
Cisco Meeting App

Troubleshooter for desktop and mobile apps, WebRTC, and SIP endpoints

November 19, 2018

Contents

1	What's changed?	5
2	Problems Installing a Cisco Meeting App	6
2.1	Windows app msi installer not working	6
2.1.1	.msi file cannot be found	6
2.1.2	.msi installer is downloaded but doesn't run.	6
2.2	OS X installer not working	6
2.2.1	dmg file cannot be found	7
2.2.2	dmg installer downloads but is not running	7
3	Issues Logging into a Cisco Meeting App	8
3.1	App reports "no network" in the sign in dialog	8
3.2	App reports "unable to resolve ip address" in the sign in dialog	8
3.3	App reports "unable to connect – check your username and try again" in the sign in dialog	9
3.4	App reports "unable to connect –try again later" in the sign in dialog	9
3.5	App reports "username or password is incorrect" in the sign in dialog	10
3.6	App reports certificate warning	11
3.6.1	Certificate warnings on iOS devices	11
4	Issues Logging out of a Cisco Meeting App	12
4.1	App not responsive	12
5	Issues after logging into a Cisco Meeting App	13
5.1	App diagnostic log	13
5.2	Something missing in the app user interface	13
5.3	Microphone, speaker and camera devices issue	13
5.4	High latency/packet loss when using clustered Call Bridges	14
5.5	Cannot delete chat messages	14
6	Issues with spaces using the Cisco Meeting App	15
6.1	Negative values in call duration	15
6.2	Participants not going away	15
7	Audio Issues	16
7.1	Participant cannot hear the other participant	16
7.2	One participant's audio is very low	16

7.3	Participant is receiving corrupted audio	16
7.4	Echo on the call	17
7.5	Background noise	17
8	Video Issues	18
8.1	Participant is getting no video	18
8.2	Video is low resolution	19
8.3	Video is badly corrupted	19
8.4	Layout issues	20
8.5	Content sharing/receiving issue	20
9	Issues with features when signed in	21
9.1	Invite button is missing	21
9.2	Missing invitation details	21
9.3	Cannot remove a participant during a call	21
9	Guest issues	23
9.4	Guest access disabled	23
9.5	Cannot join call as a guest using the Chrome browser	23
9.6	Intelligent pairing is not detecting the nearby video system	24
9	Notifications	25
9.7	Notifications not shown by the iOS app when it is not visible on the screen	25
10	Space Management Issues	26
10.1	Video address does not match the name of the space	26
10.2	Video address not set	26
10.3	A member of a space is missing	27
11	Issues with SIP Endpoints	28
11.1	Call cannot be established	28
11.2	Call cannot be hung up	29
11.3	Participant doesn't receive audio/video	30
11.4	Participant receives bad audio/video	30
11.5	Dual stream/presentation Issue	31
11.6	Issues moving call from the app to an endpoint	32
12	WebRTC Browser Certificate Issues	33
12.1	Google Chrome - "Cannot connect to the real join.example.com" or "Your connection is not private"	33

12.2	Issues with bundled certificates	35
13	WebRTC Client Issues	37
13.1	WebRTC client connection issues	37
13.2	Unable to reach web client landing page	37
13.3	WebRTC client call drops	39
14	Customization Issues	40
14.1	Customized feature not working	40
Appendix A	Collecting Logs	1
Collecting logs	1
Collecting a pcap file	1
Collecting the live.json file	3
Collecting Diagnostic Information from the Cisco Meeting App	3
Collecting diagnostic information from the Cisco Meeting Server	4
Obtaining log and crash files for a Windows or OS X app	4
Obtaining crash files for an iOS app	4
Collecting a SIP and DNS trace	5
Collecting XMPP log files	6
Appendix B	Client Diagnostic Log Analysis	8
Media sessions info – audio session	8
Media sessions info – video session	9
Media diagnostics	10
Call Bridge selection	11
Appendix C	Server Diagnostic Log Analysis	12
Recent log messages	12
Finding the corresponding client log	12
Audio media session	13
Video media session	13
Client device information	15
Appendix D	Log Analysis	16
Cisco Legal Information	18
Cisco Trademark	20

1 What's changed?

Date	Summary of changes
Nov 2018	A new section Section 3.6.1 to troubleshoot certificate warnings in iOS devices has been added.

2 Problems Installing a Cisco Meeting App

2.1 Windows app msi installer not working

If you are having issues getting the msi installer on to your Windows desktop, find the appropriate issue in this section and follow the suggested steps.

2.1.1 .msi file cannot be found

1. Check the msi download URL
2. SSH to the MMP and type the command `webbridge` to display the msi download URL
3. Copy and paste the msi download URL into the browser's address bar and retry the download.

If the download fails again, make sure that the configured URL is correct (matches the path to the installer) and that the msi is deployed correctly.

2.1.2 .msi installer is downloaded but doesn't run.

1. Check that your operating system is supported by Cisco Meeting App.

You can find the information in the [Operating System Support](#) section in **App FAQs for admins**.

2. Try the Cisco msi file.

Get the msi file from Cisco Support and see whether the msi file can successfully install the app. If it does, check your msi file and messages in any log files to try to pinpoint the issue.

2.2 OS X installer not working

If you are having issues getting the dmg installer on your Mac, find the appropriate issue in this section and follow the suggested steps.

Do the same if a guest is trying to enter a meeting via browser on a Mac, and the Mac attempts to download and install the OS X app, but fails.

2.2.1 dmg file cannot be found

1. SSH to the MMP and type the command **webbridge** to display the dmg download URL.
2. Copy and paste the dmg download URL into the browser's address bar and retry the download.

If the download fails again, make sure that the configured URL is correct (matches the path to the installer) and that the dmg is deployed correctly.

2.2.2 dmg installer downloads but is not running

1. Check that the operating system that you are running is supported by Cisco Meeting App.

You can find the information in the [Operating System Support](#) section in **App FAQs for admins**.

2. Try the Cisco dmg file.

Get the dmg file from the Cisco website and see whether it can successfully install the Cisco Meeting App. If it does, check your dmg file and messages in any log files to try and pinpoint the issue.

3 Issues Logging into a Cisco Meeting App

If your users are experiencing issues when logging into a Cisco Meeting App, ask for the error message and follow the suggested steps.

3.1 App reports “no network” in the sign in dialog

Check the network connection by trying to open a standard web sites such as www.google.com.

If your internet connection is good, there may be a firewall issue. Make sure that port 5222 is open.

3.2 App reports “unable to resolve ip address” in the sign in dialog

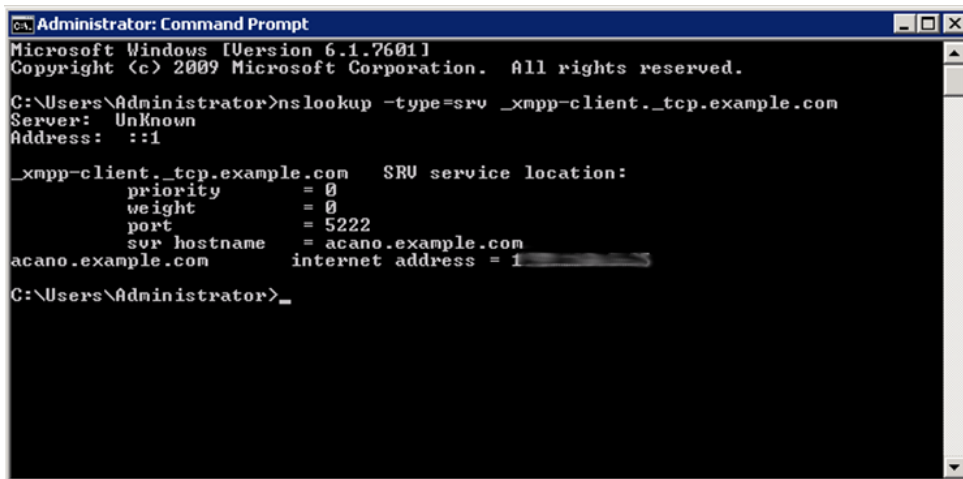
This message means that the app is unable to resolve a domain to an IP address.

1. Ask the user to look up the domain using `nslookup`.

For example, at the command prompt type your equivalent of

```
nslookup -type=srv _xmpp-client._tcp.example.com
```

to see whether the expected IP address and port are displayed, for example:



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nslookup -type=srv _xmpp-client._tcp.example.com
Server: Unknown
Address: ::1

_xmpp-client._tcp.example.com SRV service location:
    priority = 0
    weight = 0
    port = 5222
    srv hostname = acano.example.com
acano.example.com internet address = 1[REDACTED]

C:\Users\Administrator>
```

If there are multiple records, the one with the lowest priority and highest weight is selected first.

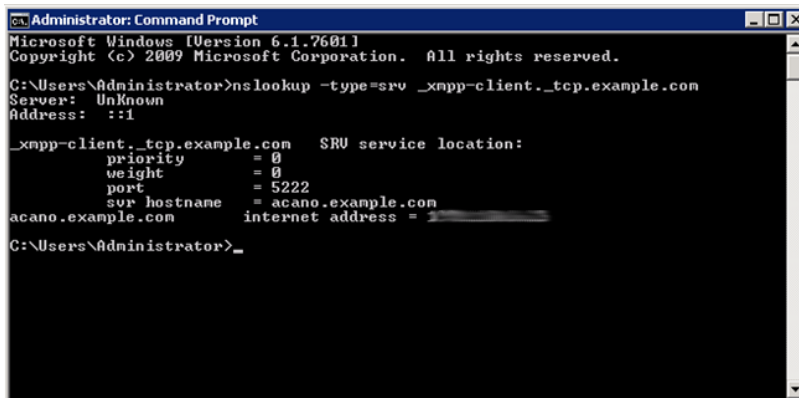
3.3 App reports “unable to connect – check your username and try again” in the sign in dialog

1. Check the xmpp-client SRV records and DNS A record.

Either they are wrongly configured or they are not configured yet. For example, at the command prompt, type your equivalent of

```
nslookup -type=svr _xmpp-client._tcp.example.com
```

to see whether you see the expected IP and port.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nslookup -type=svr _xmpp-client._tcp.example.com
Server: Unknown
Address: ::1

_xmpp-client._tcp.example.com SRV service location:
    priority = 0
    weight = 0
    port = 5222
    svr hostname = acano.example.com
acano.example.com internet address = 192.168.1.100

C:\Users\Administrator>
```

3.4 App reports “unable to connect –try again later” in the sign in dialog

This message means that the domain has resolved to an IP address but the XMPP server does not respond.

1. Check whether the resolved IP address is reachable (that is, is port 5222 to XMPP server blocked).

At the command prompt, try to telnet port 5222 via puTTY. The following is an example of trying to telnet a Cisco Meeting Server via port 5222 on a Cisco router. If you get connection refused, it means either the port is blocked by network or, the server is not running.

```

User Access Verification
Password:
881wB>en
Password:
881wB#telnet 192.168.25.2
Trying 192.168.25.2 ...
% Connection refused by remote host
881wB#telnet 192.168.25.2
Trying 192.168.25.2 ... Open

```

2. Check that the domain part of the sign in username is the same as the XMPP domain, for example:

login username: fredsmith@example.com

xmpp domain: example.com

To perform the check, SSH to the MMP and type the command **xmpp** to see the XMPP domain. If the login username domain part differs from the XMPP domain, change the login username domain part to match the XMPP domain.

3.5 App reports “username or password is incorrect” in the sign in dialog

1. Open the Core server logs and search for the LDAP lookup; has the LDAP account been suspended or is it wrong?

Date	Time	Logging level	Message
2015-04-04	15:54:31.164	Info	no user 'fredsmith@example.com' found for authorisation
2015-04-04	15:54:31.164	Info	unsuccessful login request from fredsmith@example.com

2. Check that the user is listed in the on the **Status > Users** page on the web admin.
3. Check whether the user can sign in to another application using these credentials, and check with your LDAP admin team.

3.6 App reports certificate warning

If you get the warning “Certificate failure. The connecting server is not presenting a valid certificate”:

1. Check the XMPP certificate requirement in our [Certificate guide](#), in particular the need to specify:
 - the DNS record for the XMPP server in the CN field of the certificate
 - the XMPP domain name and the DNS record for the XMPP server in the subjectAltName field.

If you still have this issue, send Cisco Support the following:

- the XMPP certificate,
- the output from the MMP command `xmpp`,
- the output of a DNS lookup on `_xmpp-client._tcp.example.com`.

3.6.1 Certificate warnings on iOS devices

The following applies if you are using a private CA to sign the XMPP certificate or manually installing a certificate.

From iOS version 10.3 and later, after installing a certificate as a profile, you must also turn on the trust. To turn on SSL trust for that certificate, follow these steps.

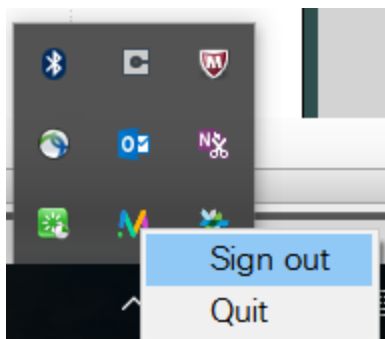
1. Open **Settings > General > About > Certificate Trust Settings**.
2. Under **ENABLE FULL TRUST FOR ROOT CERTIFICATES**, turn on trust for the certificate.

4 Issues Logging out of a Cisco Meeting App

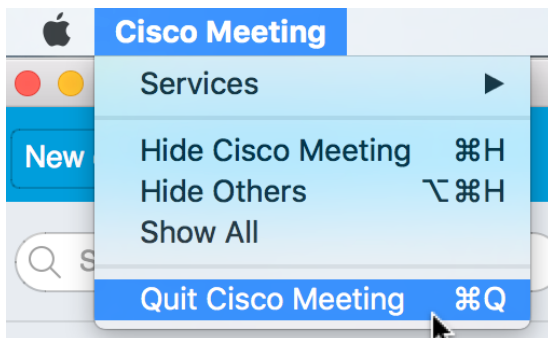
4.1 App not responsive

If the app is not responding, you may need to quit the app.

On a Windows PC, find the Cisco Meeting App icon in the bottom right-hand corner, right mouse click, and select **Quit**.



On a Mac, find the Cisco Meeting App icon in the top left-hand corner, mouse click, and select **Quit Cisco Meeting**.



Locate the app folder, zip all the files in the folder and send the zip file to Cisco Support.

On a Windows PC, the client folder is at

C:\Users\\AppData\Roaming\cisco\client

On a Mac, the client folder is at **/Users/<username>/Library/Caches/com.cisco.client/**

5 Issues after logging into a Cisco Meeting App

5.1 App diagnostic log

The app diagnostic log is a useful tool to identify the cause of a problem. Refer to [Collecting Logs](#) for information on using the diagnostic tool.

5.2 Something missing in the app user interface

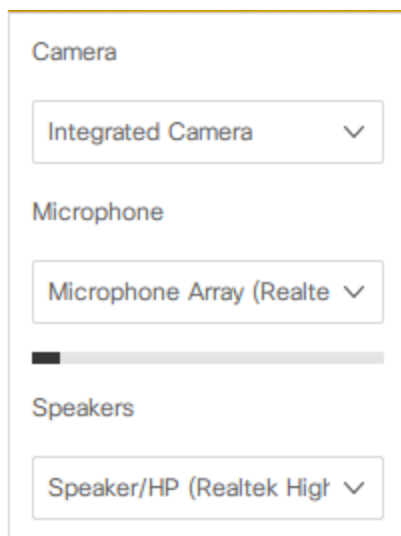
If you notice something missing, such as missing spaces, a missing button or icon, chat messages lost, or contacts lost, take a screenshot and click on the **Diagnostics** button. Send the screenshot and xmppLog file to Cisco Support.

5.3 Microphone, speaker and camera devices issue

If you cannot see that any Microphone, Speaker or Camera devices which are listed in the drop-down list on the app, do the following:

- check that any external devices are plugged in properly.
- check if the drivers are up-to-date.

If that did not solve the issue, take a screen shot and click on the **Diagnostics** button. Send the screen shot and xmppLog file to Cisco support.




5.4 High latency/packet loss when using clustered Call Bridges

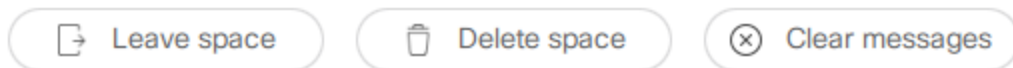
If your server deployment includes a cluster of Call Bridges, you may find an app is hosted by a Call Bridge that is not the closest one to the app. This can introduce latency and impact the quality of the call. To avoid this:

- The user must log out from all Cisco Meeting Apps. Since the homing expiration time varies between different apps and versions, the safest way to remove a homed app is to log out from all instances for that user for more than 2 to 3 hours.

5.5 Cannot delete chat messages

This is a feature that needs to be enabled via the API. If it is not enabled you will not see the **Clear messages** button. Once this is enabled, select a space and click the  button.

Then click **Clear messages**. You will be asked confirm that you want to delete all messages.

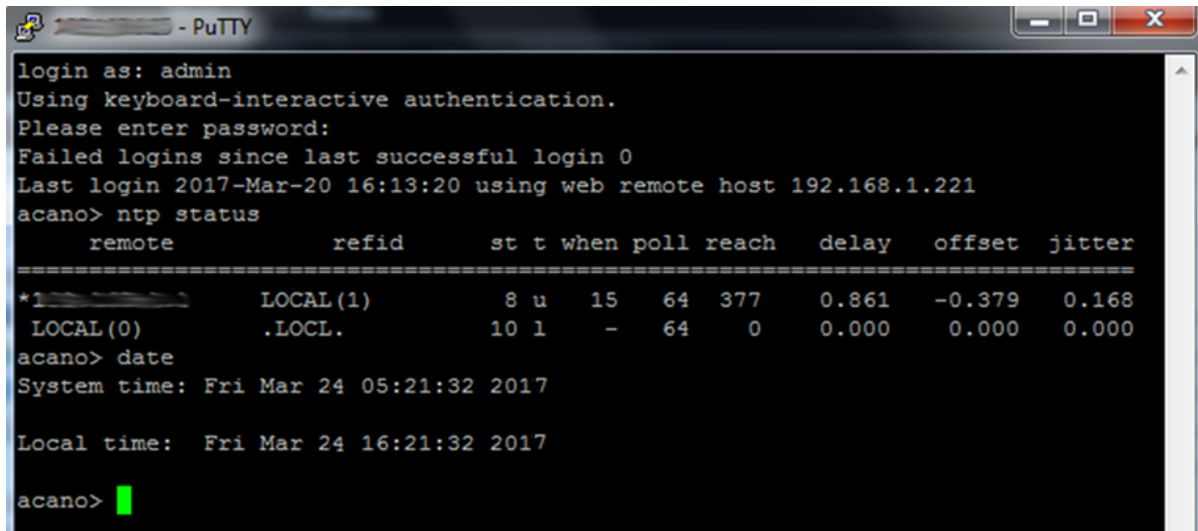


Note: You cannot delete individual messages. All messages are deleted permanently. All members will be notified when you delete messages.

6 Issues with spaces using the Cisco Meeting App

6.1 Negative values in call duration

Using NTP to sync the time in the app with the Call Bridge timer. Check the NTP status and time on the Cisco Meeting Server.



```

login as: admin
Using keyboard-interactive authentication.
Please enter password:
Failed logins since last successful login 0
Last login 2017-Mar-20 16:13:20 using web remote host 192.168.1.221
acano> ntp status
      remote          refid          st t when poll reach  delay  offset  jitter
=====
*192.168.1.221      LOCAL(1)         8 u  15  64  377  0.861  -0.379  0.168
LOCAL(0)          .LOCL.           10 l   -  64   0  0.000   0.000  0.000
acano> date
System time: Fri Mar 24 05:21:32 2017

Local time:  Fri Mar 24 16:21:32 2017

acano> █

```

6.2 Participants not going away

If you are the only participant in the space but still see participants in the list, then there is an issue with participant call disconnection.

Please take the client diagnostic log and collect the corresponding server-side client diagnostic log. Also download the log file from the Cisco Meeting Server. Please send all these files to Cisco Support.

7 Audio Issues

If your users are experiencing issues with sound during a meeting, look for the issue in this section and follow the suggested steps.

7.1 Participant cannot hear the other participant

Ask the sending participant to check that:

- Their microphone is not muted.
- They are not muted by another participant.
- Their microphone is selected. To check, ask them to try to change the microphone device at the far end.
- If the sending participant is using iOS, go to the iPhone/iPad settings and check that Cisco Meeting App has permission to use the microphone.
- There is no other application using the same microphone as Meeting.

Ask the receiving participant to check that:

- Speaker volume is sufficiently high.
- The participant can hear sounds when clicking the **Test speakers** button.
- Their speaker device is selected. Ask them to try to change the speaker.

7.2 One participant's audio is very low

Ask the sending participant to:

- Check that their microphone is selected, and ask them to try to change the microphone.

Ask the receiving participant to:

- Check that their speaker device is selected.
- Check that their speaker volume is sufficiently high.

7.3 Participant is receiving corrupted audio

If only one participant is receiving corrupted audio, check that participant's speaker is working, and if their internet connection is good. If the network connection is poor, the video quality should also be poor.

If all, or several, participants are receiving corrupted audio:

- Change the sending participant's microphone to test whether it is causing the issue.
- Check that the sending participant does not have poor network connection, (in this case, the other participants should receive poor quality video from this participant as well).
- Collect diagnostics logs and check media statistics. Refer to the section [Collecting Logs](#).

7.4 Echo on the call

In a point-to-point call, the participant who cannot hear the echo is probably the one generating it. Check whether their speaker is too close to their microphone.

In a multi-site call, locate the participant who is generating the echo by muting the microphones one at a time until the echo disappears. Then check whether their speaker is too close to their microphone.

7.5 Background noise

When there is background noise in a call, locate the participant who is generating the noise by muting microphones one at a time until the noise disappears.

Change this participant's microphone to test whether that is the issue.

Ask the participant to move to a quieter room.

It is always recommended that if a user is not speaking, they need to mute their microphone.

8 Video Issues

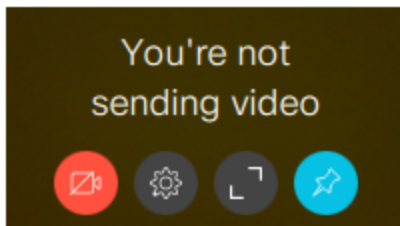
If your users are experiencing issues with video during a meeting, look for the issue in this section and follow the suggested steps.

8.1 Participant is getting no video

If a participant is not receiving video:

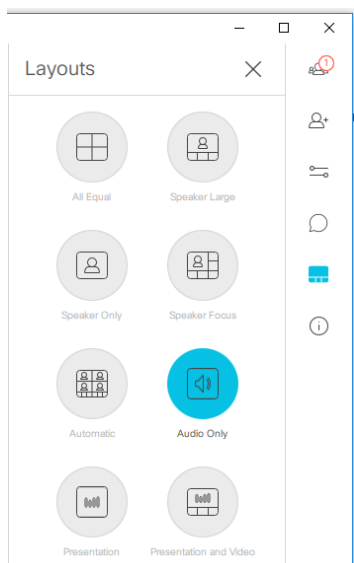
1. Check the sending participant's selfview.

2. If the video is stopped, tell the participant to click  to start sending video.



3. Check on the receiving participant's layout settings.

If **Audio only** is selected, tell the participant to change it to another layout.



8.2 Video is low resolution

1. If the participant with low video resolution is using Cisco Meeting App, ask them to click



, to open the **Settings** page. Click **Advanced** to adjust the **Bandwidth** settings. Ask them to change it to a higher bandwidth and test the video resolution again. Also check the settings for **Video quality**.

2. If far end is a Cisco Meeting App, ask that participant to adjust bandwidth settings if necessary.

Note: When you using Meeting App for a meeting, the video resolution and bandwidth used adjusts automatically according to your network. You should not need to adjust the bandwidth from the default settings as the app will automatically respond to network conditions.


If the steps above do not fix the issue, may be the call rate is being down-speeded during the call due to network packet loss or latency. Conduct more testing with endpoints at other locations. Check whether the issue always occurs for a specific location or a specific endpoint.

Take a [diagnostic log](#) and check media statistics and send it to your Cisco support contact.

8.3 Video is badly corrupted

1. Check for packet loss due to a network problem. Try to place a call with endpoints at different locations to see whether the issue changes with network path.
2. Check for packet loss due to QoS:
 - a. Try to place a call with a low call rate.



- b. If you are using Meeting, click , to open the **Settings** page. Click **Advanced** to lower the **Bandwidth** settings. Test again.

Note: When you using Meeting App for a meeting, the video resolution and bandwidth used adjusts automatically according to your network. You should not need to adjust the bandwidth from the default settings as the app will automatically respond to network conditions.

3. Check for encode/decode issues. If possible, place a number of calls using different endpoints and the same endpoint running different software versions. If the issue does not occur on all calls it may be related to a specific endpoint and software version.
4. Check the camera sending the video. Ask the far end participant to place a call with another endpoint or camera.
5. Take a [diagnostic log](#) and send it to your Cisco support contact.

8.4 Layout issues

If you see a layout that is not what you have selected, or has an unexpected aspect ratio, it may be due to low network bandwidth causing the call rate to reduce speed. Try to use wired Ethernet cable and change to a different location.


If you still have a problem then obtain the client diagnostic log while in a call, and collect the corresponding server-side client diagnostic log. Send these files to Cisco Support.

8.5 Content sharing/receiving issue

If participants have content sharing issues, such as:

- cannot receive content at start of sharing, or during content sharing
- content is not clear
- content streaming gets dropped



Click , to open **Settings** page. Click **Advanced** to verify that enough bandwidth is allowed. The default bandwidth setting is 1200 Kbps .

Note: When you are using Meeting App for a meeting, the video resolution and bandwidth used adjusts automatically according to your network. You should not need to adjust the bandwidth from the default settings as the app will automatically respond to network conditions.



Also check the network devices to see if there is any packet loss or a lack of bandwidth resources.

Check Cisco Meeting Server settings to verify if content sharing is enabled.

If you still have the issue, take the client diagnostic logs for both sending and receiving app while sharing, and when the content gets dropped. Also collect the corresponding server-side client diagnostic log and send the logs to Cisco Support.

9 Issues with features when signed in

9.1 Invite button is missing

If a space has guest access disabled then you will not see the **Invite** button. If you have space editing permissions, click  to allow non-member access. Refer to the help by clicking on the  icon from the main screen.

9.2 Missing invitation details

Note: coSpaces are now called spaces. However, the API keeps the term coSpaces to ensure that scripting works.

If any details are missing from space invitations, check the following:

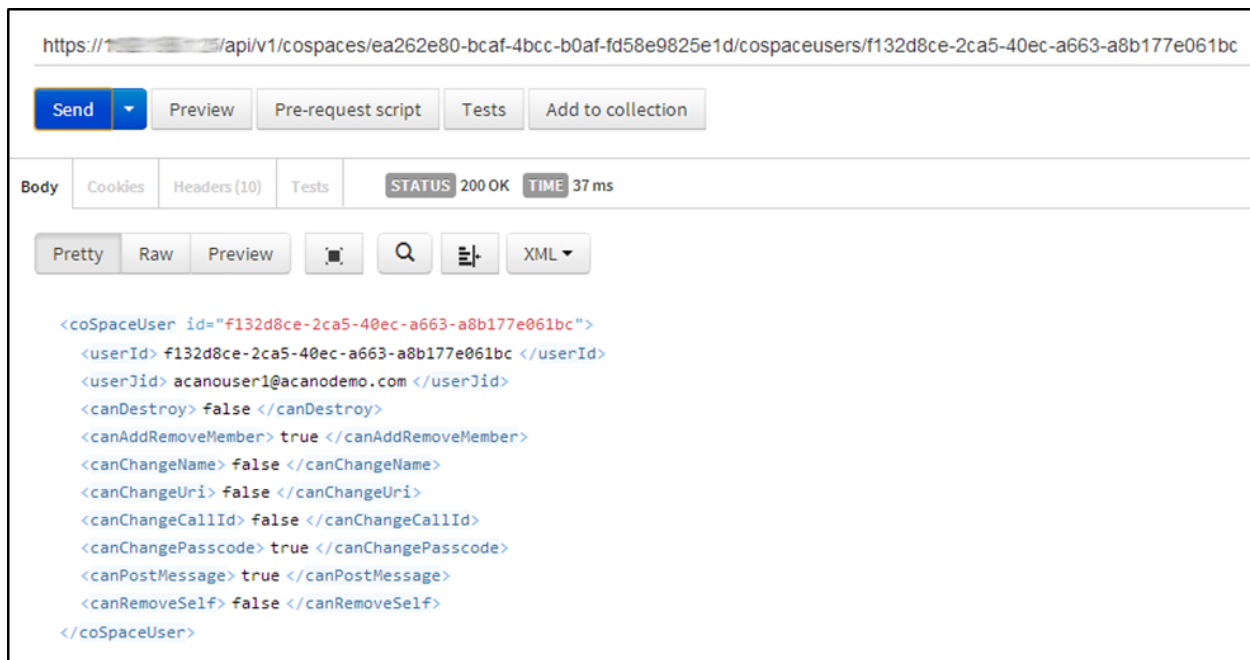
- If the Video URL is missing, sign in to the Web Admin Interface and check the “URI user part” for this space in **Configuration > Spaces**.
- If the Phone number is missing, sign in to the Web Admin Interface and check the “IVR numeric ID” for this coSpace at **Configuration > General**.
- If the Call ID is missing, sign in to the Web Admin Interface and check the “Call ID” for this coSpace at **Configuration > Spaces**.
- If the Web link is missing, sign in to the Web Admin Interface and check the “Guest account client URI” for this space at **Configuration > General**.

9.3 Cannot remove a participant during a call

During a call, users might be able to remove participants by clicking on their video pane and selecting **Remove**. If a participant cannot remove another participant:

- Check whether the user is a member of the space.
If the user is signed in to Cisco Meeting App but is only in this call as a guest, then the user cannot add or remove participants.
- If the user is a member, check whether they have the permission to remove and add participants. The API URL format to do this is `https://<server_IP_address>/api/v1/cospaces/<coSpace_id>/cospaceusers/<user_id>`. If `<canAddRemoveMember>` is set to true, then the user has permission to remove other participants from a call.

The following is an example (using the Postman tool) and you can see that this participant user should be able to remove/add participants because the parameter `<canAddRemoveMember>` is set to true.



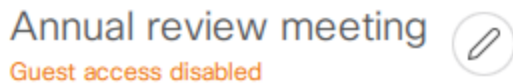
The screenshot shows a Postman interface for an API endpoint. The URL is `https://1[redacted]/api/v1/cospaces/ea262e80-bcaf-4bcc-b0af-fd58e9825e1d/cospaceusers/f132d8ce-2ca5-40ec-a663-a8b177e061bc`. The response status is 200 OK and the time taken is 37 ms. The response body is XML, showing a `<coSpaceUser>` object with various attributes. The `<canAddRemoveMember>` attribute is set to `true`.

```
<coSpaceUser id="f132d8ce-2ca5-40ec-a663-a8b177e061bc">
  <userId> f132d8ce-2ca5-40ec-a663-a8b177e061bc </userId>
  <userId> acanouser1@acanodemo.com </userId>
  <canDestroy> false </canDestroy>
  <canAddRemoveMember> true </canAddRemoveMember>
  <canChangeName> false </canChangeName>
  <canChangeUri> false </canChangeUri>
  <canChangeCallId> false </canChangeCallId>
  <canChangePasscode> true </canChangePasscode>
  <canPostMessage> true </canPostMessage>
  <canRemoveSelf> false </canRemoveSelf>
</coSpaceUser>
```

9 Guest issues

9.4 Guest access disabled

If guest access is disabled, you will see a message just below the space name when you search or select a space.



If you have space editing permissions, you can edit the space and allow guest access. For instructions, refer to the help by clicking on the help icon.

9.5 Cannot join call as a guest using the Chrome browser

As a guest user, anyone can join a call on Chrome – either via a guest user web link or by providing the Meeting ID. If a guest experiences issues, check the following:

If the user sees the message: **Unable to connect – try again later**


1. If the web bridge is configured on the web admin, sign in to the Web Admin Interface and check the **Guest Account JID Domain** in **Configuration > General**. It has to match a domain that is configured on the XMPP server.

Web bridge settings	
Guest account client URI	<input type="text"/>
Guest account JID domain	<input type="text" value="example.com"/>
Custom background image URI	<input type="text"/>
Custom login logo URI	<input type="text"/>

If a user sees the message **Unable to connect to server**:

1. Check the Web Bridge trust certificate configuration using the MMP command line interface. The Web Bridge must trust the Call Bridge certificate. For details, see the Cisco Meeting Server Deployment Guide.

In the example below, there is trust bundle; it must be the certificate that is used by the Call Bridge.

```
acano> webbridge
Enabled                : true
Interface whitelist    : a:446
Key file               : acano25.key
Certificate file       : acano25.pem
Trust bundle  : acano25.pem
HTTP redirect          : Disabled
Clickonce URL         : none
MSI download URL      : none
DMG download URL      : none
iOS download URL      : none
acano>
```

In addition, refer to this FAQ [Troubleshooting Web Bridge connectivity issues](#).

9.6 Intelligent pairing is not detecting the nearby video system

Intelligent pairing is always enabled by default for Meeting App. The Cisco video system in range must have software version CE8.0 or above. Ensure that the video system is within range so Meeting App can detect it.

For more information on configuring and troubleshooting Proximity for video systems, refer to the endpoint [documentation](#).

9 Notifications

9.7 Notifications not shown by the iOS app when it is not visible on the screen

Notifications will only be shown when the app is in the foreground (open and visible). Refer to this FAQ [Why can't I receive notifications on certain versions of Cisco Meeting App on iOS devices?](#).

10 Space Management Issues

10.1 Video address does not match the name of the space

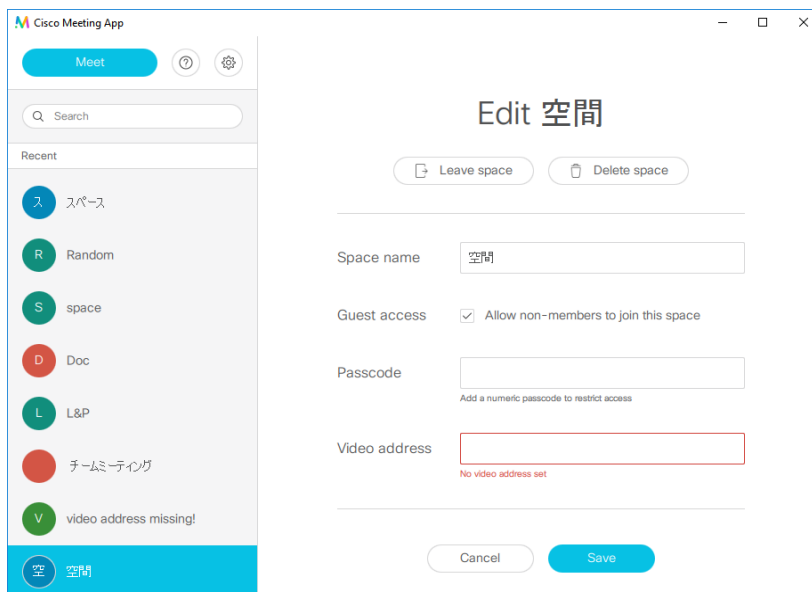
This will not be a problem. It is sometimes necessary to have a video address that does not match the name of the space. Several spaces can have the same name, but the video address must be unique.


When a space name is entered in the app, the Cisco Meeting App automatically creates a unique video address which is as similar to the space name as possible. Users with space editing permissions can edit the video address if they wish to. For instructions, refer to the help from the **Edit space** screen.

10.2 Video address not set

You can only edit the video address of a space if the guest access is enabled. If the space name contains ASCII characters, the app automatically generates a space address based on the space name.

If the space name does not contain ASCII characters, the space address will not be set and the field will be empty. Meeting App displays the following message when you try to enable guest access from the **Edit space** screen when no address has been set.



If you have space editing permissions, click  from any space and enter a video address with ASCII characters. The app will show you if your choice is available or

suggest one that closely matches your search. Click **Save** to save your changes and exit this screen.

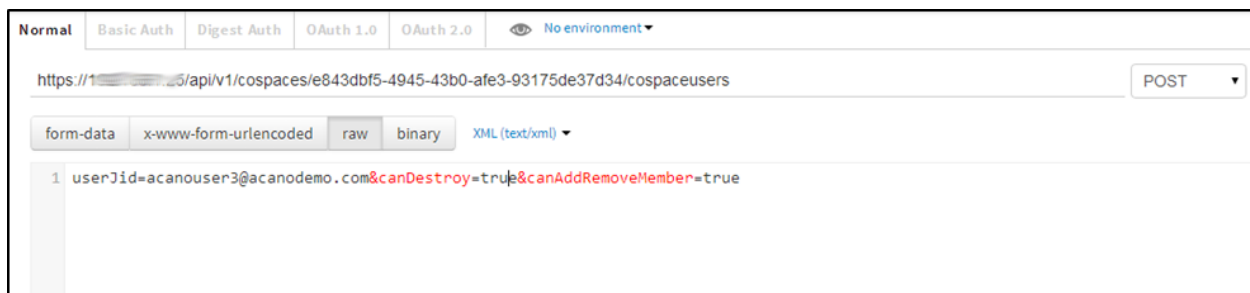
10.3 A member of a space is missing

If a user account is removed accidentally, the user is removed from the spaces that they were a member of. To add the user to the spaces as a member again, first re-create the user and then do one of the following:

- Sign in to Meeting App as a member of that space and add the removed user.
- Add the user via the API. The API URL format is
`https://<cisco_meeting_server_IP_address>/api/v1/cospaces/<coSpace_id>/cospaceusers.`

The following is an example of adding a member via the API.

`https://<cisco_meeting_server_IP_address>/api/v1/cospaces/e843dbf5-4945-43b0-afe3-93175de37d34/cospaceusers`



The user should now be able to log in to Meeting App and see the space.

11 Issues with SIP Endpoints

If your users are experiencing issues with a SIP call, look for the issue in this section and follow the suggested steps.

11.1 Call cannot be established

If the caller gets disconnected right away after placing the call:

1. If the call is placed from Meeting App, check the Outbound calls dial plan on the Cisco Meeting Server; a matched dial plan rule must be configured to route the outbound call.

Outbound calls

Domain	SIP proxy to use	Local contact domain	Local from domain	Trunk type	Behavior	Priority	Encryption	
meeting.example.com	proxy.example.com		example.com	Standard SIP	Continue	90	Encrypted	[edit]
conference.example.com	proxy1.example.com		example.com	Standard SIP	Continue	80	Encrypted	[edit]
example.demo	fe.example.demo	calbridge.example.com	example.com	Lync	Stop	60	Auto	[edit]
demo	proxy2.example.com		example.com	Standard SIP	Stop	10	Auto	[edit]
<match all domains>	proxy3.example.com		example.com	Standard SIP	Continue	0	Unencrypted	[edit]
				Standard SIP	Stop	0	Auto	Add New Reset

2. If the call is placed from an external SIP endpoint, check the dial plan on the external SIP call control device. A matched dial plan rule must be configured to route the call out to the Meeting Server. If that is correct, then check the dial plan on the Meeting Server. A matched Inbound calls dial plan rule must be configured to route the incoming call.

Call matching

Domain name	Priority	Targets spaces	Targets users	Targets IVRs	Targets Lync	Tenant	
meeting.example.com	100	yes	yes	yes	no	no	[edit]
	0	yes	yes	yes	no		Add New Reset

3. Check that the SIP trunk on the external SIP call control device is active.

If the call is placed, but the caller never hears the ring tone and the called party never gets the incoming call:

1. If the call is placed from Meeting App, check the Outgoing calls dial plan on the Meeting Server; a matched dial plan rule must be configured to route the call out to the expected external call control device.

Outbound calls

Filter Submit

	Domain	SIP proxy to use	Local contact domain	Local from domain	Trunk type	Behavior	Priority	Encryption	
<input type="checkbox"/>	meeting.example.com	proxy.example.com		example.com	Standard SIP	Continue	90	Encrypted	Edit
<input type="checkbox"/>	conference.example.com	proxy1.example.com		example.com	Standard SIP	Continue	80	Encrypted	Edit
<input type="checkbox"/>	example.demo	fe.example.demo	callbridge.example.com	example.com	Lync	Stop	60	Auto	Edit
<input type="checkbox"/>	demo	proxy2.example.com		example.com	Standard SIP	Stop	10	Auto	Edit
<input type="checkbox"/>	<match all domains>	proxy3.example.com		example.com	Standard SIP	Continue	0	Unencrypted	Edit
					Standard SIP	Stop	0	Auto	Add New Reset

1
Delete

2. If the call is placed from an external SIP endpoint, check the dial plan on the external SIP call control device, a matched dial plan rule must be configured to route the call to Meeting Server.
3. Check the Meeting Server and the external SIP call control device; ensure that there is no call loop caused by wrong dial plan configuration.

If the called party sees the incoming call and hears the ring tone, but the caller never hears it, or the called party has answered the call, but the caller still hears the ring tone, or the call gets disconnected right after the called party answers the call, follow these steps:

1. Try to call SIP endpoints at different locations - and via different SIP trunks, if applicable.
2. Try to place a call in both directions.
3. If some test calls work, compare the working scenario(s) with the non-working scenario, including the model and software version of the SIP call control device and of the SIP endpoints. Compare network locations and configuration. Possible causes could be device compatibility, network connectivity and incorrect configuration.

Recreate all the above steps with SIP detailed tracing enabled on the Cisco Meeting Server, look at the logs, and send it to Cisco support.

11.2 Call cannot be hung up

If one participant hangs up the call, and the other(s) get stuck in the call and do not see that the call has been disconnected, place a single test call and collect the following information:

- Software version of your Cisco Meeting Server
- Type of Server or virtualized deployment
- Type and version of your computer's operating system and your browser
- Output of the MMP command **webbridge**
- Live.json file (see [Appendix A](#))
- Log (see [Appendix A](#))

- Diagnostics log (client and server side, see [Appendix A](#))
- pcap on the Call Bridge and computer.

Send the information to Cisco Support.

11.3 Participant doesn't receive audio/video

If one participant does not receive audio and/or video:

1. Check the firewall settings.

It is likely that the firewall is blocking the media port(s). Check the Deployment Guide and external SIP solution for the media port range.

If the firewall is not blocking media, place a single test call and collect the following information:

- Software version of your Cisco Meeting Server
- Type of Server or virtualized deployment
- Type and version of your computer's operating system and your browser
- Output of the MMP command **webbridge**
- Live.json file (see [Appendix A](#))
- Log (see [Appendix A](#))
- Diagnostics log (client and server side, see [Appendix A](#))
- pcap on the Call Bridge and computer.

11.4 Participant receives bad audio/video

If one participant receives bad audio and/or video:

1. Try to place a test call using a lower bandwidth.

Bad audio/video is probably caused by packet loss or network delay. By using a lower bandwidth, check whether the audio/video improves.

2. If possible, use a different codec on the SIP endpoint.

A possible cause is an encode/decode issue. Try to change the audio/video codec and check whether the issue is solved.

If this issue is still encountered, place a single test call and collect the following information:

- Software version of your Cisco Meeting Server
- Type of Server or virtualized deployment
- Type and version of your computer's operating system and your browser
- Output of the MMP command **webbridge**
- Live.json file (see [Appendix A](#))
- Log (see [Appendix A](#))
- Diagnostics log (client and server side, see [Appendix A](#))
- pcap on the Call Bridge and computer.

Then email Cisco Support with this information.

11.5 Dual stream/presentation Issue

If participants cannot receive dual stream video/presentation.

1. Check the firewall settings.

It is likely that the firewall is blocking the media port(s). Check the Cisco Meeting Server Deployment Guide and external SIP solution documentation for the dual stream media port range.

2. If possible, use a different codec on SIP endpoint.

A possible reason is an encode/decode issue. Change audio/video codec for dual stream/presentation and check whether the issue is solved.

If this issue still occurs, place a single test call and collect the following information:

- Software version of your Cisco Meeting Server
- Type of Server or virtualized deployment
- Type and version of your computer's operating system and your browser
- Output of the MMP command **webbridge**
- Live.json file (see [Appendix A](#))
- Log (see [Appendix A](#))
- Diagnostics log (client and server side, see [Appendix A](#))
- pcap on the Call Bridge and computer.
- GET on API `calllegs/<calllegid>/calllegdetailed` trace for the client call

Then send this information to Cisco Support.

11.6 Issues moving call from the app to an endpoint

If a user is trying to move the call to an endpoint, and the endpoint does not ring:

1. Check the Web Admin Interface configuration of **Outbound calls**, and make sure an outbound rule is configured with the domain that is used to move the call. For example, if you want to move a call to endpoint@conference.example.com, make sure you have an outbound rule (see below) that has conference.example.com as the **Domain**.

Outbound calls

Filter Submit

	Domain	SIP proxy to use	Local contact domain	Local from domain	Trunk type	Behavior	Priority	Encryption	
<input type="checkbox"/>	meeting.example.com	proxy.example.com		example.com	Standard SIP	Continue	90	Encrypted	edit
<input type="checkbox"/>	conference.example.com	proxy1.example.com		example.com	Standard SIP	Continue	80	Encrypted	edit
<input type="checkbox"/>	example.demo	fe.example.demo	calbridge.example.com	example.com	Lync	Stop	60	Auto	edit
<input type="checkbox"/>	demo	proxy2.example.com		example.com	Standard SIP	Stop	10	Auto	edit
<input type="checkbox"/>	<match all domains>	proxy3.example.com		example.com	Standard SIP	Continue	0	Unencrypted	edit
					Standard SIP	Stop	0	Auto	Add New Reset

1
Delete

2. Place a call from the app to the endpoint to check the connectivity. If the test call can be connected, but the moving call fails, please replicate this issue and take a SIP trace on the Cisco Meeting Server. Send the logs to Cisco Support with a description of the problem.

12 WebRTC Browser Certificate Issues

If your users are experiencing issues with WebRTC browser certificate, look for the issue in this section and follow the suggested steps.

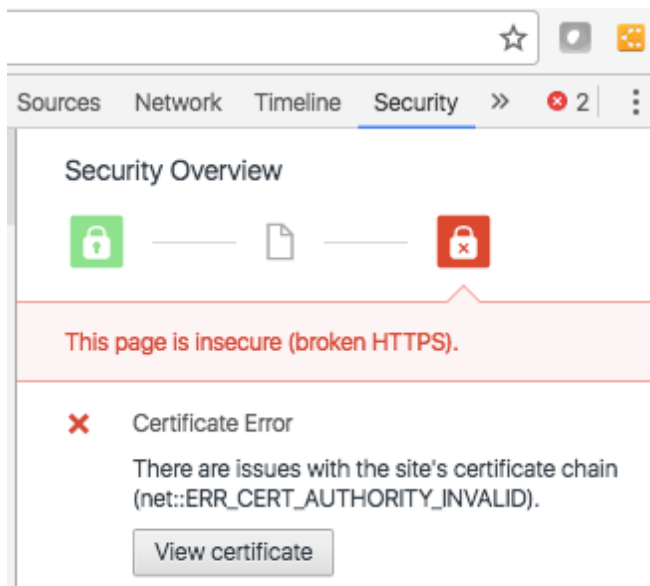
12.1 Google Chrome - "Cannot connect to the real join.example.com" or "Your connection is not private"

When your Chrome browser gives the errors "Cannot connect to the real join.example.com" or "Your connection is not private", try the following:

1. Click on the padlock in the address field, then **Details**.

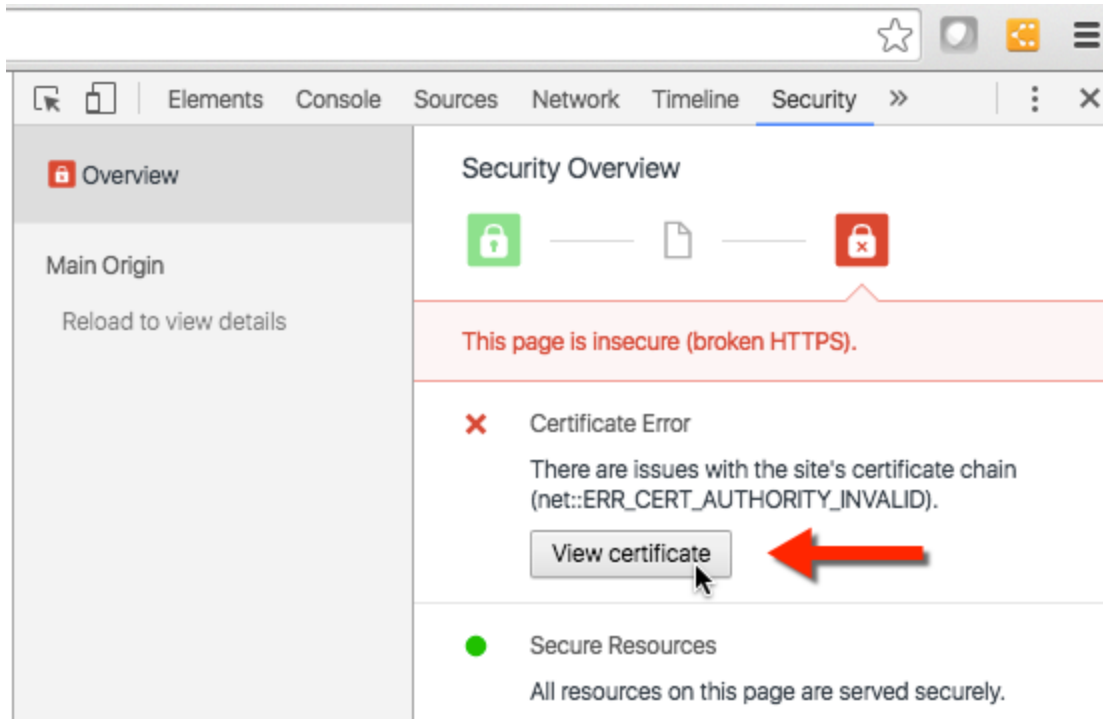


2. Check the error message given. In this example, the certificate is signed by an authority that is not trusted by the computer.

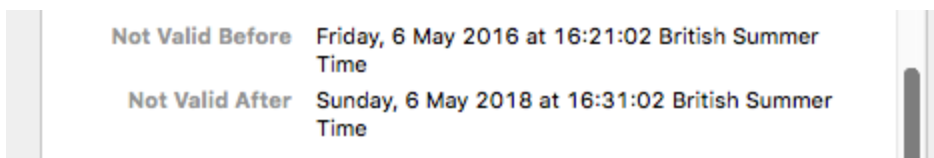


This can mean that the certificate is self-signed, or that the certificate is signed by an authority that is not trusted by the browser. It could also mean that a certificate bundle is not uploaded and assigned correctly to the Web Bridge.

3. For further details, click **View certificate**.



4. Open **Details** and check when the certificate is valid.



The browser compares the certificate details with your computer, so also check if your computer's date and time settings are correct.

If the certificate is expired, renew it on Cisco Meeting Server and replace the expired certificate.


5. Check that the certificate is issued to the URL you have typed in the address field. In Chrome for OS X, look for **Subject Name > Common Name**. In Chrome for PC, look for **Issued to**.

Subject Name	_____
Country	GB
State/Province	London
Locality	Uxbridge
Organization	Cisco
Organizational Unit	UXB
Common Name	uxb-vc-0.cisco.com

Issued to: uxb-vc-0.cisco.com

Issued by: tsca-4096-sha2

Valid from 06/05/2016 **to** 06/05/2018



If the certificate is issued in the wrong name (wrong URL), you need to re-issue the appropriate certificate on Cisco Meeting Server.

12.2 Issues with bundled certificates

If the signing authority is not trusted, there could be issues with bundled certificates. Firefox, for instance, would report "The certificate is not trusted because no issuer chain was provided." Try the following:

1. Log in to the Cisco Meeting Server via SSH, using your MMP credentials. Execute the commands `pki list` and `webbridge` and check whether the CA Bundle file is uploaded and assigned to the Web Bridge. If not, upload the bundle certificate and assign it to the Web Bridge by issuing the command `webbridge certs <private_key> <cert> <bundle_cert>`.

```
Last login 2014-Aug-07 06:47:00 using SSH remote host 10.10.10.10
acano> pki list
webadmin.crt
webadmin.key
webbridge.crt
gd_bundle-g2-g1.crt ←
newwebbridge.crt
newwebbridge.key
oldwebbridge.crt
acano> webbridge
Enabled : true
Interface whitelist : b:443
Key file : newwebbridge.key
Certificate file : newwebbridge.crt
CA Bundle file : gd_bundle-g2-g1.crt ←
Trust bundle : webadmin.crt
HTTP redirect : Disabled
Clickonce URL : none
MSI download URL : none
DMG download URL : none
iOS download URL : none
acano>
```

2. After the bundle certificate has been uploaded and assigned to the Web Bridge, check whether the issue has gone.

To learn more about certificate bundles, see

http://en.wikipedia.org/wiki/Intermediate_certificate_authorities. Our Certificate Guidelines are also a useful reference for understanding the different types of certificates and the implications of using intermediate signing authorities.

13 WebRTC Client Issues

13.1 WebRTC client connection issues

If the WebRTC Client has difficulty joining a meeting or transmitting audio/video, a good starting point is to test the browser's WebRTC support.

1. Go to <https://apprtc.appspot.com> using Chrome. Then open another tab, and type `chrome://webrtc-internals/` which will show ICE information. If you see a self-view this validates that Chrome can access your camera and microphone, that STUN packets are not being blocked on the part of the network visiting that site, and that the capabilities of the device will cope.
2. Then copy and send the link shown at the bottom to a colleague and initiate a point-to-point call with live two-way audio and video.

Success of these tests indicate that calls with Cisco Meeting App (web) should also be successful providing you have the same firewall configurations between the Cisco Meeting Server and the browser as you do between the two browsers in the call.

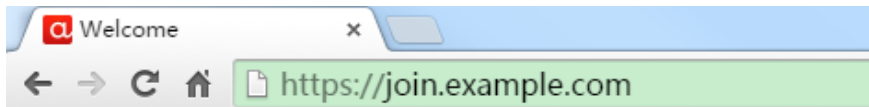
Should any of these tests fail, PC or network issues should be investigated by taking Wireshark traces on the computers.

13.2 Unable to reach web client landing page

1. Check that the Web Bridge is running and enabled:
SSH to the MMP and type the command `webbridge` to determine whether the Web Bridge is enabled.

```
acano> webbridge
Enabled                : true
Interface whitelist   : b:443
Key file               : join150.key
Certificate file      : join150.pem
Trust bundle          : acano150.pem
HTTP redirect         : Disabled
Clickonce URL         : none
MSI download URL     : none
DMG download URL     : none
iOS download URL     : none
acano>
```

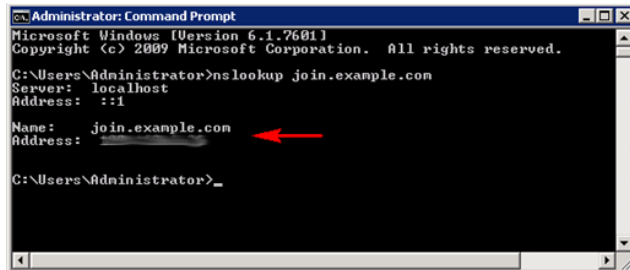
2. Check that the DNS server address is configured:
 - a. At the Windows command prompt, type command `ipconfig /all`
 - b. On a Mac terminal, type command `scutil --dns` The DNS server address must be the DNS that either has the required A record configured or is able to forward the DNS query to another DNS server that can service this query.
3. Verify the IP address that the FQDN in the web URL resolves to is correct: An example web URL is <https://join.example.com>.



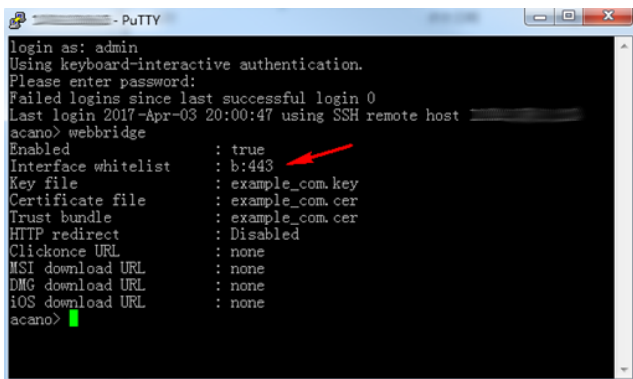
At the Windows command prompt, type your equivalent of:

```
nslookup join.example.com
```

Note the resolved IP address.



4. Verify that this IP address is associated with the interface that the Web Bridge is listening to. SSH to the MMP and type the command `webbridge` to see which interface the Web Bridge is listening to. Then type the command that is equivalent to `ipv4 b` on your Cisco Meeting Server to check the IP address.



```

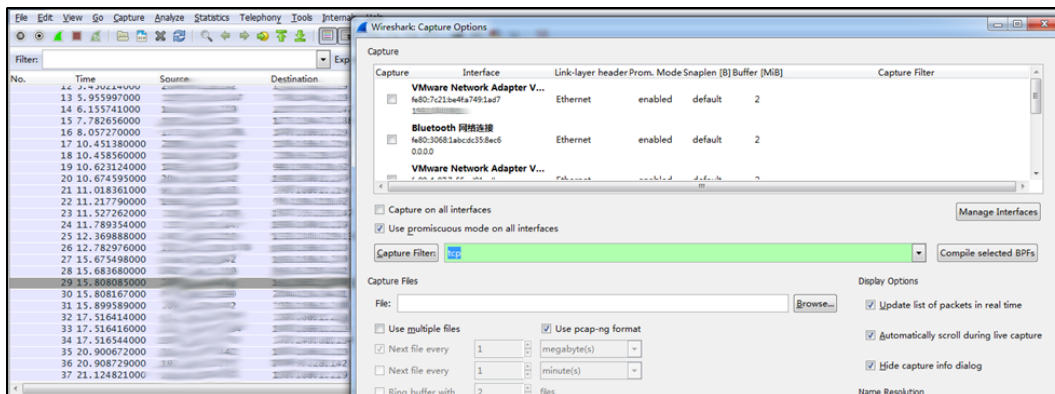
acano> ipv4 b
IPv4 configuration:
address: [redacted]
default: false
dhcp: false
enabled: true
gateway: [redacted]
macaddress: 00:0C:29:48:5F:E6
prefixlen: 24
route: 200.100.1.0/24
IPv4 observed values
Addresses:
192.168.6.26/24
Routes:
source destination gateway global
0.0.0.0 0.0.0.0 0.0.0.0 false
0.0.0.0 0.0.0.0 0.0.0.0 false
0.0.0.0 0.0.0.0 0.0.0.0 false
0.0.0.0 0.0.0.0 0.0.0.0 false
0.0.0.0 0.0.0.0 192.168.6.254 false
acano>

```

13.3 WebRTC client call drops

One of the causes of such issues could be a firewall closing TCP connections.

If you are able to reproduce the problem, take a Wireshark trace on the PC running Chrome, but use 'tcp' as a capture filter to avoid capturing all the UDP media traffic to see if there is anything at a network level that could be causing this.



Also enable the Javascript console in Chrome (Ctrl-Shift-J on Windows). Right-click on it and make sure 'Preserve Log on Navigation' is selected. When the call next drops, send the logs and the Wireshark trace to Cisco Support.

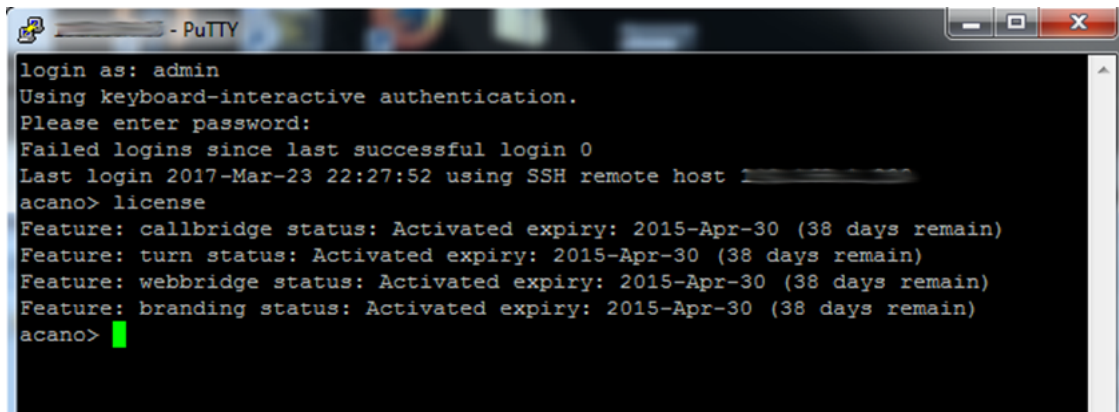
14 Customization Issues

14.1 Customized feature not working

If you cannot get the customized background images, log or voice prompts to display or be heard, then check that the license and customization files are in place.

Note: You can only see customized images on webRTC app and not in the native apps.

1. To verify that the license is in place, issue the command **license** on MMP. Call Bridge reboot is required after uploading a license file.



```
login as: admin
Using keyboard-interactive authentication.
Please enter password:
Failed logins since last successful login 0
Last login 2017-Mar-23 22:27:52 using SSH remote host [redacted]
acano> license
Feature: callbridge status: Activated expiry: 2015-Apr-30 (38 days remain)
Feature: turn status: Activated expiry: 2015-Apr-30 (38 days remain)
Feature: webbridge status: Activated expiry: 2015-Apr-30 (38 days remain)
Feature: branding status: Activated expiry: 2015-Apr-30 (38 days remain)
acano>
```

Note: In a split arrangement where the components are deployed across two servers (Core and Edge), the branding licenses are only required on the Core server, they are not required on the Edge server.

2. For WebRTC customization, all customization files must be placed together in a zip file. Follow the instructions in Cisco Meeting Server Customization Guidelines.
3. Make sure customization file sizes, properties and names meet the requirements in the Customization Guidelines. You can find errors in the event log.

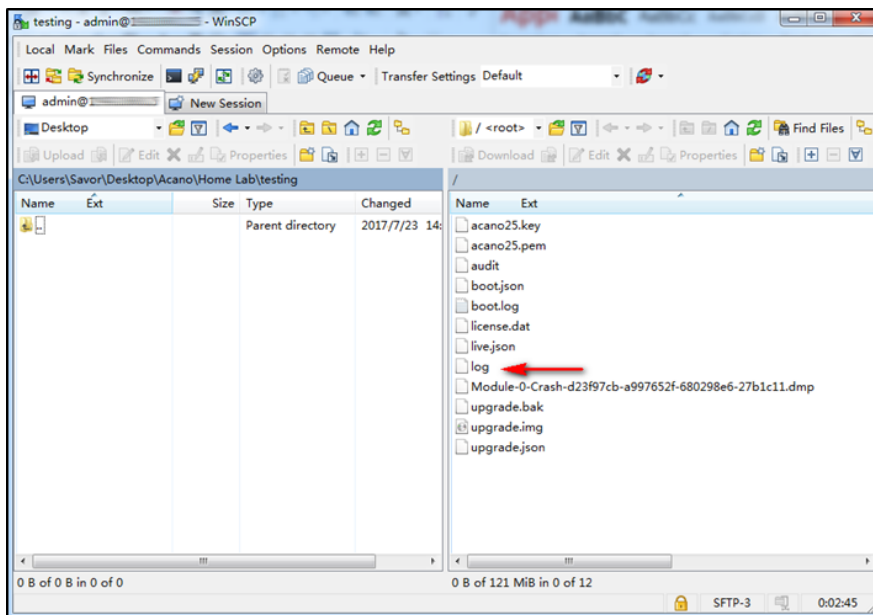
Note: IVR and call branding is not relevant for clients, only for SIP calls.

Appendix A Collecting Logs

If the steps in the previous sections do not solve your issue and you need to email the file to your Cisco Support contact, it is helpful to attach logs. This section tells you how to collect them.

Collecting logs

1. Log in to the Cisco Meeting Server via WinSCP, using your MMP login credentials.
2. Find the file called “log” under the root directory and drag it to your local PC. This is the log to send to Cisco support.



Collecting a pcap file

1. Log in to the Cisco Meeting Server via SSH, using your Web Admin Interface login credentials.
2. Check which interface the Call Bridge is listening to by executing the command **callbridge**.

```

acano> callbridge
Listening interfaces : a
Key file             : acano25.key
Certificate file     : acano25.pem
acano> _

```

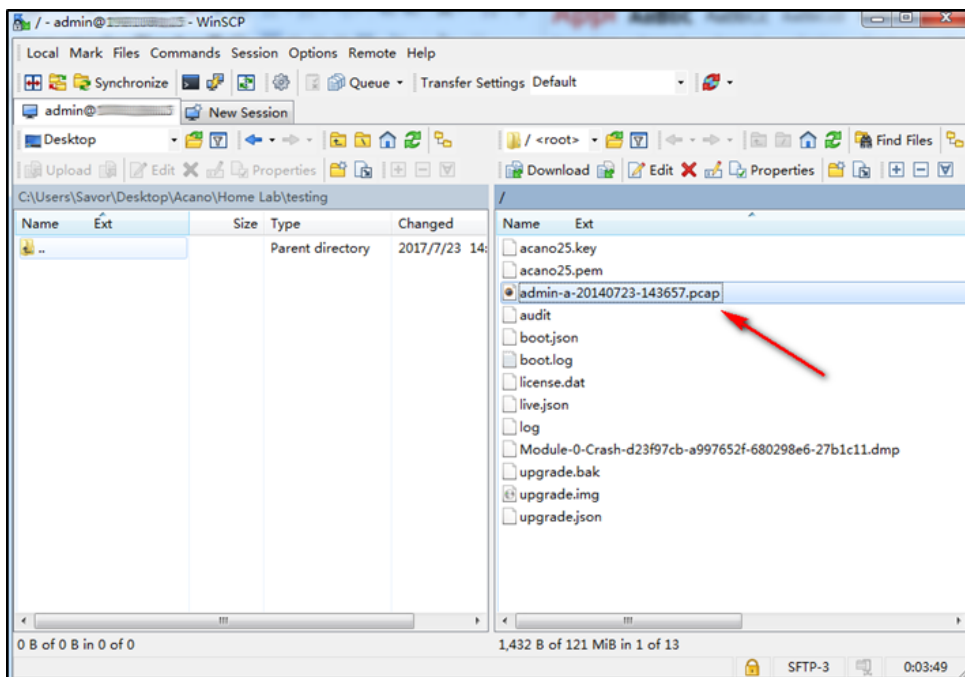
3. Start capturing packets on this interface by executing command `pcap <interface>`
Example: `pcap a`.
4. Recreate the issue.
5. Press **Ctrl+C** to stop capturing.
6. A pcap file has been created and the file name is shown; in this example, the file name is `admin-a-20140723-143657.pcap`.

```

acano> pcap a
Packet capture running: press Ctrl-C to stop
Packet capture available in admin-a-20140723-143657.pcap
acano>

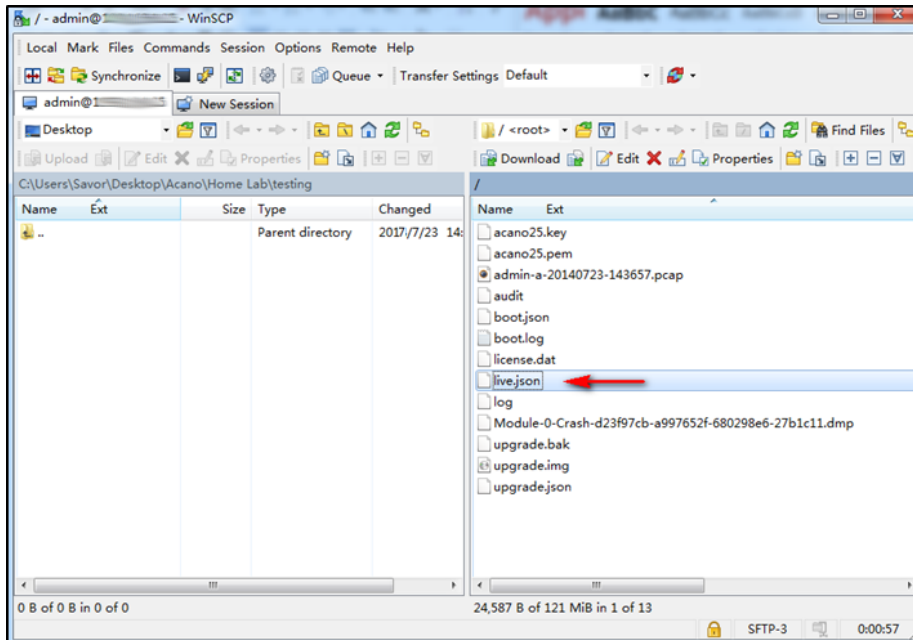
```

7. Log in to the Cisco Meeting Server via WinSCP, using the Web Admin Interface login credentials. Drag the file to your local PC.




Collecting the live.json file

1. Log in to the Cisco Meeting Server via WinSCP, login credential are the same as the MMP credentials.
2. Find the file called “live.json” under the root directory and drag it to your local PC.




Collecting Diagnostic Information from the Cisco Meeting App

If you have any problem using the app, follow these steps:

1. If Cisco Support has advised you to do so, click  to open the settings screen.
2. Click **Diagnostics**.
3. Save or send the file:
 - Windows and OS X: A **Save diagnostics file** window opens. Select a location on your computer to save a log file. Email to your Cisco support contact with a description of the problem for troubleshooting.
 - Web app: The diagnostics information is available in a new tab. Save and email the file with a description of the problem to your Cisco support contact.
 - iOS: The app opens a new email and populates it with all the information needed for troubleshooting and attaches the diagnostics file. Enter the email address and send it to your Cisco support contact.

During a meeting in Windows and OS X apps, user can do one of the following to save a log file:

- click on  from the in-meeting menu options.
- Press **Ctrl+d** (on Windows) or **cmd+d** (on OS X) - this is the only way to send diagnostics when you are sharing content.

A **Save diagnostics file** window displays and lets you save a file. Email the file to your Cisco support contact with a description of the problem.

Collecting diagnostic information from the Cisco Meeting Server

When you generate a diagnostic log on an app that is in a call, the Cisco Meeting Server also generates a server side diagnostic log automatically.

1. Go to the Web Admin Interface, **Status > General**. At the bottom of the page, you can find the diagnostics log with time stamp. Download the one with correct time stamp.

Call diagnostic logs			
<input type="checkbox"/>	Log name	Time	Download link
<input type="checkbox"/>	"acanouser3@acanodemo.com" diagnostics	2017-07-23 21:33:22.649208 +0800	[download]

Obtaining log and crash files for a Windows or OS X app

To find the crash files on Windows, go to **C:\Users\\AppData\Roaming\cisco**

To find the crash files on OS X, go to **~Library/Caches/com.cisco.client/**

Email the most recent files along with your full contact details to your Cisco Support contact. There may be more than one file with the same time stamp for each event; send them all.

Obtaining crash files for an iOS app

To download the log/crash file, sync the iPad or iPhone with iTunes on your PC or Mac; the crash reports are stored at:

- On Windows 7: **C:\Users\\AppData\Roaming\Apple computer\Logs\CrashReporter\MobileDevice**

- On Mac: `~/Library/Logs/CrashReporter/MobileDevice`

Email the most recent files along with your full contact details to your Cisco Support contact. There may be more than one file with the same time stamp for each event; send them all.

Collecting a SIP and DNS trace

1. Make sure that the test call will be unencrypted: sign in to the Web Admin Interface and go to **Configuration > Call settings**.
2. Flush the DNS cache on the Cisco Meeting Server or virtualized deployment: Sign in to the MMP and execute the following commands in turn: `dns mmp flush` and `dns app flush`

```

acano> dns ?
Configure DNS and DNSSEC

Usage:
  dns
  dns (mmp|app) add forwardzone <domain-name> <server ip>
  dns (mmp|app) del forwardzone <domain-name> <server ip>
  dns (mmp|app) add trustanchor <anchor>
  dns (mmp|app) del trustanchor <zonename>
  dns (mmp|app) lookup <A/AAAA/SRV> <hostname>
  dns (mmp|app) flush
  dns (mmp|app) add rr <DNS RR>
  dns (mmp|app) del rr <owner-name> <type>
acano> dns mmp flush
acano> dns app flush
acano>

```

3. On a virtualized deployment, sign in to the MMP and issue the command `dns flush`.

```

acano> dns ?
Usage:
  dns
  dns add forwardzone <domain-name> <server ip>
  dns del forwardzone <domain-name> <server ip>
  dns add trustanchor <anchor>
  dns del trustanchor <zonename>
  dns lookup (A|AAAA|SRV) <hostname>
  dns flush
  dns add rr <DNS RR>
  dns del rr <owner-name> <type>
acano> dns flush
acano>

```

4. Enable SIP tracing and DNS tracing:
 - a. In the Web Admin Interface go to **Logs > Detailed Tracing**.
 - b. Enable SIP traffic tracing and DNS tracing. In most cases, enabling for 30

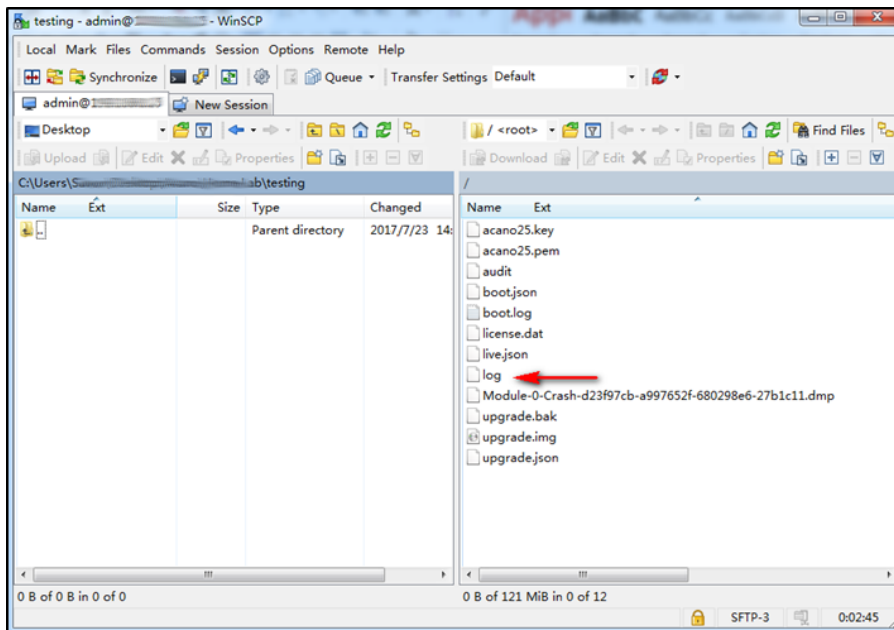
minutes is enough.

Detailed tracing

The screenshot shows three sections for tracing configuration:

- SIP traffic tracing:** SIP traffic tracing status is Disabled. Buttons: Enable for 1 minute, Enable for 10 minutes, Enable for 30 minutes, Enable for 24 hours, Disable.
- DNS tracing:** DNS logging status is Disabled. Buttons: Enable for 1 minute, Enable for 10 minutes, Enable for 30 minutes, Enable for 24 hours, Disable.
- API tracing:** API logging status is Disabled. Buttons: Enable for 1 minute, Enable for 10 minutes, Enable for 30 minutes, Enable for 24 hours, Disable.

5. Recreate the issue by placing a single test call.
6. After the problem has been reproduced disable tracing as soon as possible.
7. Log in to the Cisco Meeting Server via WinSCP, using your Web Admin Interface login credentials.
8. In the root directory find the file called “log” and drag it to your local PC.



9. Zip the log files and send it to Cisco Support.

Collecting XMPP log files

You must close the Meeting App before collecting the XMPP log. This is because the logs are only updated when the app is closed. The logs are available here:

For Mac `~Library/Caches/com.cisco.client/`

For Windows `c:\Users<user_name>\AppData\Roaming\cisco`

For iOS tap three times in the call screen to send diagnostics. This will include the xmpp log in the email.

Alternatively, use the **Diagnostics** button in the **Settings** screen.

Or, in the event that you want to use logs that are already on the device, attach the device to a Mac or PC and use iTunes to download the logs (select the iDevice in iTunes then go to apps, scroll down to see shared files).

Appendix B Client Diagnostic Log Analysis

There is information in the diagnostic log that is useful when investigating some common issues such as media negotiation, packet loss, jitter and key frame requests (Fast Update Request).

This appendix provides some tips for finding this information in the log.

Media sessions info – audio session

In the Media session info section (see below), look for the line starting Audio session.

```

2284 === Media sessions info =====
2285 ==== Media session FE48560 ====
2286   Change object awaiting 0 responses
2287   -- Message counter --
2288   Session offers sent 2 response 2, pending 0
2289   Session answers received 2
2290   Selections sent 2 response 2, pending 0
2291   Selections received 1
2292   Advertisement sent 1 response 1, pending 0
2293   Configures sent 0 response 0, pending 0
2294   Configures received 0
2295   Streams advertised:
2296   Audio: 25703630-d8ef-4e88-bbe9-8d3129d3016f
2297   Main video: de6ac16d-ec14-4fc1-9297-a83afc6bc6b7
2298   Streams requested from far end:
2299     bdc7d5b4-5a73-419b-8d09-ead2ff8c00ac with multiplexId 2 @ 1010x688; aspect ratio 1010:688; layout 3
2300     4e1a1422-0984-45a4-9577-dfc3c304d472 with multiplexId 1
2301   Audio session: 25703630-d8ef-4e88-bbe9-8d3129d3016f
2302   Remote media: 209.9.228.135:3478; control: 209.9.228.135:3478
2303     215 seconds ago: media -:50139; control: -:50391
2304     215 seconds ago: media 209.9.228.135:3478; control: 209.9.228.135:3478
2305     215 seconds ago: media 209.9.228.135:3478; control: 209.9.228.135:3478
2306   Estimated bandwidth: Unknown
2307   Interfaces:
2308     10.86.8.11 media 51164 control 51165
2309     ::1 media 51166 control 51167
2310     127.0.0.1 media 51168 control 51169
2311     2001::9d38:6ab8:3890:efe:8380:bbfb media 51170 control 51171
2312     fe80::3890:efe:8380:bbfb media 51172 control 51173

```

There you find the remote and local media interfaces including the IP address and port used in each case.

Further down in this same audio session you find the information about chosen codec and bitrate for audio (see below).


```

2498 Ice complete: 1
2499 DTLS not started media complete 1 control complete 1
2500 Tx statistics:
2501 Multiplex ID 100
2502 SSRC fa4104ef
2503 Payload type 98
2504 Codec opus
2505 Clock rate 48000
2506 Packets Total 10569
2507 Bitrate 67.9 Kbps
2508 Round trip time 215ms
2509 Encryption on
2510 Rx statistics:
2511 Multiplex ID 1
2512 SSRC 1cb7b15f
2513 Payload type 98
2514 Codec opus
2515 Clock rate 48000
2516 Packets Total 10672
2517 Bitrate 77.5 Kbps
2518 Encryption on
    
```

Media sessions info – video session

Further down is the video session section.

```

2519 Video session: de6ac16d-ec14-4fc1-9297-a83afc6bc6b7
2520 Remote media: 209.9.228.135:3478; control: 209.9.228.135:3478
2521 215 seconds ago: media -:50389; control: -:50313
2522 215 seconds ago: media 209.9.228.135:3478; control: 209.9.228.135:3478
2523 Estimated bandwidth: 18454873 over 1 tx streams
2524 Interfaces:
2525 10.86.8.11 media 51174 control 51175
2526 :::1 media 51176 control 51177
2527 127.0.0.1 media 51178 control 51179
2528 2001::9d38:6ab8:3890:efe:8380:bbfb media 51180 control 51181
2529 fe80::3890:efe:8380:bbfb media 51182 control 51183
    
```









Here you find the remote and local media interfaces including IP address and port for each interface.

Further down in this same video session section, you find information about the chosen codec, bitrate for audio and keyframe requests (see below). Packet loss can generate keyframe requests.

```

2715 Ice complete: 1
2716 DTLS not started media complete 1 control complete 1
2717 Tx statistics:
2718 Multiplex ID 200
2719 SSRC e7ee89ea
2720 Payload type 96
2721 Codec H264
2722 Clock rate 90000
2723 Packets Total 17619
2724 Dropped 2 Curr 0.0 pct
2725 Bitrate 720.4 Kbps
2726 Round trip time 217ms
2727 Encryption on
2728 Resolution 768x448
2729 Framerate 28.9 fps
2730 Keyframes Requests 6
2731 Keyframes 0
2732 Configured bitrate 1024.0 Kbps
2733 Flow control bitrate 1024.0 Kbps
2734 Rx statistics:
2735 Multiplex ID 2
2736 SSRC 5501d8bc
2737 Payload type 96
2738 Codec H264
2739 Clock rate 90000
2740 Packets Total 18526
2741 FEC 9
2742 Dropped 72 Curr 0.0 pct
2743 Bitrate 721.6 Kbps
2744 Encryption on
2745 Resolution 768x448
2746 Framerate 25.3 fps
2747 Keyframes Requests 363
2748 Keyframes 59
2749 Configured bitrate 0.0 Kbps
2750 Flow control bitrate 0.0 Kbps

```

 Chosen TX video codec
 0.0% packet loss TX
 Video codec TX bitrate
 keyframe requests TX
 Chosen RX video codec
 0.0% packet loss RX
 Video codec RX bitrate
 keyframe requests RX

Media diagnostics

Information in the Media Diagnostics section can be useful: in the following example, you see issues such as audio echo, low available CPU and packet loss.

```

3166 ===== Media Diagnostics =====
3167
3168 1 848 1 0 0 audio echo
3169
3170

```

```

3473 ===== Media Diagnostics =====
3474
3475 2 468 40 0 1005 low available CPU
3476
3477

```

```

1099 ===== Media Diagnostics =====
1100
1101 1 448 1 2 0 audio echo
1102 34 2790 50 1 24 packet loss
1103 38 308 50 1 35 packet loss
1104

```

Call Bridge selection

In XMPP info section, you can find the Call Bridge homing your app after Call Bridge selection procedure.

```

813 === XMPP info =====
814 Connected to 200.100.1.79
815 Choosing from 3 servers after 500ms
816 Server ukcore1.example.com (score 3710886328):
817   RTT direct: Unreachable
818   RTT via 200.100.1.80: 2ms local + 0ms remote
819   RTT via 200.100.1.25: 3ms local + 1ms remote
820   RTT via 200.100.1.77: 2ms local + 1ms remote
821   RTT via 200.100.1.79: 2ms local + 0ms remote
822 Server ukcore2.example.com (score 3251570200):
823   RTT direct: Unreachable
824   RTT via 200.100.1.80: 2ms local + 0ms remote
825   RTT via 200.100.1.25: 3ms local + 0ms remote
826   RTT via 200.100.1.77: 2ms local + 1ms remote
827   RTT via 200.100.1.79: 2ms local + 0ms remote
828 Server uscore1.example.com (score 1782068193):
829   RTT direct: Unreachable
830   RTT via 200.100.1.80: 2ms local + 0ms remote
831   RTT via 200.100.1.25: 3ms local + 0ms remote
832   RTT via 200.100.1.77: 2ms local + 1ms remote
833   RTT via 200.100.1.79: 2ms local + 0ms remote
834 Chosen best server ukcore1.example.com with RTT 2
835 === End XMPP info =====

```

Homed by ukcore1 ←

If you see it is chosen by request of server, it means this specific user has already homed by the Call Bridge and the homing session timer has not got expired. So no Call Bridge selection procedure involved.

```

815 === XMPP info =====
816 Connected to 200.100.1.79
817 Choosing from 3 servers after 0ms
818 Server ukcore1.example.com chosen by request of server
819 === End XMPP info =====

```

Homed by ukcore1 ←

Appendix C Server Diagnostic Log Analysis

There is information in the diagnostic log that is useful when investigating some common issues such as media negotiation, packet loss, jitter and key frame requests (Fast Update Request).

This appendix provides some tips for finding this information in the log.

Recent log messages

```

diagnostics request received for "acanouser1@acanodemo.com"...

Recent log messages:
21:11:35.819 Info user "acanouser1@acanodemo.com": sending diagnostics response...
21:11:01.609 Info participant "acanouser1@acanodemo.com" joined coSpace ea262e80-bcaf-4bcc-b0af-fd58e9825e1d (acanouser1.coSpace)
21:11:01.527 Info call 6: allocated for acanouser1@acanodemo.com "Windows PC client" conference participation
21:11:01.147 Info new session created for user "acanouser1@acanodemo.com"
21:10:56.558 Info participant "acanouser2@acanodemo.com" joined coSpace ea262e80-bcaf-4bcc-b0af-fd58e9825e1d (acanouser1.coSpace)
21:10:56.477 Info call 5: allocated for acanouser2@acanodemo.com "iPad client (iPad2,2)" conference participation
21:10:56.301 Info new session created for user "acanouser2@acanodemo.com"
21:10:53.297 Info successful login request from acanouser2@acanodemo.com
21:09:20.607 Info successful login request from acanouser1@acanodemo.com
11:42:49.416 Info participant "user2.lync@acanodemo.com" left coSpace fb425a00-df72-4864-8776-f81ff0cc5716 (acanouser2.coSpace)
11:42:49.416 Info call 4: ending: remote SIP teardown
11:42:47.647 Info participant "user2.lync@acanodemo.com" joined coSpace fb425a00-df72-4864-8776-f81ff0cc5716 (acanouser2.coSpace)
11:42:46.834 Info conference "acanouser2.coSpace": unencrypted call legs now present
11:42:46.819 Info call 4: incoming encrypted SIP connection from "sip:user2.lync@acanodemo.com" to local URI "sip:acanouser2.cospace@acanodemo.com" (Lync)
11:42:46.819 Info call 4: recognised as Lync
11:21:13.603 Info participant "user2.lync@acanodemo.com" left coSpace fb425a00-df72-4864-8776-f81ff0cc5716 (acanouser2.coSpace)
11:21:13.603 Info call 3: ending: remote SIP teardown
11:21:11.919 Info participant "user2.lync@acanodemo.com" joined coSpace fb425a00-df72-4864-8776-f81ff0cc5716 (acanouser2.coSpace)
  
```

Finding the corresponding client log

Because the Core server log is generated when a client log is created, there is a pair of logs to help troubleshoot an issue from both “ends” of a call.

To identify which of the server logs matches a specific client log, the same information is displayed in both. The screen shot below shows an example of the information that is the same in both server-side and client-side logs.

```

client diagnostics:
Acano PC Client version 1.1.2.3
== User interface info =====
Video display D9D898
Video stream 0
Video display 63681F0
Call: DFECE8
Video stream D6E05C
== End user interface info =====
  
```

Audio media session

Both of the following screenshots are taken from a server log. The first shows the media interface chosen on server and on client.

```

Audio: af38227e-2887-45c1-9313-fed5b2c180cd
Main video: e5fd0880-73be-4390-b947-86b3da1abf08
Streams requested from far end:
    90f56b55-043c-41a0-b807-3dc5c9e52132 with multiplexId 1
Audio session: af38227e-2887-45c1-9313-fed5b2c180cd
Remote media: 192.168.1.239:36242; control: 192.168.1.239:36243
    13 seconds ago: media -:36242; control: -:36243
Estimated bandwidth: Unknown
Interfaces:
fe80::4c97:7c55:ad91:edbe media 49670 control 49671
192.168.164.1 media 49672 control 49673
fe80::7c21:be4f:a749:1ad7 media 49674 control 49675
192.168.198.1 media 49676 control 49677
::1 media 49678 control 49679
127.0.0.1 media 49680 control 49681
fe80::e886:403f:f9dd:d50c media 49682 control 49683
192.168.1.210 media 49684 control 49685
    
```

Audio session (points to 'Audio: af38227e-2887-45c1-9313-fed5b2c180cd')

Server media interface (points to 'Remote media: 192.168.1.239:36242; control: 192.168.1.239:36243')

Client media interface (points to '192.168.1.210 media 49684 control 49685')

The second screen shot is about codec and bitrate used in the call. The codec is negotiated during call set up process.

Note: Even though this is the server log, TX is the bit rate received by the server—the reference point is the client not the server.

```

Ice complete: 1
DTLS not started media complete 1 control complete 1
Tx statistics:
  Multiplex ID      100
  SSRC              9ad13cce
  Payload type      98
  Codec             opus
  Clock rate        48000
  Packets Total     1628
  Bitrate           68.0 Kbps
  Round trip time   2ms
  Encryption        on
Rx statistics:
  Multiplex ID      1
  SSRC              45a937ab
  Payload type      98
  Codec             opus
  Clock rate        48000
  Packets Total     1621
  Bitrate           77.5 Kbps
  Encryption        on
    
```

Note: Reference Point is the Client (points to 'Tx statistics:')

Chosen TX Audio Codec (points to 'Codec opus')

Audio Codec TX Bitrate (points to 'Bitrate 68.0 Kbps')

Chosen RX Audio Codec (points to 'Codec opus')

Audio Codec RX Bitrate (points to 'Bitrate 77.5 Kbps')

Video media session

These examples are from the server log.

```

Video session: a01fb6a5-5562-4f03-811d-17482b32f347
Remote media: 192.168.1.25:43472; control: 192.168.1.25:43473
 34 seconds ago: media -:43472; control: -:43473
Estimated bandwidth: 32645161 over 1 tx streams
Interfaces:
 192.168.1.106 media 50638 control 50639
 ::1 media 50640 control 50641
 127.0.0.1 media 50642 control 50643
 2001::5ef5:79fb:14bb:2d78:3f57:fe95 media 50644 control 50645
 fe80::14bb:2d78:3f57:fe95 media 50646 control 50647

```

Video session Remote (server) media interface

Client media interface

```

Ice complete: 1
DTLS not started media complete 1 control complete 1
Tx statistics:
  Multiplex ID      200
  SSRC              6db666f8
  Payload type      96
  Codec             H264
  Clock rate        90000
  Packets Total     3559
  Bitrate           1277.5 Kbps
  Round trip time   2ms
  Encryption        on
  Resolution        768x448
  Framerate         29.9 fps
  Keyframes         Requests 2
  Keyframes         0
  Configured bitrate 1472.0 Kbps
  Flow control bitrate 1472.0 Kbps
Rx statistics:
  Multiplex ID      2
  SSRC              429d5ebe
  Payload type      96
  Codec             H264
  Clock rate        90000
  Packets Total     2663
  Bitrate           658.9 Kbps
  Encryption        on
  Resolution        288x352
  Framerate         29.6 fps
  Display           29.6 fps
  Keyframes         Requests 2
  Keyframes         7
  Configured bitrate 0.0 Kbps
  Flow control bitrate 0.0 Kbps

```

Note: Reference point is the client

Chosen TX video codec

Video codec TX bitrate

Keyframe requests TX

Chosen RX video codec

Video codec RX bitrate

Keyframe requests RX

Note: Normally there are only 1 or 2 keyframe requests (typically at the beginning of the call); therefore if there are several of them this can indicate a problem. Generally, a keyframe request is sent when a device (server or client) realizes that it is receiving packet loss.

Client device information

The following screenshot is from a server log.

```
== Media info =====  
Audio playback device: Speakers (3- Logitech USB Heads) ← Speaker  
  Input 0: 4  
    playing back SSRC 45a937ab  
  Input 1: 0  
Audio capture device: Microphone (2- TANDBERG Audio) ← Microphone  
  
===== OS & CPU =====  
  
WindowsVer Major 6 Minor 1 : Service Pack 1  
CPU Intel Stepping 6 Model 7 Family 6 Type 0 XModel 1 XFamily 0 ← Client OS & CPU  
Freq 2527 Cores 2 Threads 2 Caps 0x3f Rating 4043.199951
```

Appendix D Log Analysis

There is information in the log that is useful when investigating some common issues such as Cisco Meeting App sign in, join a call, left a call and call drop.

This appendix provides some tips for finding this information in the log.

Acanouser1 logged in from Cisco Meeting App.

Sep 21 05:57:03 user.info acano host:server: INFO : new session created for user acanouser1@example.com

Acanouser1 join a space

```
Sep 21 05:57:04 user.info acano host:server: INFO : call 8: allocated for acanouser1@example.com "Windows PC client" conference participation
```

```
Sep 21 05:57:04 local0.info acano host:server: INFO : participant "acanouser1@example.com" joined coSpace 373d13a0-da03-4137-9c56-1cf83eff6a0b (acanouser1.cospace)
```

Acanouser1 left the space by the user

```
Sep 21 05:57:11 user.info acano host:server: INFO : acanouser1@example.com resource user "67b8d47dc57fe63d": deactivating due to session resource teardown
```

```
Sep 21 05:57:11 user.info acano host:server: INFO : call 8: tearing down ("acanouser1@example.com" conference media)
```

```
Sep 21 05:57:11 local0.info acano host:server: INFO : participant "acanouser1@example.com" left coSpace 373d13a0-da03-4137-9c56-1cf83eff6a0b (acanouser1.cospace)
```

Acanouser1 left the space due to network connection problem

```
Sep 21 05:58:00 user.info acano host:server: INFO : call 9: inactivity notification; tearing down...
```

```
Sep 21 05:58:00 user.info acano host:server: INFO : resource 0:0 for "acanouser1@example.com"; deactivating due to call drop
```

```
Sep 21 05:58:00 user.info acano host:server: INFO : resource 0:0 for "acanouser1@example.com"; sending stream failure indication, size 98
```

```
Sep 21 05:58:00 user.info acano host:server: INFO : user "acanouser1@example.com", ephemeral invitation no longer valid due to call drop
```

```
Sep 21 05:58:00 local0.info acano host:server: INFO : participant "acanouser1@example.com" left coSpace 373d13a0-da03-4137-9c56-1cf83eff6a0b (acanouser1.cospace)
```

Acanouser1 was removed from Cisco Meeting Server due to timeout

Sep 14 11:00:20 user.info acano host: server: INFO : destroying client instance for "user1@example.com" on keep-alive timeout

Sep 14 11:00:20 user.info acano host: server: INFO : deinstantiating user user1@example.com

A report of long delay and call drop

Sep 14 12:47:57 user.warning acano host: server: WARNING : call 9068 (acanouser1): video round trip time of 1643 ms observed...

Sep 14 13:20:09 user.info acano host: server: INFO : call 9068: inactivity notification; tearing down...

Sep 14 13:20:09 user.info acano host: server: INFO : user "user1@example.com", ephemeral invitation no longer valid due to call drop

Sep 14 13:20:09 local0.info acano host: server: INFO : participant "acanouser1@example.com" left coSpace 373d13a0-da03-4137-9c56-1cf83eff6a0b (acanouser1.cospace)

Cisco Legal Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

© 2018 Cisco Systems, Inc. All rights reserved.

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)