

MeetingApps für die Dateifreigabe konfigurieren und Fehler beheben

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Netzwerkdigramm](#)

[Konfigurieren](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Dateifreigabesymbol ist nicht sichtbar](#)

[Dateien hinzufügen und Freigabeschaltflächen sind für die Benutzer nicht sichtbar](#)

[Datei-Upload fehlgeschlagen](#)

Einleitung

Dieses Dokument beschreibt den schrittweisen Prozess zur Konfiguration und Fehlerbehebung von MeetingApp für die Dateifreigabe auf dem Cisco Meeting Server (CMS).

Mit Beiträgen von Vikas Kumar, Sateesh Katukam, Aviral Pal, Cisco TAC Engineers.

Voraussetzungen

Anforderungen

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

- Grundlegendes zur CMS-API für die Konfiguration von Meeting-Anwendungen
- Cisco Meeting Server Version 3.5 und höher

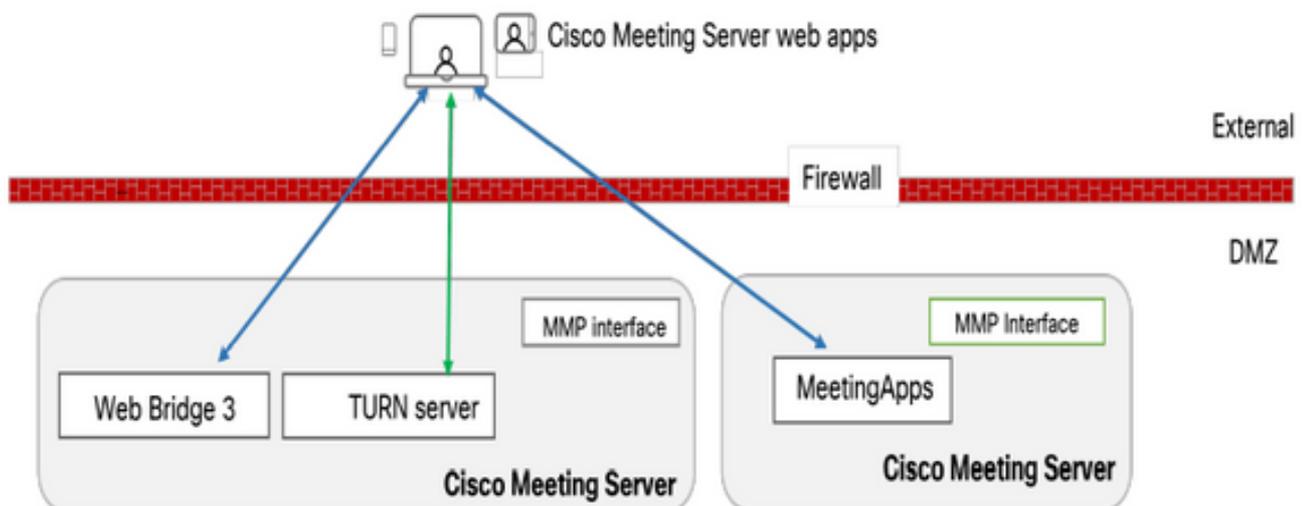
Verwendete Komponenten

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

Hintergrundinformationen

- Der MeetingApp-Dienst wurde eingeführt, um die Dateifreigabe von Web App Version 3.5 zu unterstützen. Meeting-Teilnehmer können Dateien in einem Meeting freigeben.
- Der MeetingApps-Dienst muss im eigenständigen Meeting Server-Knoten konfiguriert werden, und auf diesem Knoten müssen keine anderen Dienste ausgeführt werden. Die MeetingApps können je nach Anforderung für externe Benutzer und intern im DMZ-Netzwerk konfiguriert werden.
- Der MeetingApps-Service muss im DMZ-Netzwerk bereitgestellt werden, damit externe Benutzer Dateien gemeinsam nutzen können. Er muss einer öffentlichen IP-Adresse zugewiesen werden, und die Firewall-Ports auf der DMZ müssen für den öffentlichen Zugriff geöffnet werden. Der MeetingApps-Dienst kann auf einem Meeting Server 1000 oder Meeting Server auf VM-Bereitstellungen konfiguriert werden.
- Nur ein angemeldeter Web-App-Benutzer mit entsprechenden Berechtigungen kann Dateien in einem Meeting freigeben.
- Die Dateifreigabe unterstützt maximal fünf Dateien mit jeweils 10 MB.
- Die freigegebene Datei kann nur während des Meetings heruntergeladen werden. Teilnehmer, die nach Beginn eines Meetings dem Meeting beitreten, können nur die Dateien anzeigen oder herunterladen, die nach dem Meeting freigegeben werden.
- EXE-Dateien können nicht freigegeben werden.
- MeetingApps-Dienste können nicht auf einem Meeting Server 2000 konfiguriert werden.
- Die Funktion zur Dateifreigabe funktioniert nicht, wenn Ihr Cluster über eine Meeting Server 2000-Bereitstellung verfügt.

Netzwerkdiagramm



Web-Bridges in Ihrer Umgebung müssen für die Kommunikation mit MeetingApps konfiguriert sein, damit die in der Konferenz freigegebenen Dateien hochgeladen oder heruntergeladen werden können.

Konfigurieren

Gehen Sie folgendermaßen vor, um Folgendes zu konfigurieren:

1. SSH in die MMP und melden Sie sich an.

2. Konfigurieren Sie die von MeetingApps verwendete Schnittstelle und den Port für die Kommunikation mit dem folgenden Befehl:

Meetingapps https listen <Schnittstelle> <Port>

```
cms.lab.local> meetingapps https listen a 8443
```

3. Konfigurieren Sie das Zertifikatschlüsselpaar für MeetingApps mithilfe des Befehls

Meetingapps https certs <Schlüsseldatei> <cert-fullchain-Datei>

```
cms.lab.local> meetingapps https certs cms csr_005056BD020C.pem CABundle.crt
```

4. Generieren Sie den geheimen Schlüssel mit dem folgenden Befehl:

Meetingapps gensecret

Kopieren Sie den generierten Schlüssel, um die Web Bridge später zu konfigurieren (bei Schritt 7). Bei jeder Ausführung des Befehls wird ein neuer geheimer Schlüssel generiert, und Web Bridge muss mit dem neuen Schlüssel konfiguriert werden.

```
cms.lab.local> meetingapps gensecret
4prtW5Bl10yIV45iDfdI2Zj19CuZynv2Ct6P5kLJB8SMujht6ykpMPpOHqv0l3mYXs1Qys4DsmsyKDZC
ChvDkxWH8lcxUzheiogRdrDCblEp77rETKlFeRulcXOOE63jH2GNVOMB0fAE27CLmB5dzKoHLQp2ZVQs
bdtJ3eXnt2tBuhJnhAhXzTCmcbJMOkTXu3EVYq25qxwfESxrc8j3ZoV2fgdRFPw5qM93yVEfsUfYG4gz8
NMNX6Jc8T3FdrXq5
```

5. Aktivieren Sie den MeetingApps-Dienst mithilfe des Befehls

Meetingapps aktivieren

```
cms.lab.local> meetingapps enable
SUCCESS: HTTPS Key and certificate pair match
SUCCESS: HTTPS full chain of certificates verifies correctly
SUCCESS: meetingapps enabled
```

6. Vor der Konfiguration der Web Bridge für die Verbindung mit MeetingApps müssen alle Web Bridges mithilfe des folgenden Befehls deaktiviert werden:

webbridge3 deaktivieren

```
cms.lab.local> webbridge3 disable
```

7. Alle Web Bridges in Ihrer Einrichtung müssen mit den MeetingApps kommunizieren, um die in der Konferenz freigegebenen Dateien hoch- oder herunterzuladen. Konfigurieren Sie die Web Bridge für die Verbindung mit den MeetingApps mithilfe des folgenden Befehls:

webbridge3 Meetingapps fügen <Hostname> <Port> <Sekretärin> hinzu

```
cms.lab.local> webbridge3 meetingapp add 10.106.84.xx 8443 cvsgghdybsnow
```

8. Aktivieren Sie alle Web Bridges mithilfe des Befehls

webbridge3 enable

9. Dateifreigabe in einem Meeting : API-Parameter **fileReceiveAllowed** (true|false) wurde eingeführt, um die Dateifreigabe auf CallProfile- oder Anrufebene zu aktivieren oder zu deaktivieren.

Legen Sie **fileReceivedAllowed** in callProfile auf **true fest**, und weisen Sie es der CoSpace- oder Systemebene zu.

/api/v1/callProfiles/07f4ae27-206a-4206-ba87-419c9ac891f1

participantLimit	<input type="checkbox"/>	1000	- present
locked	<input type="checkbox"/>	true	- present
recordingMode	<input type="checkbox"/>	<unset>	
streamingMode	<input type="checkbox"/>	<unset>	
passcodeMode	<input type="checkbox"/>	<unset>	
passcodeTimeout	<input type="checkbox"/>		
gatewayAudioCallOptimization	<input type="checkbox"/>	<unset>	
hyncConferenceMode	<input type="checkbox"/>	<unset>	
lockMode	<input type="checkbox"/>	needsActivation	- present
sipRecorderUri	<input type="checkbox"/>		
sipStreamerUri	<input type="checkbox"/>		
muteBehavior	<input type="checkbox"/>	<unset>	
messageBannerText	<input type="checkbox"/>		
chatAllowed	<input type="checkbox"/>	<unset>	
raiseHandEnabled	<input type="checkbox"/>	<unset>	
notesAllowed	<input type="checkbox"/>	<unset>	
captionsAllowed	<input type="checkbox"/>	<unset>	
backgroundBlurAllowed	<input type="checkbox"/>	<unset>	
fileReceiveAllowed	<input checked="" type="checkbox"/>	false	

Modify

10. Zulässiger Dateiupload: API-Parameter **fileUploadAllowed** (true|false) wurde eingeführt, damit der Benutzer die Freigabedatei im CallLegProfile zulassen kann.

Legen Sie **fileUploadAllowed** in callLegProfile auf **true fest**, und weisen Sie es der Cospace- oder Systemebene zu.

api/v1/callLegProfiles/265f0b94-0c06-425d-9686-16d288b6032d

needsActivation	<input type="checkbox"/>	<unset> v
defaultLayout	<input type="checkbox"/>	telepresence v - present
participantLabels	<input type="checkbox"/>	<unset> v
presentationDisplayMode	<input type="checkbox"/>	<unset> v
presentationContributionAllowed	<input type="checkbox"/>	true v - present
presentationViewingAllowed	<input type="checkbox"/>	true v - present
endCallAllowed	<input type="checkbox"/>	<unset> v
disconnectOthersAllowed	<input type="checkbox"/>	<unset> v
addParticipantAllowed	<input type="checkbox"/>	<unset> v
muteOthersAllowed	<input type="checkbox"/>	<unset> v
videoMuteOthersAllowed	<input type="checkbox"/>	<unset> v
muteSelfAllowed	<input type="checkbox"/>	true v - present
videoMuteSelfAllowed	<input type="checkbox"/>	true v - present
changeLayoutAllowed	<input type="checkbox"/>	true v - present
layoutTemplate	<input type="checkbox"/>	
controlRemoteCameraAllowed	<input type="checkbox"/>	<unset> v
audioGainMode	<input type="checkbox"/>	<unset> v
meetingTitlePosition	<input type="checkbox"/>	<unset> v
chatContributionAllowed	<input type="checkbox"/>	<unset> v
noteContributionAllowed	<input type="checkbox"/>	<unset> v
changeRoleAllowed	<input type="checkbox"/>	<unset> v
captionContributionAllowed	<input type="checkbox"/>	<unset> v
fileUploadAllowed	<input checked="" type="checkbox"/>	true v

Modify

Überprüfung

Überprüfen Sie die Konfiguration, indem Sie den folgenden Befehl eingeben: **Webbridge3**

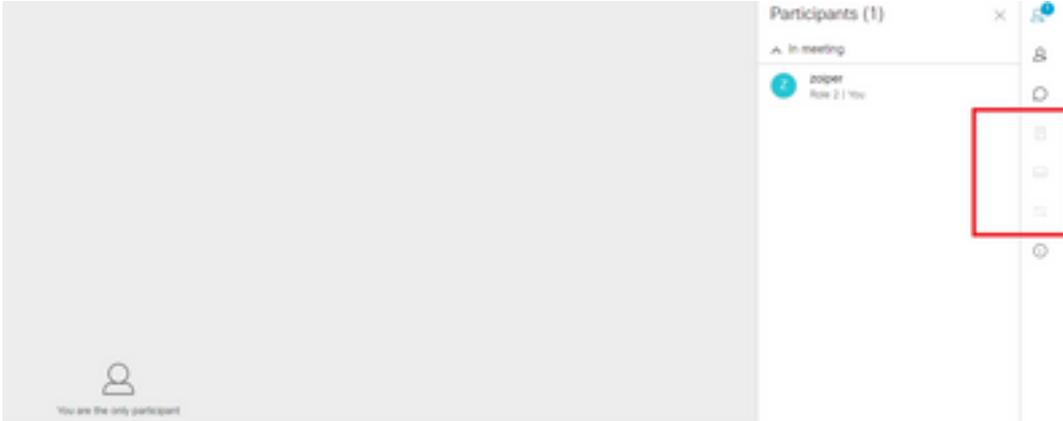
```
cms.lab.local> webbridge3
Enabled : true
HTTPS listening ports and interfaces : a:443
HTTPS Key file : cms_csr_005056BD020C.key
HTTPS Full chain certificate file : Chain.crt
HTTPS Frame-Ancestors : none
HTTP redirect : Enabled, Port:80
C2W listening ports and interfaces : a:9999
C2W Key file : cms_csr_005056BD020C.key
C2W Full chain certificate file : Chain.crt
C2W Trust bundle : Chain.crt
Meetingapps address : 10.106.80.100
Meetingapps port : 8443
Beta options : none
```

```
cms.lab.local> meetingapps
Enabled : true
Https interface : a
Https port : 8445
Https key file : cms_csr_005056BD020C.key
HTTPS Full chain certificate file : cms_csr_005056BD020C.pem
SecretKeyGenerated : true
```

Fehlerbehebung

Um die Verfügbarkeit der MeetingApps zu überprüfen, können Sie die API verwenden.
https://hostname/IP_Adresse:port/api/ping

Dateifreigabesymbol ist nicht sichtbar



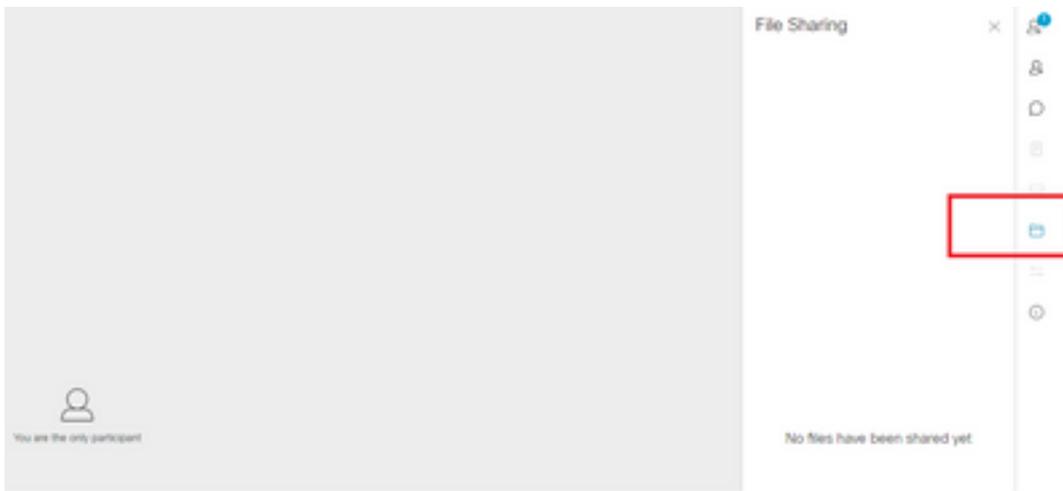
Stellen Sie sicher, dass Meeting-Apps und webbridge3 korrekt konfiguriert sind und beide Dienste im CMS ausgeführt werden. Unter calls fileReceiveAllowed API parameter wird auf der Anrufebene ODER der Anrufprofile-API auf true gesetzt.

`/api/v1/calls/29789762-a6ce-4131-9da3-9d0633615bf1`

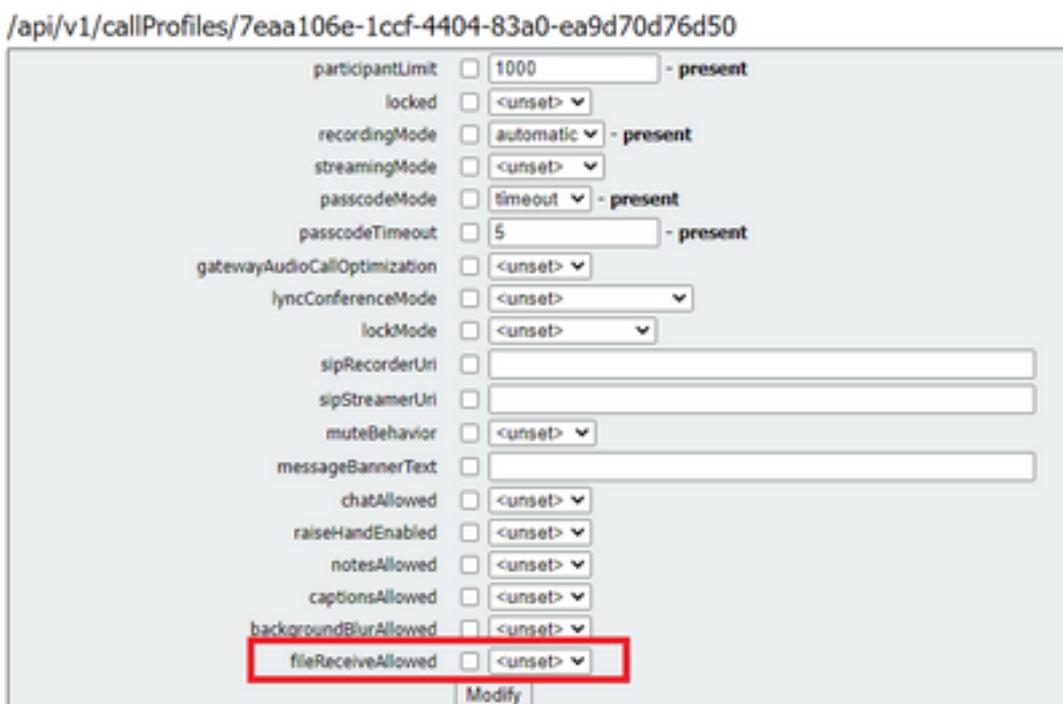
locked	<input type="checkbox"/>	false	- present
recording	<input type="checkbox"/>	true	- present
streaming	<input type="checkbox"/>	false	- present
allowsAllMuteSelf	<input type="checkbox"/>	false	- present
allowsAllPresentationContribution	<input type="checkbox"/>	false	- present
joinAudioMuteOverride	<input type="checkbox"/>	<unset>	
messageText	<input type="checkbox"/>		
messagePosition	<input type="checkbox"/>	middle	- present
messageDuration	<input type="checkbox"/>	0	- present
activeWhenEmpty	<input type="checkbox"/>	false	- present
panePlacementHighestImportance	<input type="checkbox"/>		
panePlacementSelfPaneMode	<input type="checkbox"/>	<unset>	
panePlacementActiveSpeakerMode	<input type="checkbox"/>	<unset>	
messageBannerText	<input type="checkbox"/>		
chatAllowed	<input type="checkbox"/>	true	- present
raiseHandEnabled	<input type="checkbox"/>	true	- present
notesAllowed	<input type="checkbox"/>	false	- present
captionsAllowed	<input type="checkbox"/>	false	- present
backgroundBlurAllowed	<input type="checkbox"/>	false	- present
fileReceiveAllowed	<input type="checkbox"/>	false	- present

DateiReceiveAllowed aktivieren: Auf Anrufebene

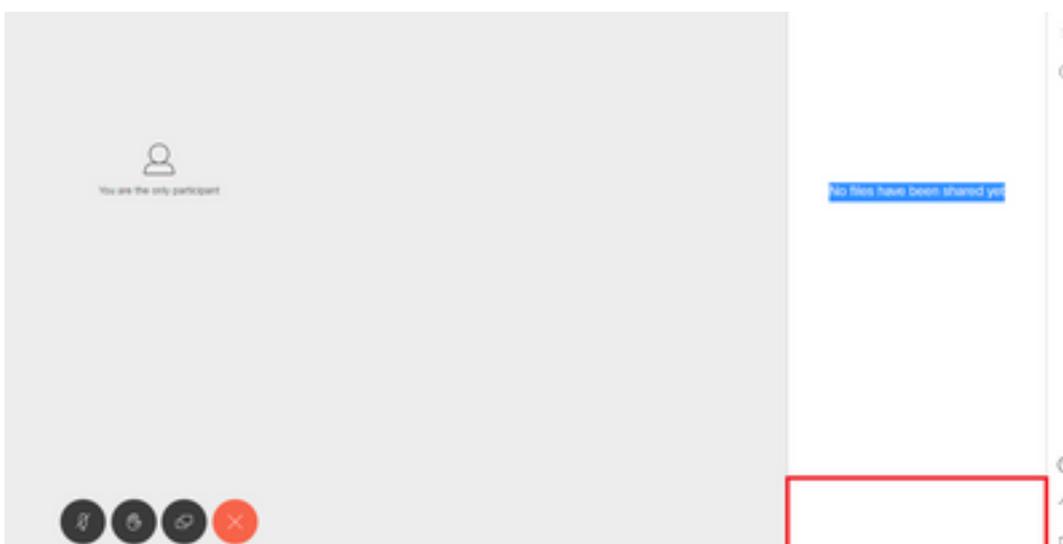
Nach der Aktivierung wird die Dateifreigabe der Option angezeigt.



Auf Ebene der Anrufprofile: Ein CallProfile kann in einem Cospace oder auf Systemebene zugewiesen werden.

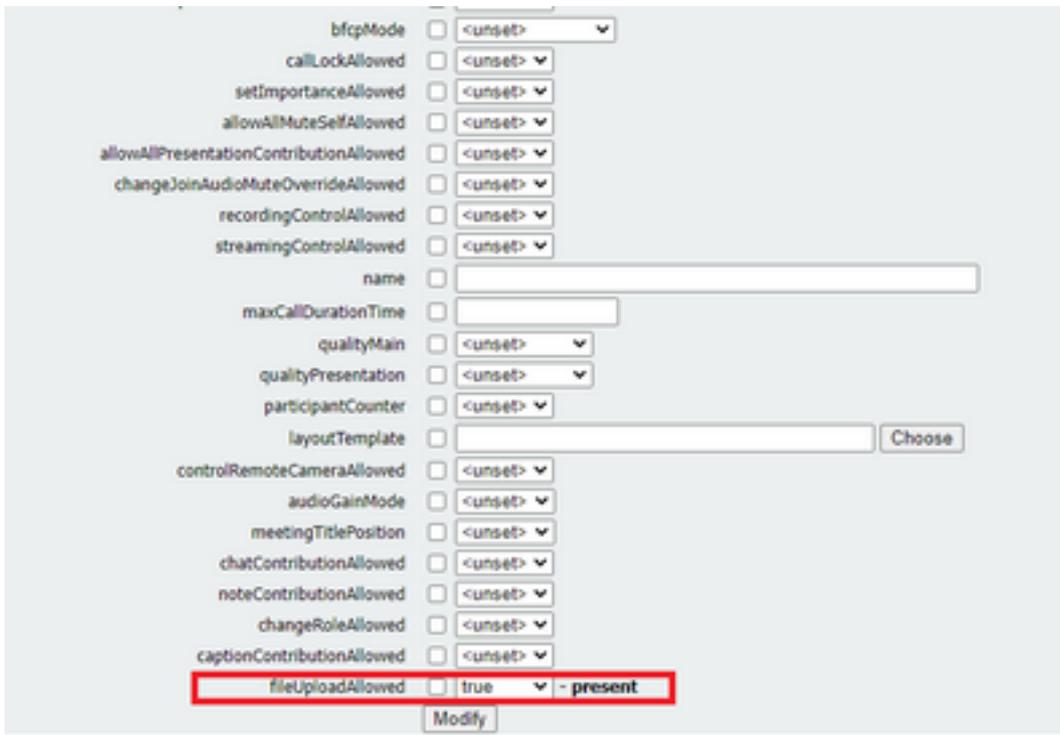


Dateien hinzufügen und Freigabeschaltflächen sind für die Benutzer nicht sichtbar

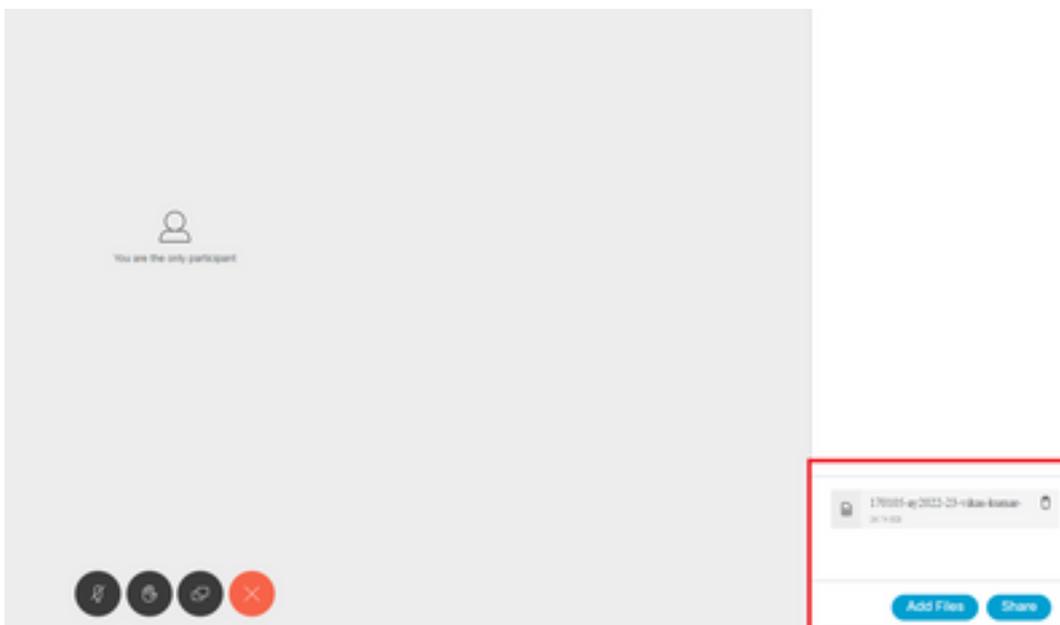


Das Hinzufügen von Dateien und die Freigabeschaltflächen sind für Benutzer erst sichtbar, wenn fileUploadAllowed auf true festgelegt ist, damit ein Teilnehmer Dateien in einem Meeting freigeben kann. fileUploadAllowed unterstützt die callLegProfiles-Methode oder die callLegs-Methode

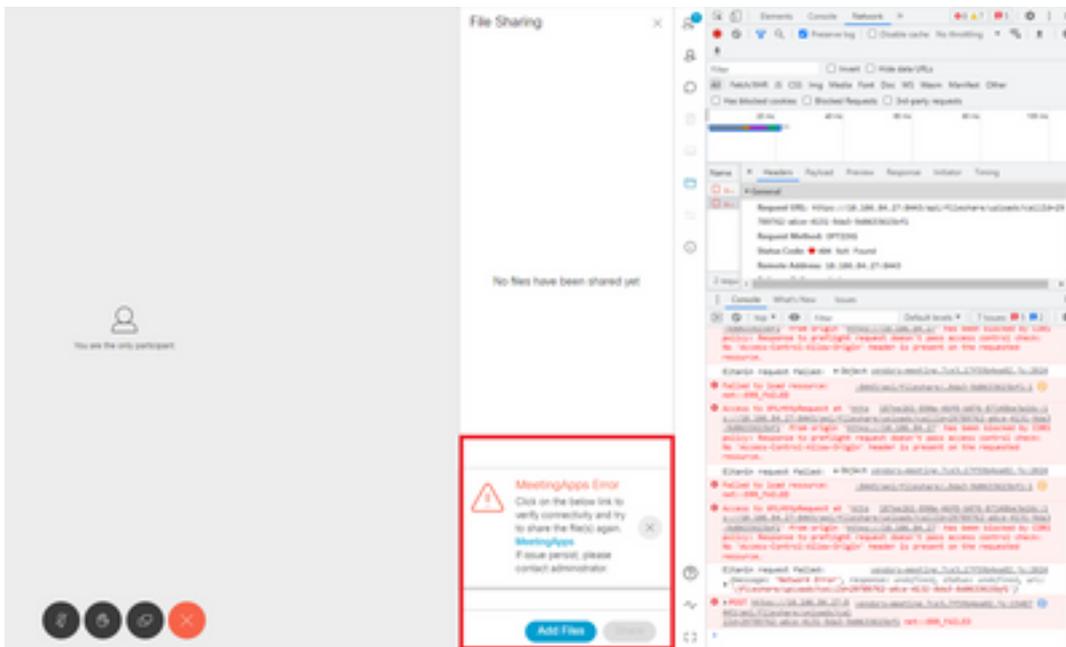
callLegProfiles kann im Cospace oder auf Systemebene zugewiesen werden.



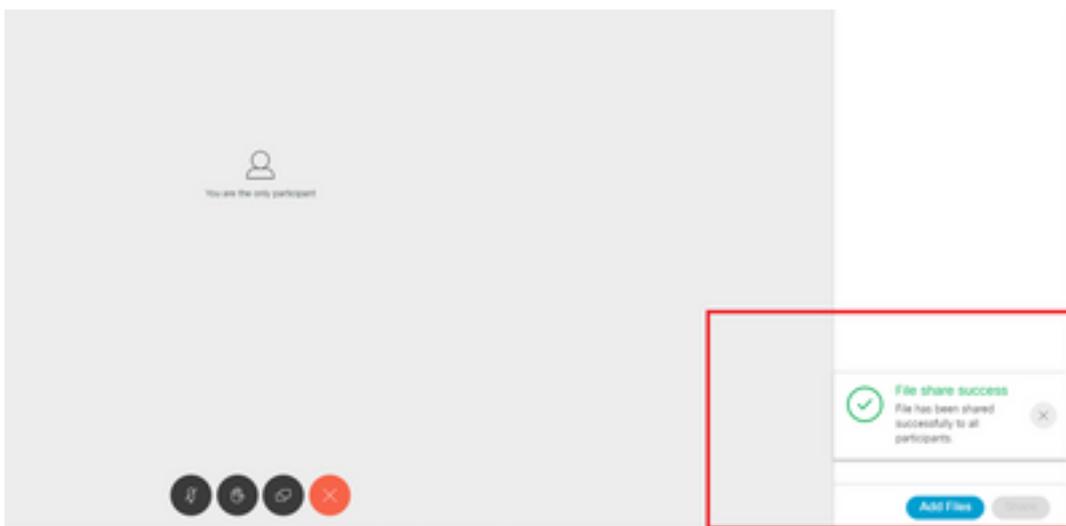
Nach dieser Änderung sehen wir, dass die Schaltfläche "Datei hinzufügen und freigeben" aktiviert ist:



Datei-Upload fehlgeschlagen



Dieses Problem ist auf ein Kommunikationsproblem zwischen Client und Server oder ein Problem zwischen Meeting-Anwendungen und Webbridge-Konfiguration zurückzuführen. Nachdem das Problem behoben wurde, wird die Datei schließlich erfolgreich hochgeladen:



Informationen zu dieser Übersetzung

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