

Configuración de la Grabadora en CMS/Acano Call Bridge

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Implementaciones](#)

[Implementaciones admitidas](#)

[Otra configuración](#)

[Configurar](#)

[Paso 1. Configurar una carpeta compartida NFS en un servidor Windows](#)

[Paso 2. Configurar y habilitar el grabador en el servidor Grabador](#)

[Paso 3. Crear un usuario de API en el CB](#)

[Paso 4. Agregue la grabadora al CB mediante la API](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe los pasos de configuración necesarios para configurar el grabador en el componente Call Bridge (CB) de Cisco Meeting Server (CMS).

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- CMS 1.9 o superior
- Postman de Google Chrome
- CMS Application Program Interface (API)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El CMS Recorder está disponible desde la versión 1.9 del servidor CMS (antiguo Acano). La grabadora permite grabar reuniones y guardar las grabaciones en un almacenamiento de documentos de sistema de archivos de red (NFS).

La grabadora se comporta como un cliente Extensible Messaging and Presence Protocol (XMPP), por lo que el servidor XMPP debe estar habilitado en el servidor que aloja el Call Bridge.

La licencia de grabadora es necesaria y debe aplicarse en el componente CallBridge y no en el servidor de grabadora.

El directorio Network File System (NFS) es necesario y se puede configurar en Windows Server o Linux.

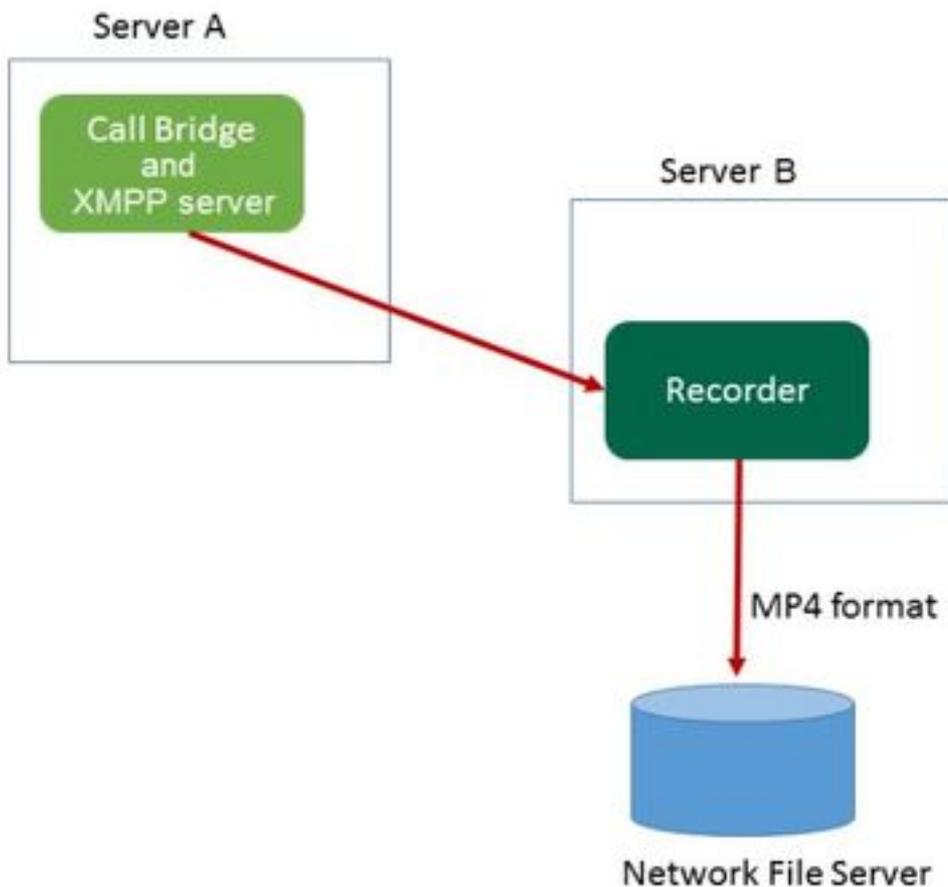
- Para el servidor Windows, siga los pasos para [Implementar el sistema de archivos de red](#) en Windows
- Para Linux, siga los pasos para [Implementar el sistema de archivos de red](#) en Linux

Nota: Para NFS que se ejecuta en Windows Server 2008 R2 hay un hotfix para el [problema de Permiso](#).

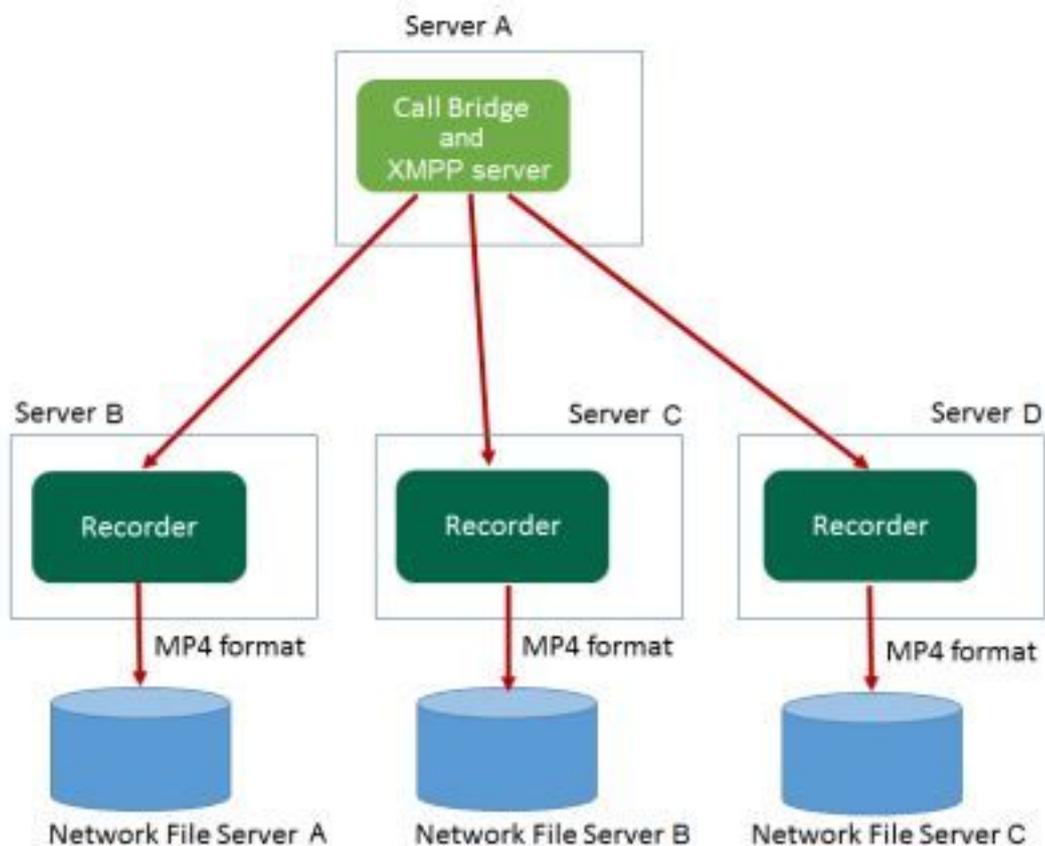
Implementaciones

Implementaciones admitidas

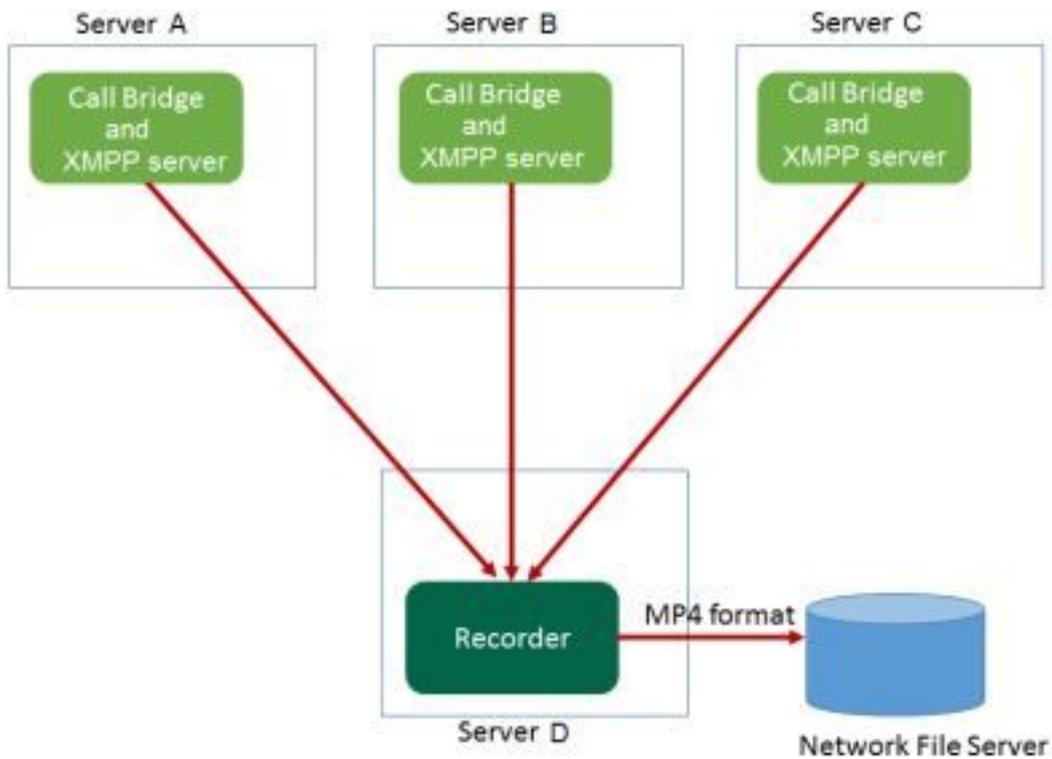
1. La grabadora debe estar alojada en un servidor CMS/Acano que sea remoto al servidor que aloja el CB, como se muestra en esta imagen



2. También se admite la implementación redundante de la grabadora. Si se configura la redundancia, las grabaciones se equilibran de carga entre todos los dispositivos de grabación (servidores). Esto significa que todos los BC utilizan cada grabadora disponible, como se muestra en esta imagen

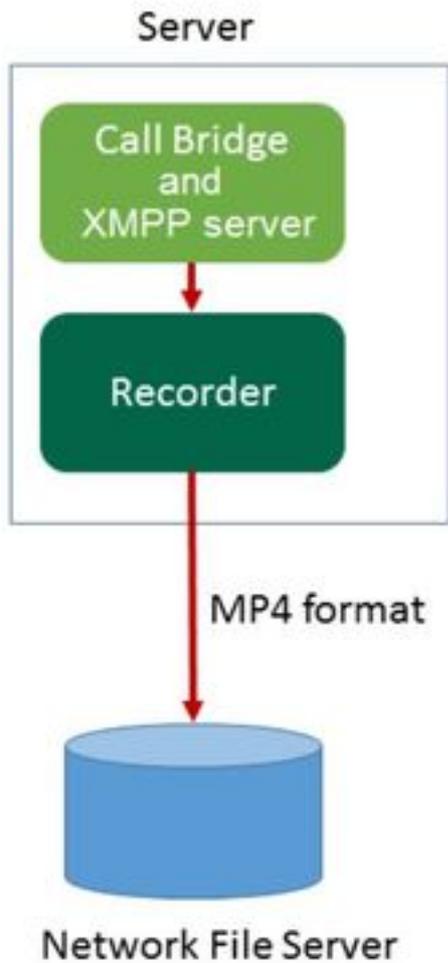


3. Lo mismo se aplica al contrario, cuando hay varios BC. Todos los nodos CB utilizan la Grabadora disponible para ellos, como se muestra en esta imagen



Otra configuración

La grabadora también puede estar alojada en el mismo servidor que el CB, pero sólo debe utilizarse para realizar pruebas o implementaciones muy pequeñas, consulte la siguiente imagen para su referencia. El inconveniente aquí es que sólo son posibles 1-2 grabaciones simultáneas:



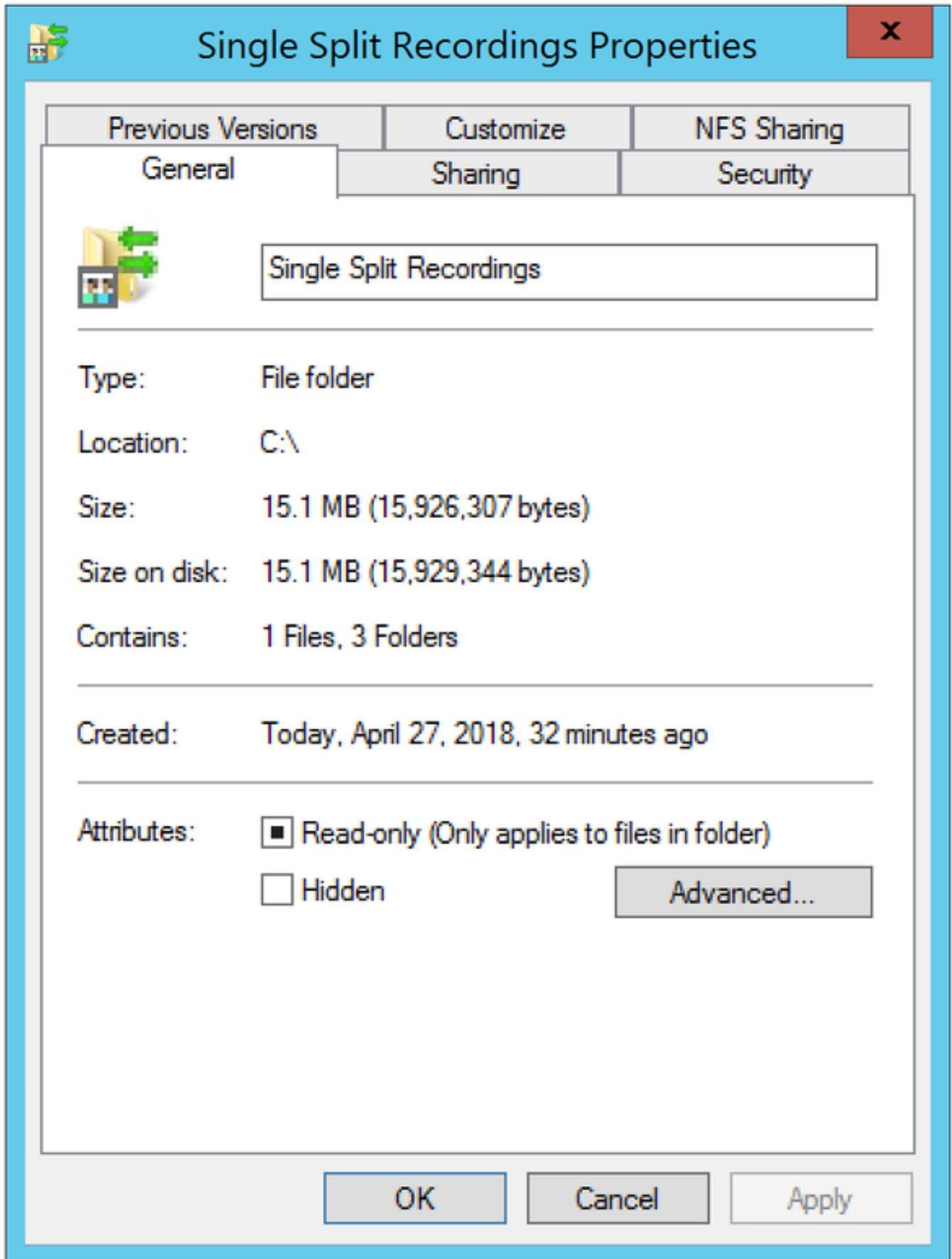
Configurar

Paso 1. Configurar una carpeta compartida NFS en un servidor Windows

a. Con el Explorador de Windows, cree una nueva carpeta para el recurso compartido NFS. En este ejemplo, se ha creado en mi disco local una carpeta denominada **Grabaciones divididas únicas**

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. Haga clic con el botón derecho del ratón en la carpeta y seleccione **Propiedades**



c. Seleccione la pestaña **Compartir NFS** en la parte superior derecha. Muestra la carpeta como **No compartida**. En este ejemplo, la carpeta se ha compartido previamente, de lo contrario, debe ver una ruta de red en blanco y la carpeta se muestra como **No compartida**

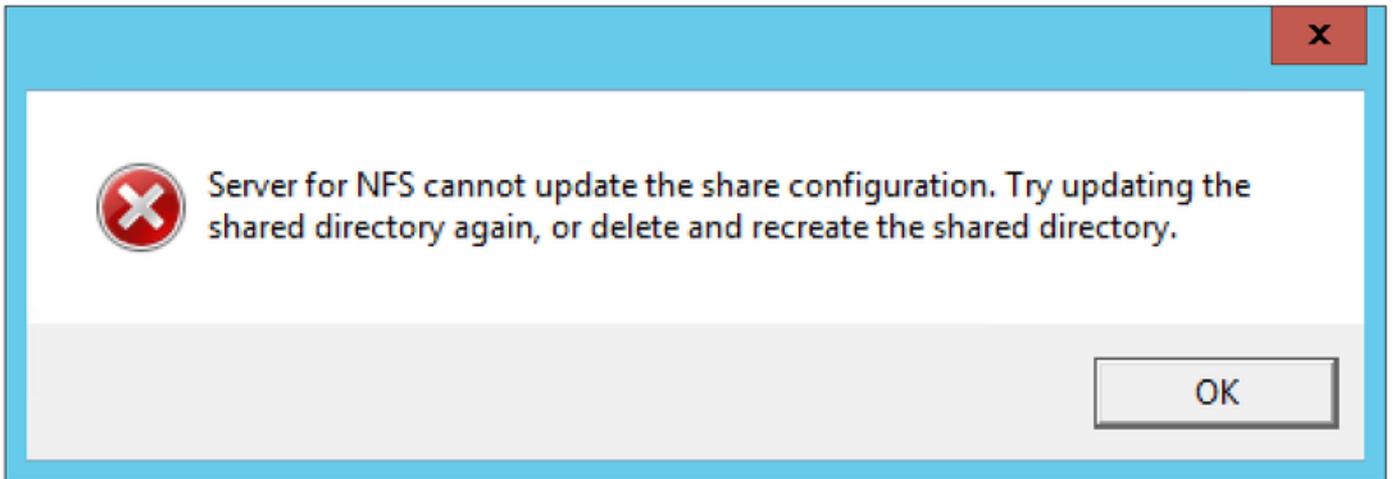
d. Seleccionar **Gestión de recursos compartidos NFS**

e. Marque la casilla de verificación situada junto a **Compartir esta carpeta**

f. Introduzca el nombre del recurso compartido de carpeta en **Nombre del recurso compartido** sin espacios

Nota: Esto es utilizado por los clientes NFS y la grabadora CMS para encontrar esta carpeta.

Nota: Asegúrese de que no haya espacios en el nombre del recurso compartido de carpetas. Si la hay, no podrá guardar los cambios y aparecerá este error Window:



g. Deje la codificación en su valor predeterminado **ANSI (Instituto nacional estadounidense de estándares)** valor

h. De forma predeterminada, todas las casillas de verificación de autenticación están marcadas. Desactive todas las **Kerberos** opciones de autenticación que dejan sólo el **Sin autenticación de servidor [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. Seleccionar **Permitir acceso Unix de usuario no asignado (por UID/GID)**

j. En la parte inferior, seleccione **Permisos** para establecer permisos en el recurso compartido de red

Nota: El valor predeterminado es Sólo lectura para todos los equipos. La grabadora debe tener acceso de lectura y escritura, de modo que pueda cambiar el valor predeterminado para **TODAS LAS MÁQUINAS** o agregar reglas específicas para la grabadora. La mejor práctica sería inhabilitar el acceso a **TODAS LAS MÁQUINAS** cambiando a **Sin acceso** y agregando nuevos permisos para la IP de los servidores que necesitan acceso al recurso compartido.

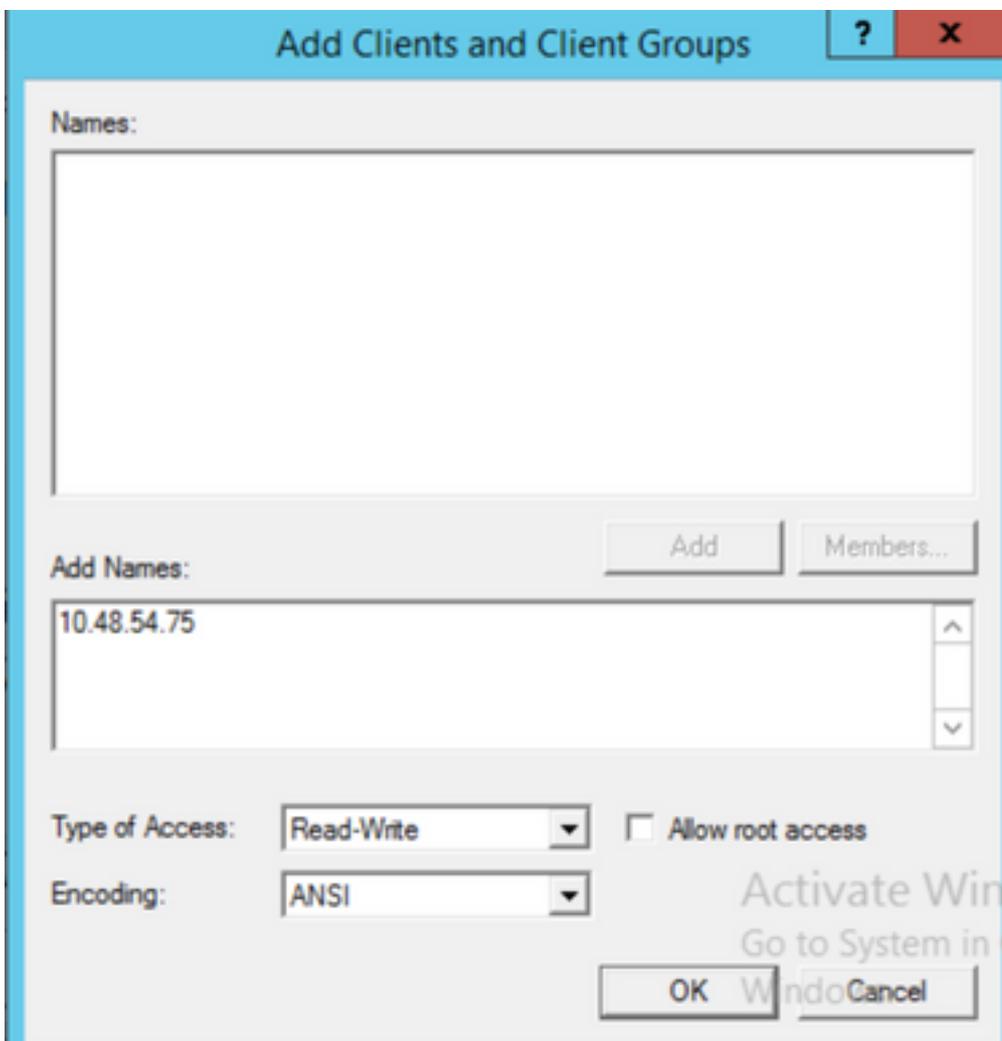
k. Para agregar permisos a la grabadora, seleccione **Agregar**

l. IN **Agregar nombres**, introduzca la dirección IP del servidor de grabadoras. En este ejemplo, mi servidor de grabadoras es 10.48.54.75

m. Seleccionar **leer-escribir** acceso

n. Dejar codificación como **ANSI (Instituto nacional estadounidense de estándares)**

o. Salir **Permitir acceso raíz** inhabilitado



p. Seleccione **Aceptar** para cerrar el diálogo de permisos

p. Seleccionar **TODAS LAS MÁQUINAS**

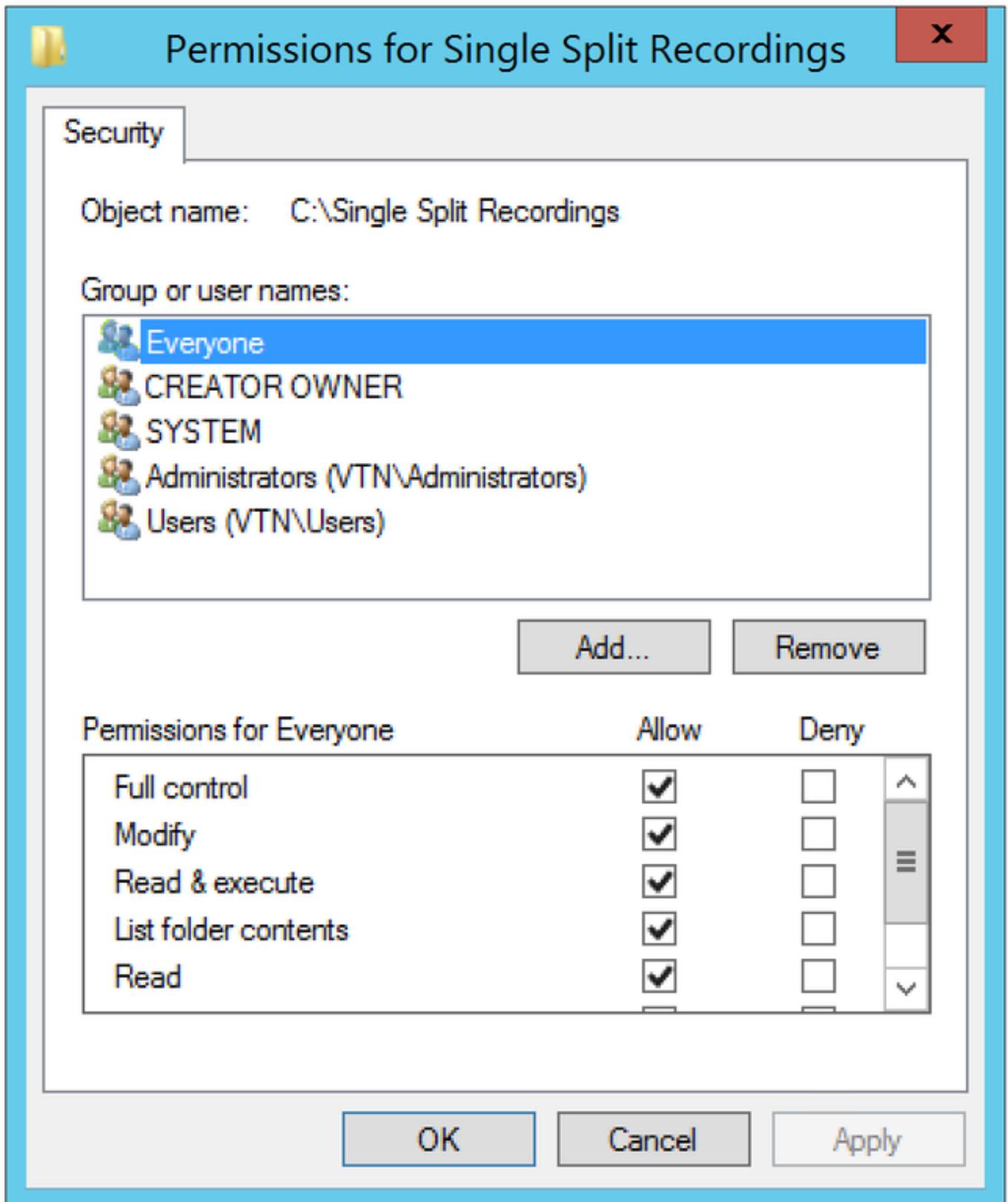
r. Cambiar **Tipo de acceso** a **Sin acceso**

s Seleccionar **OK** para cerrar la ventana permisos

t. Seleccionar **OK** para volver a la ventana Propiedades de carpeta

u. Seleccionar **Security**

Nota: El grupo **Todos** debe tener acceso completo a la carpeta. Si no aparece en la lista, seleccione **Editar** para abrir el editor de permisos. Seleccione **Add** para agregar un usuario y, en el campo names, escriba **Todos** el seleccionado OK. Seleccione **Todos** en la lista y marque la casilla de verificación **Control completo** y seleccione **Aceptar**. Seleccione **Aceptar** de nuevo para cerrar las propiedades. Si se configura correctamente, se asemeja a la siguiente imagen:



Paso 2. Configurar y habilitar el grabador en el servidor Grabador

a. Configure la Grabadora para escuchar en las interfaces que elija con este comando:

graborder hear <interface[:port] whitelist>

b. Si la grabadora está en el CB local, la interfaz debe ser el "loopback", así que utilice este comando:

grabadora escuchar lo:8443

c. Si desea escuchar en una interfaz específica, digamos "a", utilice lo siguiente:

grabadora escuchar a:8443

Nota: Si configura el registrador en un nodo de CB agrupado, la interfaz debe ser la interfaz de escucha local del nodo en el que se está configurando el registrador.

d. Establezca el archivo de certificado que utilizará el grabador. Puede utilizar un certificado que ya existe y un archivo de clave privada utilizado por el CB, por ejemplo.

recorder certs <keyfile> <certificate file>

e. Agregue el certificado CB al almacén de confianza de grabadores mediante el comando:

recorder trust <crt-bundle>

El paquete crt debe contener el certificado utilizado por el CB, si es diferente. Si se encuentra en un clúster, éste debe contener los certificados de cada banco central del grupo.

f. Especifique el nombre de host o la dirección IP del NFS, y el directorio en el NFS para almacenar las grabaciones:

recorder nfs <hostname/IP>:<directory>

Nota: La Grabadora no se autentica en el NFS, pero es importante que el Servidor de Grabadora tenga acceso de lectura y escritura al directorio NFS.

g Habilite la Grabadora, con el uso del comando:

Recorder Enable

Paso 3. Crear un usuario de API en el CB

Cree un usuario de API en el CB, esto es necesario para configuraciones adicionales mediante la función API:

Cree el usuario con estos pasos:

a. Conéctese a través de Secure Shell (SSH) o consola al CB con el uso de las credenciales de administrador.

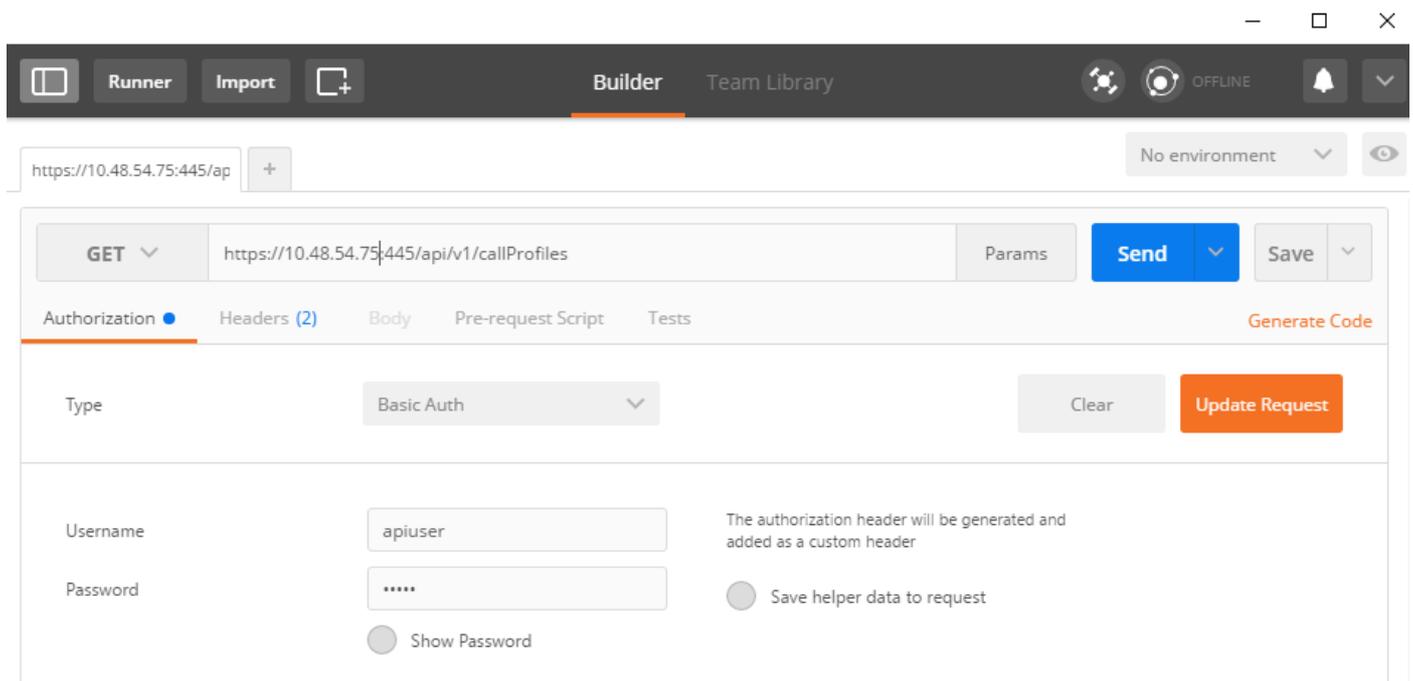
b. El usuario agrega <username> api, luego presione la tecla **Return** e ingrese la contraseña

seguida de la **Return Key**.

Paso 4. Agregue la grabadora al CB mediante la API

1. Descargue e instale Postman desde [aquí](#)

2. Escriba la URL de acceso de API en la barra de direcciones, por ejemplo: **https://<Callbridge_IP>:445/api/v1/<Entity>**. Luego, configure en authentication, el nombre de usuario y la contraseña del Paso 3, en Authorization with **Basic Auth** as type



Nota: Esto supone que actualmente no hay ninguna grabadora o callProfile configurada en el CB. De lo contrario, puede modificar una grabadora que existe o callProfile mediante el método PUT.

3. Agregue la grabadora al CB con la API

a. Enviar un POST vacío con https://<Callbridge_IP>:445/api/v1/grabadores

b. Enviar un GET con la misma URL en (a), copiar la ID de la grabadora, sin los presupuestos en el Bloc de notas

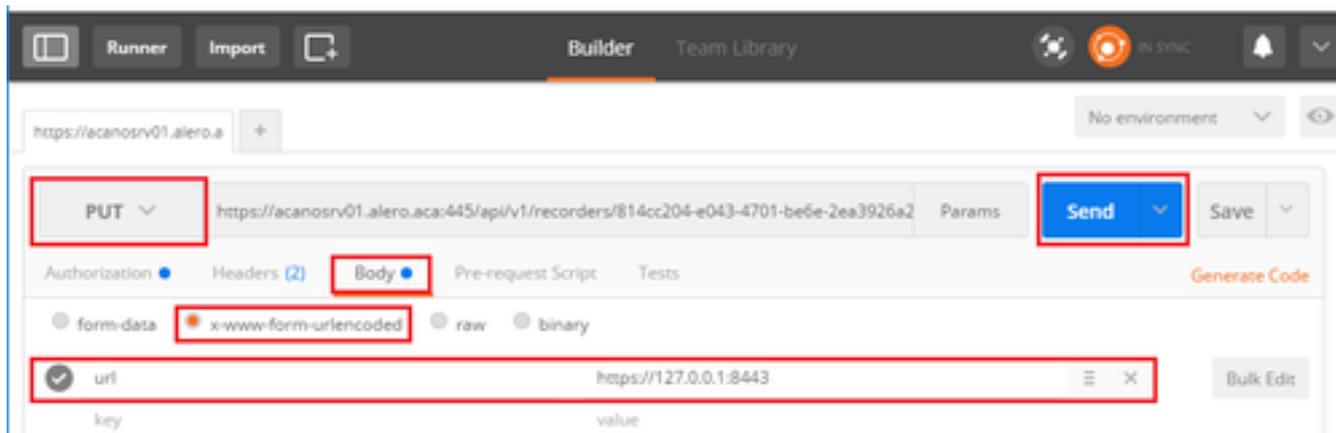
c. Establezca la URL del grabador enviando una PUT con https://<Callbridge_IP>:445/api/v1/grabders/<grabderid> y añádala en BODY antes de ejecutar la PUT:

url=<https://127.0.0.1:8443> (si el registrador está en el CB local)

or

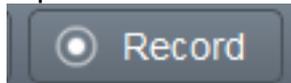
url=<https://<dirección IP del registrador>:8443> (si el registrador no está en el CB local)

Por ejemplo:



Nota: **dtmfProfile**, **callProfile** y **callLegProfile** son particularmente importantes para los terminales SIP que se unen a una conferencia cospace. Permiten que el terminal pueda iniciar/detener la grabación de una llamada hacia/desde el espacio de conexión.

A partir de CMA 1.9.3 y CMS 2.0.1, los tonos DTMF no son obligatorios ahora que hay



que se agrega al cliente cuando la grabadora está presente en el callbridge al que está conectado el cliente o cuando se conoce por él. El botón de registro también se ha agregado a WebRTC desde CMS 2.3.

4. Crear un callProfile

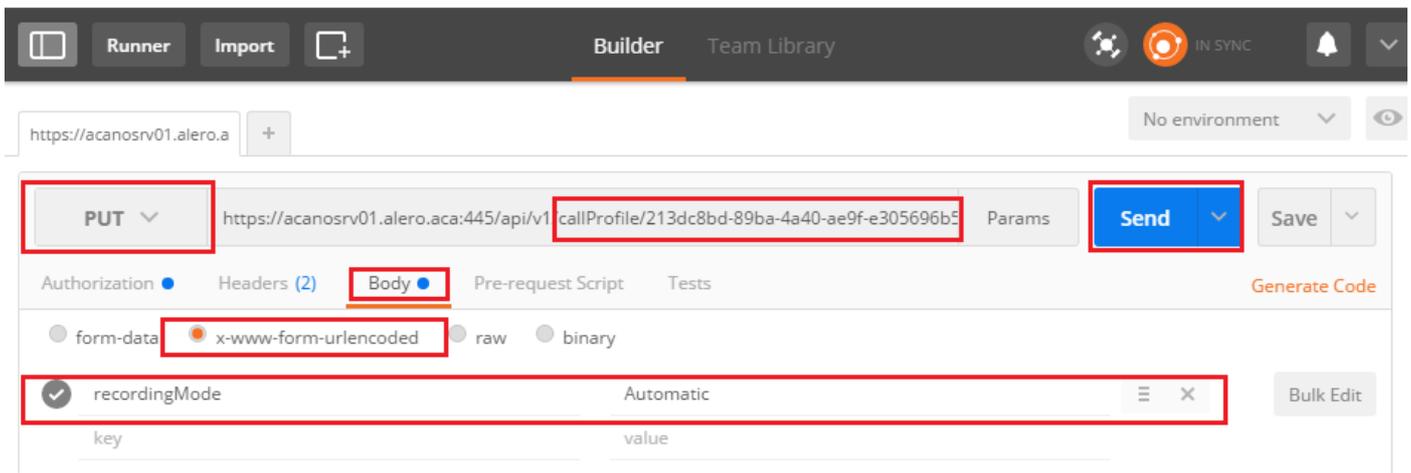
- Enviar un POST vacío con **https://<Callbridge_IP>:445/api/v1/callProfiles**
- Enviar un GET con la misma URL en (a), copiar la ID de callProfile, sin los presupuestos en el Bloc de notas
- Establezca el modo de grabación en el callProfile enviando un PUT con **https://<Callbridge_IP>:445/api/v1/callProfiles/<call profile ID>** y agregue el en BODY antes de ejecutar el PUT.

recordMode=Manual (si desea que los autores de llamadas empiecen a grabar usando entradas DTMF)

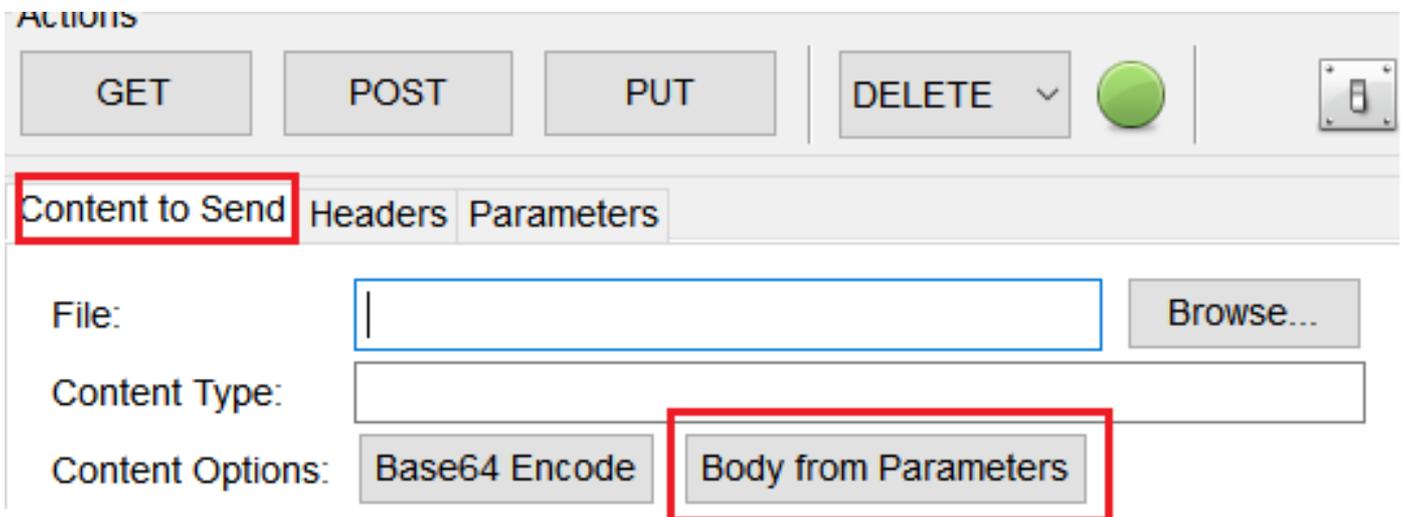
or

recordMode=Automático (si la grabación se iniciará automáticamente cuando se inicien llamadas)

Por ejemplo:



Nota: Si utiliza POSTER de firefox, debe seleccionar **Content to Send** y luego **Body from Parameters** antes de enviar el PUT/POST, de esta manera se compila en los códigos que el CB puede entender. Como en la siguiente imagen:



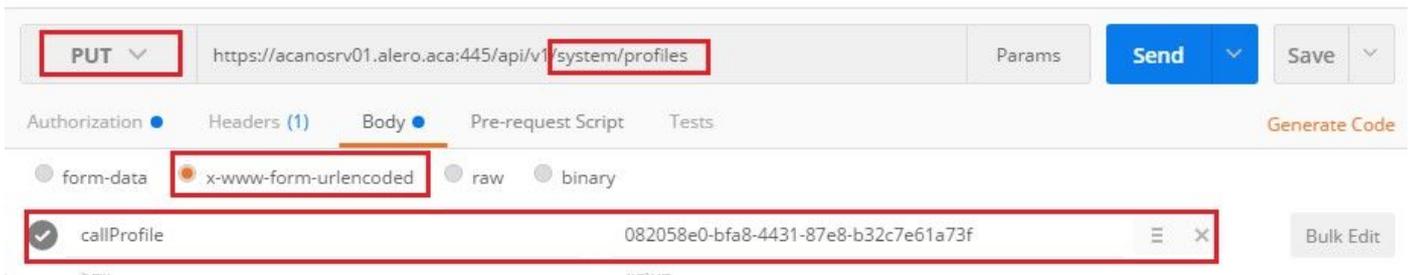
5. Agregar perfil de llamada a los perfiles del sistema

El callProfile define si las llamadas pueden ser grabaciones y si se pueden realizar con o sin intervención del usuario.

Enviar un PUT con https://<Callbridge_IP>:445/api/v1/system/profiles después de agregar el callProfile en BODY

callProfile=<call profile ID>

Por ejemplo:

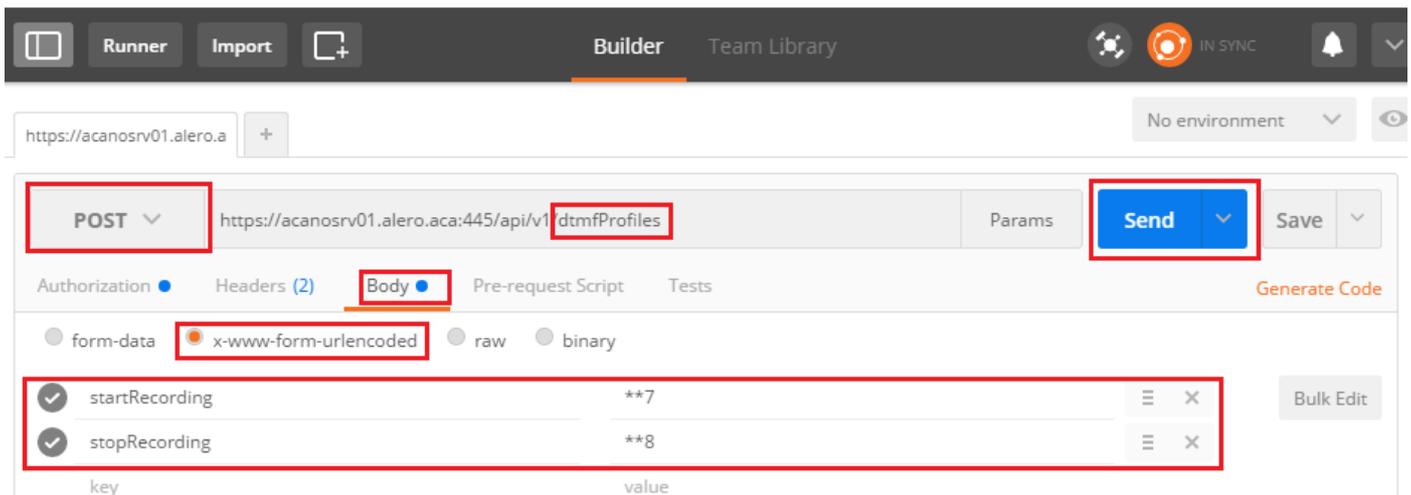


Si el modo de grabación se establece en Manual, debe establecer un perfil DTMF para definir cómo los usuarios pueden iniciar y detener grabaciones utilizando tonos DTMF.

6. Crear el perfil DTMF

a. Envíe una publicación con [https:// <Callbridge IP>:445/api/v1/dtmfProfiles](https://<Callbridge IP>:445/api/v1/dtmfProfiles) después de establecer `startRecording=**7` y `stopRecording=**8` (por ejemplo) en BODY como `startRecording=**7&stopRecording=**8`.

Por ejemplo:



b. Envíe un GET para ver el nuevo perfil DTMF y, a continuación, copie el ID sin los presupuestos en el bloc de notas.

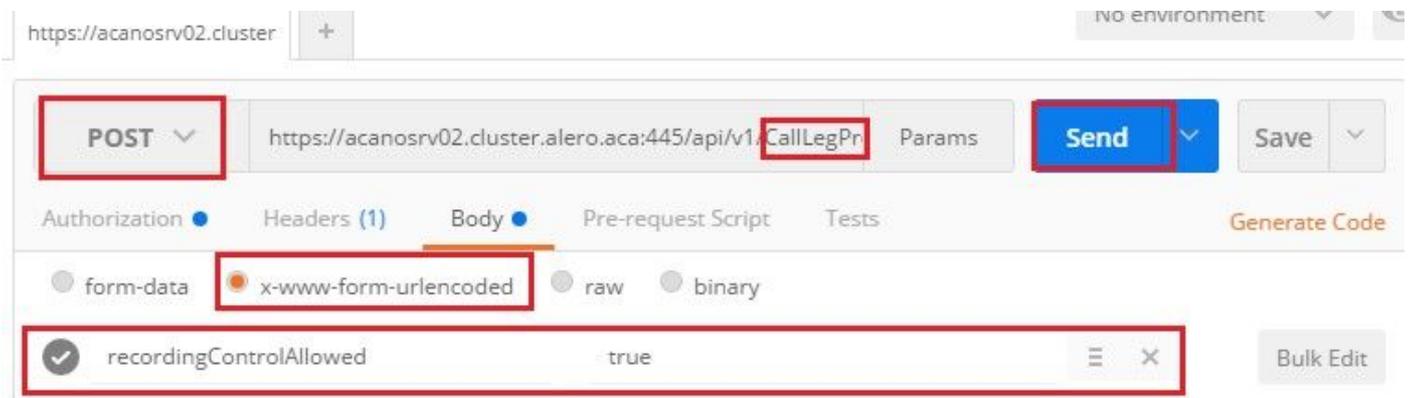
7. Crear perfil de CallLeg

CallLegProfiles determina el comportamiento de la llamada entrante. En este caso, determina si se puede grabar una llamada.

Cree un perfil de segmento de llamada de la siguiente manera:

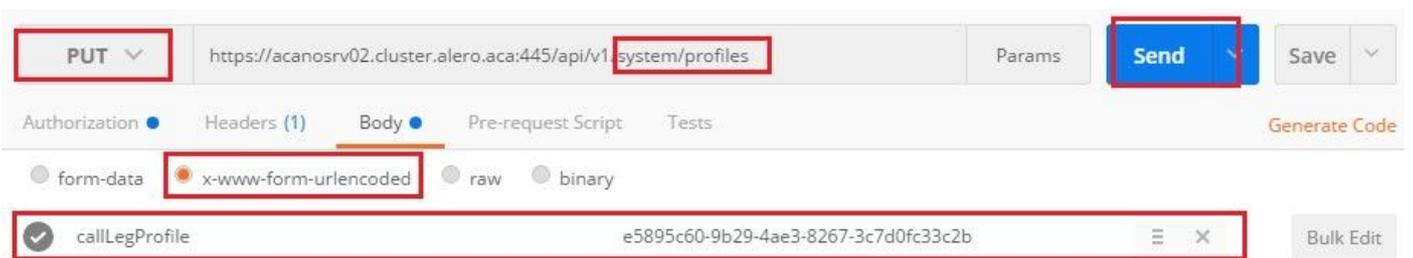
a. Envíe una publicación con <https://<Callbridge IP>:445/api/v1/CallLegProfiles> después de haber agregado la función de grabación `ControlAllowed=true` en el CUERPO:

Por ejemplo:



b. Aplique CallLegProfile, enviando un PUT con https://<Callbridge_IP>:445/api/v1/system/profiles y agregando callLegProfile=<callLegProfile_ID> en el CUERPO:

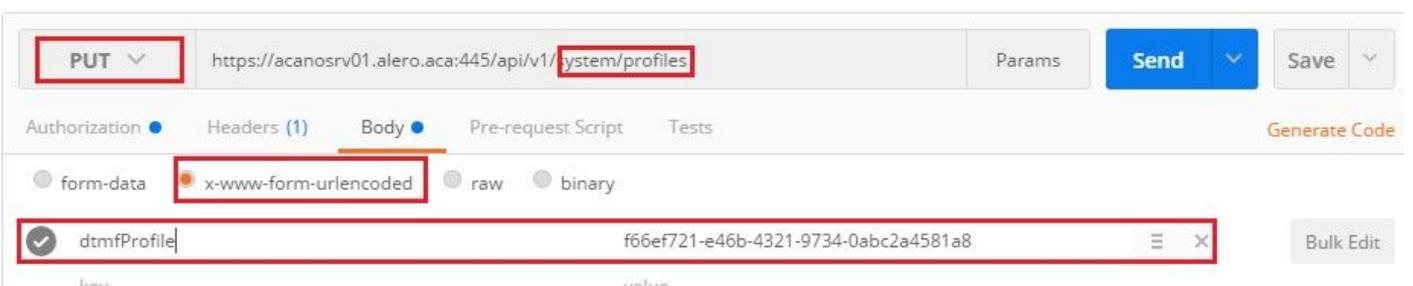
Por ejemplo:



8. Aplique el perfil DTMF:

Enviar un PUT con https://<Callbridge_IP>:445/api/v1/system/profiles después de agregar el dtmfProfile en BODY dtmfProfile=<dfmt Profile ID>

Por ejemplo:



Verificación

Utilice esta sección para confirmar que la configuración funcione correctamente.

1. Una vez configurado, verifique su estado con estos comandos, puede obtener un resultado similar al de la siguiente imagen

registrador

CB local independiente:

```
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
```

O si se agrupa 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. Enviar un GET para ver el perfil del sistema, debe ver el **callProfile**, **CallLegProfile** y **dtmfProfile** (suponiendo que se hayan configurado todas) en el resultado con

[https:// <Callbridge_IP>:445/api/v1/system/profiles](https://<Callbridge_IP>:445/api/v1/system/profiles)

Por ejemplo:

```
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. Para comprobar qué se ha configurado en el CallProfile, utilice esto en la API

[https:// <Callbridge_IP>:445/api/v1/callProfiles/<callProfile_ID>](https://<Callbridge_IP>:445/api/v1/callProfiles/<callProfile_ID>)

Se muestran los métodos de grabación configurados, Automático o Manual, como se muestra en la siguiente ilustración:

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

4. Para comprobar lo que está configurado en el CallLegProfile, utilice esta API

[https:// <Callbridge_IP>:445/api/v1/callLegProfiles/<callLegProfile_ID>](https://<Callbridge_IP>:445/api/v1/callLegProfiles/<callLegProfile_ID>)

Ejemplo de salida:

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

5. Para comprobar qué se ha configurado en el perfil DTMF, utilice esto en la API

[https:// <Callbridge_IP>:445/api/v1/dtmfProfiles/<dtmfProfile_ID>](https://<Callbridge_IP>:445/api/v1/dtmfProfiles/<dtmfProfile_ID>)

Esto muestra que se han establecido métodos de grabación, ya sea Automático o Manual, como se muestra:

```

<?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>

```

Nota: Los perfiles DTMF no funcionan en las llamadas punto a punto, por lo que sólo puede utilizar la grabación manual en un espacio.

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Para mostrar lo que se registra con respecto al grabador, ejecute el comando:

seguimiento de syslog

La salida mostrada es similar a esta:

```

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

```

En este ejemplo, acanosrv05 es el servidor que aloja el registrador y los otros nodos CB que se conectan a él son 10.48.54.75 y 10.48.54.76.

Esto muestra que el CB remoto se conecta y autentica correctamente con el Grabador.

Si la grabadora es local al CB, la conexión provendría de la IP de loopback:

```
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
```

Nota: La mayoría de los registros relacionados con los procesos de grabadora se muestran en el syslog como recorder-proxy, lo que indica dónde podría estar fallando el registrador.

Otros syslogs se muestran de la siguiente manera para la grabadora:

En este caso, se encuentra un dispositivo de grabación y la grabación se inicia automáticamente:

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

Si la grabación falla, compruebe si se encuentra un dispositivo de grabación:

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

Si ve tal advertencia, verifique el certificado en el registro de grabadores para asegurarse de que es el correcto utilizado para configurar el CB.

Verifique el syslog para ver si el almacenamiento NFS está montado:

- Si el almacenamiento NFS no está montado, se muestra "Error al montar el almacenamiento NFS"
- Verifique y asegúrese de que la carpeta NFS establecida en el servidor de grabadores:/nombre de carpeta es la misma que la configurada en el almacenamiento NFS

Ejecute la API para comprobar las alarmas relacionadas con la grabadora:

- **https://<callBridge_IP>api/v1/system/alarms**
- Si hay poco espacio en disco, se muestra "graborderLowDiskSpace" (GrabadoraLowDiskSpace)
- Luego verifique que el almacenamiento NFS al que hace referencia el registrador tenga suficiente espacio en disco

Información Relacionada

- [Soporte Técnico y Documentación - Cisco Systems](#)