FAQs and Troubleshooting

This chapter provides FAQs and troubleshooting hints for various Cisco WebEx Social components.

This chapter is organized as follows:

Installation and Upgrade FAQs and Troubleshooting

Installation and Upgrade Troubleshooting

This section provides the following troubleshooting information:

Symptom The Topology page on the Director is empty after upgrade.

Possible Cause After upgrading Cisco WebEx Social to a newer version, the System > Topology page on the Director displays an empty server list.

Recommended Action Refresh your web browser using F5 or Ctrl-F5 (for hard refresh).

Symptom After an upgrade, the Director's Health page displays Integrity check alerts.

Possible Cause This issue may arise if the scheduled run of the Integrity service coincides with the upgrade process in which case the integrity check expectably fails because files are changing.

Recommended Action Manually rerun the integrity check on the affected nodes. Take these steps:

Step 1 Find the affected nodes' hostnames by looking at the Health page and taking note of the Host column of each occurrence of the alert.

Step 2 Log in to each of the affected nodes using user admin and execute this command:

sudo /opt/cisco/bin/integrity.sh --run-check

Step 3 After running this command, verify the messages log for this particular node in the Director logs to check for any errors resulting from the integrity check script. The alerts from the Director's Health page should disappear in a few minutes.

Symptom Some nodes are inaccessible using SSH right after fresh installation.

Possible Cause The Unified Access Password did not propagate successfully to all nodes.

Recommended Action Reset your Unified Access Password using the Director. Take these steps:

Step 1 Sign in to the Director.

Step 2 Go to System > Configuration > Unified Access.

Step 3 Check the box for each component for which to propagate the unified access password. Make sure Grub is selected.

Step 4 Enter your new **Unified Password**. This can be your previous password or a new one.

Step 5 Click **Save**.

Symptom The upgrade of the Message Queue nodes fails.

Possible Cause Puppet on the Message Queue nodes fails thus preventing the nodes from upgrading to the newer release. Indication that the problem has occurred is if the Director's Topology page displays the preceding release number for the Message Queue nodes. Another indication is having the following error appear in the *HOSTNAME*_puppet.log on the Message Queue node:

```
err: Could not retrieve catalog from remote server: Error 400 on SERVER: Invalid
parameter provider at /opt/cisco/software/puppet/manifests/classes/rabbitmq.pp:85 on
node mq1.example.com
```

Recommended Action

Step 1 Use SSH to log in to the Director as admin.

Step 2 Select **Drop to shell** from the menu.

Step 3 Execute the command:

sudo service puppetmaster restart

Step 4 Use SSH to log in to each Message Queue node as admin.

Step 5 Select **Drop to shell** from the menu.

Step 6 Execute the command:

sudo service puppet debug

Core Functionality FAQs and Troubleshooting

Core Functionality FAQs

Q. Why does the resulting LAR file not contain posts when I am exporting a community?

A. A post always belongs to a user. Communities are only related to a post through a share connection. That is why no posts are exported to the LAR file when exporting a community. For a list of what is exported, see the checked boxes on the Export page.

Core Functionality Troubleshooting

This section provides the following troubleshooting information:

Symptom File attached to an update is not visible in full page view.

Possible Cause This issue can appear when you have your browser idle in Cisco WebEx Social for a long period (for example: > 8 hours). More specifically, these conditions must have all been true:

- The Cisco Social session timeout has been increased in Web.xml to more than the default 8 hours.
- The attachment clean-up interval parameter (com.cisco.ecp.vdl.attachment.cleanup.job.interval) has not been changed.
- The update has been posted after waiting on the compose screen for a significant amount of time (more than com.cisco.ecp.vdl.attachment.cleanup.job.interval).

Recommended Action To prevent this issue from appearing again, sign in to the Director, go to Application > Portal > Advanced Portal Properties and search for com.cisco.ecp.vdl.attachment.cleanup.job.interval. Set its value to be one hour longer than the session timeout. (Note that the com.cisco.ecp.vdl.attachment.cleanup.job.interval is in minutes while the session timeout is in hours.)

Symptom Community creation pauses indefinitely.

Possible Cause This issue may be due to you NFS storage being unreachable.

Recommended Action Check to see if your NFS storage is running and responding and that it is reachable from the network segment Cisco WebEx Social is in.

Email Integration FAQs and Troubleshooting

Email Integration FAQs

Q. How do I set the log trace levels for Postfix?

A. If you suspect an issue between Postfix and the SMTP server Postfix is talking to, you can enable verbose logging of all SMTP messaging in the maillog file. Take these steps:

Step 1 Log in to each Worker node as admin and run this command: **sudo vi /etc/postfix/main.cf**

Step 2 In the vi editor, add the following line (assuming it is not already present in the file):

```
debug_peer_list = example.com
```

where *example.com* is the domain of the SMTP server that Postfix is sending to.

Step 3 Save the changes.

Step 4 Run this command to restart Postfix: **sudo service postfix restart**

It is recommenced to undo the changes after you are finished troubleshooting. To undo the changes:

Step 1 Log in to each Worker node as admin and run this command: **sudo vi /etc/postfix/main.cf**

Step 2 In the vi editor, remove the line that you added.

Step 3 Save the changes.

Step 4 Run this command to restart Postfix: **sudo service postfix restart**

Q. What is the size of an email notification and can I control it?

A. Mail notifications vary in size depending on the content (how much text and how many images are included) but cannot exceed 5MB. The summary size of all text inside an email notification cannot exceed 1MB and the summary size of all images cannot exceed 4MB. In case the former limitation is exceeded, a Read More link is displayed. In case the later limitation is exceeded, a generic thumbnail is displayed instead of images. These limits are not configurable.

Q. Why are some images from the post displayed as thumbnails in the email notification?

A. When the cumulative size of the post images exceeds a certain limit or another size limit is reached (see Q. What is the size of an email notification and can I control it?) images (starting from the bottom) are replaced in the email notification for that post by generic file type thumbnails to minimize size. How many images are replaced depends on how much size needs to be saved. As a side effect, bottom images that need to be replaced but have also been inserted one or more times up the post, are all displayed as thumbnails, even if the size restrictions do not require this.

Q. How do I verify that Inbound Email is functioning properly?

A. Take these general steps:

- SMTP server
  - Verify that the SMTP server is configured properly and that a forward zone and an MX record are in place for the domain of the email recipients, otherwise undeliverable mail notifications might be received.
- Postfix MTA

  - Ensure that the postfix service is running on the Worker node behind the port specified in the configuration (the default is 25)
  - Ensure that the firewall is not blocking the postfix service
  - Verify that messages are properly deferred from the postfix queues. If not, there might be some problem communicating with SubethaSMTP—either the server is not running or postfix is not configured properly.
- SubethaSMTP MDA
  - Ensure that the SubethaSMTP server is running on the Worker node behind the port specified in the configuration (the default is 2025)
- NFS
  - Verify that the specified folder has bean created (the default is data\inboundmail) on the NFS storage and that the owner of the folder is quad:quad. Otherwise there might be problems storing new messages.
- OracleDB
  - Verify that the sender email address belongs to a WebEx Social user and that the user is active and has accepted the license agreement.
  - Verify that the user has permission to create content (in the corresponding community). Not having permission should result in respective log messages being written to the App Server log.
- MongoDB
  - Verify that the recipients and messageThread collections exist
  - Verify that there is a recipient whose _emailAddress matches the local part of the email address of the email recipient
  - Verify that the recipient's classNameId value is proper (Group in case of writing to a community, PostMapping in case of writing to a post, MBCategory in case of writing to a discussion category) and that the classPK points to an existing object of the determined type
  - In the case of an email reply, verify that the parent massage can be looked up by its in-reply-to, references or threadindex headers

Q. Now that the inbound and outbound email uses RabbitMQ instead of ActiveMQ, has anything changed in respect to how the features work?

A. The features function the same way as before. Hoever, a set of new Advanced Portal Properties has been added to compensate for differences between the two message queue implementations:

For inbound email:

- inboundmail.retry.interval=5000
- inboundmail.max.retry.count=4
- inboundmail.initial.pool.size=3
- inboundmail.max.pool.size=5
- inboundmail.idle.threads.keepalive=10000
- inboundmail.pool.queue.capacity=10

For inbound email:

- outbound.retry.interval=5000
- outbound.max.retry.count=4

- outbound.instant.initial.pool.size=2
- outbound.instant.max.pool.size=3
- outbound.instant.idle.threads.keepalive=10000
- outbound.instant.pool.queue.capacity=6
- outbound.digest.initial.pool.size=1
- outbound.digest.max.pool.size=1
- outbound.digest.idle.threads.keepalive=10000
- outbound.digest.pool.queue.capacity=2

Email Integration Troubleshooting

This section provides the following troubleshooting information:

Symptom A reply created using Outlook/OWA is added as first level comment in WebEx Social instead of as a reply.

Possible Cause Your organization is using Microsoft Exchange Server 2003 without the KB908027 fix applied.

Recommended Action Apply the fix or upgrade to the latest version of Microsoft Exchange Server 2003. For more information, see http://support.microsoft.com/kb/908027.

Symptom Out of the Office auto replies to WebEx Social email notifications are added as content in WebEx Social.

Possible Cause The user account sending the Out of Office message is hosted on Microsoft Exchange Server 2003.

Recommended Action Mail accounts running on later versions of Microsoft Exchange Server or IBM Lotus Domino should not run into this issue.

Symptom A number of (or all) users did not receive their email digests (summary of important updates).

Possible Cause You have recently increased or decreased worker.digestscheduler.mainJobRepeatInterval. After the value has been modified and saved, the Digest Scheduler waits for that interval before it runs again. Depending on a number of related factors some users may be skipped when creating digests.

Recommended Action Wait for worker.digestscheduler.mainJobRepeatInterval to run out (30 min. if left at its default), then the digests should start arriving on schedule.

Possible Cause The user has requested a daily digest and you have set worker.digestscheduler.mainJobRepeatInterval to a large value that makes the next run of the Digest Scheduler to fall into the next day.

Recommended Action When you are setting the worker.digestscheduler.mainJobRepeatInterval parameter, take the "Daily Digest Notification Time" value (Director > Application > Portal > Email Digest) in consideration. Set worker.digestscheduler.mainJobRepeatInterval to a value that allows the Digest Scheduler to run at least once in the time frame between "Daily Digest Notification Time" and the end of the day.

For example if you have set "Daily Digest Notification Time" to 23:00 (11 pm), that leaves the Digest Scheduler only 1 hour to start and complete its run; ensure this by setting worker.digestscheduler.mainJobRepeatInterval to less than an hour.

Possible Cause The user has recently changed their time zone. If the new time zone has already been notified, the affected user does not receive their daily report.

Recommended Action Keeping the time zone setting should allow the user to receive future daily reports on schedule.

Symptom Users receive multiple daily digests.

Possible Cause The Administrator has changed the Daily Digest Notification Time after the daily digest has been sent out for the day.

Recommended Action If you want to avoid duplicate daily digests when changing Daily Digest Notification Time to an earlier time, ensure you make the change before the original time comes for the day.

Possible Cause The user has recently changed their time zone. If the new time zone has not been notified yet, the affected user receives a second report.

Recommended Action Keeping the time zone setting should allow the user to receive future daily reports on schedule.

Symptom Users receive multiple weekly digests.

Possible Cause The Administrator has changed the Weekly Digest Notification Date forward after the weekly digest has been sent out for the week.

Recommended Action If you want to avoid duplicate weekly digests, ensure you make the change to Weekly Digest Notification Date before the original time comes for the week.

Symptom Inbound email does not appear as content in Cisco WebEx Social.

Possible Cause The Worker node is restarting or has just been restarted.

Recommended Action Wait for about 10 minutes. After that, the emails that have been sent should appear as content.

Symptom Some replies are saved as new posts containing the entire email thread as opposed to comments to the original content.

Possible Cause This issue can arise if the original email has not yet been processed by Cisco WebEx Social.

Recommended Action If you experience this issue often, check the Dashboard for the Worker nodes (Director GUI > Stats). If the App Server/Worker nodes are under heavy load—as indicated by the CPU and Load charts—then consider adding more App Server or Worker nodes, or both.

Possible Cause This issue can arise if some of the SMTP headers that Cisco WebEx Social uses to identify the message thread have been deleted or lost.

Recommended Action Check to see if the all these SMTP headers are present in the email and if they have a meaningful value:

- In-Reply-To
- References
- Thread-Index

If one or more of the headers are missing, investigate to find out why and at what stage these headers have been lost.

Symptom Users are not receiving any emails generated by Cisco WebEx Social.

Possible Cause Your email relay is not relaying messages coming from Cisco WebEx Social.

Recommended Action Configure your email relay host to properly relay messages coming from Worker nodes.

Symptom Video thumbnails do not display in email notifications.

Possible Cause Worker nodes do not have the Show and Share (SNS) security certificates installed. Because email notifications are generated on the Worker role, all Worker nodes should have access to the Show and Share server to be able to access video thumbnail and URL data.

Recommended Action Ensure that you have installed the SNS security certificates on all App Server and Worker nodes. For installing the certificates on App Server nodes, see "Cisco Show And Share" in the *Cisco WebEx Social Administration Guide*. To install the certificates on Worker nodes, complete the following steps on each Worker node:

Step 1 Using your preferred method, copy the SNS certificate PEM file to the /home/admin directory on the Worker node.

Step 2 Log in to the Worker node as admin and select **Drop to shell**.

Step 3 Run this command:

cd /usr/java/default/lib/security/

Step 4 Import the PEM certificate file into the Java keystore by typing the following command:

sudo ../../bin/keytool -import -keystore cacerts -alias <*certificate alias*> -file /home/admin/<*certificate filename*>

where *certificate alias* is an arbitrary name such as the SNS server hostname; *certificate filename* is the name of the PEM file containing the certificate.

Step 5 When prompted, enter the keystore password: *changeit*

Step 6 Restart the Worker service:

service worker restart

Symptom Email notifications about alerts and announcements stop sending out.

Possible Cause This issue may appear after the Worker node is restarted. Alerts and announcements are then held in pending state because the main alerts/announcements job has entered an ERROR state.

Recommended Action Take the following steps to restore the notifications:

Note The following steps are only to be taken by or under the supervision of Cisco Advanced Services.

Step 1 Log in to Oracle.

Step 2 Check in what state the triggers are by executing this Oracle statement:

```
select count(*)
from worker_triggers wt
where wt.trigger_state = 'ERROR';
```

Step 3 If you receive more that "0" out of this step then execute the following statement to bring the triggers back to operational state:

update worker_triggers wt

```
set wt.trigger_state = 'WAITING'
where wt.strigger_state = 'ERROR';
```

Email and Office Plug-in FAQs and Troubleshooting

Email and Office Plug-in FAQs

Q. Does the Cisco WebEx Social Email Plug-in log information on the user computer?

A. Yes. These are the log file locations depending on the email client:

- Microsoft Outlook on Windows 7: %USERPROFILE%\AppData\Local\Cisco\WebEx Social Email Plugin\WebexSocialPluginLog.txt
- Microsoft Outlook on Windows XP: %USERPROFILE%\Local Settings\Application Data\Cisco\WebEx Social Email Plugin\WebExSocialPluginLog.txt
- IBM Lotus Notes: %USERPROFILE%\AppData\Local\Lotus\Notes\Data\quadlogs

Calendar FAQs and Troubleshooting

Calendar FAQs

Q. Can I switch a user from Microsoft Exchange to Lotus Domino (or vice versa)?

A. The described is not possible in the current release. After the user account has been configured to connect to a certain type of calendar server, it cannot be changed. In Account Settings, the user continues to see the same type of calendar server even if the administrator changes the type for the organization in Control Panel.

Q. In what time zone are the calendar events displayed?

A. The Calendar application displays events in the time zone of the browser. Server-side, all dates are accepted and returned in UTC. Date transformation to user time is performed in the browser.

Calendar Troubleshooting

This section provides the following troubleshooting information:

Symptom LDAP user cannot connect to Microsoft Exchange Server through WebDAV.

Possible Cause (Only if "Use LDAP Directory Synchronization" is checked in the Calendar Configuration under Server > Common Configurations.) The user email address has been changed. Because WebEx Social uses the prefix of the email address to construct the WebDAV URL, the user can be prevented from connecting to Microsoft Exchange.

Recommended Action Ask the user to complete these steps:

Step 1 Open your profile menu and click Account Settings.

Step 2 Click Calendar and WebEx login.

Step 3 Under Microsoft Exchange, change the Server URL as follows:

1. Identify your email prefix in the URL. It is the ending part starting right after the last forward slash (/). For example if your URL is http://dev.example.com/Exchange/emma.jones, "emma.jones" is your email prefix.
2. Replace your previous email prefix with your new email prefix. For example if your email prefix has been changed from emma.jones to ejones, your URL should look like this: http://dev.example.com/Exchange/ejones

Step 4 Click Test.

The connection should succeed.

Symptom Domino users who connect through SSL cannot connect after upgrading WebEx Social.

Possible Cause The IBM Lotus Domino SSL security certificate has been invalidated by WebEx Social.

Recommended Action Reimport the SSL security certificate. See the Administration Guide for detailed instructions.

Symptom I added a new attendee to a recurring meeting using Microsoft Outlook but the new name does not appear in the Calendar application in Cisco WebEx Social.

Possible Cause There is a know issue with some versions of Microsoft Exchange Server when calendaring information is fetched over WebDAV.

Recommended Action Use Microsoft Outlook Web Access to edit the recurring meeting instead of Microsoft Outlook.

Video Calls FAQs and Troubleshooting

Video Calls FAQs

Q. How do I check what Call Plug-in version is available on WebEx Social?

A. Open the following URL:

http://<*WS base url*>/plugin/cwc/CWICPluginVersion

where <*WS base url*> is the URL you use to access WebEx Social.

Q. Why does the video always appear on top hiding other WebEx Social elements?

A. With the intention to provide the best possible video experience to users, WebEx Social tries to use hardware acceleration when available. Because of that most other HTML elements cannot be placed on top of the video frame. Some web browsers may behave differently than others.

Q. Does the WebEx Social Call Plug-in log information during installation?

A. If you face problems when installing or uninstalling the WebEx Social Call Plug-in, locate the installation log under:

Windows 7: %USERPROFILE%\AppData\Local\Temp\WebCommunicator.LOG

Windows XP: %USERPROFILE%\Local Settings\Temp\WebCommunicator.LOG

Mac OSX: /private/var/log/install.log

Q. Does the WebEx Social Call Plug-in log information during operation?

A. If you suspect the WebEx Social Call Plug-in is not operating correctly, locate the operation log under:

Windows 7: %USERPROFILE%\AppData\Local\softphone.log

Windows XP: %USERPROFILE%\Local Settings\Application Data\softphone.log

Mac OSX: /Users/{$USER}/Library/Application Support/softphone.log

Q. How do I enable JavaScript logging for the Call Pug-in?

A. Appending "?isDebug=true" at the end of the URL in your browser allows you to view detailed operational information about the WebEx Social Call Plug-in in tools such as FireBug.

Q. What is the device configuration file and how do I download it?

A. The device configuration file is an XML file that is downloaded from the Cisco Unified Communications Manager (CUCM) by the Cisco WebEx Social Call Plug-in over TFTP. You can download is for troubleshooting purposes by pointing your browser to this URL: http://<*CUCM_Server*>:{6970|69}/ecp<*user screen name*>.cnf.xml where *CUCM server* is the IP address of FQDN of your CUCM.

Q. What are the dial rules files and how do I download them for troubleshooting purposes?

A. The Cisco WebEx Social Call Plug-in downloads two additional files from the CUCM server that contain dialing rules. These are:

- AppDialRules—Contains the rules that the plug-in applies to any phone number before making a call so that the outgoing call could have a correct and complete phone number. You can download the file for troubleshooting purposes by going to this URL: http://<*CUCM_Server*>:6970/CUPC/AppDialRules.xml

  Example:

```
<DialRule BeginsWith="408902" NumDigits="10" DigitsToRemove="2" PrefixWith=""/>
<DialRule BeginsWith="1408902" NumDigits="11" DigitsToRemove="3" PrefixWith=""/>
<DialRule BeginsWith="408525" NumDigits="10" DigitsToRemove="3" PrefixWith="8"/>
<DialRule BeginsWith="408526" NumDigits="10" DigitsToRemove="3" PrefixWith="8"/>
```

- DirLookupDialRules—Contains rules that are applied to a number in case of directory look-ups such as reverse look ups during an incoming call. You can download the file for troubleshooting purposes by going to this URL: http://<*CUCM_Server*>:6970/CUPC/DirLookupDialRules.xml

  Example:

```
<DialRule BeginsWith="22101" NumDigits="10" DigitsToRemove="1" PrefixWith="2"/>
<DialRule BeginsWith="902" NumDigits="7" DigitsToRemove="0" PrefixWith="+1408"/>
<DialRule BeginsWith="8256" NumDigits="8" DigitsToRemove="1" PrefixWith="+1206"/>
<DialRule BeginsWith="8525" NumDigits="8" DigitsToRemove="1" PrefixWith="+1408"/>
```

Q. How do I remove a whitelisted domain (user selected "Always Allow" in the Cisco Call Plug-in security dialog box.)

A. The preference to always allow a domain is stored on the user computer. To remove a whitelisted domain:

- On Windows—Delete the registry entry for the domain at HKCU\Software\Cisco Systems, Inc.\Web Communicator\AlwaysAllow*domain.name*

  Where *domain.name* is the name of the whitelisted domain.

- On Mac OS X—Delete the entry for the domain associated with com.cisco.CiscoWebCommunicator from the Mac OS X user defaults system.

Video Calls Troubleshooting

This section provides the following troubleshooting information:

Symptom I choose to send my video but the remote device does not display it.

Possible Cause A network/Internet security software on your computer is blocking the outbound connection.

Recommended Action The security software may or may not notify you of blocked connections. In both cases the solution is to whitelist the WebEx Social Call Plug-in in your security software.

Symptom Video originating from WebEx Social does not utilize the entire screen on some hardware communication devices.

Possible Cause The device does not have RTCP enabled. RTCP allows devices connected to CUCM to negotiate the best possible video resolution between endpoints. The option is enabled on the WebEx Social Call Plug-in by default.

Recommended Action In your Cisco Unified Communications Manager, ensure RTC is enabled for any devices that receives video from WebEx Social.

Symptom Error appears when the WebEx Social Call Plug-in is trying to load: “The Call Plug-in loaded successfully but there was a problem registering your phone.”

Possible Cause Another device of the same type (Client Services Framework/ECP) has already registered onto the Cisco Unified Communications Manager (CUCM).

Recommended Action To see if another device has registered, go to the CUCM > Device > Phone and search for ECP<*username*> where <*username*> is the screen name of the user.

The IP Address column shows the IP address from which the ECP device is currently registered. If the Status column displays “Unregistered”, IP Address is the last address that have been registered with that device. If the status is Registered or the IP Address does not correspond to the last location from where you used your Cisco WebEx phone, then some other application is using the ECP device. Unregister the device and reload the Cisco WebEx Social Call Plug-in before retrying a call.

Symptom Call cannot be placed with the Cisco WebEx Social Call Plug-in.

Possible Cause The Cisco WebEx Social Call Plug-in cannot download the device configuration file from the CUCM. The Call Plug-in reports the following:

```
0x107dd0000] csf.ecc: libXML2 msg: "Namespace prefix xsi for type on device is not
defined"
22-Jun-2012 16:12:55,207 -0700 ERROR [0x107dd0000] csf.ecc: insecureRetrieveConfig()
file tftp://example.com/ecpapkshirs.cnf.xml requires security
22-Jun-2012 16:12:55,207 -0700 ERROR [0x107dd0000] csf.ecc.api: fetchDeviceConfig()
could not obtain config for ecpapkshirs
```

```
22-Jun-2012 16:12:55,207 -0700 INFO  [0x107dd0000] csf.ecc.api:
getLastTFTPServerUsed() =
22-Jun-2012 16:12:55,207 -0700 INFO  [0x107dd0000] csf.ecc.api:
getLastCCMCIPServerUsed() =
22-Jun-2012 16:12:55,207 -0700 INFO  [0x107dd0000] csf.ecc.api: connect(eSoftPhone,
ecpapkshirs, )
22-Jun-2012 16:12:55,207 -0700 ERROR [0x107dd0000] csf.ecc: doConnect() failed - No
local IP address set! : eNoLocalIpConfigured
```

The Call Plug-in only supports unsecured devices. If the CUCM device is configured otherwise, this may prevent the Call Plug-in from downloading the device configuration file.

Recommended Action Check if there is network connectivity between the Call Plug-in and the CUCM. Also check if the device configuration file contains this line: <capfAuthMode>0</capfAuthMode>. If the value is different than 0, then the device in CUCM has been set up as secured, which is not supported by the Call Plug-in. To remedy this, change Device > Phone > *<username>* > Certification Authority Proxy Function (CAPF) Information > Certificate Operation to No Pending Operation.

Search FAQs and Troubleshooting

Search Troubleshooting

This section provides the following troubleshooting information:

Symptom When I do a global or local search I get the “Internal Server 500” error.

Possible Cause The service is not operational.

Recommended Action Check if the master Search Store, all slave Search Store nodes and the Index Store (if enabled) are operational. These are actions you can take:

On Search Store nodes, run this command as admin:

sudo service search status

On the Index Store node, run this command as admin:

sudo service searchcache status

Check if Solr administration console on each of the above nodes is accessible—see Accessing the Search Store Administration Console, page 2-9, and Accessing the Index Store Administration Console, page 2-9.

Possible Cause Misconfiguration.

Recommended Action Check if the master Search Store, all slave Search Store nodes and the Index Store (if enabled) are properly configured in portal-ext.properties on the App Server. These parameters must be set in accordance with your specific deployment:

solr.masters

solr.slave.region.1 (and other slaves if solr.slave.regions > 1)

search.cache.url

search.cache.post.url

search.cache.video.url

search.cache.social.url

search.cache.follower.url

Possible Cause Not enough disk space.

Recommended Action Take these steps:

Step 1 First check if this is indeed the cause:

- If the disk space on the node is getting low, you must have received an alert about this on the Health page of the Director.
- You can also check manually. To do that, run this command on each Search Store machine (see Running Linux Commands on Nodes, page 2-2):

  df -h

  In the output, find the line that has "/" in the "Mounted on" column. A volume that is out of disk space will show 100% in the "Use%" column.

Step 2 Stop Search:

service search stop

Step 3 Clean up disk space.

Step 4 Restart Search:

service search start

Possible Cause Server errors (500 Internal Server Error).

Recommended Action If you are getting "500 Internal Server Error" in the logs (the App Server logs, the master/slave Search Store logs, or the Index Store request logs) instead of 200 status codes for each request, then the machine may be out of disk space or the indexes may be corrupt.

If the machine is out of disk space, see the "Out of disk space" Possible Cause above.

Otherwise the indexes may be corrupt. Take these corrective steps:

Step 1 First verify that the indexes are indeed corrupted. Check solr-out.log in solr\bin\logs. Indexes are most probably corrupt if the log file contains either of the following:

- "lucene" error messages
- Non-200 statuses of HTTP requests

- Lock-related error messages such as “org.apache.solr.common.SolrException: Lock obtain timed out: SimpleFSLock”

Another symptom is to see a core or more missing in the Index Store administrator portal. There should be a total of 5 cores linked as “Admin post”, “Admin video”, “Admin social”, “Admin follower”, and “Admin autocomplete”. If any of those cores is missing, chances are that it is corrupt and you should see 404 error messages in the Index Store logs for the missing core.

Step 2 After you have identified the machine that stores the corrupt indexes, log in to it as admin and stop solr:

- For Search Store machines:

  sudo service search stop

- For Index Store machines:

  sudo service searchcache stop

Step 3 Delete data directories for all cores. See Checking Where solr Indexes Reside, page 2-3 to understand how to identify the data directories.

Step 4 Restart solr:

- For Search Store machines, run this command as admin:

  sudo service search start

- For Index Store machines, run this command as admin:

  sudo service searchcache start

Symptom When I open My Library I get the “An unexpected error occurred” message.

Possible Cause For possible causes and recommended actions, see Symptom When I do a global or local search I get the “Internal Server 500” error., page 1-16 and take all steps related to Index Store.

Symptom The My View page is not displayed correctly/Search does not give results/The POST document in the Search administration console is missing.

Possible Cause All these symptoms appear when the Index Store has run out of disk space.

Recommended Action To resolve the issue, take these steps:

Step 1 Follow the instructions in your ESXi documentation to increase the disk size of the Index Store virtual machine.

Step 2 After increasing the disk size, log in to the Index Store node as admin and then select **Drop to Shell**.

Step 3 Delete the contents of /opt/cisco/searchcache/multicore/post/data/index/:

rm /opt/cisco/searchcache/multicore/post/data/index/*

Step 4 Do full search reindexing:

a. Sign in to an App Server node as an administrator.

b. Click the down-arrow to the right of your name in the Global Navigation bar.

c. Select **Account Settings** from the drop-down menu.

d. Go to **Serve** > **Server Administration** > **Resources**.

e. Click the **Use Faster Multi-threaded approach** box next to Reindex all search indexes.

f. Click the **Execute** button that appears next to the **Reindex all search indexes** action.

Health and Performance Monitoring FAQs and Troubleshooting

Health and Performance Monitoring Troubleshooting

This section provides the following troubleshooting information:

Symptom I restarted monit but monitoring does not seem to be working for that node.

Possible Cause The initialization of monit has not completed.

Recommended Action Wait for the initialization delay of monit (about 2 minutes).

Symptom I do not receive health data for a node.

Possible Cause If a node is marked as “Disabled” in the Topology page on the Director, monit does not perform checks on that node.

Recommended Action Enable the node.

Symptom This error appears for some nodes “CRITICAL: STATUS integrity: status failed (1) for /var/monit/check_integrity.sh”

Possible Cause This error is known to sometimes appear on new deployments on the Director’s Health page. It may appear multiple times for multiple hosts and is caused by a pair of missing directories (/misc and /net), part of the autofs package, as evidenced by these log messages in the messages log:

```
Mar 21 12:49:26 ce2app1 integrity.sh: S.5....T.
/opt/cisco/quad_synthetic/MonitorTest.py
Mar 21 12:49:26 ce2app1 integrity.sh: missing     /misc
Mar 21 12:49:26 ce2app1 integrity.sh: missing     /net
Mar 21 12:49:26 ce2app1 integrity.sh: (FAIL) 69.52s Verifying RPM packages -> 3
package verification errors
Mar 21 12:49:26 ce2app1 integrity.sh: Total time elapsed: 82.72s
Mar 21 12:49:26 ce2app1 integrity.sh: Total Tests Performed: 18
Mar 21 12:49:26 ce2app1 integrity.sh: Tests Passed: 17
Mar 21 12:49:26 ce2app1 integrity.sh: Tests Failed: 1
```

```
Mar 21 12:49:26 ce2app1 integrity.sh: Compliance Rating: 94%
```

Recommended Action Reinstall the autofs package on the affected nodes. Take these steps:

Step 1 Find the affected nodes' hostnames by looking at the Health page and taking note of the Host column of each occurrence of the error.

Step 2 Log in to each of the affected nodes using user admin and execute this command:

sudo yum reinstall autofs

Step 3 On each of the affected nodes, manually run the integrity script to verify that the error does not appear anymore:

sudo /var/monit/check_integrity.sh

Logs FAQs and Troubleshooting

Logs FAQs

Q. How do I access Cisco WebEx Social logs?

A. All logs are accessible through HTTP from the Director. Visit this URL to see them:

http://<*director*>/logs

Where <director> is the URL you use to access the Director web UI.

Use user admin and your unified access password to log in.

Alternatively, if you need to perform advanced actions with logs such as tracing logs in real time, log in to the Director node, go to /opt/logs and then enter the directory for the date you need.

Q. What is security logging?

A. Starting from this release, security and auditing logs (new for 3.0 and later releases) have been grouped into high level security categories and consolidated into one audit.log per App Server node. In addition, the log message format has been improved to make it easier to process and aggregate.

Note, however, that you can enable debugging in the App Server logs to cause the same logging to show in the normal App Server application logs.

Q. What message categories are defined in the security and auditing log?

A. The following categories are defined:

- security.auth—Authentication events related to signing in, signing out, and so on.
- security.authentication—Authentication events related to signing in, signing out, and so on.
- security.authorization—Authorization events, such as creating a Post, sharing a Post with a user, editing a Post, and so on.
- security.admin—Changes to administrative screens, such as those on the control panel, as well as configuration changes to control panels of applications (for example: External Document Repository, Community Calendar, and so on).
- security.threat—Log messages from AntiSamy (post security HTML sanitizer), CSRF mismatch token violations, and so on.
- security.policy—Reserved for future use.

Q. What is the message format used in the security and auditing log?

A. The basic security event logging format is shown below. Some of the fields may be empty if they are not applicable to that event.

Date/time Date and time the message was logged.

Host Originating host.

Process Name: quad

Log Level: Is always INFO.

Category: What type of security event this is. See Q. What message categories are defined in the security and auditing log?

Thread Name: What thread within Tomcat did the event originate in.

Principal: User account this message pertains to.

Source: Where the message comes from, for example the IP address of the system performing the action.

Component: What area is affected.

Action: What type of action is taking place on the resource.

Resource: What is being affected (for example: Post, Message Boards).

Status: Success or Failure.

Reason: Additional information.

Q. I see a particular log for one day, but not another. Why is this?

A. Log files does not get created unless that log was written to.

Q. I want to check a log file for a past date but the directory for that date seems to have disappeared.

A. To prevent the disk space from filling up, the oldest log directories are deleted when the /opt partition on the Director exceeds 85% disk usage.

Q. I see log files dating back six months or more. Are they not taking free disk space?

A. To prevent the disk space from filling up, the oldest log directories are deleted when the /opt partition on the Director exceeds 85% disk usage. Logs are not deleted before that, regardless of their age.

Logs Troubleshooting

Symptom I used “Apply All“ or “Reset All” to modify the log trace levels of all App Server and Worker nodes but the changes does not seem to propagate to all nodes of those types.

Possible Cause Possible reasons include:

- The RabbitMQ service is down or not accessible from the App Server node.
- The Oracle database is locked or not accessible
- portal-log4j.xml or portal-log4j-ext.xml is corrupted

Director FAQs and Troubleshooting

Director FAQs

Q. Enable/Disable buttons are missing for some roles on the Topology page.

A. Starting from release 3.0, you do not have the option to Enable/Disable most roles. Only the App Server, Worker, and Cache roles have Enable/Disable buttons.

Q. What is Certificate Management?

A. Certificate Management is a feature of the Director UI whose main function is to help streamline the management and deployment of various certificates and keys used throughout Cisco WebEx Social from one centralized UI. Additionally, because the uploaded keystores/certificates are persisted as part of the Director DB, they are preserved during backup and restores.

In the current version the following functional areas are managed by Certificate Management:

- WebEx Meetings SSO keystore management
- WebEx Instant Messaging keystore management
- Certificate Authority/Trust Certificate management, including LDAPS (LDAP over SSL), Visual Voicemail (replaces the existing Visual Voicemail keystore UI), OpenSocial, Show and Share integration (when connecting over SSL), and SharePoint integration (when connecting over SSL).

Director Troubleshooting

This section provides the following troubleshooting information:

Symptom I have uploaded a new security certificate using Application > Security but it does not seem to be taking effect.

Possible Cause Puppet did not restart the nodes that the certificates were pushed to.

Recommended Action Manually restart all App Server and Worker nodes.

You can also check if the certificate files have been copied correctly to their respective locations, as follows:

- On the Director, the keystore/truststore certificates are staged in the /opt/cisco/software/puppet/data/static/local directory with these filenames:

  Cisco WebEx Meetings keystore: webex-sso.jks

  CIsco WebEx IM keystore: webex-im-sso.jks

  Truststore: cacerts

- On App Server nodes, the locations are as follows:

  Cisco WebEx Meetings keystore: /opt/cisco/pki/webex-sso.jks

  Cisco WebEx IM keystore: /opt/cisco/pki/webex-im-sso.jks

  Truststore: /usr/java/latest/lib/security/cacerts

Symptom After adding a node to the Topology page and deploying that node the node displays ERROR under Version Info ("Last config update: ERROR").

Possible Cause The last Puppet run has failed.

Recommended Action Log in to the node in question as admin and run the following command before you refresh the note statuses by clicking Refresh All on the Topology page:

sudo service puppet debug

If this command doesn't bring the status to normal, try the remaining Recommended Actions.

Possible Cause There is a significant time difference between the Director's clock and other nodes' clocks.

Recommended Action Synchronize the clocks on all nodes (preferably to a central NTP server). Do the following:

- If you have an NTP server and would like to synchronize date and time to it, configure the NTP server IP address using the Director UI. See the *Cisco WebEx Social Administration Guide* for details. If you have done that and the clocks are not yet synchronized, the reason might be that the time difference was too great for NTP to equalize which will be reflected in the logs in the following fashion:

```
Aug 21 13:49:31 ds-director ntpd[17795]: time correction of 25374 seconds exceeds
sanity limit (1000); set clock manually to the correct UTC time.
```

To correct significant time differences, set the clocks manually using the date command (see next bullet).

- If you don't want to use an NTP server, set the clocks manually using the date command. Take these steps:

Step 1 Log in as admin to the node whose clock you want to set.

Step 2 Run **date** to check the current time. This command will print both the date and the time.

Step 3 After you have verified that the clock is indeed ahead or behind, run this command to set it:

sudo date -s "*DD MMM YYYY HH:MM:SS*"

where *DD MMM YYYY HH:MM:SS* is the date followed by the time in 24-hour format. FOr example if you want to set the clock to Apr 19th 2012, 11:14:00 pm, type "19 APR 2012 11:14:00"

Or if you need to only set the time:

sudo date +%T -s "*HH:MM:SS*"

where *HH:MM:SS* is the time in 24-hour format.

After you have synchronized the clocks on all nodes, run sudo service puppet debug on all nodes that are showing ERROR on the Topology page.

Possible Cause There is a certificate mismatch between the node and the Director.

Recommended Action Take these steps to resolve the mismatch:

Step 1 Run these commands on the Director node (see Running Linux Commands on Nodes, page 2-2).

salt-key -d <*node FQDN*>; service salt-master restart

puppetca --clean <*node FQDN*>; service puppetmaster restart

where <*node FQDN*> is the fully qualified domain name of the new node.

Step 2 Run these commands on the new node (see Running Linux Commands on Nodes, page 2-2).

rm -rf /etc/salt/pki/* ; service salt-minion restart

rm -rf /var/lib/puppet/ssl/* ; service puppet restart

Step 3 Run this command on the Director node to verify that the connection can be made:

salt '<*node FQDN*>' cmd.run 'echo -n $(cat /opt/cisco/version.info)'

where <*node FQDN*> is the fully qualified domain name of the new node.

Step 4 Verify the output. The expected outpus will be similar to this:

quad.ecp-deploy.com: 3.4.0.09000.739,2013-06-06 11:57 UTC,OK

Worker FAQs and Troubleshooting

Worker FAQs

Q. What tasks are processed by the Worker role?

A. In the current release the following features leverage the worker framework.

- Email digest generation
- Outbound and inbound email processing
- Metrics and reports generation
- Activity feed processing
- Data migration

Message Queue FAQs and Troubleshooting

Message Queue Troubleshooting

This section provides the following troubleshooting information:

Symptom Executing “service rabbitmq-server stop” doesn't seem to stop RabbitMQ.

Possible Cause The described case is a known defect.

Recommended Action Try executing **sudo killall -u rabbitmq** as admin.

Symptom I removed a node from a cluster and now rabbitmq is not functioning correctly.

Possible Cause The described case is a known defect.

Recommended Action As admin, stop rabbitmq on the remaining cluster nodes, then execute "**rm -rf /opt/cisco/rabbitmq/data**" and finally restart rabbitmq on all nodes.

Symptom RabbitMQ fails to start and shows this error "ERROR: failed to load application amqp_client: {"no such file or directory","amqp_client.app"}"

Possible Cause A RabbitMQ plug-in has frozen.

Recommended Action Run the following commands as admin to reset the amqp_client plug-in:

sudo rabbitmq-plugins disable rabbitmq_management

sudo service rabbitmq-server stop

sudo service rabbitmq-server start

sudo rabbitmq-plugins enable rabbitmq_management

Symptom On a fresh install, RabbitMQ fails to start with the following error the RabbitMQ logs: "Can't set short node name!\nPlease check your configuration\n"

Full log message:

```
/var/log/rabbitmq/startup_log
Activating RabbitMQ plugins ...
0 plugins activated:

{error_logger,{{2012,12,1},{0,56,34}},"Can't set short node name!\nPlease check your
configuration\n",[]}
{error_logger,{{2012,12,1},{0,56,34}},crash_report,[[{initial_call,{net_kernel,init,['Argu
ment__1']}},{pid,<0.20.0>},{registered_name,[]},{error_info,{exit,{error,badarg},[{gen_ser
ver,init_it,6},{proc_lib,init_p_do_apply,3}]}},{ancestors,[net_sup,kernel_sup,<0.10.0>]},{
messages,[]},{links,[<0.17.0>]},{dictionary,[{longnames,false}]},{trap_exit,true},{status,
running},{heap_size,377},{stack_size,24},{reductions,180}],[]]}
```

Possible Cause The RabbitMQ rpm package was upgraded and RabbitMQ was stopped or restarted before puppet could replace the configuration.

Recommended Action Log in to the Message Queue node and then run the following commands as user admin:

sudo sed -i 's/sname/name/g' /usr/lib/rabbitmq/lib/*/sbin/*

sudo service puppet debug

This should start RabbitMQ without errors.

Symptom Both ActiveMQ nodes appear to be running as Master.

Possible Cause After NFS issues, the file locking required for the Master/Slave mechanism to function may not work properly, resulting in both ActiveMQ nodes running as Master at the same time. To be sure that you are experiencing this scenario, run the following command on both AMQ nodes:

netstat -an | grep 8161

You should see one of the nodes have output like this:

```
tcp        0      0 :::8161                     :::*                        LISTEN
```

If you see this on both nodes, you are running into this scenario.

Recommended Action Take this steps:

Step 1 Ensure that access to NFS is restored and NFS is healthy.

Step 2 Stop both ActiveMQ services:

a. Log in to one of the ActiveMQ nodes and run:

sudo service monit stop

sudo service puppet stop

sudo service activemq stop

b. Log in to the other ActiveMQ node and run:

sudo service monit stop

sudo service puppet stop

sudo service activemq stop

Step 3 Having stopped both ActiveMQ services, log in to any ActiveMQ node and ensure that you do not see the following file: /mnt/auto/jms/data/kahadb/lock

- If you do not see the lock file, proceed to the next step.
- If you see the lock file, verify that ActiveMQ is truly stopped by taking these steps on each ActiveMQ node:

a. Run **ps -ef | grep activemq**

b. Take note of the PID (5441 in the example below):

```
activemq  5441     1  0 Nov30 ?        00:00:15
/opt/cisco/activemq/bin/linux-x86-64/wrapper
/opt/cisco/activemq/bin/linux-x86-64/wrapper.conf wrapper.syslog.ident=ActiveMQ
wrapper.pidfile=/opt/cisco/activemq/bin/linux-x86-64/./ActiveMQ.pid
wrapper.daemonize=TRUE wrapper.lockfile=/var/lock/subsys/ActiveMQ
...

...
org.tanukisoftware.wrapper.WrapperSimpleApp org.apache.activemq.console.Main start
root     26063 10937  0 00:25 pts/0    00:00:00 grep activemq
```

c. Run **sudo kill *PID*** where PID is the number you took note of in the previous step.

d. Run **ps -ef | grep activemq** again. The output should be similar to the following:

root 26063 10937 0 00:25 pts/0 00:00:00 grep activemq

Step 4 Start ActiveMQ on just one of the nodes by running the following command on that node:

sudo service activemq start

Step 5 Wait 2-5 minutes, then rerun the netstat command:

netstat -an | grep 8161

- If you see the same output as above, continue with the next step.

```
tcp        0      0 :::8161                     :::*                        LISTEN
```

- If not, then periodically check if the ActiveMQ process has started by running: **ps -ef | grep activemq**

  The expected output should be similar to the following:

```
activemq  5441     1  0 Nov30 ?        00:00:15
/opt/cisco/activemq/bin/linux-x86-64/wrapper
/opt/cisco/activemq/bin/linux-x86-64/wrapper.conf wrapper.syslog.ident=ActiveMQ
wrapper.pidfile=/opt/cisco/activemq/bin/linux-x86-64/./ActiveMQ.pid
wrapper.daemonize=TRUE wrapper.lockfile=/var/lock/subsys/ActiveMQ
activemq  5443  5441  0 Nov30 ?        00:29:01 java -Dactivemq.home=../..
-Dactivemq.base=../.. -Djavax.net.ssl.keyStorePassword=password
-Djavax.net.ssl.trustStorePassword=password
-Djavax.net.ssl.keyStore=../../conf/broker.ks
-Djavax.net.ssl.trustStore=../../conf/broker.ts -Dcom.sun.management.jmxremote
-Dorg.apache.activemq.UseDedicatedTaskRunner=true
-Dderby.storage.fileSyncTransactionLog=true -Dcom.sun.management.jmxremote.port=8002
-Dcom.sun.management.jmxremote.authenticate=false
-Dcom.sun.management.jmxremote.ssl=false -Dcom.cisco.ecp.Role=Messaging
-XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=/opt/cisco/activemq
-XX:ErrorFile=/opt/cisco/activemq/diagnostic-info.quadjms-crash.txt
-XX:OnOutOfMemoryError=../../bin/quadjms_diagnostics.sh
-XX:OnError=../../bin/quadjms_diagnostics.sh -Xms128m -Xmx4096m
-Djava.library.path=../../bin/linux-x86-64/ -classpath
../../bin/wrapper.jar:../../bin/run.jar -Dwrapper.key=apcwlYMEtZ4ACu7S
-Dwrapper.port=32000 -Dwrapper.jvm.port.min=31000 -Dwrapper.jvm.port.max=31999
-Dwrapper.pid=5441 -Dwrapper.version=3.2.3 -Dwrapper.native_library=wrapper
-Dwrapper.service=TRUE -Dwrapper.cpu.timeout=10 -Dwrapper.jvmid=1
org.tanukisoftware.wrapper.WrapperSimpleApp org.apache.activemq.console.Main start
root     26063 10937  0 00:25 pts/0    00:00:00 grep activemq
```

Step 6 After you see the above output from netstat, go to the other ActiveMQ node and start ActiveMQ:

sudo service activemq start

Step 7 Wait 2-5 minutes, then rerun the netstat command:

netstat -an | grep 8161

You should not get a return from this command. If you do, then you have run back into the issue again and you need to troubleshoot NFS to find the root cause.

Step 8 Run the following commands on both ActiveMQ nodes to restart the services stopped at the beginning of this procedure:

sudo service monit start

sudo service puppet start

My Library FAQs and Troubleshooting

My Library Troubleshooting

This section provides the following troubleshooting information:

- Symptom The My Library page does not seem to be responding to user actions: dialogs are not opening up, the Delete button does nothing, and so on.

Symptom The My Library page does not seem to be responding to user actions: dialogs are not opening up, the Delete button does nothing, and so on.

Possible Cause A Javascript error has occurred on the page. Possible Javascript errors include:

- File not found/loaded. This type of error is displayed in red color and contains the missing file name.
- Inline Javascript failure. This error occurs if Javascript code inside a .jsp file has failed and any processing of the rest of the code in the .jsp file has been halted. Example follows:

```
$LAB.wait() error caught:
SyntaxError: missing ; before statement
```

Recommended Action Try reloading the page; if the problem persists, try loading the page with another web browser.

Streams FAQs and Troubleshooting

Streams Troubleshooting

This section provides the following troubleshooting information:

- Symptom Connection Manager crashes with an out of memory exception.

Symptom Connection Manager crashes with an out of memory exception.

Possible Cause Increase the maximum memory allocated for JVM.

UC Integrations FAQs and Troubleshooting

UC Integrations Troubleshooting

This section provides the following troubleshooting information:

- Symptom These errors appear when the user tries to switch the Cisco Call Plug-in from computer audio to desktop phone mode: [cwic] eUnknownFailure, [cwic] Login Error, and [cwic] unregisterPhone

Symptom These errors appear when the user tries to switch the Cisco Call Plug-in from computer audio to desktop phone mode: [cwic] eUnknownFailure, [cwic] Login Error, and [cwic] unregisterPhone

Possible Cause The list of Unified Communications Manager (UCM) servers contains an IP address that does not correspond to a UCM server.

Recommended Action Sign in to Cisco WebEx Social as Administrator, go to Account Settings > Server > Common Configurations > WebDialer, find the offending entry in the list of Registered UCM Clusters and correct or remove it. Use the Cisco Call Plug-in log on the user computer to identify the offending UCM entry.

OpenSocial FAQs and Troubleshooting

OpenSocial FAQs

Q. Are external OAuth applications supported?

A. No. OAuth applications that fetch data from external service providers (such as Twitter, Google, and Yahoo) are not yet supported.

OpenSocial Troubleshooting

This section provides the following troubleshooting information:

Symptom When adding a OpenSocial application, the application title is displayed but the application content is not visible.

Possible Cause Unknown.

Recommended Action Refresh the browser window and the contents should appear.

Synthetic Monitoring FAQs and Troubleshooting

Synthetic Monitoring Troubleshooting

This section provides the following troubleshooting information:

Symptom Posts created manually using the ciscosyntheticmonitoruser are not removed.

Possible Cause The Cisco WebEx Social indexes were not updated properly.

Recommended Action Sign in to Cisco WebEx Social using the ciscosyntheticmonitoruser user, go to My Library and delete the posts manually.

Symptom Synthetic monitoring reports “Search Created Post Not Found” or similar search related failure.

Possible Cause The value of the batch.manager.fetch.interval.secs advanced portal property exceeds 600 (10 min).

Recommended Action Lower the value of batch.manager.fetch.interval.secs to below 600. The recommended value is 300 (5 min).

Possible Cause An App Server node is running LDAP synchronization with a large LDAP database. In this case you see a corresponding alarm in the Director's Health page.

Recommended Action Wait for a few hours and the error should stop appearing. If it does not, then there is probably a different possible cause.

Symptom “Invalid authentication” error appears in the App Server log and the Director’s Health page.

Possible Cause It is possible that on very busy systems the API calls used by Synthetic Monitor can expire leading to an error message in the logs. This can also leave behind Synthetic Monitor posts.

Recommended Action The error is not critical. If it keeps reappearing frequently, contact your Cisco representative. Synthetic Monitor posts that are left behind will be deleted after 24 hours.

Using Jabber with Cisco WebEx Social FAQs and Troubleshooting

Using Jabber with Cisco WebEx Social FAQs

Q. What do I need to know before I start troubleshooting Using Jabber with Cisco WebEx Social?

A. Have the following in mind:

- All Cisco WebEx Social does is call URLs for user-initiated outgoing chat and phone requests; the rest is handled by Cisco Jabber
- Incoming chat and call request are handled entirely by Cisco Jabber
- If the outgoing request reaches Cisco Jabber but it can't process it, the issue may be among the following:
  - The XMPP userID is invalid
  - The phone number is not routable in the CUCM dial plan

  In either case, the issue will need to be investigated between Cisco Jabber and the chat or unified communications server.
- To replicate an issue, type the URL that was used into a new browser tab and observe the outcome:
  - Use a tool like Firebug to find the URL (example: xmpp:user@example.com)
  - If Cisco Jabber doesn't launch, there is likely an issue with the default programs configuration in the OS
  - If the correct URL is being sent but another application launches instead of Cisco Jabber, check if your default programs configuration

Using Sametime with Cisco WebEx Social FAQs and Troubleshooting

Using Sametime with Cisco WebEx Social FAQs

Q. Why does the Sametime Connect chat window sometimes appear behind the browser window?

A. This may happen when you initiate chat with a user who is in Offline or Do Not Disturb state. In this case the operating system may randomly send the desktop dialog box that opens to behind the browser window, leading the user to the impression that their action was of no effect.

Using Sametime with Cisco WebEx Social Troubleshooting

This section provides the following troubleshooting information:

Symptom Sametime Connect does not launch when invoked from Cisco WebEx Social if the latter uses HTTPS.

Possible Cause This may happen when your organization uses HTTPS to access Cisco WebEx Social because the local Sametime service only supports HTTP and your users' web browsers may block outgoing HTTP requests as a security measure.

Recommended Action To allow Cisco WebEx Social to launch Sametime you need to instruct your users to enable Mixed Content. Enabling mixed content varies from browser to browser. Consult your web browser's documentation or search the internet for detailed steps.

Possible Cause Another possible reason is that the local Sametime service is not running.

Recommended Action To check if this is indeed the case, point your web browser to http://localhost:59449/stwebapi/listservices and check the result:

- If you see the Sametime Local WebApi Services List populated with services, then the local Sametime service is running
- If you see a blank page or an HTTP error, then the service is not running or is blocked by a firewall or another security application.

After you have determined the result, take the appropriate action to start the service (see the Sametime documentation) or to unblock the service in your security software.

SSL Termination FAQs and Troubleshooting

SSL Termination FAQs

Q. How do I check if an App Server node is SSL/HTTS enabled?

A. The simplest way to see if an App Server node has the certificate is simply to open the Cisco WebEx Social sign-in page. Major web browsers display a padlock icon in the Address bar if the connection is SSL-encrypted. By clicking the padlock icon you can view details about the system's certificate.

Q. Where is the security certificate located?

A. The SSL/HTTPS certificate and private key are uploaded using the Director which pushes them to the following locations on your App Server nodes:

- SSL/HTTPS Certificate: /etc/pki/tls/certs/localhost.crt
- SSL/HTTPS Private key: /etc/pki/tls/private/localhost.key

SSL Termination Troubleshooting

This section provides the following troubleshooting information:

- Symptom SSL sessions cannot be open to one or more App Server nodes.

Symptom SSL sessions cannot be open to one or more App Server nodes.

Possible Cause The SSL termination settings on the Director (Application > Security > Cluster Security) are not applied to all App Server nodes.

Recommended Action Log in to each App Server node as admin and run this command:

sudo service puppet debug

Running this command normally corrects the problem. If it does not, it outputs information that can help you understand the reason for the failure.

Possible Cause The security certificates you uploaded using the Director (Application > Security > HTTPS/SSL) were not propagated to all App Server nodes or the quad service was not restarted.

Recommended Action Log in to each App Server node as admin and run this command:

sudo service puppet debug

If this does not help, manually restart the quad service on each App Server node. Run this command:

sudo service quad restart

Chat FAQs and Troubleshooting

- Chat Troubleshooting, page 1-34

Chat Troubleshooting

This section provides the following troubleshooting information:

- Symptom A user cannot change their availability using Cisco Jabber after setting it in Cisco WebEx Social.

Symptom A user cannot change their availability using Cisco Jabber after setting it in Cisco WebEx Social.

Possible Cause This may happen when the WebEx IM option has been selected as Chat server and the session priority in the Cisco WebEx Social chat server settings has been set higher than or equal to Cisco Jabber's default session priority value (127 as of this writing).

Recommended Action As administrator, go to **Account Settings > Server > Common Configurations > Chat** and lower **Session Priority** to below 127.

Centralized Credentials Management (Master Account) FAQs and Troubleshooting

Centralized Credentials Management (Master Account) Troubleshooting

This section provides the following troubleshooting information:

Symptom Master Account does not accept valid usernames and passwords.

Possible Cause LDAP authentication is set to use email addresses as usernames. The Master Account feature only supports screen name as username.

Recommended Action Sign in to Cisco WebEx Social as Administrator, select **Account Settings** from your profile menu, go to Portal > Settings > Authentication > General > How do users authenticate? and change the setting to “By screen name“.

Session Centralization FAQs and Troubleshooting

Session Centralization FAQs

Q. How do I check on which memcached node a user session is stored?

A. Complete these steps:

Step 1 Using the user’s browser, find the cookie named JSESSIONID tied to your Cisco WebEx Social site name and look at its content which contains a SessionID.

Step 2 In the SessionID, find the memcached server ID. The SessionID format is as follows:

<alphanumeric number>-<**memcached server id**>.<cisco webex social node>jvm

where memcached server id is n1, n2, and so on.

Step 3 Go to a App Server node and open Tomcat's configuration file /opt/cisco/quad/tomcat/conf/Catalina/localhost/ROOT.xml.

Step 4 Search for MemcachedBackupSessionManager to find the session centralization configuration section.

Step 5 In this section, find the memcachedNodes parameter.

Step 6 Use the memcachedNodes parameter to identify the IP address or hostname of the memcached server id you found earlier (n1, n2, and so on).

Step 7 Telnet to the identified host on port 11211.

telnet <*memcached server host*> 11211

Step 8 You see a blank prompt. Type this command:

get <*session id*>

where *session id* is the value of the JSESSIONID cookie.

Step 9 Examine the output:

- If you get encoded data back from this command, this means that the session is stored on this memcached.
- If you simply get END returned instead, that means that the session is not stored on memcached at all.

Step 10 Type **quit** to exit the telnet session to memcached.

Q. How do I find the current session count from memcached?

A. Complete these steps:

Step 1 Find the user ID by signing in as the user and going to Account Settings. The very first number on the details page is the user ID (15379119 for example).

Step 2 Sign in to the Director user interface and go to the System > Topology page.

Step 3 Find the hostnames of all Cache nodes.

Step 4 Telnet to each Cache node:

telnet <*memcached server host*> 11211

Step 5 In each telnet session run this command:

get <user id>

where *user id* is the user ID that you identified earlier.

Step 6 Examine the output:

- If you see an output, it contans a comma-separated list of all the session IDs created by the user. Count them up to find the current session count.
- If you don't get an output, try with he next Cache node.

Step 7 To close the telnet session, type **quit**.

Q. How do I reset the session count?

A. In rare cases such as when the user computer crashes the session count in memcached may not be properly cleaned up preventing the user from signing in to Cisco WebEx Social. To reset a user's session count to allow them to sign in, complete these steps:

Step 1 Find the user ID by signing in as the user and going to Account Settings. The very first number on the details page is the user ID (15379119 for example).

Step 2 Follow the steps in Q. How do I check on which memcached node a user session is stored? to find out which memcached node stored the user sessions.

Step 3 Telnet to the memcached node that you identified in the previous step:

telnet <*memcached server host*> 11211

Step 4 In the telnet session run this command:

delete <user id>

where *user id* is the user ID that you identified earlier.

Step 5 To close the telnet session, type **quit**.