

# CMS/Acano Call Bridge でのレコーダーの設定

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[導入](#)

[サポートされる展開](#)

[その他のセットアップ](#)

[設定](#)

[ステップ1:Windows ServerでNFS共有フォルダを設定する](#)

[ステップ2 : レコーダサーバでレコーダを設定し、有効にします](#)

[ステップ3:CBでAPIユーザを作成する](#)

[ステップ4:APIを使用してレコーダをCBに追加する](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

## 概要

このドキュメントでは、Cisco Meeting Server(CMS)のCall Bridge(CB)コンポーネントでレコーダを設定するために必要な設定手順について説明します。

## 前提条件

### 要件

このドキュメントに特有の要件はありません。

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CMS 1.9以降
- Google Chrome からの Postman
- CMS アプリケーション プログラミング インターフェイス (API)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 ( デフォルト ) 設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

# 背景説明

CMS Recorderは、CMS (旧Acano) サーバのリリース1.9から入手できます。レコーダは、会議を記録し、ネットワークファイルシステム(NFS)ドキュメントストレージに記録を保存する機能を提供します。

レコーダはExtensible Messaging and Presence Protocol(XMPP)クライアントのように動作するため、Call BridgeをホストするサーバでXMPPサーバを有効にする必要があります。

レコーダライセンスが必要であり、レコーダサーバではなくCallBridgeコンポーネントに適用する必要があります。

ネットワークファイルシステム(NFS)ディレクトリが必要で、Windows ServerまたはLinuxでセットアップできます。

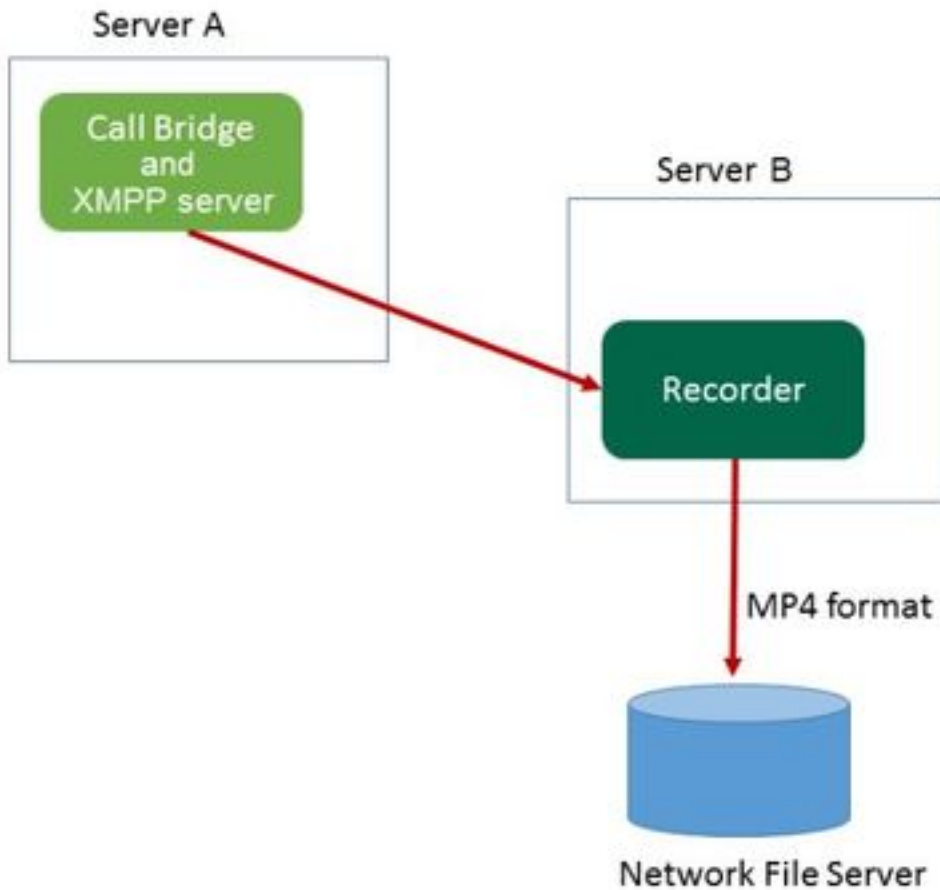
- Windows Serverの場合は、Windows上でネットワークファイルシステムを[展開](#)します
- Linuxの場合は、Linuxにネットワークファイルシステムを[展開](#)します

注：Windows Server 2008 R2で稼働するNFSには、権限の問題に対するホットフィックス[があります](#)。

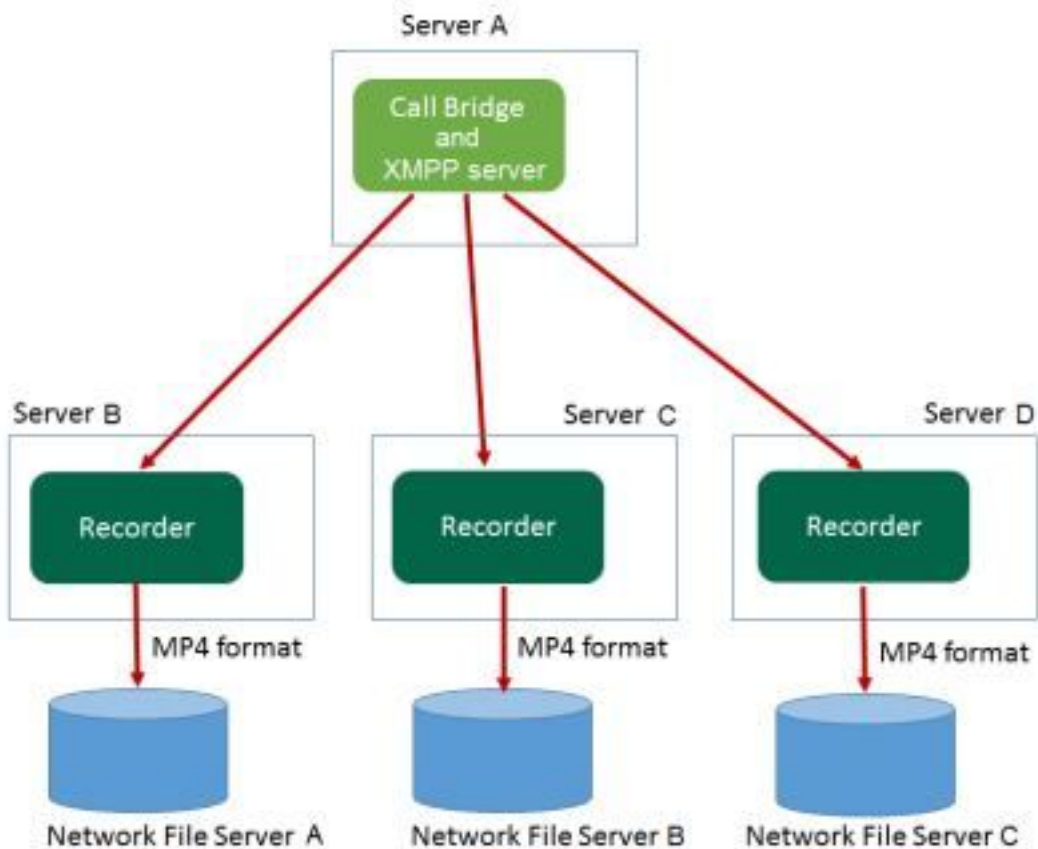
# 導入

## サポートされる展開

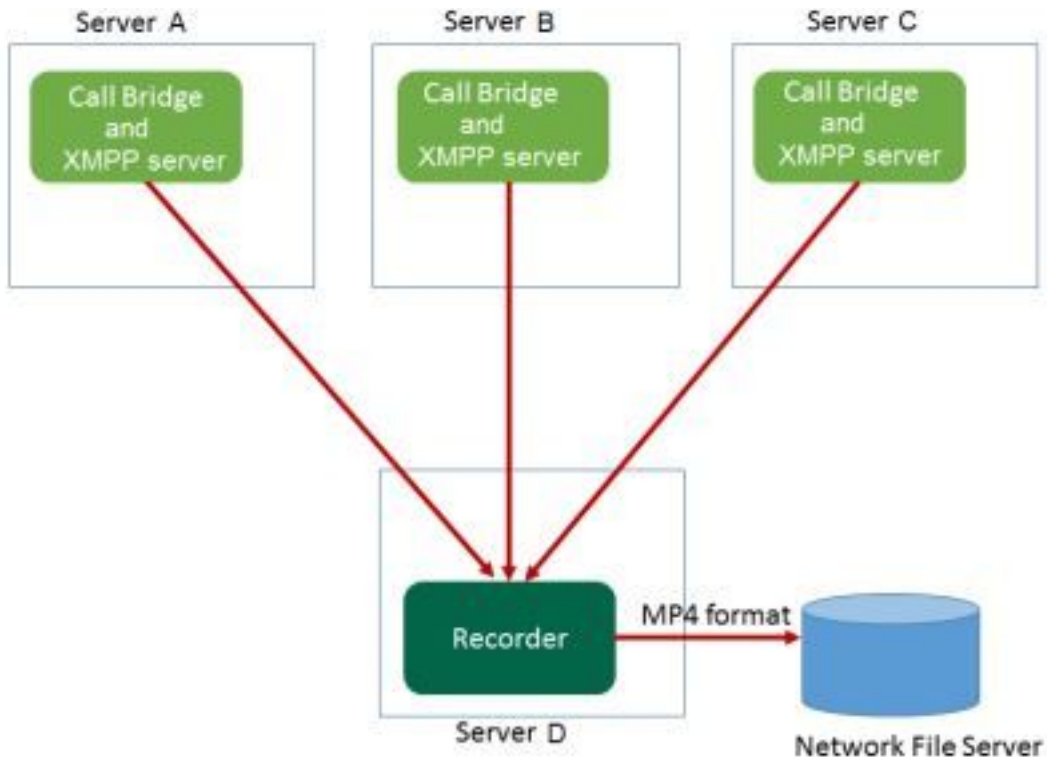
1.次の図に示すように、レコーダは、CBをホストするサーバに対してリモートのCMS/Acanoサーバでホストされている必要があります



2.レコーダーの冗長展開もサポートされています。冗長性が設定されている場合、録音はすべての録音デバイス（サーバ）間で負荷分散されます。これは、次の図に示すように、すべてのCBが使用可能なすべてのレコーダーを使用することを意味します

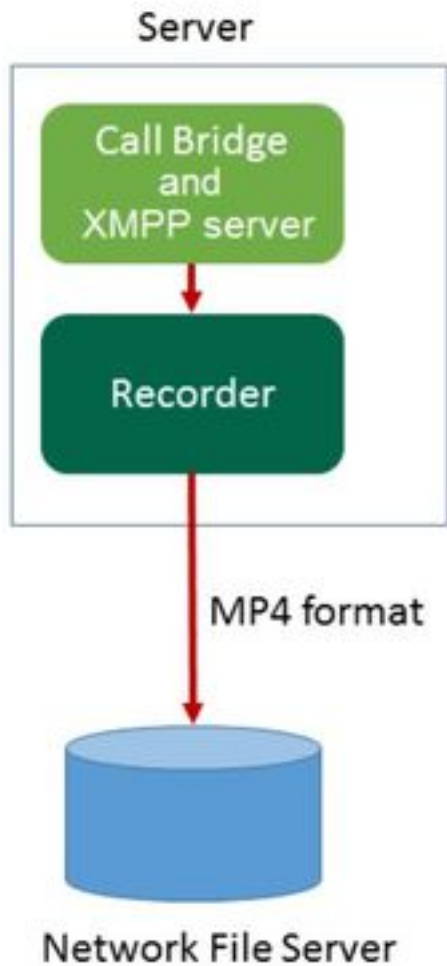


3.複数のCBが存在する場合は、逆も同様です。すべてのCBノードは、次の図に示すように、使用可能なレコーダを使用します



### その他のセットアップ

レコーダはCBと同じサーバ上でホストすることもできますが、これはテストまたは非常に小規模な導入にのみ使用する必要があります。詳細については、次の図を参照してください。ここでの欠点は、同時録音が1～2個しかないということです。



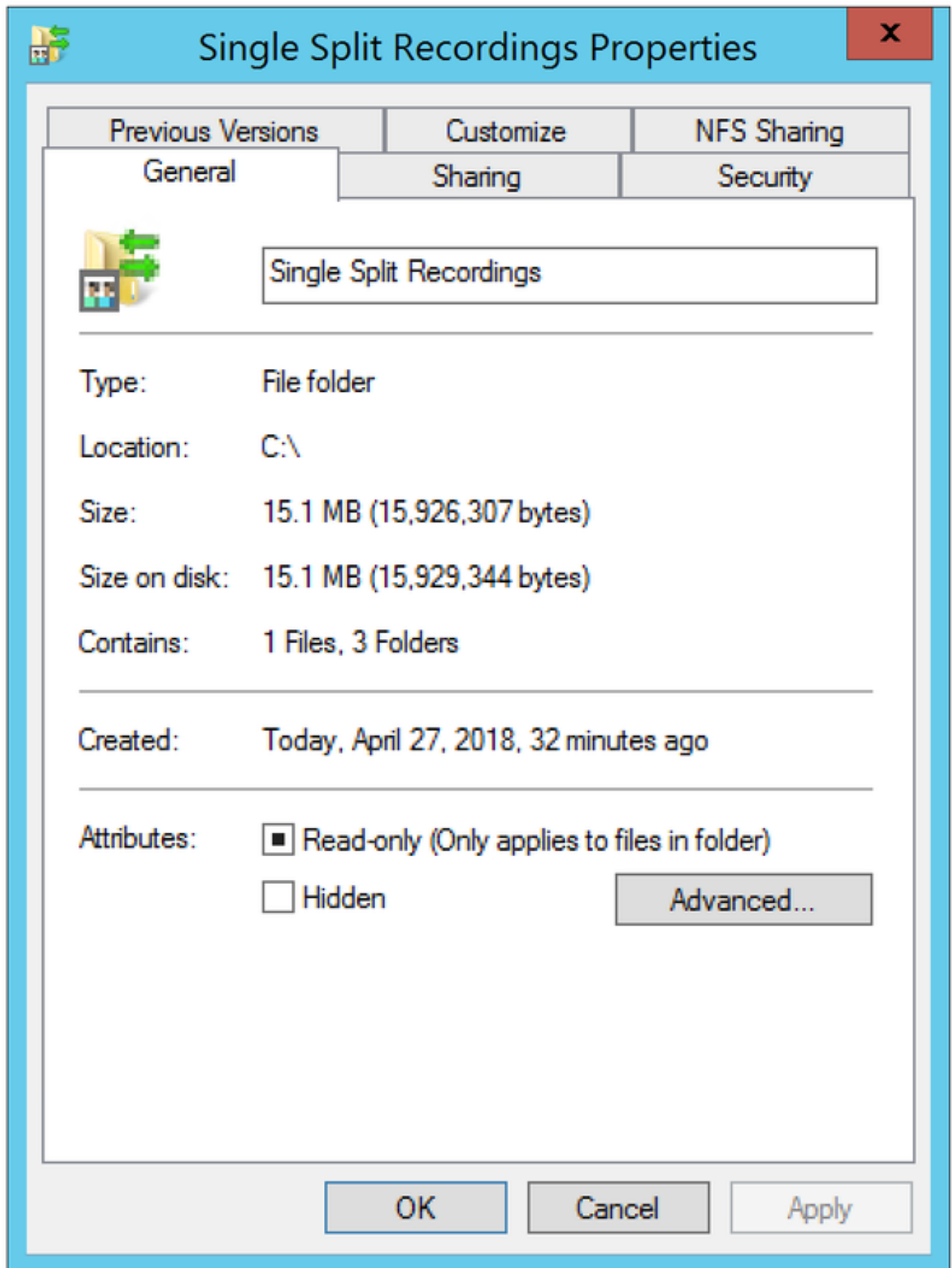
## 設定

### 1:Windows ServerNFS

#### a.WindowsNFSSingle Split Recordings

Name	Date modified	Type	Size
ExchangeSetupLogs	9/6/2017 2:48 PM	File folder	
inetpub	5/30/2017 6:34 PM	File folder	
PerfLogs	8/22/2013 10:52 AM	File folder	
Program Files	10/11/2017 6:33 PM	File folder	
Program Files (x86)	1/3/2018 2:04 PM	File folder	
root	9/6/2017 2:37 PM	File folder	
Shares	4/26/2018 3:50 PM	File folder	
Single Split Recordings	4/27/2018 10:37 AM	File folder	
Users	6/2/2017 3:13 PM	File folder	
Windows	4/21/2018 7:31 AM	File folder	
BitlockerActiveMonitoringLogs	9/6/2017 5:43 PM	File	1 KB

#### b. Properties



c. 右上の[NFS Sharing]

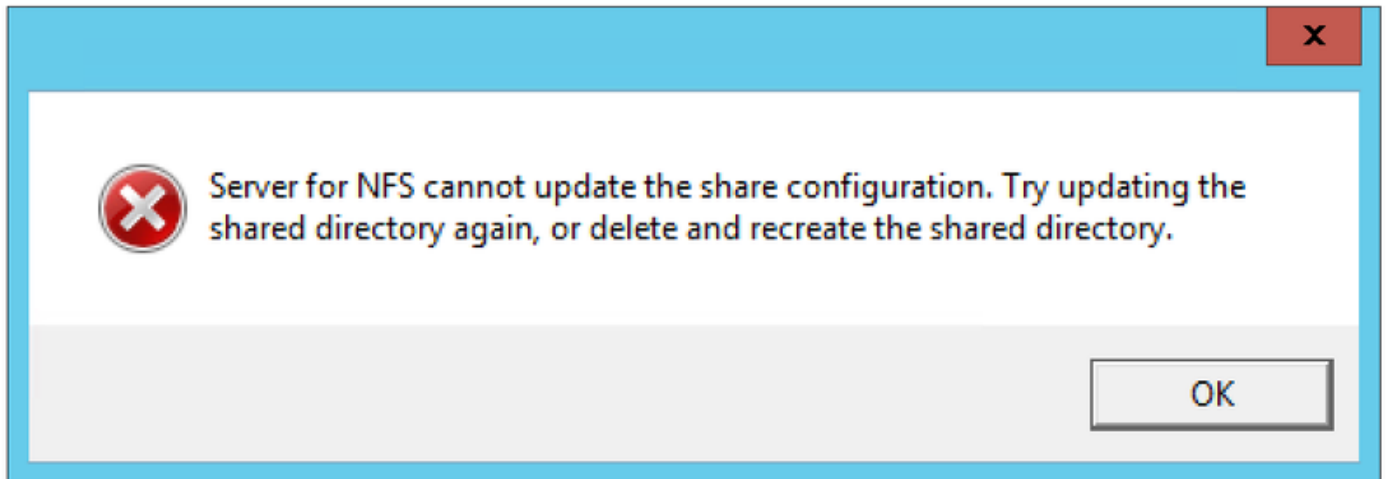
d. NFS

e. Share this folder

f.

注：これは、NFSクライアントとCMSレコーダがこのフォルダを見つけるために使用します。

注：フォルダの共有名にスペースがないことを確認します。存在する場合、変更を保存できず、次のエラーメッセージが表示されます。



g. ANSI

h. Kerberos No server authentication [Auth\_SYS]

Kerberos v5 privacy and authentication [Krb5p]  
 Kerberos v5 integrity and authentication [Krb5i]  
 Kerberos v5 authentication [Krb5]  
 No server authentication [Auth\_SYS]  
 Enable unmapped user access  
     Allow unmapped user Unix access (by UID/GID)  
     Allow anonymous access  
    Anonymous UID:   
    Anonymous GID:

i. Allow unmapped user Unix access (by UID/GID)

j.

注：すべてのマシンのデフォルトは読み取り専用です。レコーダには読み取り/書き込みアクセス権が必要です。これにより、すべてのマシンのデフォルトを変更したり、レコーダに特定のルールを追加したりできます。ベストプラクティスは、すべてのマシンへのアクセス

を無効にすることです。これをNo Accessに変更し、共有へのアクセスが必要なサーバのIPに新しい権限を追加します。

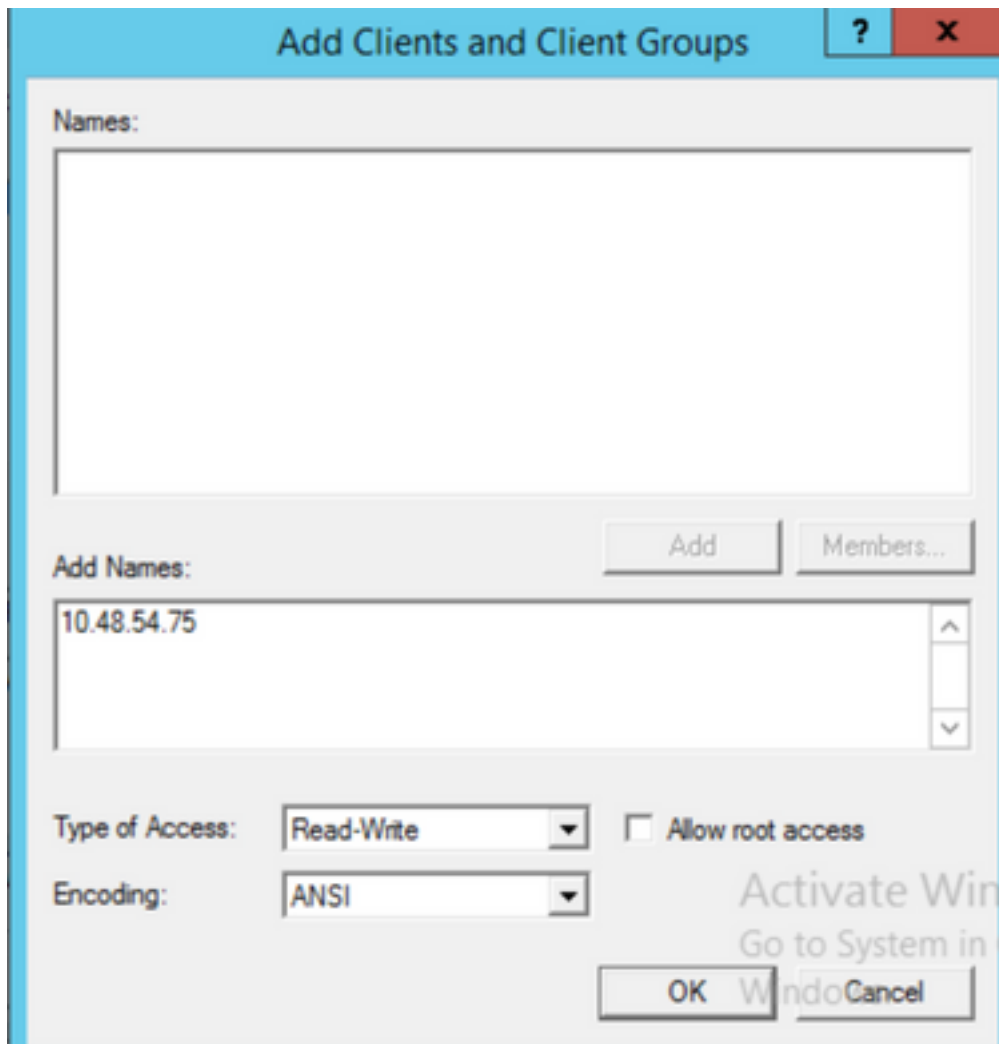
k.

l. IP 10.48.54.75

m. access

n ANSI

o.



p. [OK]

q.

r.Change

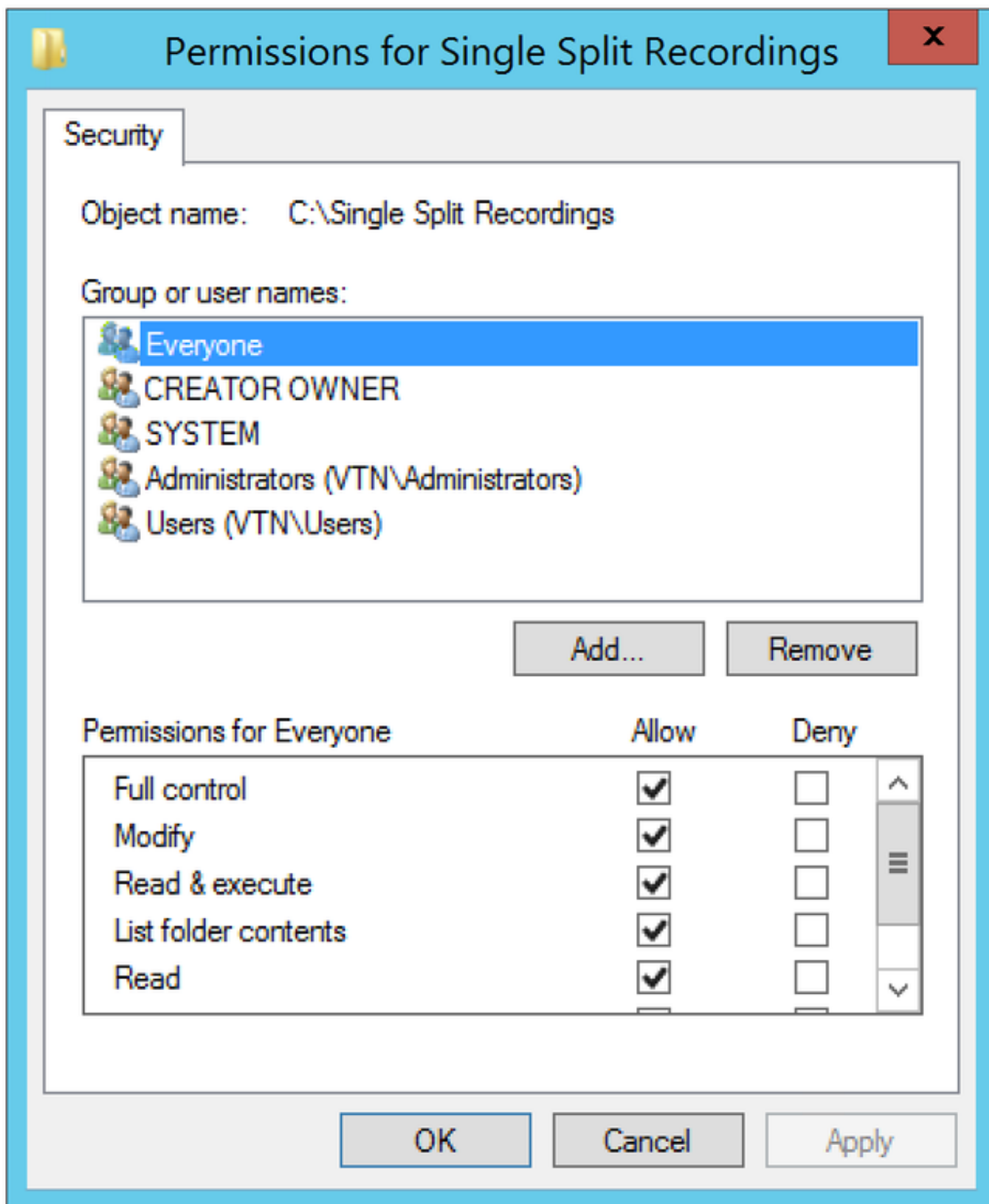
OK Permissions

t. OK []

u.



注：Everyoneグループには、フォルダへのフルアクセス権が必要です。リストにない場合は、[編集]を選択して権限エディタを開きます。ユーザーを追加するには[追加]を選択し、[名前]フィールドにEveryoneと入力して[OK]を選択します。リストの[全員]を選択し、[フルコントロール]のチェックボックスをオンにし、[OK]を選択します。[OK]を再び選択して、プロパティを閉じます。正しく設定されている場合、次の図のようになります。



ステップ2：レコーダサーバでレコーダを設定し、有効にします

a.次のコマンドを使用して、指定したインターフェイスでレコーダーがリスンするように構成します。

```
recorder listen <interface[:port] whitelist>
```

b.レコーダーがローカル CB にある場合は、インターフェイスを「ループバック」に設定する必要がありますので、次のコマンドを使用します。

```
recorder listen lo:8443
```

c.特定のインターフェイスでリスンする場合は、「a」と言って、次を使用します。

```
recorder listen a:8443
```

注：クラスタ化されたCBのノードでレコーダを設定する場合、そのインターフェイスは、レコーダが設定されているノードのローカルリスニングインターフェイスである必要があります。

d.レコーダーで使用する証明書ファイルを設定します。たとえば、すでに存在する証明書と CB によって使用される秘密キー ファイルを使用することができます。

```
recorder certs <keyfile> <certificate file>
```

e.次のコマンドを使用して、CB 証明書をレコーダー信頼ストアに追加します。

```
recorder trust <crt-bundle>
```

crt-bundleには、CBで使用される証明書が異なる場合は含まれている必要があります。クラスタ内にある場合は、クラスタ内のすべての CB の証明書が含まれている必要があります。

f.NFS のホスト名または IP アドレス、および NFS 上の録音を保存するディレクトリを指定します。

```
recorder nfs <hostname/IP>:<directory>
```

注：レコーダーは NFS に認証されませんが、レコーダー サーバには NFS ディレクトリに対する読み取り/書き込みアクセス権があることが重要です。

g.次のコマンドを使用して、レコーダーを有効にします。

```
recorder enable
```

### ステップ3:CBでAPIユーザを作成する

CB 上に API ユーザを作成します。これは、API 関数を使用した追加の設定に必要です。

次の手順を使用してユーザを作成します。

a. 管理者クレデンシャルを使用して、セキュア シェル (SSH) またはコンソール経由で CB に接続します。

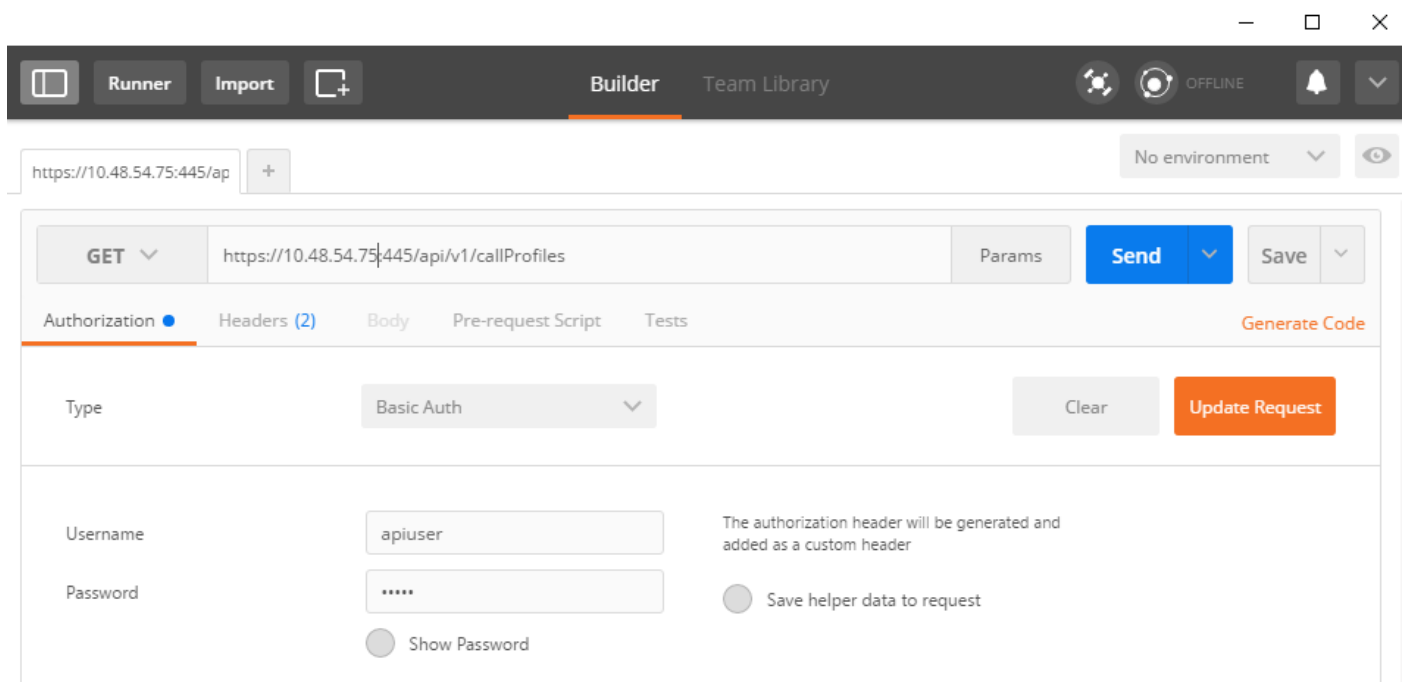
b. ユーザの <username> api を追加し、Return キーを押してパスワードを入力し、Return キーを押します。

## ステップ4:APIを使用してレコーダをCBに追加する

1. ここからPostmanをダウンロードしてインストールする

2. アドレスバーにAPIアクセスURLを入力します。例

: [https://<Callbridge\\_IP>:445/api/v1/<entity>](https://<Callbridge_IP>:445/api/v1/<entity>)。次に、認証、ステップ3のユーザ名とパスワードを設定し、タイプとして[Authorization]の[Basic Auth]に設定します



注：これは、CB に現在設定されているレコーダーまたは callProfile がないことを前提としています。それ以外の場合は、PUT 方式を使用して、存在するレコーダーや callProfile を変更できます。

を選択します。 APIを使用してレコーダをCBに追加します

a. [https://<Callbridge\\_IP>:445/api/v1/recorders](https://<Callbridge_IP>:445/api/v1/recorders) を使用して空の POST を送信します。

b. ( a ) と同じ URL を使用して GET を送信し、レコーダー ID を引用符なしでメモ帳にコピーします。

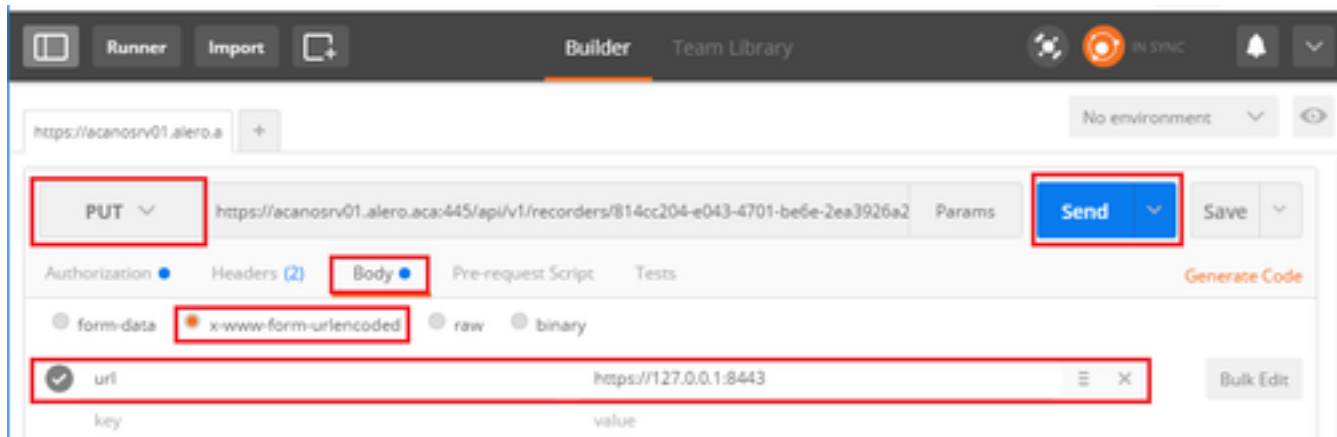
c. PUTを実行する前に、[https://<Callbridge\\_IP>:445/api/v1/recorders/<recorderid>](https://<Callbridge_IP>:445/api/v1/recorders/<recorderid>)でPUTを送信し、これをBODYに追加して、レコーダのURLを設定します。

url=<https://127.0.0.1:8443> (レコーダーがローカル CB にある場合)

または


url=https://<IP Address of recorder>:8443 (レコーダーがローカル CB にない場合)

以下に、いくつかの例を示します。



注 : dtmfProfile、callProfile および callLegProfile は、cospace 電話会議に参加する SIP エンドポイントにとって特に重要です。これにより、エンドポイントは cospace 発着のコールの録音を開始/停止できるようになります。

CMA 1.9.3およびCMS 2.0.1と同様に、DTMFトーンは不要です。ここでは、

 ボタンをクリックします。 CMS 2.3からWebRTCにもレコードボタンが追加されました。

#### 4. callProfileの作成

a. [https://<Callbridge\\_IP>:445/api/v1/callProfiles](https://<Callbridge_IP>:445/api/v1/callProfiles) を使用して空の POST を送信します。

b. ( a ) と同じ URL を使用して GET を送信し、callProfile ID を引用符なしでメモ帳にコピーします。

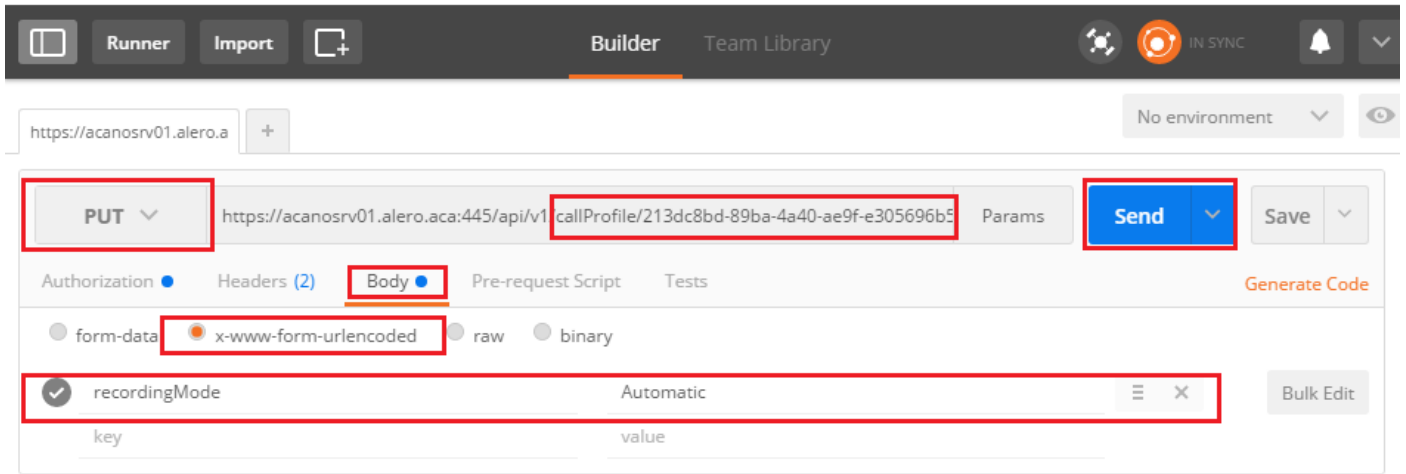
c. PUTを実行する前に、[https://<Callbridge\\_IP>:445/api/v1/callProfiles/<call profile ID>](https://<Callbridge_IP>:445/api/v1/callProfiles/<call profile ID>)を使用してPUTを送信し、callProfileのrecordingModeを設定します。

recordingMode=Manual ( 発信者に DTMF エントリを使用して録音を開始させたい場合 )

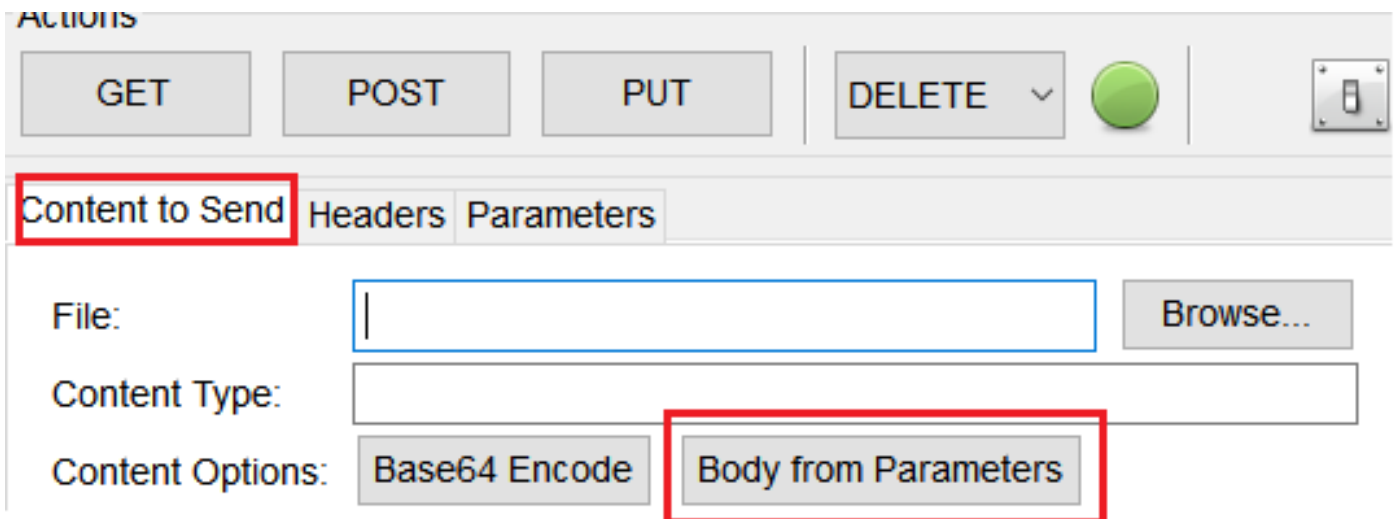
または

recordingMode=Automatic ( コールの開始時に自動的に録音を開始する場合 )

以下に、いくつかの例を示します。



注：FirefoxからPOSTERを使用する場合は、[送信するコンテンツ]を選択して、PUT/POSTを送信する前にBody from Parametersを選択する必要があります。これにより、CBが理解できるコードにコンパイルされます。次の図のように：



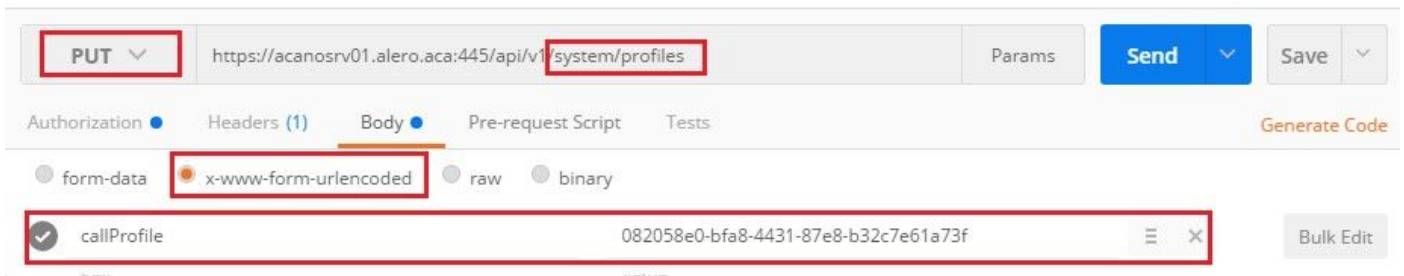
## 5. システムプロファイルへのコールプロファイルの追加

callProfileにより、通話の録音が可能かどうか、また録音にユーザの介入が必要かどうか定義されます。

callProfileをBODYに追加した後、<https://<Callbridge IP>:445/api/v1/system/profiles>を使用してPUTを送信します。

callProfile=<call profile ID>

以下に、いくつかの例を示します。

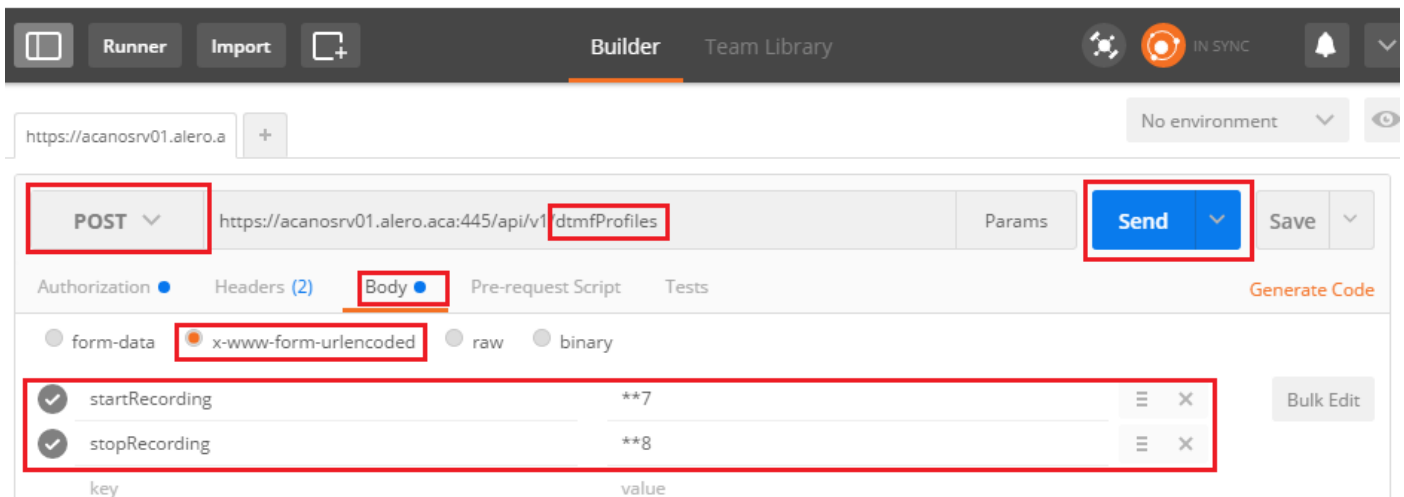


recordingMode が [Manual] に設定されている場合は、ユーザが DTMF トーンを使用して録音を開始および停止する方法を定義する DTMF プロファイルを設定する必要があります。

## 6. DTMFプロファイルの作成

a.startRecording=**\*\*7** および stopRecording=**\*\*8** (例) を startRecording=**\*\*7**&stopRecording=**\*\*8** として BODY に設定した後で、<https://<Callbridge IP>:445/api/v1/dtmfProfiles> を使用して Post を送信します。

例：



b.GET を送信して新しい DTMF プロファイルを表示し、引用符なしで ID をメモ帳にコピーします。

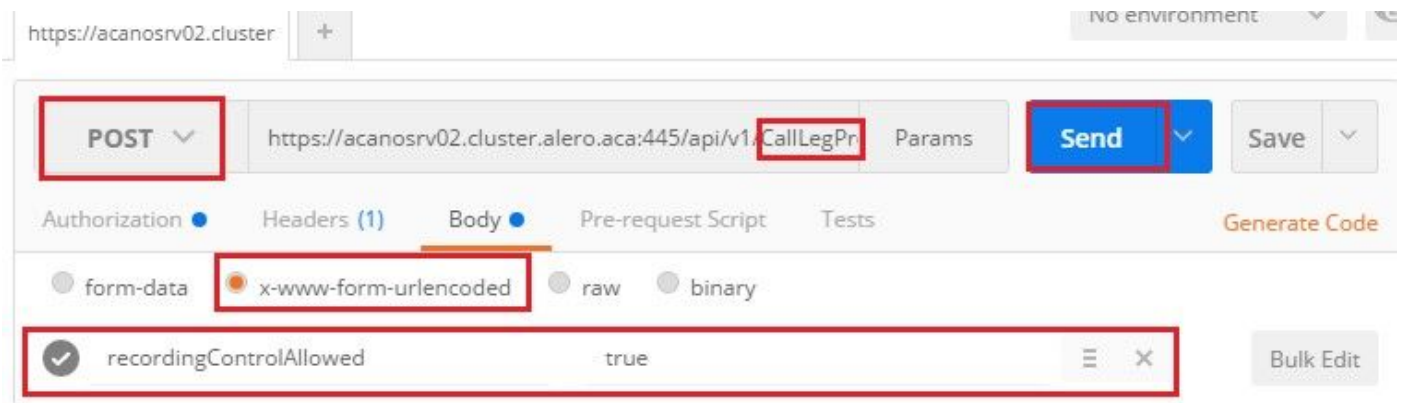
## 7. CallLegプロファイルの作成

CallLegProfiles は通話の動作を決定します。このケースでは、通話の録音が可能かどうかを判定します。

次のようにコール レッグ プロファイルを作成します。

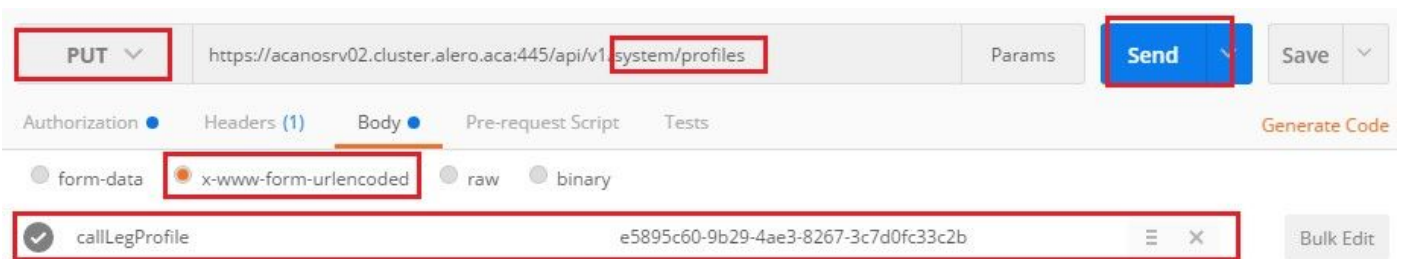
a.recordingControlAllowed=true を BODY に追加した後で、<https://<Callbridge IP>:445/api/v1/CallLegProfiles> を使用して Post を送信します。

以下に、いくつかの例を示します。



b. <https://<Callbridge IP>:445/api/v1/system/profiles> を使用してPUTを送信し、callLegProfile=<callLegProfile\_ID>をBODYに追加して、CallLegProfileを適用します。

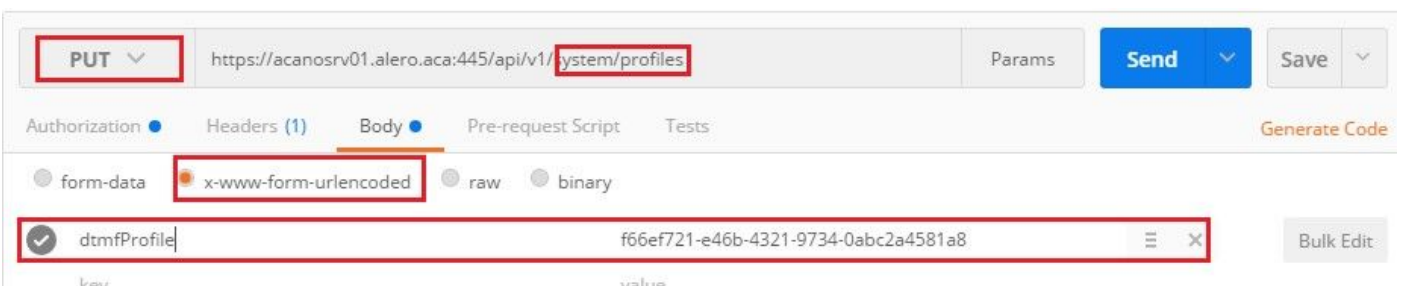
例：



8. DTMFプロフィールを適用します。

dtmfProfile を BODY dtmfProfile=<dfmt Profile ID> に追加した後、<https://<Callbridge IP>:445/api/v1/system/profiles> を使用してPUTを送信します。

以下に、いくつかの例を示します。



## 確認

このセクションでは、設定が正常に機能していることを確認します。

1. 設定が完了したら、次のイメージに似た出力が得られます

recorder

ローカル スタンドアロン CB :

```
acanosrv01> recorder
Enabled                : true
Interface whitelist    : lo:8443
Key file               : callbridgecert.key
Certificate file       : callbridgecert.cer
Trust bundle          : callbridgecert.cer
NFS domain name       : 10.48.36.246
NFS directory         : /acano
```

またはクラスタ化された CB :

```
acanosrv05> recorder
Enabled                : true
Interface whitelist    : a:8443
Key file               : forallcert05.key
Certificate file       : forallcert05.cer
Trust bundle          : TrustBundle.crt
NFS domain name       : 10.48.36.246
NFS directory         : /cluster-alero-aca-recordings
```

2. GETを送信してシステムプロファイルを表示するには、結果にcallProfile、CallLegProfile、およびdtmfProfile ( これらすべてが設定されていると仮定 ) が表示されている必要があります。

<https://<Callbridge IP>:445/api/v1/system/profiles>

以下に、いくつかの例を示します。

```
1 <?xml version="1.0"?>
2 <profiles>
3   <callLegProfile>9591bd29-dc78-4656-bab1-328b2fd505fe</callLegProfile>
4   <callProfile>cf8cf197-a314-4c2e-93d5-4400551efcd6</callProfile>
5   <dtmfProfile>110ed4b0-fcb2-45e1-9b5c-724f7b037b35</dtmfProfile>
6 </profiles>
```

3. CallProfileに設定されていることを確認するには、APIでこれを使用します

<https://<Callbridge IP>:445/api/v1/callProfiles/<callProfile ID>>

これは、以下のように録音方法が自動または手動のいずれかに設定されていることを示します。



```
<?xml version="1.0"?>
<callProfile id="af73f145-829b-42ed-898d-f111f6259626">
  <recordingMode>automatic</recordingMode>
</callProfile>
```

4. CallLegProfileに設定されていることを確認するには、このAPIを使用します

[https://<Callbridge\\_IP>:445/api/v1/callLegProfiles/<callLegProfile\\_ID>](https://<Callbridge_IP>:445/api/v1/callLegProfiles/<callLegProfile_ID>)

出力例 :

```
1 <?xml version="1.0"?>
2 <callLegProfile id="9591bd29-dc78-4656-bab1-328b2fd505fe">
3   <recordingControlAllowed>true</recordingControlAllowed>
4 </callLegProfile>
```

5. DTMFプロフィールで設定されていることを確認するには、APIでこれを使用します

[https://<Callbridge\\_IP>:445/api/v1/dtmfProfiles/<dtmfProfile\\_ID>](https://<Callbridge_IP>:445/api/v1/dtmfProfiles/<dtmfProfile_ID>)

これは、以下のように録音方法が自動または手動のいずれかに設定されていることを示します。

```
<?xml version="1.0"?>
<dtmfProfile id="110ed4b0-fcb2-45e1-9b5c-724f7b037b35">
  <muteSelfAudio></muteSelfAudio>
  <unmuteSelfAudio></unmuteSelfAudio>
  <toggleMuteSelfAudio></toggleMuteSelfAudio>
  <lockCall></lockCall>
  <unlockCall></unlockCall>
  <muteAllExceptSelfAudio></muteAllExceptSelfAudio>
  <unmuteAllExceptSelfAudio></unmuteAllExceptSelfAudio>
  <endCall></endCall>
  <nextLayout></nextLayout>
  <previousLayout></previousLayout>
  <startRecording>**7</startRecording>
  <stopRecording>**8</stopRecording>
  <allowAllMuteSelf></allowAllMuteSelf>
  <cancelAllowAllMuteSelf></cancelAllowAllMuteSelf>
  <allowAllPresentationContribution></allowAllPresentationContribution>
  <cancelAllowAllPresentationContribution></cancelAllowAllPresentationContribution>
  <muteAllNewAudio></muteAllNewAudio>
  <unmuteAllNewAudio></unmuteAllNewAudio>
  <defaultMuteAllNewAudio></defaultMuteAllNewAudio>
  <muteAllNewAndAllExceptSelfAudio></muteAllNewAndAllExceptSelfAudio>
  <unmuteAllNewAndAllExceptSelfAudio></unmuteAllNewAndAllExceptSelfAudio>
</dtmfProfile>
```

注：DTMF プロファイルはポイントツーポイントコールでは機能しないため、スペースでは手動録音しか使用できません。

## トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

レコーダーに関して記録されている内容を表示するには、次のコマンドを実行します。

### syslog follow

表示される出力は次のようになります。

```
Jun 20 20:38:49 kern.info acanosrv05 recorder-proxy[1]: 2016/06/20 20:38:49 Connection from
10.48.54.75:39439: Authentication succeeded
Jun 20 20:38:49 kern.info acanosrv05 recorder-proxy[1]: 2016/06/20 20:38:49 Connection from
10.48.54.75:39439: Connection terminated
Jun 20 20:38:53 kern.info acanosrv05 recorder-proxy[1]: 2016/06/20 20:38:53 Connection from
10.48.54.76:35141: Authentication succeeded
Jun 20 20:38:53 kern.info acanosrv05 recorder-proxy[1]: 2016/06/20 20:38:53 Connection from
10.48.54.76:35141: Connection terminated
```

この例では、acanosrv05 がレコーダーをホストするサーバで、それに接続しているその他の CB ノードが 10.48.54.75 と 10.48.54.76 です。

これは、リモート CB がレコーダーと正しく接続し、認証していることを示しています。

レコーダーが CB に対してローカルの場合、接続はループバック IP から発生します。

```
Jun 20 20:40:52 kern.info acanosrv01 recorder-proxy[1]: 2016/06/20 20:40:52 Connection from 127.0.0.1:45380: Authentication succeeded
Jun 20 20:40:52 kern.info acanosrv01 recorder-proxy[1]: 2016/06/20 20:40:52 Connection from 127.0.0.1:45380: Connection terminated
```

**注：**レコーダー プロセスに関連するほとんどのログは、recorder-proxy として syslog に表示されます。これらは、レコーダーが失敗している可能性のある箇所を示します。

レコーダーのその他の syslog は次のとおりです。

このケースでは、録音デバイスが見つかり、録音が自動的に開始されます。

```
Jun 20 21:16:19 user.info acanosrv02 host:server: INFO : recording device 1: available (1 recordings)
```

録音に失敗した場合は、録音デバイスが見つかったかどうかを確認します。

```
Jun 20 21:16:19 user.info acanosrv02 host:server: INFO : No recording device found
```

このような警告が表示された場合は、レコーダーの信頼で証明書を確認し、それがCBの設定に使用される正しい証明書であることを確認します。

syslog を調べて、NFS ストレージがマウントされているかどうかを確認します。

- NFSストレージがマウントされていない場合、「Failed to mount NFS storage」と表示されます
- レコーダサーバ：/Folder-nameに設定されているNFSフォルダが、NFSストレージに設定されているNFSフォルダと同じであることを確認します

API を実行して、レコーダーに関連するアラームを確認します。

- [https://<callBridge\\_IP>api/v1/system/alarms](https://<callBridge_IP>api/v1/system/alarms)
- ディスクの空き容量が少ない場合、「recorderLowDiskSpace」が表示されます
- 次に、レコーダーによって参照されるNFSストレージに十分なディスク領域があることを確認します

## 関連情報

- [テクニカル サポートとドキュメント – Cisco Systems](#)