

Recorder in CMS/Acano Call Bridge konfigurieren

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Bereitstellungen](#)

[Unterstützte Bereitstellungen](#)

[Andere Einrichtung](#)

[Konfigurieren](#)

[Schritt 1: Konfigurieren eines NFS-Freigabeordners auf einem Windows-Server](#)

[Schritt 2: Konfiguration und Aktivierung der Aufzeichnung auf dem Rekorder-Server](#)

[Schritt 3: Erstellen eines API-Benutzers auf der CB-Karte](#)

[Schritt 4: Hinzufügen des Recorders zur CB-Einheit mithilfe der API](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument werden die Konfigurationsschritte beschrieben, die zum Einrichten des Recorder auf der Call Bridge (CB)-Komponente eines Cisco Meeting Server (CMS) erforderlich sind.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- CMS 1.9 oder höher
- Postman von Google Chrome
- CMS-API (Application Program Interface)

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren

(Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Der CMS Recorder ist ab Version 1.9 des CMS-Servers (ehemals Acano) erhältlich. Der Recorder bietet die Möglichkeit, Meetings aufzuzeichnen und die Aufzeichnungen auf einem NFS-Dokumentenspeicher (Network File System) zu speichern.

Der Recorder verhält sich wie ein Extensible Messaging and Presence Protocol (XMPP)-Client, sodass der XMPP-Server auf dem Server, der die Call Bridge hostet, aktiviert werden muss.

Recorder-Lizenz ist erforderlich und muss auf die CallBridge-Komponente und nicht auf den Recorder-Server angewendet werden.

NFS-Verzeichnis (Network File System) wird benötigt und kann auf Windows Server oder Linux eingerichtet werden.

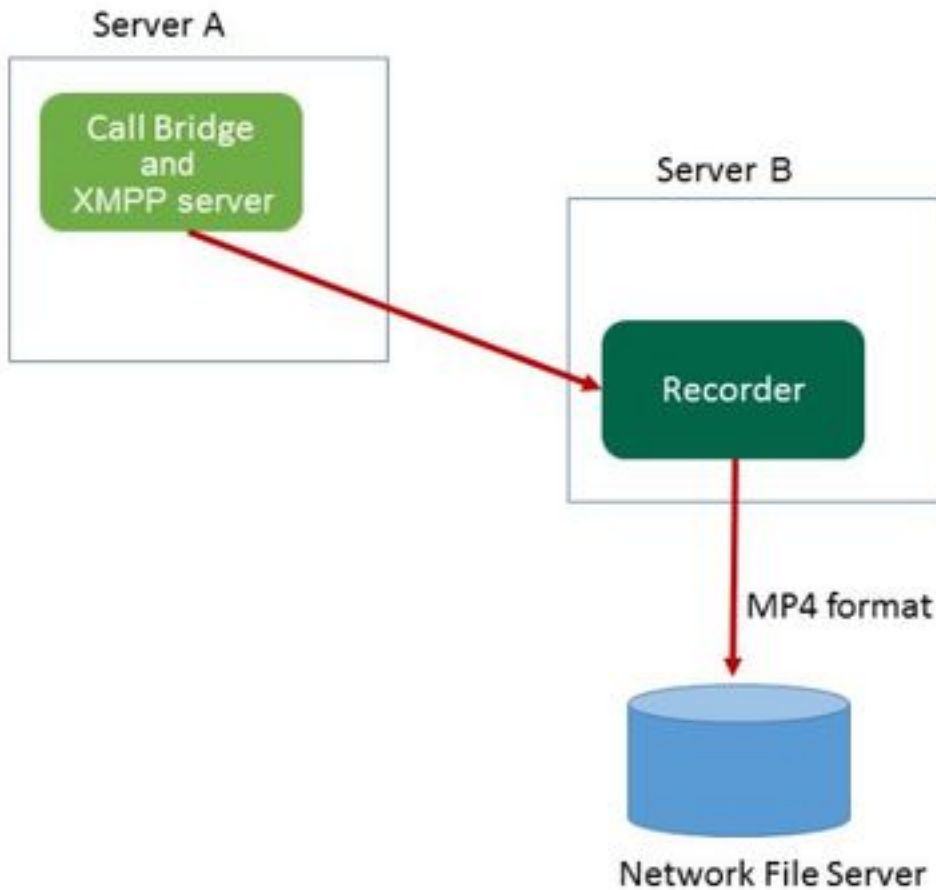
- Führen Sie für Windows-Server die Schritte aus, um das [Netzwerkdateisystem](#) unter Windows [bereitzustellen](#).
- Führen Sie für Linux die Schritte aus, um das [Netzwerkdateisystem](#) unter Linux [bereitzustellen](#).

Hinweis: Für NFS, das auf Windows Server 2008 R2 ausgeführt wird, gibt es einen Hotfix für [Berechtigungsprobleme](#).

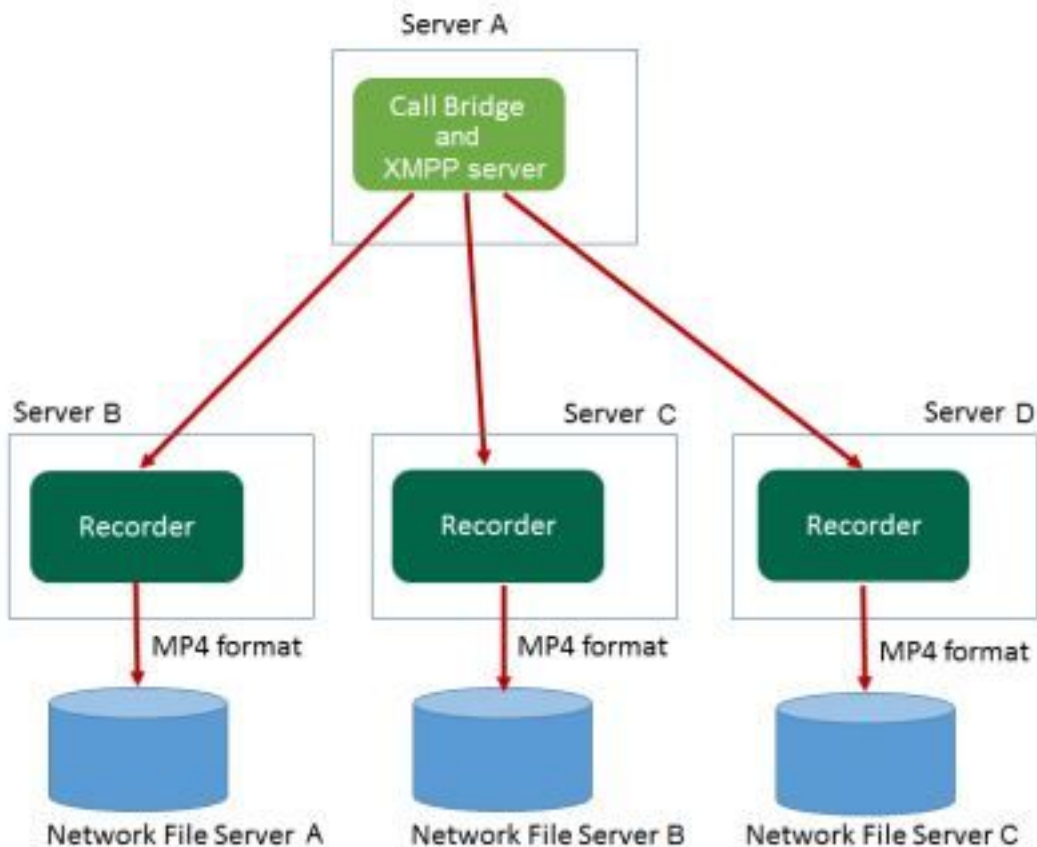
Bereitstellungen

Unterstützte Bereitstellungen

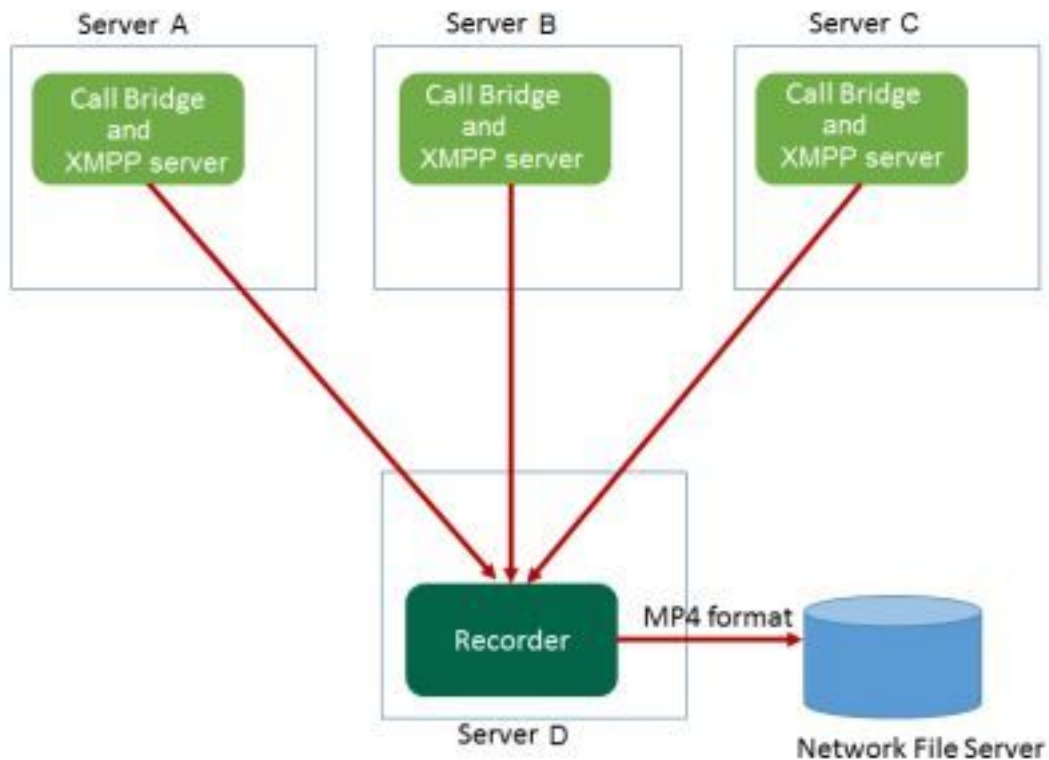
1. Der Rekorder muss auf einem CMS/Acano-Server gehostet werden, der sich remote zum Server befindet, der das CB hostet, wie in diesem Bild gezeigt



2. Die redundante Bereitstellung des Recorder wird ebenfalls unterstützt. Wenn Redundanz eingerichtet ist, wird der Lastausgleich für die Aufzeichnungen zwischen allen Aufzeichnungsgeräten (Servern) vorgenommen. Das bedeutet, dass jedes CB jeden verfügbaren Recorder verwendet, wie in diesem Bild gezeigt

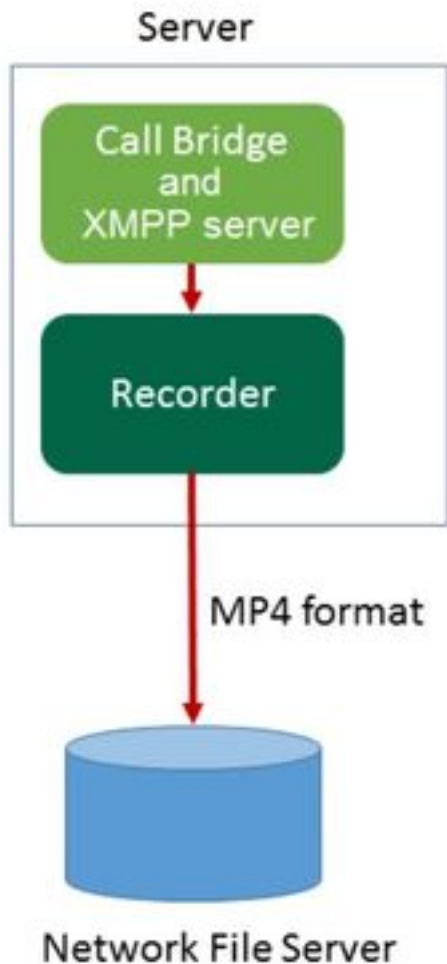


3. Dasselbe gilt im Gegenteil, wenn es mehrere Zentralbanken gibt. Alle CB-Knoten verwenden den Recorder, der ihnen zur Verfügung steht, wie in diesem Bild gezeigt



Andere Einrichtung

Der Rekorder kann auch auf dem gleichen Server wie das CB gehostet werden, aber dieser darf nur zum Testen oder für sehr kleine Bereitstellungen verwendet werden, siehe nächstes Bild als Referenz. Der Nachteil ist, dass nur 1-2 gleichzeitige Aufnahmen möglich sind:



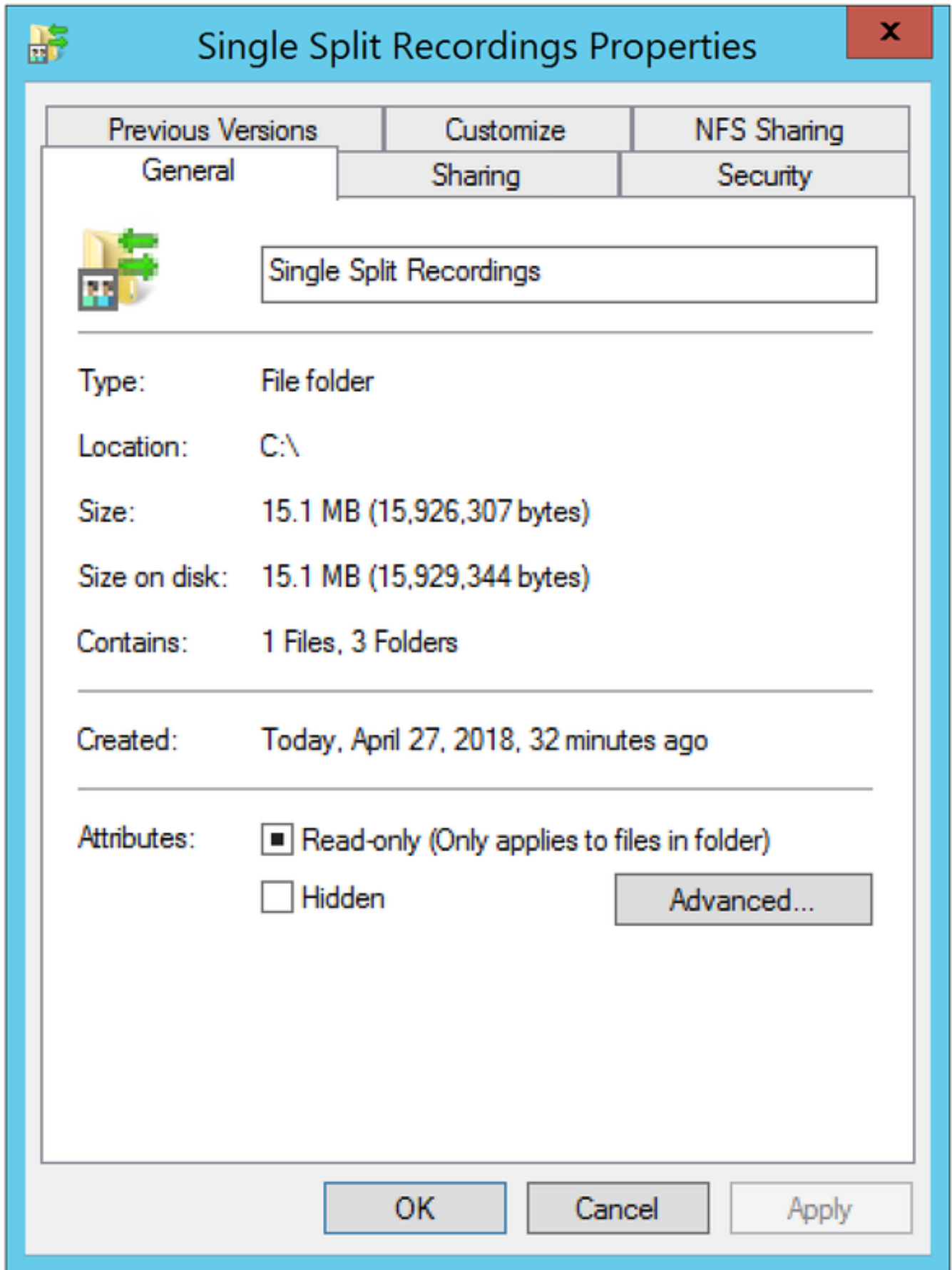
Konfigurieren

Schritt 1: Konfigurieren eines NFS-Freigabeordners auf einem Windows-Server

a) Erstellen Sie mit Windows Explorer einen neuen Ordner für Ihre NFS-Freigabe. In diesem Beispiel wurde ein Ordner mit dem Namen **Single Split Recordings** auf meiner lokalen Festplatte erstellt.

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) Klicken Sie mit der rechten Maustaste auf den Ordner, und wählen Sie **Eigenschaften**



c) Wählen Sie die Registerkarte **NFS-Freigabe** oben rechts aus. Der Ordner wird als **Nicht freigegeben** angezeigt. In diesem Beispiel wurde der Ordner zuvor freigegeben. Andernfalls muss ein leerer Netzwerkpfad angezeigt werden, und der Ordner wird als **Nicht freigegeben** angezeigt.

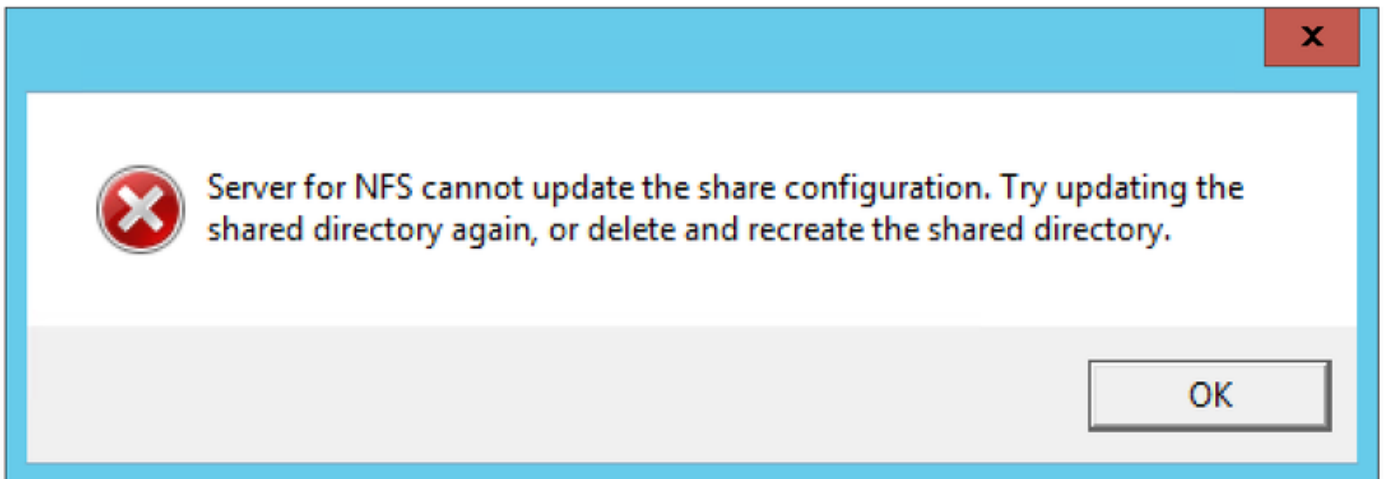
d) Auswählen **NFS-Freigabe verwalten**

e Aktivieren Sie das Kontrollkästchen neben **Diesen Ordner freigeben**

f. Geben Sie den Namen der Ordnerfreigabe in den **Freigabennamen** ohne Leerzeichen ein.

Hinweis: Diese wird von den NFS-Clients und dem CMS-Rekorder verwendet, um diesen Ordner zu finden.

Hinweis: Stellen Sie sicher, dass sich in Ihrem Namen für die Ordnerfreigabe kein Leerzeichen befindet. Wenn dies der Fall ist, können Sie die Änderungen nicht speichern. Das Fehlerfenster wird angezeigt:



B. Lassen Sie die Codierung unverändert. **ANSI Wert**

h. Standardmäßig sind alle Authentifizierungs-Kontrollkästchen markiert. Deaktivieren Sie alle Optionen **Kerberos** Authentifizierungsoptionen, bei denen nur **Keine Serverauthentifizierung [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. Auswählen **Unzugeordneten Benutzer-Unix-Zugriff zulassen (nach UID/GID)**

j. Wählen Sie unten **Berechtigungen** um Berechtigungen für die Netzwerkfreigabe festzulegen.

Hinweis: Der Standardwert ist Schreibgeschützt für alle Computer. Der Rekorder muss über Lese- und Schreibzugriff verfügen, sodass Sie die Standardeinstellung für **ALLE MASCHINEN** ändern oder spezifische Regeln für Ihren Rekorder hinzufügen können. Best Practice wäre es, den Zugriff auf ALLE SYSTEME zu deaktivieren, indem der Zugriff auf **keinen Zugriff** geändert und neue Berechtigungen für die IP-Adresse der Server hinzugefügt werden, die Zugriff auf die Freigabe benötigen.

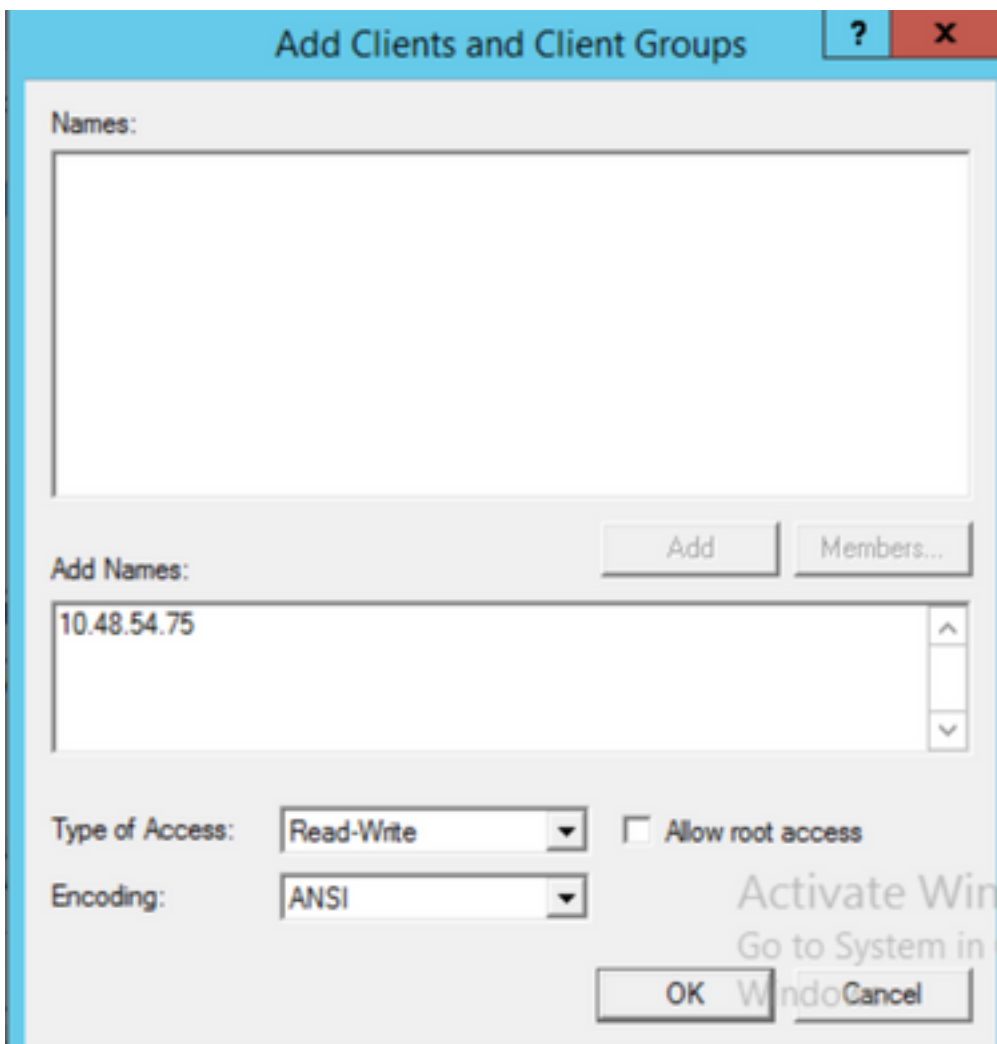
K Um Berechtigungen für die Rekorder hinzuzufügen, wählen Sie **Hinzufügen**

l. In **Namen hinzufügen** Geben Sie die IP-Adresse Ihres Recorder-Servers ein. In diesem Beispiel ist mein Rekorder-Server 10.48.54.75.

m. Auswählen **Lesen und Schreiben** Zugriff

n Kodierung verlassen als **ANSI**

o Urlaub **Root-Zugriff zulassen** deaktiviert



p. Wählen Sie **OK**, um das Dialogfeld "Berechtigungen" zu schließen.

q Auswählen **ALLE MASCHINEN**

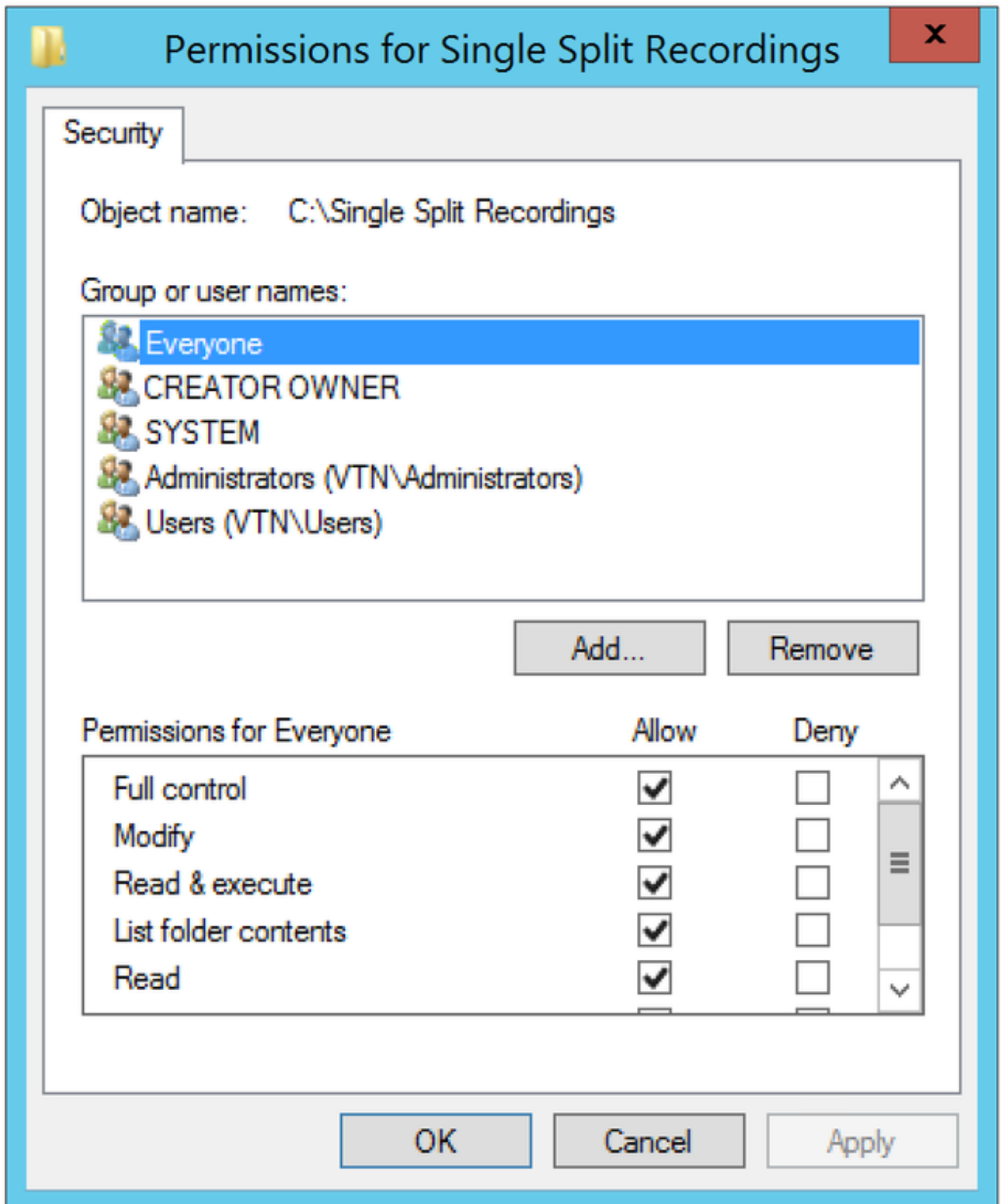
r Ändern **Art des Zugriffs** an **Kein Zugriff**

s. Auswählen **OK** um das Berechtigungsverfahren zu schließen

t lä Auswählen **OK** erneut, um zum Fenster "Ordneigenschaften" zurückzukehren.

u Auswählen **Sicherheit**

Hinweis: Die Gruppe **Jeder** muss vollen Zugriff auf den Ordner haben. Wenn sie nicht aufgeführt ist, wählen Sie **Bearbeiten** aus, um den Berechtigungs-Editor zu öffnen. Wählen Sie **Hinzufügen**, um einen Benutzer hinzuzufügen, und geben Sie im Feld Namen **Jeder** ein, und wählen Sie OK aus. Wählen Sie **Jeder** in der Liste aus, markieren Sie das Kontrollkästchen für **Vollzugriff** und wählen Sie **OK**. Wählen Sie erneut **OK**, um die Eigenschaften zu schließen. Bei korrekter Konfiguration ähnelt es dem nächsten Bild:



Schritt 2: Konfiguration und Aktivierung der Aufzeichnung auf dem Rekorder-Server

a) Konfigurieren Sie den Recorder so, dass die von Ihnen ausgewählte(n) Schnittstelle(n) mit dem folgenden Befehl überwacht wird:

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

b) Wenn sich der Rekorder im lokalen CB befindet, muss die Schnittstelle auf "Loopback" gesetzt

sein. Verwenden Sie daher den folgenden Befehl:

Zum Wiedergeben anhören: 8443

c) Wenn Sie eine bestimmte Schnittstelle anhören möchten, sagen wir "a", dann verwenden Sie:

Rekorder hören a:8443

Hinweis: Wenn Sie den Rekorder auf einem Knoten mit geclustertem CB konfigurieren, muss die Schnittstelle die lokale Überwachungsschnittstelle des Knotens sein, auf dem der Rekorder konfiguriert wird.

d) Legen Sie die Zertifikatsdatei fest, die vom Rekorder verwendet werden soll. Sie können z. B. ein bereits vorhandenes Zertifikat und eine vom CB verwendete private Schlüsseldatei verwenden.

recorder certs <keyfile> <Zertifikatdatei>

e Fügen Sie das CB-Zertifikat mithilfe des folgenden Befehls zum Recorder Trust Store hinzu:

recorder trust <crt-Paket>

Das CRT-Paket muss das von der CB verwendete Zertifikat enthalten, falls es sich dabei um ein anderes handelt. In einem Cluster müssen die Zertifikate aller CBs im Cluster enthalten sein.

f. Geben Sie den Hostnamen oder die IP-Adresse des NFS und das Verzeichnis im NFS zum Speichern der Aufzeichnungen an:

recorder nfs <Hostname/IP>:<directory>

Hinweis: Der Rekorder authentifiziert sich nicht beim NFS, aber es ist wichtig, dass der Recorder-Server über Lese-/Schreibzugriff auf das NFS-Verzeichnis verfügt.

B. Aktivieren Sie die Rekorder, indem Sie den Befehl:

Rekorder aktivieren

Schritt 3: Erstellen eines API-Benutzers auf der CB-Karte

Erstellen Sie einen API-Benutzer im CB. Dies ist für weitere Konfigurationen über die API-Funktion erforderlich:

Erstellen Sie den Benutzer mit den folgenden Schritten:

a) Verbinden Sie sich über Secure Shell (SSH) oder Konsole mit der CB unter Verwendung der Administratorberechtigungen.

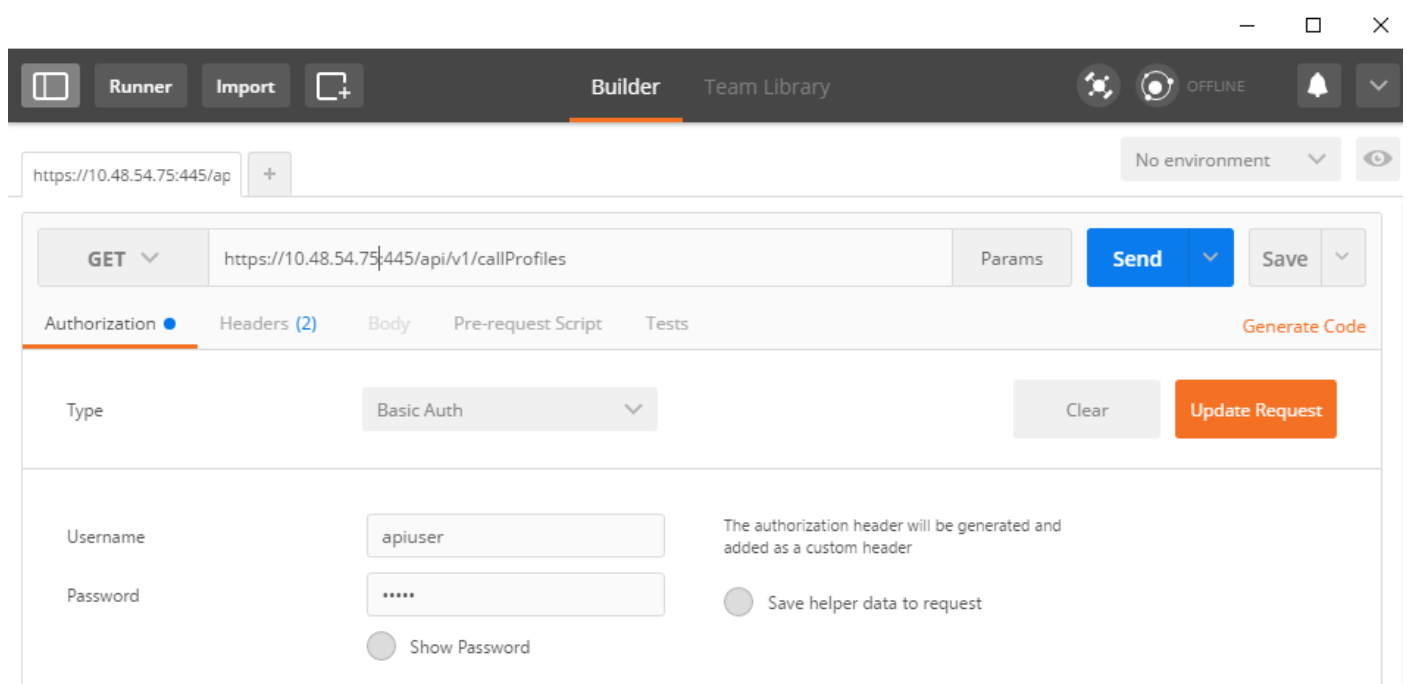
b) Fügen Sie **<Benutzername>** api hinzu, drücken Sie dann die **Rückgabetaste**, und geben Sie das Kennwort gefolgt vom **Rückgabetaste** ein.

Schritt 4: Hinzufügen des Recorders zur CB-Einheit mithilfe der API

1. Postman von [hier](#) herunterladen und installieren

2. Geben Sie die URL für den API-Zugriff in die Adressleiste ein, z. B.:

https://<Callbridge_IP>:445/api/v1/<entity>. Legen Sie dann in authentication, Benutzername und Kennwort aus Schritt 3, unter Authorization with **Basic Auth (Autorisierung mit Basic Auth als Typ)** fest.



Hinweis: Dies setzt voraus, dass derzeit kein Recorder oder CallProfile auf der CB-Seite konfiguriert ist. Andernfalls können Sie einen vorhandenen Rekorder und/oder callProfile mithilfe der PUT-Methode ändern.

3. Hinzufügen des Recorders zur CB über die API

a) Senden Sie einen leeren POST-Test mit https://<Callbridge_IP>:445/api/v1/recorders.

b) Senden Sie eine GET-Datei mit derselben URL in (a), kopieren Sie die Rekorder-ID, ohne die Kostenvoranschläge in den Editor.

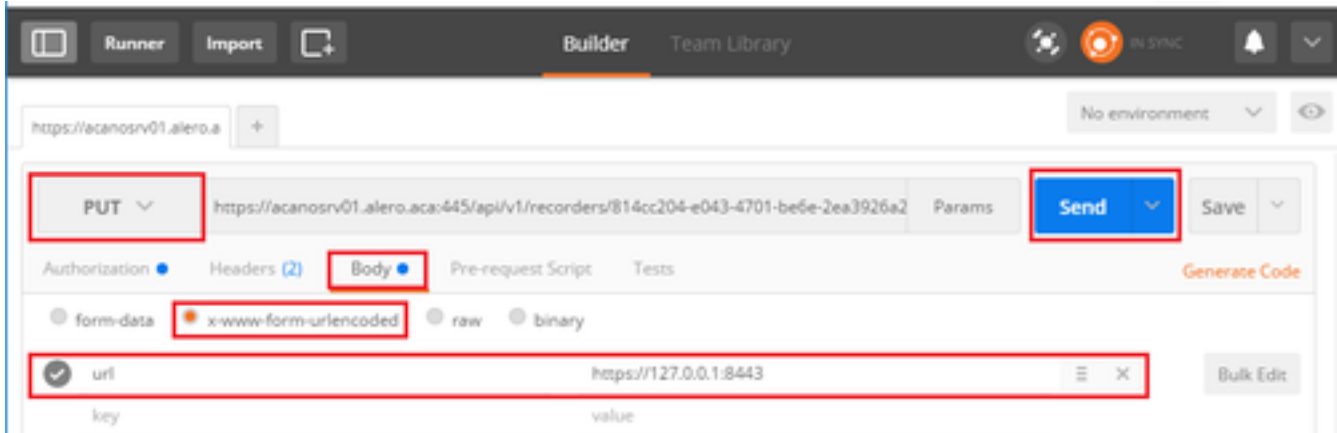
c) Legen Sie die URL des Rekorder fest, indem Sie einen PUT mit https://<Callbridge_IP>:445/api/v1/recorders/<recorderid> senden und diesen in BODY einfügen, bevor Sie das PUT ausführen:

url=<https://127.0.0.1:8443> (wenn sich der Rekorder im lokalen CB befindet)

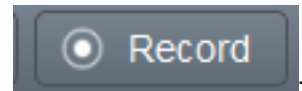
oder

url=https://<IP-Adresse des Rekorder>:8443 (wenn sich der Rekorder nicht im lokalen CB befindet)

Beispiel:



Hinweis: **dtmfProfile**, **callProfile** und **callLegProfile** sind besonders wichtig für SIP-Endpunkte, die einer Konferenz im Leerraum beitreten. Sie ermöglichen dem Endpunkt, die Aufzeichnung eines Anrufs vom/zum Standort zu starten/zu beenden.



Ab CMA 1.9.3 und CMS 2.0.1 sind die DTMF-Töne nicht mehr erforderlich. Taste, die dem Client hinzugefügt wird, wenn der Rekorder auf der Callbridge vorhanden ist oder der der Client verbunden ist. Die Aufzeichnungstaste wurde auch aus CMS 2.3 zu WebRTC hinzugefügt.

4. Erstellen eines Anrufprofils

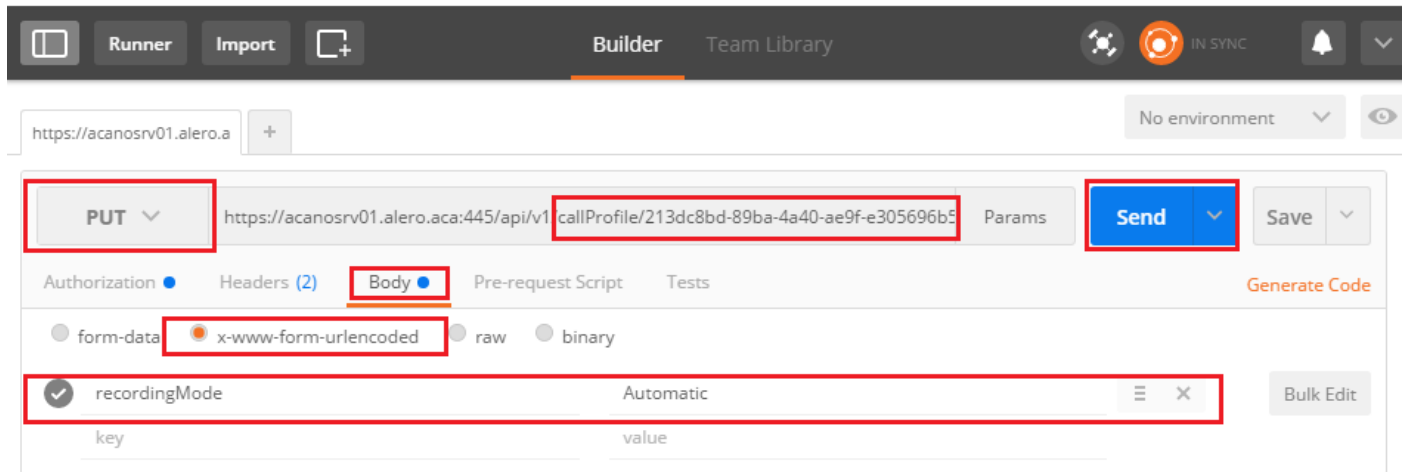
- a) Senden Sie einen leeren POST mit **https://<Callbridge_IP>:445/api/v1/callProfiles**.
- b) Senden Sie eine GET-Nachricht mit derselben URL in (a), kopieren Sie die CallProfile-ID, ohne die Kostenvoranschläge in den Editor.
- c) Legen Sie den RecordingMode im callProfile fest, indem Sie ein PUT mit **https://<Callbridge_IP>:445/api/v1/callProfiles/<call profile ID>** senden und das in BODY hinzufügen, bevor Sie das PUT ausführen.

recordingMode=Manual (wenn die Aufzeichnung von Anrufern mithilfe von DTMF-Einträgen gestartet werden soll)

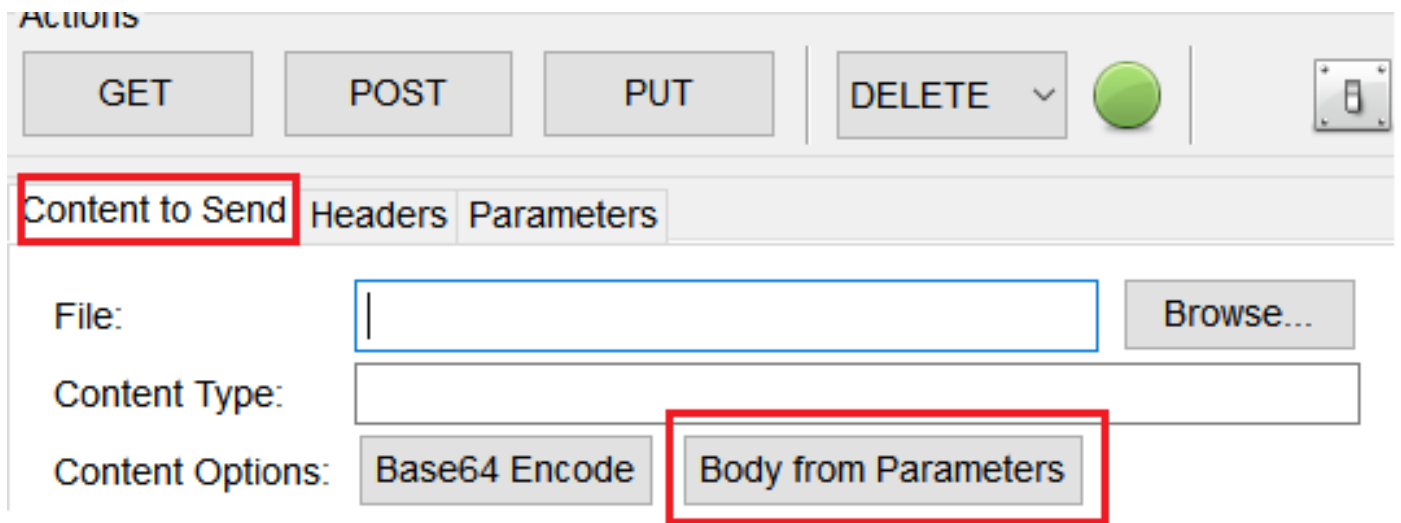
oder

recordingMode=Automatisch (wenn die Aufzeichnung beim Starten von Anrufen automatisch gestartet werden soll)

Beispiel:



Hinweis: Wenn Sie POSTER von Firefox verwenden, müssen Sie **Inhalt zu senden** auswählen und dann **Body aus Parameters** auswählen, bevor Sie den PUT/POST senden. Auf diese Weise wird er in den Code(s) kompiliert, die das CB verstehen kann. Wie im nächsten Bild:



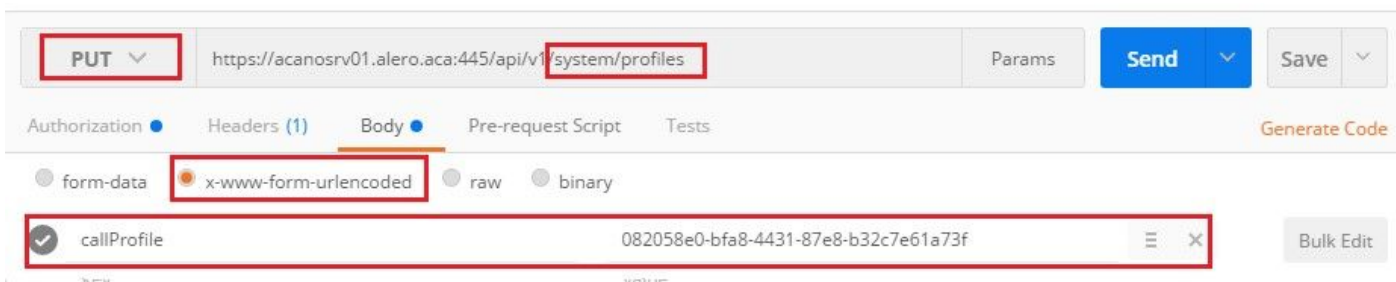
5. Hinzufügen eines Anrufprofils zu den Systemprofilen

Das callProfile definiert, ob Anrufe aufgezeichnet werden können und ob sie mit oder ohne Benutzereingriff durchgeführt werden können.

Senden Sie ein PUT mit https://<Callbridge_IP>:445/api/v1/system/profiles, nachdem Sie das CallProfile in BODY hinzugefügt haben.

callProfile=<Anrufprofil-ID>

Beispiel:

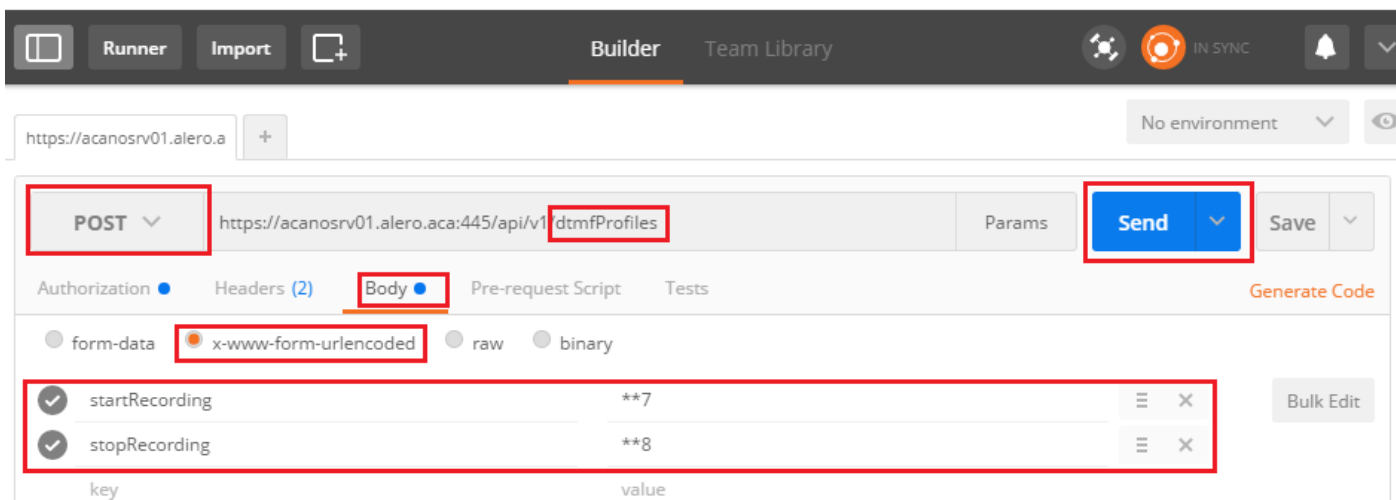


Wenn der recordingMode auf Manual (Manuell) festgelegt ist, müssen Sie ein DTMF-Profil festlegen, um festzulegen, wie die Benutzer Aufzeichnungen mithilfe von DTMF-Tönen starten und beenden können.

6. DTMF-Profil erstellen

a) Senden Sie einen Post mit <https://<Callbridge IP>:445/api/v1/dtmfProfiles>, nachdem Sie die StartRecording=**7- und stopRecording=**8 (z. B.) in BODY als startRecording=**7&stopRecording=**8 festgelegt haben.

Beispiel:



b) Senden Sie eine GET, um das neue DTMF-Profil anzuzeigen, und kopieren Sie dann die ID ohne die Kostenvoranschläge auf notepad.

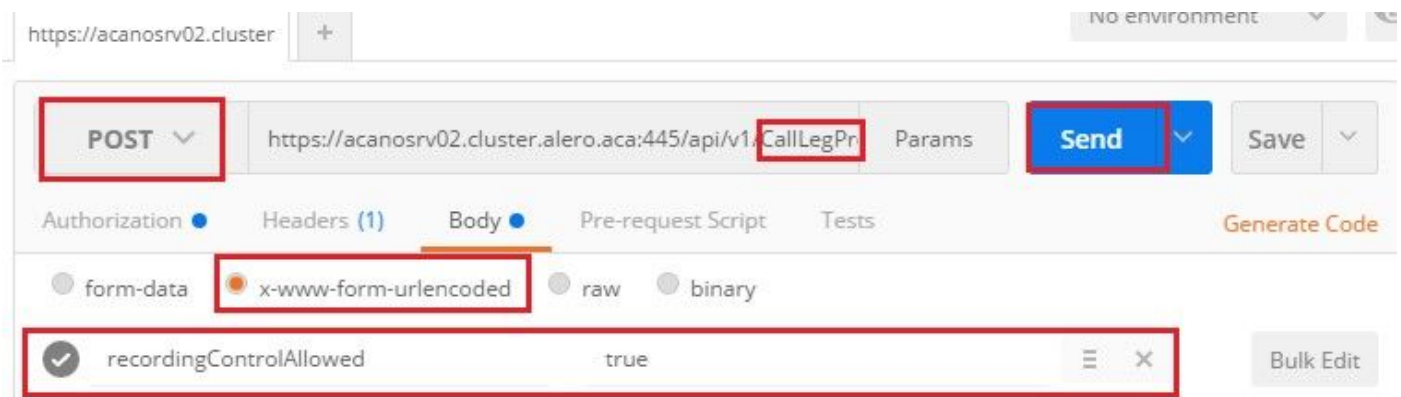
7. Erstellen eines CallLeg-Profiles

CallLegProfiles bestimmt das Verhalten im Gespräch. In diesem Fall wird bestimmt, ob ein Anruf aufgezeichnet werden kann.

Erstellen Sie wie folgt ein Anrufzustandsprofil:

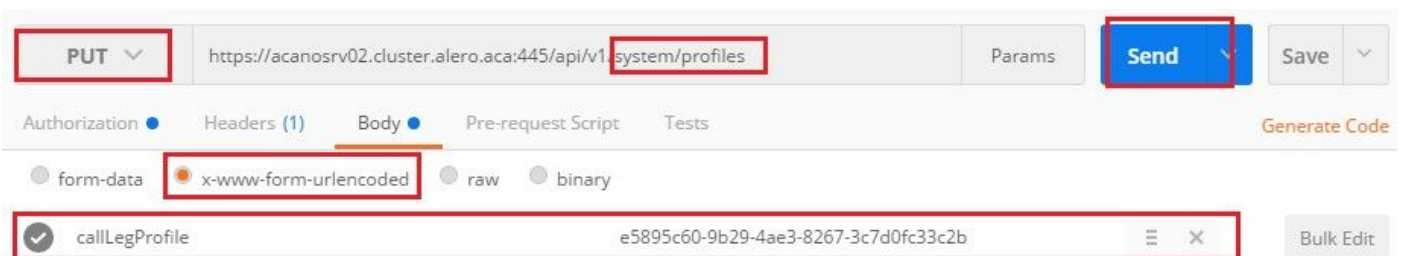
a) Senden Sie einen Post mit <https://<Callbridge IP>:445/api/v1/CallLegProfiles>, nachdem Sie recordingControlAllowed=true im BODY hinzugefügt haben:

Beispiel:



b) Wenden Sie das CallLegProfile an, indem Sie ein PUT mit https://<Callbridge_IP>:445/api/v1/system/profiles senden und callLegProfile=<callLegProfile_ID> im BODY hinzufügen:

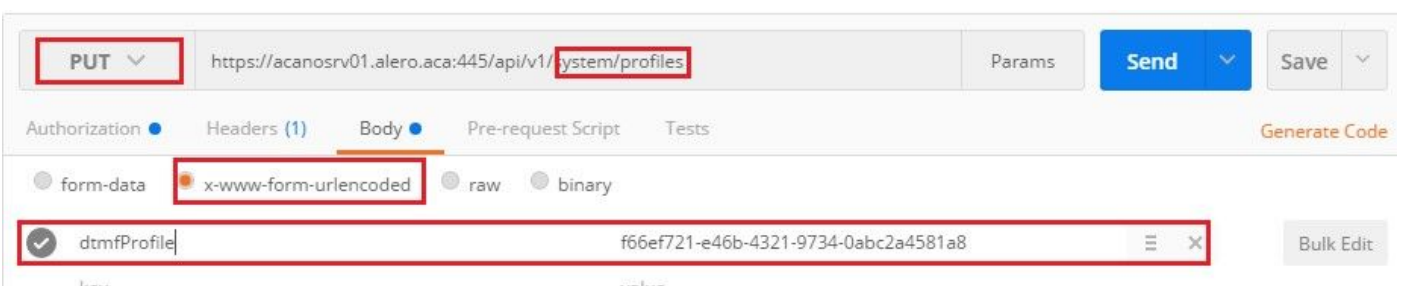
Beispiel:



8. DTMF-Profil anwenden:

Senden Sie ein PUT mit https://<Callbridge_IP>:445/api/v1/system/profiles, nachdem Sie das dtmfProfile in BODY dtmfProfile=<dfmt Profile ID> hinzugefügt haben.

Beispiel:



Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

1. Nach der Konfiguration können Sie den Status mit diesen Befehlen überprüfen und eine ähnliche Ausgabe wie im nächsten Bild erhalten.

Rekorder

Lokales eigenständiges 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
```

Oder wenn CB in Clustern:

```
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. Senden Sie eine GET, um das Systemprofil anzuzeigen. Sie müssen im Ergebnis **CallProfile**, **CallLegProfile** und **dtmfProfile** sehen (vorausgesetzt, alle wurden konfiguriert) mit

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

Beispiel:

```
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. Verwenden Sie diese API, um zu überprüfen, was im CallProfile konfiguriert wurde.

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

Hier sehen Sie, wie die Aufzeichnungsmethoden entweder "Automatisch" oder "Manuell" eingestellt wurden:

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

4. Verwenden Sie diese API, um zu überprüfen, was im CallLegProfile konfiguriert wurde.

https://<Callbridge_IP>:445/api/v1/callLegProfiles/<callLegProfile_ID>

Beispielausgabe:

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

5. Verwenden Sie diese API, um zu überprüfen, was im DTMF-Profil konfiguriert wurde.

https://<Callbridge_IP>:445/api/v1/dtmfProfiles/<dtmfProfile_ID>

Dies zeigt, dass die Aufzeichnungsmethoden, entweder "Automatisch" oder "Manuell", wie folgt eingestellt wurden:

```

<?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>

```

Hinweis: DTMF-Profile funktionieren nicht bei Point-to-Point-Anrufen, daher können Sie die manuelle Aufzeichnung nur an einem Ort verwenden.

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Führen Sie den folgenden Befehl aus, um anzuzeigen, was in Bezug auf den Rekorder protokolliert wird:

Syslog folgen

Die angezeigte Ausgabe ähnelt der folgenden:

```

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

```

In diesem Beispiel ist acanosrv05 der Server, der den Rekorder hostet, und die anderen mit ihm verbundenen CB-Knoten sind 10.48.54.75 und 10.48.54.76.

Dies zeigt an, dass das Remote-CB die Verbindung mit dem Recorder richtig herstellt und sich authentifiziert.

Wenn der Rekorder lokal im CB-Bereich vorhanden ist, stammt die Verbindung von der Loopback-IP-Adresse:

```
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
```

Hinweis: Die meisten Protokolle, die sich auf die Rekorder-Prozesse beziehen, werden im Syslog als Recorder-Proxy angezeigt. Diese geben einen Hinweis darauf, wo der Rekorder fehlschlagen könnte.

Weitere Syslogs werden für den Rekorder wie folgt angezeigt:

In diesem Fall wird ein Aufzeichnungsgerät gefunden und die Aufzeichnung automatisch gestartet:

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

Wenn die Aufzeichnung fehlschlägt, prüfen Sie, ob ein Aufzeichnungsgerät gefunden wurde:

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

Wenn eine solche Warnung angezeigt wird, überprüfen Sie das Zertifikat in der Rekorder-Vertrauenswürdigkeit, um sicherzustellen, dass es für die Konfiguration der CB richtig ist.

Überprüfen Sie im Syslog, ob der NFS-Speicher bereitgestellt ist:

- Wenn der NFS-Speicher nicht gemountet ist, wird "NFS-Speicher konnte nicht bereitgestellt werden" angezeigt
- Überprüfen und vergewissern Sie sich, dass der NFS-Ordner auf dem Rekorder-Server:/Folder-Name mit dem auf dem NFS-Speicher konfigurierten Ordner übereinstimmt.

Führen Sie eine API aus, um Alarme zu überprüfen, die sich auf den Rekorder beziehen:

- https://<callBridge_IP>api/v1/system/alarmen
- Wenn wenig Speicherplatz vorhanden ist, wird "recorderLowDiskSpace" angezeigt
- Überprüfen Sie anschließend, ob der vom Rekorder referenzierte NFS-Speicher über genügend Speicherplatz verfügt.

Zugehörige Informationen

- [Technischer Support und Dokumentation - Cisco Systems](#)