4. Configure os certificados que o webbridge envia ao callbridge para a confiança do c2w

WebBridge3 c2w certs wb3.key wb3trust.cer

5. Configure o armazenamento confiável que o WB3 usa para confiar no certificado callBridge. Isso precisa ser o mesmo que o certificado usado no pacote de CA callbridge (e deve ser um pacote de certificados intermediários no topo e CA raiz no final, seguido por um único retorno de carro).

Webbridge3 c2w trust rootca.cer

6. Habilitar webbridge3

Webbridge3 enable

```

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

```

Alterações de configuração do CallBridge (toda a conexão SSH)

Etapa 1. Configure a confiança callBridge com o certificado/pacote de CA que assinou o certificado c2w webbridge3.

Callbridge trust c2w rootca.cer

Etapa 2. Reinicie o callBridge para que a nova relação de confiança entre em vigor. Isso descarta todas as chamadas nesse callBridge específico, portanto use-o com cuidado.

reinicialização de Callbridge

Configuração de API para callBridges para conexão com webBridge3

1. Crie um novo objeto do webBridge usando o POST na API e forneça a ele um valor de URL usando o FQDN e a porta configurada na lista branca da interface c2w do webbridge (etapa 3 na configuração do webbridge3)

c2w://webbridge.darmckin.local:449

Neste ponto, o Webbridge3 funciona novamente e você pode ingressar em espaços como convidado ou, se tiver importado usuários anteriormente, eles devem poder entrar.

Permissões de criação de espaço do usuário do aplicativo Web

Seus usuários estão acostumados a criar seus próprios espaços no WebRTC? A partir do CMS 3.0, os usuários do aplicativo Web não podem criar seus próprios coSpaces, a menos que tenham um modelo de cospace atribuído a eles permitindo isso.

Mesmo com um coSpaceTemplate atribuído, isso não cria um espaço para que outras pessoas possam discar (sem URI, sem ID de chamada ou senha), mas se o coSpace tiver um callLegProfile com 'addParticipantAllowed', elas poderão discar do espaço.

Para ter cadeias de caracteres de discagem que possam ser usadas para chamar o novo espaço, coSpaceTemplate deve ter uma configuração de accessMethodTemplate (consulte as notas de

versão 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).

Na API, crie coSpaceTemplate(s) e, em seguida, crie um accessMethodTemplate(s) e atribua o coSpaceTemplate ao ldapUserCoSpaceTemplateSources ou você pode atribuir manualmente um coSpaceTemplate a um usuário em api/v1/users.

Você pode criar e atribuir vários CoSpaceTemplates e accessMethodsTemplates. Consulte o guia da API do CMS para obter mais informações (<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. At the top, the URL `/api/v1/coSpaceTemplates/b03dbf12-c480-487e-b4d8-955e491ff074` is highlighted. 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

Below the table, the configuration form for the CoSpaceTemplate is shown, with fields for name, description, callProfile, callLegProfile, and dialInSecurityProfile. A red arrow points from the URL `/api/v1/coSpaceTemplates/b03dbf12-c480-487e-b4d8-955e491ff074/accessMethodTemplates` (highlighted in yellow) to the configuration form below.

The configuration form for the CoSpaceTemplate includes the following fields:

- name: First CoSpaceTemplate (present)
- description: (empty)
- callProfile: 008e1aa7-0079-4d65-b6ae-fb218bd2e6b4 (Choose - present)
- callLegProfile: ef583b0e-a6fe-49cf-bece-b557332a76bf (Choose - present)
- dialInSecurityProfile: (empty) (Choose)

The configuration form for the AccessMethodTemplates is also shown, with fields for name, uriGenerator, callLegProfile, generateUniqueCallId, and dialInSecurityProfile. A 'Create' button is visible at the bottom.

CoSpaceTemplate (configuração da API)

Nome: Qualquer nome que você queira dar ao coSpaceTemplate.

Descrição: Breve descrição, se desejado.

callProfile: CallProfile branco você deseja que qualquer espaço criado com este modelo use? Se não for fornecido, ele usa o que está definido no nível do sistema/perfil.

calllegProfile: Qual calllegProfile você deseja que os espaços criados com este modelo usem? Se não for fornecido, ele usa o que está definido no nível do sistema/perfil.

dialInSecurityProfile: Qual dialInSecurityProfile você deseja que os espaços criados com este modelo usem? Se não for fornecido, ele usa o que está definido no nível do sistema/perfil.

AccessMethodTemplate (configuração da API)

Nome: Qualquer nome que você queira dar ao coSpaceTemplate.

uriGenerator: A expressão a ser usada para gerar valores URI para este modelo de método de acesso; o conjunto de caracteres permitido é 'a' a 'z', 'A' a 'Z', '0' a '9', '!', '-', '_', e '\$'; se não estiver vazio, ele deverá conter exatamente um caractere '\$'. Exemplo disso é \$.space que usa o nome fornecido pelo usuário ao criar o espaço e anexar ".space" a ele. "Reunião de Equipe" cria a URL 'Team.Meeting.space@domain'.

callLegProfile: Qual callLegProfile você deseja que qualquer accessMethods criado com este modelo use? Se não for fornecido, ele usará o que está definido no nível CoSpaceTemplate e, se não houver nenhum, usará o que está no nível do sistema/perfil.

generateUniqueCallId: Se deve ser gerado um ID numérico exclusivo para este método de acesso que substitui o global para o espaço conjunto.

dialInSecurityProfile: Qual dialInSecurityProfile você deseja que qualquer método de acesso criado com este modelo use? Se não for fornecido, ele usará o que está definido no nível CoSpaceTemplate e, se não houver nenhum, usará o que está no nível do sistema/perfil.

Função de bate-papo

O CMS 3.0 removeu a função de bate-papo persistente, mas no CMS 3.2 o bate-papo não persistente dentro dos espaços retornou. O bate-papo está disponível para usuários de aplicativos Web e não é armazenado em nenhum lugar. Depois que o CMS 3.2 é instalado, os usuários do aplicativo Web são, por padrão, capazes de enviar mensagens uns aos outros durante as reuniões. Essas mensagens estão disponíveis apenas durante a reunião e apenas as mensagens trocadas após o ingresso são vistas. Você não pode ingressar atrasado e rolar de volta para ver as mensagens anteriores.

Chamadas ponto a ponto WebRTC

No CMS 2.9.x, os participantes do WebRTC puderam discar de seus clientes diretamente para outros contatos. A partir do CMS 3.0, isso não é mais possível. Agora os usuários devem entrar e ingressar em um espaço. A partir daí, se eles tiverem permissão no callLegProfile (parâmetro **addParticipants** definido como True), eles poderão adicionar outros contatos. Isso faz com que o CMS disque para o participante e eles se reúnem em um espaço no CMS.

Alterações notáveis nas configurações do webBridge

O CMS 3.0 e 3.1 removeu ou realocou algumas das configurações de webbridge da GUI e elas precisam ser configuradas na API para manter a experiência consistente para os usuários. No 3.x, use **api/v1/webBridges** e **api/v1/webBridgeProfiles**.

Verifique o que você configurou atualmente para que, ao atualizar para a versão 3.0, você possa configurar os Perfis webbridge e webbridge na API adequadamente.

The image displays three sequential screenshots of a configuration interface, illustrating the removal of certain settings over time:

- CMS 2.9.x:** Shows a '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). Below this is an 'IVR' section with 'IVR numeric ID' (7772) and 'Joining scheduled Lync conferences by ID' (not allowed). An 'External access' section includes 'Web Bridge URI' (https://14.49.25.94) and 'IVR telephone number'. A 'Submit' button is at the bottom.
- CMS 3.0:** The 'Web bridge settings' section is absent. The 'IVR' section remains. The 'External access' section is still present, with the same 'Web Bridge URI' and an empty 'IVR telephone number' field. A 'Submit' button is at the bottom.
- CMS 3.1:** Both the 'Web bridge settings' and 'External access' sections are removed. Only the 'Lync Edge settings' (Server address, Username, Number of registrations) and the 'IVR' section (IVR numeric ID: 7772, Joining scheduled Lync conferences by ID: not allowed) remain. A 'Submit' button is at the bottom.

No 3.0, as configurações de Web bridge foram removidas na GUI e, em seguida, no CMS 3.1, os campos Acesso externo também foram removidos.

Configurações de Web Bridge na GUI

- **URI do cliente da conta de convidado** - usado pelo callBridge para localizar o webBridge. Se você tiver várias webBridges em sua implantação para WebRTC, esse campo já deverá estar em branco e você deverá ter URLs exclusivas em api/v1/webbridges para cada webBridge ao qual a callBridge precisa se conectar. Exclua qualquer coisa nesse campo e certifique-se de que você tenha as webBridges configuradas na API.
- **Domínio Jid da Conta de Convidado** - não é mais usado no CMS 3.0 e você pode excluí-lo.
- **Acesso de convidado via ID e senha** - removido e não substituído no CMS 3.0.
- **Acesso de convidado através de hiperlinks** - agora configurável em webBridgeProfiles na API na configuração "AllowSecrets".

The image shows two screenshots of the CMS interface for the endpoint `/api/v1/webBridges`. The top screenshot, labeled "CMS 2.9.x", displays a form with the following fields: `url` (checkbox and text input), `resourceArchive` (checkbox and text input), `tenant` (checkbox and text input with "Choose" button), `tenantGroup` (checkbox and text input with "Choose" button), `idEntryMode` (checkbox and dropdown menu), `allowWeblinkAccess` (checkbox and dropdown menu), `showSignIn` (checkbox and dropdown menu), `resolveCoSpaceCallIds` (checkbox and dropdown menu), `resolveLyncConferenceIds` (checkbox and dropdown menu), `callBridge` (checkbox and text input with "Choose" button), and `callBridgeGroup` (checkbox and text input with "Choose" button). A "Create" button is at the bottom. The bottom screenshot, labeled "CMS 3.0", shows a simplified form with fields: `url` (checkbox and text input), `tenant` (checkbox and text input with "Choose" button), `tenantGroup` (checkbox and text input with "Choose" button), `callBridge` (checkbox and text input with "Choose" button), `callBridgeGroup` (checkbox and text input with "Choose" button), and `webBridgeProfile` (checkbox and text input with "Choose" button). A "Create" button is at the bottom.

Observe que no CMS 3.0, vários campos foram removidos de `/api/v1/webBridges`.

- **resourceArchive** - agora em `webbridgeProfiles`.
- **idEntryMode** - agora preterido.
- **allowWeblinkAccess** - agora em `webBridgeProfiles` como `allowSecrets`.
- **showSign** - agora em `webBridgeProfiles` como `userPortalEnabled`.
- **resolveCoSpaceCallIds** - agora em `webbridgeProfiles`.
- **resolveLyncConferenceIDs** - agora em `webbridgeProfiles`.

The image shows a screenshot of the CMS interface for the endpoint `/api/v1/webBridgeProfiles`. The form includes the following fields: `name` (checkbox and text input), `resourceArchive` (checkbox and text input), `allowPasscodes` (checkbox and dropdown menu), `allowSecrets` (checkbox and dropdown menu), `userPortalEnabled` (checkbox and dropdown menu), `allowUnauthenticatedGuests` (checkbox and dropdown menu), `resolveCoSpaceCallIds` (checkbox and dropdown menu), and `resolveCoSpaceUris` (checkbox and dropdown menu). A "Create" button is at the bottom. The interface is labeled "CMS 3.0 onward".

WebBridgeProfile

- **resourceArchive** - se você usar planos de fundo personalizados e seu arquivo de recursos estiver armazenado em um servidor da Web, digite o URL aqui.
- **allowPasscodes** - se for falso, os usuários não terão uma opção para ingressar em reuniões como convidados. Eles só podem entrar ou usar uma URL que contenha as informações e o segredo do espaço
- **allowSecrets** - Se for definido como false, os usuários não poderão ingressar em espaços usando uma URL como https://meet.company.com/meeting/040478?secret=gPDnucF8is4W1cS87_l.zw. Os usuários

precisam usar <https://meet.company.com> e digitar a ID da chamada/ID da reunião/URI e PIN/Senha, se houver um configurado.

- **userPortalEnabled** - se estiver definido como false, a página inicial do portal do aplicativo Web não mostrará a opção de entrada. Ele exibe apenas os campos para inserir a ID da chamada/ID da reunião/URI e PIN/Senha, se houver um configurado.
- **allowUnauthenticatedGuest** - se definido como False, os convidados não poderão ingressar em nenhuma reunião - mesmo com a URL completa que contém a ID e o segredo da reunião. Quando Falso, somente os usuários que podem entrar podem ingressar em uma reunião. Exemplo. O Usuário2 está tentando usar a URL para a reunião do Usuário1. Após digitar a URL, o Usuário2 deve entrar para continuar na reunião do Usuário1.
- **resolveCoSpaceCallIds** - se definido como False, os convidados só poderão ingressar em reuniões inserindo o URI e o PIN/Senha, se usados. ID de chamada/ID de reunião/ID numérica não são aceitos.
- **resolveCoSpaceUris** - 3 configurações possíveis: desligado, domainSuggestionDisabled e domainSuggestionEnabled. Se este webBridge aceita ou não URIs SIP coSpace e coSpace accessMethod com a finalidade de permitir que os visitantes participem de reuniões do cospace.

- Quando definido como *'off'*, a associação por URI é desabilitada.

- Quando definido como *'domainSuggestionDisabled'*, a associação por URI é habilitada, mas o domínio do URI não é preenchido automaticamente ou verificado em webBridges usando esse webBridgeProfile.

- Quando definido como *'domainSuggestionEnabled'*, a associação por URI é habilitada e o domínio do URI pode ser preenchido automaticamente e verificado em webBridges usando esse webBridgeProfile.

Seção Acesso Externo removida da GUI Web

No CMS 3.1, a seção Acesso externo foi removida da GUI da Web. Se você os tiver configurado antes da atualização, será necessário reconfigurá-los na API em webbridgeProfiles.



External access

Web Bridge URI

IVR telephone number

Primeiro, você precisa criar um webbridgeProfile como descrito na seção anterior. Depois de criar um webbridgeProfile, você pode criar um Número IVR e/ou um URI de Web Bridge através dos links disponíveis na API sob o webBridgeProfile recém-criado.

[« 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>

Você pode criar até 32 números IVR ou 32 endereços webbridge por perfil de webBridge

Gravação ou transmissão

O gravador e o componente de streaming no CMS 2.9.x e anterior eram clientes XMPP, e a partir do CMS 3.0, eles são baseados em SIP. Isso agora permite que os layouts para gravações e streaming sejam alterados usando o layout padrão na API. Além disso, agora os rótulos de nome são mostrados na sessão de gravação/streaming. Consulte as notas de versão do CMS 3.0 para obter mais informações sobre os recursos de gravação/streaming -

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.

Se você tiver o gravador ou o streaming configurado no 2.9.x, será necessário redefinir as configurações no MMP e na API para que elas continuem a funcionar após a atualização.

Antes da atualização do CMS para 3.0, é recomendável fazer um backup usando 'backup snapshot <servername_date>' e depois fazer login na página webadmin em seus nós callbridge para remover todas as configurações XMPP. Em seguida, conecte-se ao MMP em seus servidores e execute estas etapas em todos os servidores centrais que possuem xmpp em uma conexão SSH:

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

Gravador

MMP

As figuras mostram um exemplo das configurações vistas no CMS 2.9.1 quando o gravador foi configurado e como ele se parece imediatamente após a atualização para 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>
```

CMS 2.9.x

CMS 3.x

Após a atualização, você deverá reconfigurar o gravador:

Etapa 1. Configurar a interface de escuta SIP.

gravador sip escutar um 5060 5061 (A interface e as portas que o gravador SIP está configurado para escutar para TCP e TLS, respectivamente. Se não quiser usar TLS, você pode usar '**recorder sip listen a 5060 none**')

Etapa 2. Configurar os certificados que o gravador usará se você estiver usando uma conexão TLS.

recorder sip certs <key-file> <cert-file> [cert-bundle] (Sem esses certificados, o serviço tls não inicia no gravador. O gravador usa o pacote crt para verificar o certificado callBridge.)

Etapa 3. Configurar o limite de chamadas.

limite do gravador <0-500|nenhum> (Define o limite para o número de gravações simultâneas que o servidor pode servir. Esta tabela está em nossa documentação e o limite do gravador deve estar alinhado com os recursos no servidor.)

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

Em `api/v1/callProfiles`, você precisa configurar o `sipRecorderUri`. Este é o URI que o callBridge disca quando precisa iniciar uma gravação. O domínio deste URI precisa ser adicionado à sua tabela de regras de saída e apontar para o gravador (ou controle de chamadas) como o Proxy SIP a ser Usado.

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

Esta figura mostra uma discagem direta para o componente gravador nas regras de saída encontradas em **Configuração > Chamadas de Saída**.

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

Esta figura mostra uma chamada para o componente gravador através de um controle de chamada (como por exemplo, 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

Note: Se você configurou o gravador para usar TLS SIP e se as chamadas estiverem falhando, verifique o nó callBridge no MMP para ver se a verificação SIP TLS está habilitada. O comando MMP é `'tls sip'`. As chamadas podem falhar porque o certificado do gravador não é confiável para callBridge. Você pode testar isso desabilitando isso no callBridge usando `'tls sip verify disable'`.

Vários gravadores?

Configure cada um como explicado e ajuste suas regras de saída de acordo. Se você usar um método direto para o gravador, altere a regra de saída para o gravador existente para o comportamento "Continuar" e adicione uma nova regra de saída abaixo da anterior com prioridade um menor que a primeira. Quando o primeiro gravador tiver atingido seu limite de chamada, ele enviará um 488 Unaccept aqui para callBridge, e o callBridge passa para a próxima regra.

Se quiser fazer o balanceamento de carga dos gravadores, use um controle de chamadas e ajuste o roteamento do controle de chamadas para que ele possa fazer chamadas para vários gravadores.

Streamer

MMP

Após a atualização de 2.9.x para 3.0, você precisa reconfigurar o streamer.

Etapa 1. Configurar a interface de escuta SIP.

streamer sip listen a 6000 6001 (A interface e as portas que o streamer SIP está configurado para ouvir TCP e TLS, respectivamente. Se não quiser usar TLS, você pode usar '**streamer sip listen a 6000 none**')

Etapa 2. Configurar os certificados que o transmissor usará se você estiver usando uma conexão TLS.

streamer sip certs <key-file> <cert-file> [crt-bundle] (Sem esses certificados, o serviço tls não inicia no streamer. O otimizador usa o pacote crt para verificar o certificado callBridge.)

Etapa 3. Configurar o limite de chamadas

limite do otimizador <0-500|nenhum> (Define o limite para o número de fluxos simultâneos que o servidor pode servir. Esta tabela está em nossa documentação e o limite do otimizador deve estar alinhado com os recursos no servidor.)

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

Em `/api/v1/callProfiles`, você precisa configurar o `sipStreamUri`. Este é o URI que o callBridge disca quando precisa iniciar o streaming. O domínio deste URI precisa ser adicionado à sua tabela de regras de saída e apontar para o dinamizador (ou controle de chamadas) como o Proxy SIP a ser Usado.

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

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

Table view XML view

Object configuration	
streamingMode	automatic
sipStreamerUri	stream@streamer.com

Esta figura mostra uma discagem direta para o componente de streaming nas regras de saída encontradas em **Configuração > Chamadas de Saída**.

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	14.49.17.246:6000		<use local contact domain>	Standard SIP	Stop	0	Auto
<input type="checkbox"/>					Standard SIP	Stop	0	Auto

Esta figura mostra uma chamada para o componente gravador através de um controle de chamada (como por exemplo, Cisco Unified Communications Manager (CUCM) ou 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 'Local from domain' column. The text 'CUCM' is written in blue above the first two rows. The text 'Expressway' is written in red above the last two rows.

Note: Se você configurou o otimizador para usar TLS SIP e se as chamadas estiverem falhando, verifique o nó callBridge no MMP para ver se a verificação SIP TLS está habilitada. O comando MMP é 'tls sip'. As chamadas podem falhar porque o certificado do transmissor não é confiável para callBridge. Você pode testar isso desabilitando isso no callBridge usando 'tls sip verify disable'.

Vários Streamers?

Configure cada um como explicado e ajuste suas regras de saída de acordo. Se você usar um método de fluxo direto para fluxo, altere a regra de saída para gravador existente para o comportamento "Continuar" e adicione uma nova regra de saída abaixo da anterior com a prioridade um a menos que a primeira. Quando o primeiro streamer atinge seu limite de chamada, ele envia um 488 Inaceitável aqui de volta para callBridge, e o callBridge passa para a próxima regra.

Se quiser fazer o balanceamento de carga dos fluxos, use um controle de chamadas e ajuste o roteamento do controle de chamadas para que ele possa fazer chamadas para vários fluxos.

Consideração do Expressway

Se você usa o Cisco Expressway para Web Proxy, deve garantir que seu Expressway está executando pelo menos X12.6 antes da atualização do CMS. Isso é exigido pelo CMS 3.0 para que o proxy da Web funcione e seja suportado.

A capacidade dos participantes do aplicativo Web aumentou em relação ao Expressways quando usado com o CMS 3.0. Para um OVA Expressway grande, a capacidade esperada é de 150 chamadas Full HD (1080p30) ou 200 chamadas de outro tipo (por exemplo, 720p30). Você pode aumentar essa capacidade agrupando Expressways, até 6 nós (onde 4 é usado para dimensionamento e 2 para redundância, portanto, até um máximo de 600 chamadas Full HD ou 800 chamadas de outros tipos).

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

O CMS Edge é reintroduzido no CMS 3.1, pois oferece capacidades maiores do que o Expressway para sessões de aplicativos Web externos. Há duas configurações recomendadas.

Especificações de borda pequena

4 GB de RAM, 4 vCPUs, interface de rede de **1 Gbps**

Essa especificação VM Edge tem potência suficiente para cobrir uma única capacidade de carga de áudio e vídeo do CMS1000, que é de 48 x 1080p, 96 x 720p, 192 x 480p e 1000 chamadas de áudio.

Para a implantação, é recomendável ter 1 servidor de borda pequeno por CMS1000 ou 4 servidores de borda pequeno por CMS2000.

Especificações de borda grande

8 GB de RAM, 16 vCPUs, interface de rede de **10 Gbps**

Essa especificação VM Edge tem potência suficiente para cobrir uma única capacidade de áudio e vídeo do CMS2000, que é de 350 x 1080p, 700 x 720p, 1000 x 480p e 3000 x chamadas de áudio.

Para a implantação, é recomendável ter 1 servidor de borda grande por CMS2000 ou por 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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.