



Logs

This chapter provides information about log file names and locations as well as other log-related information.

This chapter is organized as follows:

- [Logs Overview, page 4-1](#)
- [Log Categories to Set when Troubleshooting, page 4-1](#)
- [Log Files Stored on the Director by Role, page 4-7](#)
- [Locally-stored Log Files by Role, page 4-10](#)

Logs Overview

Most Cisco WebEx Social logs are centralized on the Director node. There are a few exceptions (log files with dynamic name patterns and non-critical logs) where log files are managed locally on nodes instead of streaming to the Director node.

Cisco WebEx Social uses rsyslog as a logging framework. rsyslog sends critical logs to the Director node but, if configured, can also stream logs to an upstream host (see the *Cisco WebEx Social Administration Guide* for details).

The central log location on the Director node is `/opt/logs/<date>/` where *date* is the date that the log message was written. For example `/opt/logs/2012_12_01/` would contain all log messages generated on Dec 1 2012.

The logs on the Director can be accessed through the Director GUI (see the *Cisco WebEx Social Administration Guide* for details) or through the Cisco WebEx Social Director API.

Log Categories to Set when Troubleshooting

When troubleshooting, you often need to increase the verbosity of a log category. In many cases the name of the log category is similar to the feature that you are troubleshooting but for some features you need to set multiple log categories or log categories that are not obvious. This section provides the feature to log category relations along with additional information that you may need when reading logs.

After looking up the category to set, use the steps in [Setting Log Trace Levels, page 2-2](#) to actually set it.

Log Categories to Set when Troubleshooting

Category	Node Types	Trace Group(s)	Trace Levels	Log Files to Collect	Keywords	Comments
Email Integration						
Inbound Email	App Server and Worker	Inbound Email	ERROR for normal operation DEBUG to gather detailed information	Worker Node: - Worker - postfix App Server: - App Server	App Server: - [mail.jms.InboundJmsListenerContainer] - [MimeMessageCollectorImpl*] - [mail.processor.MailProcessorImpl] - [processor.action.PostMailAction] - [ecp.inbound.HookFactory] - [ParentMessageIdentifierImpl:*] - [MailProcessorImpl:*] Worker: - mail.mda.MailHandler* - ecp.inbound.HookFactory*	In additional you may want to enable DEBUG level for the QUAD_EVENTING category on Worker nodes.
Outbound Email	App Server and Worker	Outbound Email	ERROR for normal operation DEBUG to gather detailed information.	Worker Node: - Worker - postfix App Server: - App Server	- [InstantListener:*] - [MailTransport:*] - [TemplateEngineImpl:*] - [SMTPHeadersInstantUtil:*] - [MailSender:*] - [DigestListener:*] - [QuadHighlightsContext:*] - [VelocityEngine:*] - [context.mail.PostCommentContext]	
Digest Scheduler (Weekly and Daily Digest Emails)	App Server and Worker	If no emails are sent to anyone: QUAD_EVENTING on App Server and Worker If specific Digest emails are not sent: Outbound Email on Worker	ERROR for normal operation DEBUG to gather detailed information.	Worker Node: - Worker - postfix App Server: - App Server	Suspected eventing issues (should be rare): [QUAD_EVENTING] Suspected issues with creating or sending emails - [InstantListener:*] - [MailTransport:*] - [TemplateEngineImpl:*] - [SMTPHeadersInstantUtil:*] - [MailSender:*] - [DigestListener:*] - [QuadHighlightsContext:*] - [VelocityEngine:*] - [context.mail.PostCommentContext] - [DigestListener:*]	
Postfix	Worker	N/A	N/A	Worker Node: - postfix	-	See Q. How do I set the log trace levels for Postfix? , page 1-5
Alerts and Announcements	App Server and Worker	Digest Scheduler Outbound Email	ERROR for normal operation DEBUG to gather detailed information.	Worker Node: - Worker - postfix App Server: - App Server	Suspected eventing issues (should be rare): [QUAD_EVENTING] Suspected issues with creating or sending emails: - [InstantListener:*] - [MailTransport:*] - [TemplateEngineImpl:*] - [SMTPHeadersInstantUtil:*] - [MailSender:*] - [DigestListener:*] - [QuadHighlightsContext:*] - [VelocityEngine:*] - [context.mail.PostCommentContext] - [DigestListener:*]	Set Outbound Email and Digest Scheduler. If you suspect an issue between Postfix and the SMTP server Postfix is talking to, see Postfix.

WebEx Social for Office/Cisco Social for Office

Category	Node Types	Trace Group(s)	Trace Levels	Log Files to Collect	Keywords	Comments
Mail and Office Plugin	-	-	-	-	-	See Open API
WebEx Social for Notes						
MSI Installer	User computer	-	For installation problems only, run the installer with option DEBUGRCP="true"	User computer: - MSI logs: C:\Users\ <user name>\appdata\local\temp\msi<number>.log<br=""></user> - Notes provisioning logs: C:\Windows\Temp\com.cisco.webxsocial.plugin.notes\NotesProvisioning.log - Notes installation logs: C:\Users\ <user>\appdata\local\lotus\notes\data\workspace\logs\< td=""> <td></td> <td>To enable general Windows Installer logging, create the following registry keys: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer\Reg_SZ: Logging Value: voicewarmupx Reg_DWORD: Debug Value: 7 Enable Group Policy logging by editing the appropriate OU or Directory Group Policy. Under Group Policy, expand Computer Configuration, expand Administrative Templates, expand Windows Components, and then select Windows Installer. Double-click Logging and then click Enabled. In the Logging box, enter the options you want to log. The log file, Msi.log, appears in the Temp folder of the system volume.</td> </user>\appdata\local\lotus\notes\data\workspace\logs\<>		To enable general Windows Installer logging, create the following registry keys: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer\Reg_SZ: Logging Value: voicewarmupx Reg_DWORD: Debug Value: 7 Enable Group Policy logging by editing the appropriate OU or Directory Group Policy. Under Group Policy, expand Computer Configuration, expand Administrative Templates, expand Windows Components, and then select Windows Installer. Double-click Logging and then click Enabled. In the Logging box, enter the options you want to log. The log file, Msi.log, appears in the Temp folder of the system volume.
Calendar Integration						
Calendar (Exchange or Notes, not Community Calendar)	App Server	Calendar (Rarely) httpclient_wire (only if you need to see the HTTP(S) requests sent and received)	ERROR for normal operation TRACE for most situations, especially if you want to see the responses from the different servers (httpclient_wire set to DEBUG will also get you the full HTML payload sent/received) INFO to track cache misses (This level should be relatively safe to use for long periods of time.) DEBUG to track all calls to the cache. Avoid using this level for long periods on production environments.	App Server	AGGREGATED_CALENDAR	
Health and Performance Monitoring						
See Analytics	-	-	-	-	-	-
Centralized log trace level setting						

Log Categories to Set when Troubleshooting

Category	Node Types	Trace Group(s)	Trace Levels	Log Files to Collect	Keywords	Comments
Portlets, Webex Social Eventing	App Server, Worker	Memcached Session Manager	INFO or DEBUG	<appserverhostname>_appserver.log <workerhostname>_worker.log <MQhostname>_message-queue.log on Message Queue	-	
Analytics						
Analytics	App Server, Worker	For metrics report generation: ANALYTICS on Worker, only For verifying events are triggered and sent: QUAD_EVENTING on App Server and Worker	ERROR for normal operation DEBUG to get more information.	*_worker.log *_appserver.log (if troubleshooting eventing, only)	For metrics report generation: - [ANALYTICS_MR_SCHEDULER] For verifying events are triggered and sent: - [QUAD_EVENTING]	Be sure to restart the Worker nodes for the log level to go into effect on that role. To log events such as sending or receiving to/from Message Queue, also set the QUAD_EVENT category to DEBUG.
Framework						
Portal UI Framework	App Server	Portal UI Framework	ERROR for normal operation DEBUG to get more information.	App Server	[ecp.bigpipe.BigPipeUtil]	Only needed if pages render incorrectly (e.g.: pieces missing, parts of the UI do not work). If you have issues viewing a particular Post, use "Post Application" debugging, instead.
Streams						

Category	Node Types	Trace Group(s)	Trace Levels	Log Files to Collect	Keywords	Comments
SocialActivity Application, Notification, QUAD_EVENTING	App Server	Issues with Streams Portlet in Streams Portlet: SocialActivity Application Issues with individual items missing from Streams Portlet: QUAD_EVENTING Streams Portlet not dynamically refreshing: Notification	ERROR for normal operation DEBUG to get more information	All: - App Server Dynamic Refresh not working: - App Server - cmanager (on App Server) - *_notifier_*.log	Issues with Streams Portlet in Streams Portlet: [socialActivities] Issues with individual items missing from Streams Portlet: - [QUAD_EVENTING] - Exceptions, such as: <ul style="list-style-type: none"> ▪ NoSuchPostException ▪ NoSuchPostVersionException ▪ Permissions-related exceptions Issues with dynamic refresh: - App Server: <ul style="list-style-type: none"> ▪ [subscription.util.NotificationsUserUtil]: Routing/gathering notification messages/data for a given user ▪ [util.packet.OutgoingPacketListener]: Sending new/updated Notification data from App Server to Notifier ▪ [xmpp.util.NotificationRouter]: Routing/gathering notification messages/data ▪ [service.impl.NotificationsFeedListenerLocalServiceImpl]: Notification data from Notifier to App Server ▪ [util.packet.IncomingPacketListener]: Notification data from Notifier to App Server ▪ [service.impl.NotificationsManagerLocalServiceImpl]: Processing of Notifications - cmanager: Look for errors with connections or authentication - notifier_*.log: Look for errors, especially those related to authentication and issues finding notification data (AKA: nodes)	SocialActivity Application—For general logging. Set ERROR for normal operation and DEBUG to get more information. Note that leaving the DEBUG level on significantly affects the performance of the system. Notification—If you want to check logs for dynamic (XMPP) updates. Set ERROR for normal operation and DEBUG to get more information. Note that leaving the DEBUG level on significantly affects the performance of the system. QUAD_EVENTING—If you still need further information (because activity creation depends on rabbitmq events). Note that turning this category to DEBUG will log every event that is occurring in WebEx Social.
Open API						
Open API	App Server	OpenAPI	ERROR for normal operation INFO to get more information.	App Server	[common.logging.QuadLoggingJerseyFilter]	Output will print out entire request and response payloads, including OAuth headers, parameters, etc. Essentially like a "sniffer" for all OpenAPI calls.
Unified Communication						

Log Categories to Set when Troubleshooting

Category	Node Types	Trace Group(s)	Trace Levels	Log Files to Collect	Keywords	Comments
Jabber Desktop Client integration	N/A	N/A	N/A	N/A	N/A	<p>Integration with Jabber for Click-to-Call or IM is simply making a call to a "tel:" or "xmpp:" URL, respectively.</p> <p>To debug, simply copy the phone number or IM user ID exactly as it is seen in the target user's profile page. Then paste that into the appropriate URL.</p> <p>Examples: tel:+14085551212</p> <p>xmpp:someone@company.com</p> <p>This should crosslaunch the Jabber client and automatically place the call or open a chat window, depending on the URL entered.</p>
CUPS Integration	App Server	Click 2 Call	<p>ERROR for normal operation</p> <p>DEBUG to get more information</p>	App Server	AXL	<p>Because most of the time the communication happens directly between the browser and CUPS, there is not much to debug on the server side.</p> <p>The server is responsible only for finding out to which node in the CUPS cluster the user belongs. The information is then passed to the browser when it makes a particular json_service call.</p>
WebEx Connect Integration (either presence in WebEx Social UI or click-to-chat in WebEx Social UI)	Client PC App Server (if SSO is used for WebEx Connect)	<p>Client PC: - HAR export (via Firebug or Chrome Developer tools)</p> <p>App Server (if SSO login issues): - WebEx Interface - In some cases, httpclient_wire</p>	<p>Client PC: N/A</p> <p>App Server: - ERROR for normal operation - DEBUG to get more information (but do not keep httpclient_wire on when not troubleshooting)</p>	<p>Client PC: HAR export</p> <p>App Server: appserver.log</p>	<p>Client PC: URLs with "/chat-proxy" in them</p> <p>App Server (needed for SSO, only): - [webapp.tool.SAML2Util] - [WebExComponent] - [xmlapi.core.XMLAPIClient]</p>	
Webdialer Integration	App Server	Click 2 Call Interface	<p>ERROR for normal operation</p> <p>DEBUG to get more information</p>	appserver.log	[uc.webdialer.*]: For issues with placing calls [webdialer_phone_preference_jsp]: For issues with the "Phone Preferences" Control Panel	
WebEx Meetings Integration	App Server	<p>App Server: - WebEx Interface</p> <p>- In some cases, httpclient_wire if you need to see the full SAML or XML request/response</p>	<p>ERROR for normal operation</p> <p>DEBUG to get more information (but do not keep httpclient_wire on when not troubleshooting)</p>	appserver.log	[webapp.tool.SAML2Util] [WebExComponent] [xmlapi.core.XMLAPIClient]	

Category	Node Types	Trace Group(s)	Trace Levels	Log Files to Collect	Keywords	Comments
Microsoft OCS Integration	App Server, Client PC (via Firebug/Dev Tools)	WebEx Social Services	ERROR for normal operation DEBUG to get more information	appserver.log, Firebug, Dev Tools, etc.	-	
Centralized Credentials Management (Master Account)						
Master Account	Worker	Master Account	ERROR for normal operation DEBUG to gather detailed information.	appserver.log	[service.impl.PaPassLocalServiceImpl] [service.impl.MongoDBLock] [service.impl.PortletConfiguration]	
Session Centralization						
Memcached Session Manager	App Server	Caching Services	INFO for normal operation DEBUG to gather detailed information (Warning: generates large volumes of messages).	appserver.log		In addition, if you are experiencing connectivity-type issues between the App Servers and memcached servers, set the Caching Services category on one or more App Server nodes as follows: INFO for normal operation. DEBUG to gather detailed information (Warning: generates large volumes of messages).
Search						
Search	App Server Worker	Search SOLR Search monitoring (Only if you suspect a search query is malformed)	Search: INFO for normal operation; Rarely DEBUG may be needed SOLR Search Monitoring: DEBUG to gather detailed information	App Server: quad_appserver.log Worker: worker_worker.log Search: search.log /opt/cisco/search/logs	[SOLR_DEBUG:65] [QuadPostEntitySelectorImpl:60] [SimpleAsyncTaskExecutor-N] [IndexerListener:78] [LuceneIndexer:134] [FullPartialAsyncIndexerImpl:167]	

Log Files Stored on the Director by Role

This sections lists the log files that each role sends to the Director.

Table 4-1 Log Files Stored on the Director

Role	Log filename
Director	%HOSTNAME%_director_web.log %HOSTNAME%_catalina.log %HOSTNAME%_localhost.log %HOSTNAME%_manager.log %HOSTNAME%_host_manager.log %HOSTNAME%_deploy_db.log %HOSTNAME%_graphite_access.log %HOSTNAME%_graphite_exception.log %HOSTNAME%_graphite_info.log %HOSTNAME%_graphite_error.log %HOSTNAME%_carbon_console.log %HOSTNAME%_salt_master.log %HOSTNAME%_mongod.log %HOSTNAME%_jsonstore.log %HOSTNAME%_analyticsstore.log
App Server	%HOSTNAME%_appserver.log %HOSTNAME%_analyticsmrscheduler.log %HOSTNAME%_catalina.log %HOSTNAME%_localhost.log %HOSTNAME%_tomcat-access.log %HOSTNAME%_manager.log %HOSTNAME%_host_manager.log %HOSTNAME%_httpd_access.log %HOSTNAME%_httpd_error.log %HOSTNAME%_cmanager.log %HOSTNAME%_cmanager_debug.log %HOSTNAME%_cmanager_info.log %HOSTNAME%_cmanager_warn.log %HOSTNAME%_cmanager_error.log %HOSTNAME%_deploy_db.log %HOSTNAME%_audit.log
Worker	%HOSTNAME%_worker.log %HOSTNAME%_catalina.log %HOSTNAME%_localhost.log %HOSTNAME%_manager.log %HOSTNAME%_host_manager.log %HOSTNAME%_httpd_access.log %HOSTNAME%_httpd_error.log %HOSTNAME%_cmanager.log %HOSTNAME%_cmanager_debug.log %HOSTNAME%_cmanager_info.log %HOSTNAME%_cmanager_warn.log %HOSTNAME%_cmanager_error.log

Table 4-1 Log Files Stored on the Director (continued)

Role	Log filename
Message Queue	%HOSTNAME%_message-queue_wrapper.log %HOSTNAME%_message-queue.log %HOSTNAME%_message-queue_shutdown_err %HOSTNAME%_message-queue_startup_err %HOSTNAME%_message-queue_shutdown.log %HOSTNAME%_message-queue_startup.log %HOSTNAME%_rabbitmq.log %HOSTNAME%_rabbitmq-sasl.log
Notifier	%HOSTNAME%_notifier.log %HOSTNAME%_notifier_nohup.out %HOSTNAME%_notifier_debug.log %HOSTNAME%_notifier_info.log %HOSTNAME%_notifier_warn.log %HOSTNAME%_notifier_error.log
Cache	%HOSTNAME%_messages
Search Store	%HOSTNAME%_search.log %HOSTNAME%_search.request.log
Index Store	%HOSTNAME%_index.log %HOSTNAME%_index.request.log
Analytics Store	%HOSTNAME%_mongod.log
JSON Store	%HOSTNAME%_mongod.log

Table 4-1 Log Files Stored on the Director (continued)

Role	Log filename
RDBMS Store	%HOSTNAME%_oracle_quad_log.xml %HOSTNAME%_oracle_alert_quad.log %HOSTNAME%_oracle_rdfprod_log.xml %HOSTNAME%_oracle_alert_rdfprod.log %HOSTNAME%_oracle_sqlnet.log
Common logs (all roles)	%HOSTNAME%_secure %HOSTNAME%_mail_log %HOSTNAME%_cron %HOSTNAME%_spooler %HOSTNAME%_boot.log %HOSTNAME%_collectd.log %HOSTNAME%_monit.log %HOSTNAME%_puppet.log %HOSTNAME%_messages %HOSTNAME%_nagios.log %HOSTNAME%_faillog %HOSTNAME%_lastlog %HOSTNAME%_snmpd.log %HOSTNAME%_yum.log %HOSTNAME%_tallylog %HOSTNAME%_vmware_tools_guestd %HOSTNAME%_wtmp %HOSTNAME%_audit_local_log %HOSTNAME%_mail_statistics %HOSTNAME%_pm-suspend.log %HOSTNAME%_prelink.log %HOSTNAME%_mod-jk.log %HOSTNAME%_rewrite.log %HOSTNAME%_ssl_access_log %HOSTNAME%_ssl_request_log %HOSTNAME%_ssl_error_log %HOSTNAME%_install.log %HOSTNAME%_install.log.syslog %HOSTNAME%_salt_minion.log

Locally-stored Log Files by Role

This sections lists the log files that some roles store locally.

Table 4-2 *Locally-stored Log Files*

Role	Log filename
RDBMS Store	/opt/oracle/app/oracle/diag/rdbms/[quad, rdfprod]/[quad, rdfprod]/cdump/* /opt/oracle/app/oracle/admin/[quad, rdfprod]/adump/* /opt/oracle/app/oracle/diag/tnslsnr*/listener/alert/log.xml /opt/oracle/app/oracle/diag/tnslsnr*/listener/trace/listener.log /opt/oracle/app/oracle/diag/rdbms/[quad, rdfprod]/[quad, rdfprod]/trace/*.trc, *.trm
Common logs (all roles)	/var/log/sa/sa* /var/log/httpd/[ssl*log] /var/log/anaconda.* /var/log/btmp /var/log/dmesg /var/log/dracut.log

