Cisco Unified Workforce Optimization

Workforce Management Troubleshooting Guide Release 10.5

First Published: June 18, 2014

Last Updated: June 18, 2014

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Workforce Management Troubleshooting Guide

Contents

Introduction

This document provides basic troubleshooting information for Cisco Workforce Management (WFM).

The troubleshooting information in this document includes:

- How to locate each service's configuration, log, and debug files.
- How to implement logging, which you can use to monitor your Workforce Management environment and troubleshoot issues.
- How to recognize and resolve some of the most common error conditions.

Technical Information

WFM Components

A WFM system contains the following components:

Installation	Components
Capture Services	WFM Capture service
Compile Services	WFM Compile service
iCalendar Services	WFM iCalendar service
Process Services	WFM Forecast service WFM Request service WFM Schedule service
Transaction Services	WFM RTE service WFM Adherence Conformance Calculator (ACC) service WFM Jetty service WFM Mana service WFM Product Adapter service WFM Sync service

See the *Workforce Management Installation Guide* for information on configuration, hardware, and third-party software requirements.

Service Failure Effects

The following table describes the primary symptoms that appear when a WFM service fails to start.

Note: The effects listed do not identify what happens when a service crashes.

Service failure effects

Service	Effect of Failure
ACC service	Historical adherence and conformance data does not appear in reports.
Capture service	Historical data cannot be retrieved from synchronized ACDs and GIS files.
Compile service	Historical data cannot be compiled by day, week, month, or year.
iCalendar service	Schedule data cannot be retrieved.
Request service	Shift budget analysis requests cannot be run.
RTE service	Adherence module cannot receive agent state changes.
Schedule service	Schedule requests cannot be run.
Sync service	Agent, team, and queue information is not automatically synchronized with the Unified CCE or Unified CCX ACD.
Jetty service	Users are unable to log in to WFM.
Product Adapter service	Data is not rendered to Unified Workforce Optimization.
Mana service	Failure notifications are not received.

Capacity and Performance

Product Limitations

There is no solution-level, automated failover or autorecovery for the WFM database. It is recommended that you back up the WFM database daily using the SQL Server backup utility.

Failover

WFM automatically connects to a secondary database when the primary ACD (if the secondary ACD exists).

Failover in non- environments is handled at the ACD's end. Since in these environments, ACD information is sent to WFM as text files at regular intervals, either the primary or secondary ACD can generate those files.

SQL Server Maintenance Recommendations

SQL Server requires regular maintenance to ensure peak performance. You can automate the maintenance task and schedule it for once a week during off-peak hours.

The common database maintenance tasks include:

- Checking data integrity. This task checks the structural integrity of the data and verifies the database is not corrupt.
- Reorganizing/rebuilding indexes. This task defragments the database indexes. Index fragmentation can cause performance issues. Indexes should be rebuilt using the Offline option in a non-Enterprise version of SQL Server.
- Updating statistics. This task performs sampling of the data in the database to optimize tables and indexes so they can be used more efficiently, thus increasing performance for the distribution of data in the tables.

- Backing up and managing log files. Regular database and transaction log backups are recommended along with truncating/shrinking the transaction logs to free up disk space and gain efficiency.

Backing Up and Restoring the WFM Database

This section describes how to back up and restore the WFM database using Microsoft SQL Server management tools.

Note: WFM supports the backup and restore only of the current version, not from one version to the next.

Note: If Cisco Security Agent (CSA) is running on your WFM server, shut CSA down before you back up the WFM database. The backup might fail if CSA is running while you use the SQL Server backup utilities.

Use the Backup and Restore features available in the Microsoft SQL Server Management Studio to back up and restore WFM databases.

Note: After you back up the WFM database, it is advisable to copy the backup files to another location for safekeeping.

Backing Up the WFM Database

Follow these steps to back up the WFM database.

To back up the WFM database:

1. On the server that hosts the WFM database, launch and log in to Microsoft SQL Server Management Studio.
2. Right-click the database name (CWFM) under the Databases node. A menu appears.
3. Choose Tasks > Back Up. The Back Update Database window appears.
4. Complete the fields and click OK.

Restoring the WFM Database

Follow these steps to restore the WFM database.

To restore the WFM database:

1. Close Unified Workforce Optimization.
2. In the Windows Services utility, stop all the WFM services.
3. On the server that hosts the WFM database, launch and log in to Microsoft SQL Server Management Studio.
4. Right-click the database name (CWFM) under the Databases node. A menu appears.
5. Choose Tasks > Restore Database. The Restore Database window appears.
6. Complete the fields and click OK.
7. Restart all the WFM services.

Defragmenting the System Hard Disk and the WFM Database

When WFM starts responding slowly and tasks take longer than normal to perform, it is time to defragment the WFM system hard disk and the WFM database.

Defragmenting the WFM Database Server

Use the administrative tools on the database server to defragment the server. Consult the OS documentation for details on defragmenting the disk.

Defragmenting the WFM Database Indexes

The data in the WFM database can often become highly fragmented after prolonged use. Rebuilding the database indexes will reorganize the data into a more efficient structure and can improve the performance of the system.

To defragment the indices of WFM database:

1. Log on to the WFM system as an administrator.
2. On the SQL Server computer, start Microsoft SQL Server Management Studio and log in. The Microsoft SQL Server Management Studio window appears.
3. In the navigation pane under Databases, right-click CWFM and select Reports > Standard Reports from the menu.
4. The Index Physical Statistics report will tell you which indexes need to be rebuilt or reorganized. Consult the SQL Server Management Studio documentation for instructions on how to do this.
5. You can also run a query to find out how much each index is fragmented and use that as a guide for rebuilding/reorganizing indexes. The query is as follows:

```
SELECT so.name as TableName, si.name As IndexName,
        si.type_desc, index_depth, index_level,
        avg_fragmentation_in_percent, fragment_count,
        avg_fragment_size_in_pages, page_count,
        avg_page_space_used_in_percent
FROM sys.dm_db_index_physical_stats(DB_ID(), NULL, NULL, NULL, 'LIMITED')
As phystat
JOIN sys.objects so ON phystat.object_id = so.object_id
JOIN sys.indexes si ON so.object_id = si.object_id
        AND phystat.index_id = si.index_id
WHERE so.type = 'U'
ORDER BY avg_fragmentation_in_percent desc, TableName, IndexName
```

The fragmentation should ideally be 0 for all tables. High levels of fragmentation will cause an extreme amount of delay when data from the table is requested. Another key indicator for WFM performance is the fragmentation level plus the page count. A table can have significant fragmentation, but if it has a low page count, then the effects of fragmentation might or might not be noticed.

Logs and Debugging

Applications and services use logging to report status and problems. Each application and service creates two files:

- **Log files** (files with the LOG file extension) contain status messages and, if problems occur, warning and other error messages. All messages in log files are identified by an error code. See for more information on error codes.
- **Debugging files** (files with the DBG file extension) are empty when debugging is not enabled. When debugging is enabled (the default setting), the files contain diagnostic information that can help resolve issues.

Log and debugging files are located in the …\CalabrioCisco\WFO_WFM\log folder on the client or server computer.

By default, logging is enabled.

The default configuration settings limit each log and debugging file to a maximum of 10 MB and 20 rolling files for WFM services and 5 MB and 5 rolling files for applications.

> **Example:** When a service's log or debug file reaches 20 MB, it is closed and renamed, and a new file is started.

Files with the CFG extension produce logs using this numbering scheme:

<name>0001.log is created and filled.
<name>0002.log is created when the first file is full.
<name>0001.log is cleared and reused when the second file is full.
<name>0002.log is cleared and reused when the third file is full.
And so on.

Files with the PROPERTIES extension produce logs using this numbering scheme:

<name>.log is always the file currently being filled.
<name>.log.1 is the most recent filled file.

Debugging logs follow these same numbering schemes, but use the DBG file extension instead of the LOG file extension.

Log Message Formats

The following are the formats used by the various log and debug file messages and an example of that format.

C++ and Java LOG File Messages

Format: `<timestamp> <level> <error code> <error text>`

Example: `2008-02-10 12:44:17,703 INFO WMPI0000 Starting WFM Post Install`

C++ DBG File Messages

Format: `<timestamp> [<thread ID>] <level> <text>`

Example: `2008-02-12 10:10:21:015 DEBUG [0xfac] corbaInitialize:: Server port is <59011>`

Java DBG File Messages

Format: `<timestamp> <level> [<thread name>] <class:line> <text>`

Example: `2007-04-07 15:40:31.954 STACK [Th2] Init#:run:113 ClaimException…`

Java (log4j) LOG File messages

Format: `<timestamp> [<thread name>] <level> [LINE-<number>] [<class:method>] <text>`

Example: `2007-04-07 14:54:00,067 [Th2] INFO [LINE-1534] [Init:un] Started.`

Configuration Files

Each application and service has an associated configuration file that controls logging and debugging (among other things). These files can be edited in a text editor to change the logging and debugging parameters.

Configuration files are located in the …\Cisco\WFO_WFM\config folder on the client or server computer.

Caution: Edit configuration files only as described in this section. Improper changes can result in logging and/or program failure, including the possible loss of data. You might want to make a safety backup of any file you edit before you make changes to it.

The WFM configuration and log files are described in the following table.

WFM configuration and log files

Application or Service	Configuration File	Log/Debug File
GIS Connector Tool	…\config\P$CAPTURE.CAL	
WFM ACC service	…\config\wfm_acc_ logger.properties	…\log\WFM_ACCXXXX. …\log\WFM_ACCXXXX.dbg
WFM Capture service	…\config\wfmCapture.properties	…\log\wfmCaptureXXXX.dbg …\log\wfmCaptureXXXX. These files include product, version, and build information in the header.
WFM Compile service	…\config\wfm_compile_ logger.properties	…\log\WFM_CompileXXXX.dbg …\log\WFM_CompileXXXX.

Application or Service	Configuration File	Log/Debug File
WFM Configuration Setup	…\config\postinstall.properties	…\log\postinstall. …\log\postinstall.dbg
WFM Forecast service	…\config\wfmforecast.properties	…\log\WFMForecastXXXX.dbg …\log\WFMForecastXXXX. These files include product, version, and build information in the header.
WFM iCalendar service	…\config\C1Calendar.properties	...\log\C1CalendarXXXX.
WFM Jetty service	…\config\jetty.properties	…\log\jetty.dbg …\log\jetty-request-YYYY_MM_DD.log
	…\config\C1Surrogate.properties	…\log\C1SurrogateXXXX.dbg …\log\C1SurrogateXXXX.
WFM Mana service	…\config\manaservice.properties	…\log\manaXXXX. …\log\manaXXXX.dbg
WFM Product Adapter service	…\config\wfmadapter.properties …\config\wfm.properties	…\log\wfmadapterXXXX.dbg …\log\wfmadapterXXXX. These files include product, version, and build information in the header.
WFM Request service	…\config\wfm_request_logger.properties	…\log\WFM_RequestXXXX.dbg …\log\WFM_RequestXXXX.

Application or Service	Configuration File	Log/Debug File
WFM RTE service	…\config\service4j-wfmrte.cfg	…\log\service4j-wfmrteXXXX.log …\log\service4j-wfmrteXXXX.dbg
	…\config\wfmrte.properties	…\log\wfmrteXXXX. …\log\wfmrteXXXX.dbg
WFM Sync service	…\config\SyncServer.cfg	SyncServerXXXX.log

Enabling Debugging

By default, debugging is enabled. When debugging is enabled, keep in mind that the more detail the debugging threshold provides, the slower the performance of your PC and the bigger the size of the debug file. High debugging thresholds might also affect the performance of other applications running on your PC.

There are four types of configuration files. Each type of file uses a different syntax to enable debugging. The procedures below describe the steps that must be followed for each type of file.

Important: Disable debugging when it is no longer needed.

The available debugging thresholds are displayed in the following table.

Note: Not all thresholds can be used in all configuration files. See the procedures below for which thresholds can be used in particular files.

Threshold	Description
Info	Tracks significant events during the normal life cycle of the application. Information messages are not errors and require no corrective action. This information can be useful when troubleshooting. It also canbe used as historical status information.
Debug	Usually sufficient for diagnosing a problem. Will not affect system performance.
Call	Tracks function entry and exit.
Trace	Provides alarge amount of diagnostic information. May affect system performance.
Stack	Provides only stack traces, which give more debugging information when errors and warnings occur.
Dump	PRovides a very large amount of detailed diagnostic information. Likely to affect system performance.
Off	Turns off debugging.

Enabling Debugging in Files with a CFG Extension

1. In a text editor, open the desired configuration file.
2. Under the section headed [Debug Log], set the debugging threshold to DEBUG, CALL, TRACE, or DUMP.

   Example: `Threshold=DEBUG`

   The threshold value must be all caps and there should be no spaces on either side of the equal sign (=).

   The line might already exist or you might have to add a new line.
3. Save the configuration file.

   The change takes effect immediately. You do not have to restart the application or service.

Enabling Debugging in Files with a PROPERTIES Extension

1. In a text editor, open the desired configuration file.
2. Locate the line that starts with:

   `log4j.rootLogger=<threshold>#com.calabrio …`
3. Replace <threshold> with DEBUG, TRACE, STACK, or DUMP.
4. Locate the line that starts with:

   `log4j.appender.DBG.Threshold=<threshold>#com.calabrio …`
5. Replace <threshold> with the same value you used in Step 2.
6. Save the configuration file.

   The change takes effect according to the splk4j.watch.check setting (by default, within 90 seconds). You do not have to restart the application or service.

Enabling Debugging in log4j Files

1. In a text editor, open the desired configuration file.
2. Locate the line that starts with:

   `log4j.rootLogger=<threshold>`
3. Replace <threshold> with DEBUG or TRACE.
4. Save the configuration file.

   Restart the application or service for the new setting to go into effect.

Enabling Debugging in CAL Files

1. In a text editor, open the desired configuration file.
2. Ensure that the following lines are set as follows:

   LogMessage=ON
   DebugMessages=DEBUG

   The available debug levels are OFF, DEBUG, CAL, TRACE, and DUMP.
3. Save the configuration file.
4. Restart the application or service for the new setting to go into effect.

Disabling Debugging

It is important to disable debugging when it is no longer needed for diagnostic purposes. Debugging can affect the performance of your PC if it is left enabled.

Disabling Debugging in Files with a CFG Extension

1. In a text editor, open the desired configuration file.
2. Under the section headed [Debug Log], set the debugging threshold to OFF.

   Example: `Threshold=OFF`

   The threshold value must be all caps and there should be no spaces on either side of the equal sign (=).
3. Save the configuration file.

   The change takes effect immediately. You do not have to restart the application or service.

Disabling Debugging in Files with a PROPERTIES Extension

1. In a text editor, open the desired configuration file.
2. Locate the line that starts with:

   `log4j.rootLogger=<threshold> …`
3. Replace <threshold> with STACK.
4. Locate the line that starts with:

   `log4j.appender.DBG.Threshold=<threshold> …`
5. Replace <threshold> with OFF.
6. Save the configuration file.

   The change takes effect according to the splk4j.watch.check setting (by default, within 90 seconds). You do not have to restart the application or service.

Disabling Debugging in log4j Files

1. In a text editor, open the desired configuration file.
2. Locate the line that starts with:

   `log4j.rootLogger=<threshold>`
3. Replace <threshold> with OFF.
4. Locate the line that starts with:

   `log4j.appender.DBG.Threshold=<threshold>`
5. Replace <threshold> with OFF.
6. Save the configuration file.

   Restart the application or service for the new setting to go into effect.

Disabling Logging and Debugging in CAL Files

1. In a text editor, open the desired configuration file.
2. Ensure that the following lines are set as follows:

   LogMessage=OFF
   DebugMessages=OFF

   The available debug levels are OFF, DEBUG, CAL, TRACE, and DUMP.
3. Save the configuration file.
4. Restart the application or service for the new setting to go into effect.

Error Messages

See the *Workforce Optimization Error Code Dictionary* for a complete list of error messages, including MANA error messages.

Troubleshooting

Diagnostic Procedures

The following procedures will help you diagnose problems with WFM.

Basic Checks

When WFM is having problems, check the following:

- The components of your WFM system are running. This includes:

ACD	Component
Cisco Unified CCE	Cisco Unified Communication Manager Cisco Unified Intelligent Contact Manager
Cisco Unified CCX	Cisco Unified Communication Manager Cisco Unified Contact Center Express
Avaya AACC	Avaya CCMS
Avaya CMS	Avaya CMS
All	Servers that host the WFM services

- The hard drives of the servers that host the WFM services and the optional offboard SQL Server are not full.
- The registry is correct (see Registry Check)
- The network is set up correctly (see Network Check)
- The SQL Server is set up correctly and running (see SQL Server Check)
- The WFM services are running
- The WFM Configuration Setup utility has run correctly (see the *WFM Installation Guide*)

Blocked Ports Check

To check whether a port is blocked:

1. Ensure that the service is running and active.
2. On the server that hosts the WFM services or any client desktop, open a command window and enter the following command:

   ```
   telnet <service computer host name/IP address> <service computer port>
   ```

   See the *WFM Installation Guide* for a list of the ports used by each WFM service.

   If the telnet operation is successful, the command window will clear. If the telnet operation fails, a connection failure message will appear.
3. Enter the following command to retrieve a list of all processes that are listening for connections and the ports used to listen:

   ```
   netstat -abo
   ```

   If you cannot find the service in the output of this command, then the service is not running, something is preventing the service from listening on the port, or there is something wrong with the service.
4. Check firewall settings on the client and server computers.
5. Check firewall logs.
6. If security software is running on the computer, check its reports and logs to see if it is blocking any communication or ports.

CPU Check

Ensure that the computer's processor is at least the minimum required for WFM and other installed software. If the processor is below the recommended level, it could be the cause of the problem.

Use Task Manager to sort processes and applications by CPU usage. Check which process seems to be using the CPU most of the time.

Use the Microsoft Performance Monitor Wizard (perfmon.exe, available in the Microsoft Download Center) for additional CPU checking.

- Add the %Processor Time counter for Processor > _Total and each CPU as well as Process >_Total and process of interest.
- Check which process seems to be using the CPU most of the time.

If the counter values for a process are a significant part of the total CPU use, it might be of concern. Short spikes are acceptable but a significant time with high CPU usage is of concern.

Try rebooting the computer to see if it fixes the problem.

Keystore Check

- Verify that C:\Program Files (x86)\Common Files\WFM\config\.keystore exists.
- Verify the self-signed WFM certificate.
- Verify the CA-signed WFM certificate.
- Verify the toot and intermediate CA certificates.

Verify the self-signed WFM certificate

In a command window, run the following command:

```
"C:\Program Files (x86)\Calabrio\WFO_WFM\Java\bin\keytool.exe" -
keystore "C:\Program Files (x86)\Common
Files\WFM\config\.keystore" -storepass Sp@nl1nk -list -v
```

The WFM certificate has the Alias name “wfm_webserver”. It should look something like the following, where 10.192.246.12 is the IP address of the WFM Transaction services server:

```
Alias name: wfm_webserver

Creation date: Jan 31, 2014

Entry type: PrivateKeyEntry

Certificate chain length: 1

Certificate[1]:

Owner: C=US, ST=MN, L=Minneapolis, O=Calabrio Inc, OU=Workforce
Management, CN=1

0.192.246.12:443

Issuer: C=US, ST=MN, L=Minneapolis, O=Calabrio Inc, OU=Workforce
Management, CN=

10.192.246.12:443
```

```
Serial number: 2a250ca462

Valid from: Thu Jan 30 07:30:40 CST 2014 until: Tue Jan 30
07:30:40 CST 2114

Certificate fingerprints:

     MD5: 3A:7F:A7:C3:E0:7A:58:1D:3A:44:F4:9F:F0:0A:C4:9E

     SHA1:
     21:58:DF:26:1F:BA:A1:58:A7:A0:85:4D:44:73:B2:54:51:AA:75
     :FF

     SHA256:
     58:27:8C:BA:3D:07:3F:E0:20:F0:23:11:E1:51:7B:6E:20:96:57
     :40:4C:

     D0:F3:CC:5E:76:6E:0B:32:A6:74:4C

     Signature algorithm name: SHA1withRSA

     Version: 1
```

Note that a self-signed WFM certificate will show both the issuer and owner as "C=US, ST=MN, L=Minneapolis, O=Calabrio Inc, OU=Workforce Management, CN=10.192.246.12:443".

Rebuild the WFM Keystore

Use the following steps on the WFM Transaction services server to rebuild the WFM keystore if it becomes corrupted. This procedure assumes you already have CA certificates in the keystore.

1. Using the Windows Services utility in the Control Panel, stop the WFM Jetty service.
2. Enter the following command on the command line:

   ```
   "C:\Program Files (x86)\Calabrio\WFO_
   WFM\Java\bin\keytool.exe" -keystore "C:\Program Files (x86)
   \Common Files\WFM\config\.keystore" -storepass Sp@nl1nk -
   exportcert -rfc -alias rddc01 -file rddc01_root_x509.cer
   ```

   replacing “rddc01” with the CA authority and “rddc01_root_x509.cer” with the name of the output file.
3. Repeat Step 2 for every CA certificate you want to preserve.
4. Delete the WFM keystore located on this path:

```
C:\Program Files (x86)\Common Filese\WFM\config\.keystore
```

5. Run WFM Configuration Setup to completion. This results in the self-signed WFM certificate to be recreated in the WFM keystore.
6. Sign the WFM certificate.

Memory Check

Ensure that the amount of memory on the computer is at least the minimum required for WFM and other installed software. If the amount of memory is below the recommended level, it could be the source of the problem.

Use the Microsoft Performance Monitor Wizard (perfmon.exe, available in the Microsoft Download Center) to perform most memory checking. Add the following counters for _Total and process of interest:

- Private Bytes
- Virtual Bytes
- Handle Count
- Thread Count

If the values for those counters keep growing without leveling out or decreasing, it is likely the process has a memory leak.

If the values for those counters for a process are a significant part of the total memory used, it might be of concern. Note that certain processes will normally use more memory than others.

Try rebooting the computer and see if it fixes the problem. Check how much and how fast processes increase their memory usage.

Network Check

On the servers that host the WFM services, verify that the IP address in the registry value

HKEY_LOCAL_MACHINE\SOFTWARE\Spanlink\WFM\Site Setup\IOR HOSTNAME (32-bit machines)

HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Node\Spanlink\WFM\Site Setup\IOR HOSTNAME (64-bit machines)

is the correct IP address of the public NIC.

To view information about the NICs on the computer:

1. Open a command window and enter ipconfig /all.
2. Verify that the host name and IP address are as expected.
3. Verify that the subnet mask is correct. It is probably 255..255.0.

If there are multiple NICs enabled, verify that the public NIC comes before the private NIC:

1. In the Control Panel, double-click Network and Dial-up Connections.
2. From the menu bar, choose Advanced > Advanced Settings.
3. On the Adapters and Bindings tab, verify that the NICs are in the correct order in the Connections pane.

Check the network connectivity by pinging from the WFM services servers to others in the configuration.

> **Example:** The server that hosts Cisco Unified CM.

Then reverse it by pinging from the other servers to the WFM services server. Do this using both host names and IP addresses and ensure that the ping results match.

If host names are used, verify that the DNS, WINS, and hosts files are correct.

If there is a problem connecting to a particular service, one the server hosting the WFM services or any client machine, try entering telnet <service IP address/host name> <service port> in a command window. (see the *WFM Installation Guide* for a list of the ports used by each WFM service).

Use a network protocol analyzer like Wireshark to analyze network communications.

If security or firewall software is running on the computer, check its reports and logs to see if it is blocking any communication or ports. Exceptions or rules should be configured to allow connections between WFM services and ports.

Verify that dynamic IP is not being used on the WFM services server. Otherwise, the IP address can change and no longer match what is configured in the registry and the WFM database.

For additional information about troubleshooting basic TCP/IP problems, see "How to Troubleshoot Basic TCP/IP Problems" on the Microsoft Support website.

Registry Check

Using Windows Regedit, do the following:

- Verify that HKEY_LOCAL_MACHINE\Software\Spanlink\WFM\Site Setup (for 32-bit machines) or HKEY_LOCAL_MACHINE\Software\Wow6432Node\Spanlink\WFM\Site Setup (for 64-bit machines) exists and contains the correct entries
- Verify that the registry entries used by the WFM ACC, Compile, and Request services exist and are valid as shown in the tables below.

WFM ACC Service Registry Entries

Key	Type	Description
Registry Path (64-bit machine)		HKEY_LOCAL_MACHINE\SOFTWARE\Wow64Node\Spanlink\WFM\ciWfmACC
SplkJSvcJavaRuntimeOptions	string	-Dsplk4j.configuration=config/wfm_acc_logger.properties -Djava.library.path=bin -Xmx256M -Xrs
SplkJSvcJNIClassPath	string	ext\\commons-collections-3.0.jar; ext\\commons-dbcp-1.2.1.jar; ext\\commons-pool-1.2.0.jar; ext\\jtds-1.2.1.jar;ext\\calabrio-time.jar; ext\\jRegistryKey.jar; ext\\log4j.jar;ext\\splkstd4j.jar; ext\\odysoftframework.jar;ext\\odysoftc3core.jar; ext\\wfm-common.jar;ext\\sqljdbc4.jar; lib\\AdherenceProcess.jar;config;.;
SplkJSvcJNIMainClass	string	com/calabrio/wfm/server/process/scheduler/Scheduler

WFM Compile Service Registry Entries

Key	Type	Description
Registry Path (64-bit machine)		HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Spanlink\WFM\ciWfmCompile
SplkJSvcJavaRuntimeOptions	string	-Dsplk4j.configuration=config/wfm_compile_logger.properties -Djava.library.path=bin -Xmx256M -Xrs
SplkJSvcJNIClassPath	string	ext\\commons-logging.jar; ext\\jRegistryKey.jar; ext\\jtds-1.2.1.jar; ext\\log4j.jar; ext\\splkstd4j.jar; lib\\compile.jar;config;.;
SplkJSvcJNIMainClass	string	com/calabrio/wfm/app/compile/Compile

WFM Request Service Registry Entries

Key	Type	Description
Registry Path (64-bit machine)		HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Spanlink\WFM\ciWfmRequest
SplkJSvcJavaRuntimeOptions	string	-Dsplk4j.configuration=config/wfm_request_logger.properties -Djava.library.path=bin -Xmx256M -Xrs

WFM Request Service Registry Entries(cont'd)

Key	Type	Description
SplkJSvcJNIClassPath	string	ext\\commons-logging.jar; ext\\jRegistryKey.jar; ext\\jtds-1.2.1.jar; ext\\log4j.jar; ext\\splkstd4j.jar; ext\\sqljdbc4.jar; ext\\odysoftframework.jar; ext\\odysoftc3core.jar; ext\\wfmservercommon.jar; lib\\request.jar; config;ext\\wfm-common.jar; ext\\calabrio-time.jar;.;
SplkJSvcJNIMainClass	string	com/calabrio/wfm/app/request/RequestService

SQL Server Check

If not using an offboard SQL Server, ensure a supported version of SQL Server is installed on the server that hosts the WFM Transaction services.

If using an offboard SQL Server, ensure that SQL Native Client is installed on all WFM servers where SQL Server is not installed.

If using a historical database (HDS) and an administrative workstation (AW) database, ensure that the SQL Server login has access to both databases.

Ensure the SQL Server login entered in WFM Configuration Setup is configured as follows:

- Uses SQL Server Authentication
- Is assigned the dbcreator and sysadmin server roles
- Does not enforce password policy

Note: If the SQL Server login user name or password is modified after WFM is installed, WFM must be reinstalled.

Make sure that the SQL Server Browser is started:

1. Start the Windows Control Panel Services utility.
2. Verify that SQL Server Browser is started and has a Startup Type of Automatic

Ensure that the SQL instance specified in WFM Configuration Setup is correct:

1. On the computer where SQL Server is installed, start the Windows Control Panel Services utility.
2. The SQL instance name should be inside parentheses after SQL Server.

   Example: `SQL Server (SQLExpress)`

It is possible that the SQL Server is using the default instance. To determine if it is:

1. Start SQL Server Management Studio.
2. In the Login dialog, select SQL Server Authentication in the Authentication field. Enter the IP address of the computer where SQL Server is installed in the Server field.

   If the login is successful, SQL Server is using the default instance.

Ensure that the password entered in WFM Configuration Setup is correct by re-entering it and letting Configuration Setup restart the WFM services.

If using an offboard SQL Server, perform a Network Check to verify that the WFM servers can communicate with the offboard SQL Server.

Run WFM Configuration Setup to apply any necessary DB schema changes. Use the Next button to navigate from step to step instead of using the navigation pane on the left, which can cause you to skip some necessary steps (especially after an upgrade or installing a patch).

Try connecting to the WFM database manually from the same computer as the application using the information specified in WFM Configuration Setup.

Make sure that the SQL Server database is not full and SQL transaction logs have not filled up the hard disk.

Ensure that the SQL Server database is not highly fragmented.

Version Check

DLL and EXE Files

1. Select the DLL or EXE.
2. Right-click and select Properties.

3. On the Details tab, verify that the file version and production version property fields display the expected version.

JAR and WAR Files

1. Open the JAR or WAR using WinZip or 7Zip.
2. Open the META-INF > MANIFEST.MF file in Notepad.
3. Check that the Specification-Version and Implementation-Version fields display the expected version.

LOG and DBG Files

The version information for the JAR, DLL, and EXE used by the application is listed at the top of the application's log and debug files.

Avaya AACC 6 ODBC Connection Check

To check the ODBC connection for Avaya AACC 6:

1. Check that the server with the InterSystems Caché database is reachable from your computer via ping <server IP address>.
2. Make sure that the Caché ODBC driver is installed on the client computer.
3. Make sure that the Caché ODBC driver on the client computer matches the Caché database version on the server.
4. Check that your computer firewall allows connection to the Caché database port (defaults to 1972).
5. Check that your ODBC DSN works:
    a. In the Data Sources (ODBC) Manager > InterSystems Caché ODBC Data Source Setup window, make sure that the IP address, port, Caché Namespace, user name, and password are correct. Note that user IDs of the user type Supervisor will not work.
    b. Click Test Connection to confirm that all parameters are valid. If it fails, the error message displayed is also kept in the CacheODBC.log in C:\Users\Public\Logs.

Note that even if the test passes, it just means that the credentials can log into the Caché database but does not guarantee that the user has access to specific views and tables.

6. Connect using SQuirreL and run SQL queries.

Administration Problems

A user modifies the ID or name of a team

A user modifies the ID or name of a team that is administered in the ACD, and that are synced with WFM. Examples of such ACDs are Cisco Unified Contact Center Enterprise or Unified Contact Center Express.

Restart the Sync service to synchronize the ACD database with the WFM database.

A user mistakenly deletes a service queue or a team

A user mistakenly deletes a service queue or a team that is administered in the ACD, and that are synced with WFM. Examples of such ACDs are Cisco Unified Contact Center Enterprise or Unified Contact Center Express.

Restart the Sync service to synchronize the ACD database with the WFM database.

Pop-up windows do not appear

Popup windows do not appear after clicking their corresponding links in WFM.

Popups are being blocked by your browser. Turn off your browser's popup blocking options.

Credentials are not correct

The following message appears when the user logs into Unified Workforce Optimization.

Credentials are not correct. Try again.

Reenter the login information and try again. If the error persists, contact your administrator. This message might indicate the user is not assigned a role. Assign a role to the user in Workforce Management to resolve this problem.

Stop running this script

When viewing a Planning page, the error message, “Stop running this script” appears.

This problem is due to a Microsoft Internet Explorer issue.

For information on correcting this issue, see Microsoft Support Article ID 175500, available at

http://support.microsoft.com/kb/175500

WFM Capture Service Problems

Note: The problems and solutions listed here apply to all ACDs.

Captured data does not match what is reported on the ACD

ACD data and the corresponding WFM captured data do not match. The contact data reported by WFM is too low.

The Capture service pulls ACD statistics 15 minutes after an interval ends. If the contact center has calls in progress for longer than 15 minutes at this time, then those calls are not included in that data capture.

The capture delay and optional daily recapture of data is configured in WFM Configuration Setup in the ACD Connection step. Set the capture delay to a value greater than the default 15 minutes, and if necessary, enable daily data recapture. See the *WFM Installation Guide* for more information on configuring capture settings.

WFM uninstaller can't stop Capture service

When uninstalling WFM software via the Control Panel Add or Remove Programs utility, the WFM uninstaller can’t stop the Capture service, and eventually times out. The Capture service is left in a stopping state.

Reinstall WFM, manually stop the Capture service, and then use the Add or Remove Programs utility to uninstall WFM.

Unified CCE

The Capture service uses JDBC to connect to the ICM AW database, so standard troubleshooting procedures for network connectivity and JDBC connections can be used.

For general troubleshooting, check the following:

- Verify that the ACD Connection primary and secondary IP addresses in the WFM Configuration Setup utility are correct.
- If using SQL authentication, verify the following:
  - The login credentials are correct
  - The SQL Server you are connecting to has the Server properties > Security > SQL Server and Windows Authentication mode option enabled
  - The login you are using has permission to access the AWDB database
- If using NT authentication, verify that WFM has been configured for NT authentication for Unified CCE (see the *WFM Installation Guide* for instructions)
- Verify network connectivity between the WFM system and the ICM.
- Verify that port 1433 is used to connect to the SQL Server database. Telnet to port 1433 on the ICM AW to rule out firewall issued.

For precision queues, check the following:

- If using ICM 9.0(3), there are some problems:
  - The retention duration for Router_Queue_Interval view is smaller than for Skill_ Group_Interval. This results in a precision queue service level of zero even though there were precision queue calls that were answered.
  - Sometimes the ServiceLevel value in ICM tables is negative. This is converted and treated as zero by the Capture service.
- Sometimes there is a record in SkillGroup_Interval that has no corresponding record in Router_Queue_Interval. This results in a precision queue service level of zero even though there were precision queue calls that were answered. A possible cause for this is that the ICM computer was shut down abruptly.

If the HDS database is more than 80% full, the purge process, rpl, will begin deleting records regardless of the retention duration configured for the tables. This can result in records missing from a table like Router_Queue_Interval while the corresponding record exists in another table such as Skill_Group_Interval.

To verify if this issue exists, enter the following command on a command line on the ICM AW:

```
"C:\icm\wfm18\dis\logfiles\dumplog rpl /bd mm/dd/yyyy /ed
mm/dd/yyyy /o"
```

Substitute an appropriate beginning date for <bd mm/dd/yyyy> and end date for <ed mm/dd/yyyy>.

> **Note**: To get more detailed information, you can modify EMSTraceMask to ffff (defaults to 0) under the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\wfm18\Distributor\EMS\CurrentVersion\Library\Processes\rpl.

The command generates the file rpl.txt and places it in the folder from which you ran the command.

In the text file, look for a line like the following:

23:08:36:491 dis-rpl Trace: 80% of the available free space is used in wfm18_hds database.

If you see this line, you might need to expand the HDS database. See “Expanding an ICM SQL Database” at http://www.cisco.com/c/en/us/support/docs/voice-unified-communications/icm-logger/20493-expand-sql.html.

Problems and Solutions

Agent historical data is not captured: agent not activated

The agent is not activated in WFM.

On the agent and user record in WFM, select the Activate this agent/user check box.

Agent historical data is not captured: wrong skill mapping

The agent is mapped to a different service queue in WFM than is configured in Unified CCE.

Change the WFM agent skill mapping to match what is configured in Unified CCE.

Historical data is not captured

(Applies to WFM 9.2(1) SR3 and newer) In WFM Configuration Setup, on the ACD Connection step, the “Use GIS to capture ACD historical data manually” check box is selected.

If you want WFM to capture data automatically by querying the ACD database, make sure this check box is cleared. Select the check box only if you intend to use GIS to capture historical data.

Historical data in the WFM database does not match the corresponding data in the GIS file

GIS files were processed before WFM queried the ACD database, resulting in the data queried from the database overwriting the data from the GIS file.

Use only one method of capturing historical data for a service queue: automatically (the default setting) or by using GIS.

(Applies to WFM 9.2(1) SR3 and newer) Make sure that in WFM Configuration Setup, on the ACD Connection step, the "Use GIS to capture ACD historical data manually" check box is selected only if you intend to use GIS to capture historical data.

Service queue historical data that is captured does not match custom report values

The custom report is using a different Unified CCE table or column than used by the WFM Capture service.

> **Example**: Let us say that the custom report uses the CALL_TYPE_INTERVAL table. This table can include calls not associated with any skill gropu or precision queue, such as when the associated script does some IVR activity first, and calls for multiple skill groups or precision queues, such as when the sasociated script queues the call to different skill groups or precision queueus based on the caller's response to an IVR prompt.

No action is required if the differences are due to the custom report using different Unified CCE tables.

Unified CCX

The Capture service uses ODBC via JDBC to connect to the Unified CCX database and Informix database, so standard troubleshooting procedures for network connectivity and JDBC connections can be used.

For general troubleshooting, check the following:

- Verify that the ACD Connection primary and secondary IP addresses in the WFM Configuration Setup utility are correct.
- Verify that the Unified CCX instance configured in the WFM Configuration Setup utility is correct.
- Verify that the login credentials are correct.
- Verify that there is network connectivity between the WFM system and Unified CCX.
- Port 1504 is used to connect to the Informix database. Telnet to port 1504 on the Unified CCX server to rule out firewall issues.

Verify that the ODBC connection is configured correctly:

- Check the acdDbMain and acdDbBackup keys in the Windows registry. The UID must match the expected username. The Server value must be based on the instance name, with the following changes:
  - Convert all letters from uppercase to lowercase
  - Replace all hyphens with underscores
  - If the server name starts with a number, add the prefix i
  - Append _uccx to the instance name
- Check for a key under HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Informix\SQLHOSTS that matches the instance name (with the changes noted in the previous bullet point). Verify that the HOST value matches the Unified CCX IP address and that the SERVICE value matches the port.

Problems and Solutions

Historical data is not captured

(Applies to WFM 9.2(1) SR3 and newer) In WFM Configuration Setup, on the ACD Connection step, the “Use GIS to capture ACD historical data manually” check box is selected.

If you want WFM to capture data automatically by querying the ACD database, make sure this check box is cleared. Select the check box only if you intend to use GIS to capture historical data.

Avaya AACC 6

For general troubleshooting, check the following:

- Ensure that the capture files are being placed in the correct folder.
- Ensure that agents, services, and DNs are configured with the correct identifiers in WFM.

Note: Avaya does not send blank files to WFM to insert zeros for days when there are no calls for the service queues. This results in no reference data for distributions and forecasts.

Problems and Solutions

Could not start the Capture service successfully

WFM Configuration Setup has not completed successfully. Specifically, the ACD Connection step is not complete. The wfmcapture.dbg debug log shows the following messages:

> FATAL WMCA2000 Could not start the capture service, but will keep trying. com.calabrio.wfm.common.repository.db.DatabaseException: unable to retrieve the acd type (no results)

Complete WFM Configuration Setup and ensure that the Capture service has started.

Could not connect to AACC 6: ODBC driver was not installed

The ODBC driver was not installed.

See the *WFM Installation Guide* for instructions on nstalling the Caché ODBC driver. Restart the Capture service.

Could not connect to AACC 6: CacheDB.jar was not installed

CacheDB.jar was not installed. The classpath in the Capture service configuration file does not point to the CacheDB.jar location. The wfmcapture.dbg debug log shows the following message:

> Could not start the capture service, but will keep trying. java.lang.ClassNotFoundException: com.intersys.jdbc.CacheDriver

Uninstalling a WFM SR or ES caused the classpath changes in the Capture service configuration file to be undone.

To resolve this, do the following:

1. Copy CacheDB.jar from <cachesys>\dev\java\lib\JDK16 where <cachesys> is the Cache install directory (i.e. D:\Avaya\Cache\CacheSys\dev\java\lib\JDK16) on your CCMS to C:\Program Files (x86)\Calabrio\WFO_WFM\ext.
2. Ensure that the correct location of CacheDB.jar is in the classpath used by the Capture service: modify the wfmcapture.properties file

   from:

   ```
   "service4j.classpath=..\config;..\ext\calabrio-
   time.jar;..\ext\SplkStd4J.jar;..\ext\wfm-
   common.jar;..\ext\commons-dbcp-1.2.1.jar;..\ext\commons-
   collections-3.0.jar;..\ext\commons-pool-
   1.2.0.jar;..\ext\jtds-
   1.2.1.jar;..\ext\sqljdbc4.jar;..\ext\log4j.jar;..\lib\wfm-
   capture.jar"
   ```

   to:

   ```
   "service4j.classpath=..\config;..\ext\calabrio-
   time.jar;..\ext\SplkStd4J.jar;..\ext\wfm-
   common.jar;..\ext\commons-dbcp-1.2.1.jar;..\ext\commons-
   collections-3.0.jar;..\ext\commons-pool-
   1.2.0.jar;..\ext\jtds-
   1.2.1.jar;..\ext\sqljdbc4.jar;..\ext\log4j.jar;..\ext\CacheD
   B.jar;..\lib\wfm-capture.jar"
   ```

3. Restart the Capture service.

Could not connect to AACC 6: wrong port in WFM Configuration Setup

The port specified in the ACD Connection step in WFM Configuration Setup is not the correct port used by the Caché database on CCMS. The wfmcapture.dbg debug log shows the following message:

> ConnectionPoolManager#getConnectionFromNewConnectionPool:91] Failed to get a connection from: primary.
> Exception: org.apache.commons.dbcp.SQLNestedException: Cannot create PoolableConnectionFactory ([Cache JDBC] Communication link failure: Connection timed out: connect)" in wfmcapture dbg file.

Run WFM Configuration Setup and change the entry on the ACD Connection step to the correct port. This should be the actual value used when CCMS was installed.

Could not connect to AACC 6: wrong credentials

The login name and/or password specified in the ACD Connection step in WFM Configuration Setup is wrong or not of the Administrator user type. The wfmcapture.dbg debug log shows the following message:

> ConnectionPoolManager#getConnectionFromNewConnectionPool:91] Failed to get a connection from: primary. Exception: org.apache.commons.dbcp.SQLNestedException: Cannot create PoolableConnectionFactory ([Cache JDBC] Communication link failure: Access Denied)

Run WFM Configuration Setup and change the entries on the ACD Connection step to the correct credentials.

Could not connect to AACC 6: wrong database name

The database name in the URL used to access the Caché database on CCMS is incorrect. It should be "CCMS_STAT" instead of "DB_NORTEL_CC7". The wfmcapture.dbg debug log shows the following message:

> NortelAcdDbConnectionPoolManager#buildDataSource:107] url: jdbc:Cache://10.192.246.150:1972/DB_NORTEL_CC7" and "ConnectionPoolManager#getConnectionFromNewConnectionPool:91] Failed to get a connection from: primary. Exception: org.apache.commons.dbcp.SQLNestedException: Cannot create PoolableConnectionFactory ([Cache JDBC] Communication link failure: Access Denied)

This issue was corrected in WFM 9.2(1) SR1.

Install WFM 9.2(1) SR1 or newer. Make sure you go through all the steps in WFM Configuration Setup and restart all the WFM services for the fix to take effect.

Directory number historical data is not captured

CDN IDs are used instead of Application IDs when configuring directory numbers in WFM.

1. Delete the existing directory numbers that are using the wrong CDN IDs.
2. Add back the directory numbers using the Application IDs instead.
3. Run Capture Historical Data.

Service queue historical data is not captured

The service queue ID does not match the Skillset ID.

1. Delete the existing service queues that are using the wrong service queue IDs.
2. Add back the service queues using the correct Skillset ID.
3. Run Capture Historical Data.

Agent historical data is not captured

There is no corresponding agent and/or user created manually in WFM forthe AACC agent. AACC agent information is not automatically synchronized to WFM.

Administrators must manually add a WFM agent and user where the WFM agent ACD ID matches the Login ID of the agent in CCMA.

The WFM agent and user must be activated (the Activate this agent/user check box is selected).

The WFM user roles must match the roles configured in CCMA and be linked to the WFM agent.

Historical data is not captured

(Applies to WFM 9.2(1) SR3 and newer) In WFM Configuration Setup, on the ACD Connection step, the “Use GIS to capture ACD historical data manually” check box is selected.

If you want WFM to capture data from Avaya cap files, make sure this check box is cleared. Select the check box only if you intend to use GIS to capture historical data.

Generic ACD

For general troubleshooting, check the following:

- Verify that WFM has been configured on the ACD Connection step in WFM Configuration Setup to use “Generic” as the ACD. The tbCaptureInstalled table in the CWFM database should show CAP_NAME set to Generic and CAP_ISMAIN set to 1.
- Verify that the files are written to the WFO_WFM\reports folder with the correct names and formats, as documented in the *GIS API Reference Guide*.
- Verify that the data in the files is self-consistent. If the fileheaders says INTERVAL: 0630 but a line of data syas the time is 09:30:00, then the file is not self-consistent. This usually means a problem with the third-party tool.
- Verify that the data in the files is consistent across all the files being written.
- Verify that the identifiers (service queue IDs, agent IDs, and so on) are correct and match the configured service queues and agents in WFM.

WFM Compile Service Problems

Nearly everything needed to diagnose WFM Compile service problems can be found in the default log files at the DEBUG level and up. Enabling TRACE or DUMP is necessary only if you need to see the queries being executed.

Failed queries are logged at the DEBUG level or higher.

WFM Forecast Service Problems

For general troubleshooting, check the following:

No or Bad Reference Data

- Use the View and Edit Historical Data page to check the data on reference dates.
- Check whether or not the WFM Capture service is running or had issues.
- Note that an Avaya ACD will not send any data if there were no calls on a specific day for the service queue, which results in no reference data for that day.

Problems and Solutions

Distribution request fails: no historical data exists for the service queue/named distribution for the selected days of the week/reference period

One or more of the following can result in no reference data for at least one of the selected distribution days of the week, causing the distribution request to fail:

- There is no or bad data for the reference date.
- The reference dates include closed days for the service queue.
- The reference dats include special events for the service queue.

> **Note**: WFM 9.2(1) SR1 ES1 contained a fix that allows a distribution request to succeed if at least one of the selected distribution days of the week have reference data. For earlier releases, use the following workaround.

Try the following to allow the distribution request to succeed:

- Use the View and Edit Historical Data page to to check the data on reference dates.
- Select additional or different distribution days of the week.
- Change the reference dates.
- Change or delete closed days and special events for the service queue.
- Run Capture Historical Data if there was an earlier problem in capturing the data.

Distribution has no data for a day of the week

Possible causes are:

- The day of the week was not specified in the distribution request.
- The reference days have no data for that day of the week.
- There are closed days or special events for the that day of the week in the reference period.

Solutions include:

- No day of the week specified: Make sure the day of the week is selected when making the distribution request.

- No reference dates data: This is expected behavior. Use the View and Edit Historical Data page to check the data on the references dates chosen. If that day of the week normally has calls, change the reference dates to include dates with data. Run Capture Historical Data if there was an earlier capture problem.
- For closed days/special events: This is expected behavior. Change or delete the closed days and special events for the service queue, or change the reference dates to a period with no closed days/special events.

WFM Installation Problems

WFM database cannot be created or updated

The Configuration Setup tool displays the following error message when the WFM database cannot be created or updated because permission was denied or a database already exists.

> Could not execute data for step Create WFM DB:
> Could not create Reports database.
> Could not update database.
> CREATE DATABASE permission denied in database 'master'.

Perform the following task to resolve the problem.

1. Verify the SQL Server Login name is configured correctly. The dbcreator and sysadmin roles must be assigned to the SQL Server Login name.

   The instructions for creating the SQL Server Login for WFM can be found in the *WFM Installation Guide*.
2. Remove the Hibernate database if it exists.
3. Run WFM Configuration Setup (postinstall.exe) again.

WFM User Interface Problems

Users cannot connect to the WFM Transaction services server using https, although http works.

An error is displayed as follows:

- Internet Explorer: “This page can’t be displayed”
- Firefox: “The connection is interrupted”
- Chrome: “SSL Connection Error”

Cause: The webserver certificate is missing from the keystore used by the Jetty webserver on the WFM Transaction services server.

Solution: This issue was fixed starting in WFM 9.2(1) SR2. WFM Configuration Setup adds the webserver certificate if it is not in the keystore.

Verify that the WFM certificates exist in the WFM keystore (see Keystore Check), and follow the procedure to rebuild the WFM keystore (see Rebuild the WFM Keystore).

The browser displays a warning about a problem with the WFM website security certificate when using https.

Cause: The WFM webserver certificate was not signed by a trusted certificate authority or was not signed correctly.

The certificate has been signed correctly if the error message is:

- Internet Explorer: “There is a problem with this website’s security certificate”
- Firefox: “Secure Connection Failed: Certificate type not approved for application.”
- Chrome: “Cannot connect to the real <IP address>”

Solution: See Keystore Check.

The browser displays a warning about a problem with the WFM website security certificate when using https with the host name

Cause: The WFM webserver certificate has the IP address in the Subject/Owner field and does not have the host name in the Subject Alternate Name field.

Solution: Use the server IP address to access WFM with https. Using the server host name is not supported when using https to access WFM.

The browser displays a warning about problems with the WFM website security certificate when using https even though it used to work.

Cause: The signed certificate has expired.

Solution: Clear the WFM keystore (see Rebuild the WFM Keystore and Keystore Check.

The browser displays an error and will not display the WFM login page when using https.

When attempting to log in using a secure connection (https) an error is displayed as follows:

- Internet Explorer: “This page can’t be displayed”
- Firefox: “The connection is interrupted”
- Chrome: “SSL Connection Error”

Cause: The WFM certificate and/or CA certificates in the WFM keystore are missing or wrong. For example, the WFM certificate was signed by a CA whose CA certificate was not added t the keystore.

Solution: Do the following:

- Sign the certificate.
- Verify that the root certificate is added to the keystore before the intermediate certificates.
- Verify that the root, all intermediate, and signed WFM certificates are added to the keystore (see Keystore Check).
- Rebuild the WFM keystore if necessary (see Rebuild the WFM Keystore).

WFM administrators cannot log in even though other users can.

The administrators are configured to authenticae using the AD Security Group.

Cause: The Active Director domain information configured in WFM Configuration Setup is incorrect.

Solution: Verify the Base DN, User Base, and Admin User Group configured are correct. They are usually case and whitespace sensitive. Use an LDAP client tool such as JXplorer to log into the Active Directory and make the equivalent LDAP queries as WFM.

WFM Service Problems

The first and last name of an agent are the same after being synced to WFM

Unified CCX systems allow an agent to be created without a first name. In WFM, agents must have a first and last name, so when an agent with no first name is synced to WFM, the Sync service copies the agent's last name and sets it to the agent's first name.

There is no workaround for this issue, this behavior is as designed. Otherwise, enter a first name for the agent in WFM.

Reporting Problems

Wait up to 30 seconds to open the Reporting application

A user might have to wait up to 30 seconds to open the Reporting application after the server is booted. This only happens to the first user who accesses a report after the server is booted.

No action required. Some time is required when the first user accesses the Reporting application. The Reporting application connects to the database, establishes privileges, and displays a menu based on the user's role. After the connection is established, you can quickly access reports.

Agent productivity report shows no data

The Agent Productivity Report shows no data for a period when agents have been continuously taking calls.

Agent sessions lasting more than 24 hours are not supported. Agents have to log out once every 24 hours to ensure productivity reports show correct data.

Report is not created when CSV option is selected

WFM or Unified Workforce Optimization fails to create a report when the CSV option is selected in the Format field. The following message appears when you try to generate a report with the CSV format.

To access CSV/PDF files, enable Internet Explorer Security Setting: Automatic prompting for file downloads

Perform the following steps to resolve the problem.

1. In the Internet Explorer, choose Tools > Internet Options. The Internet Options window appears.

2. Click the Security tab and then click Custom Level.
3. Scroll down to Automatic Prompting for File Downloads under Downloads, choose Enable, and click OK.
4. Click Yes to dismiss the warning dialog and click OK to dismiss the Internet Options window.
5. Resubmit the CSV report. The File Download dialog appears.
6. Click Open to display the report.

iCalendar Problems

Agent cannot connect with iCalendar service

The agent cannot connect with the iCalendar service.

Check that the host and port in the URL are correct. The port should be 4430 for a secure URL (https) and 8086 for an unsecure URL (http). These ports should be accessible from the iCalendar client device.

The agent receives an HTTP 401 error (Unauthorized)

The agent receives an HTTP 401 error (Unauthorized).

Ensure that the agent is using the correct username and password. Note that the user must be an agent: only agents can use the iCalendar service.

The agent receives an HTTP 403 error (Forbidden)

The agent receives an HTTP 403 error (Forbidden).

This error might occur if the calendar client application used by the agent polls the iCalendar service too often. To fix this, reduce the polling period of the calendar client application. If it appears that too many agents have this error, consider increasing the rate of allowed connections in the C1Calendar.properties file.

The agent receives an HTTP 400 or 500

An agent receives an HTTP 400 or 500 error (or any other error code not mentioned here).

This is an unexpected error. Check the iCalendar log files for more information on what is happening.

Retrieved calendar displays wrong time zone

The retrieved calendar displays the wrong time zone.

Configure the time zone the iCalendar client application. It is possible that some client applications do not allow you to specify the time zone. In that case, the calendar time zone will be either the Calabrio server time zone or the time zone of the iCalendar client device.

Language in the iCalendar is not correct

The language in the iCalendar is not correct.

Check the locale set on the iCalendar client device.

The calendar is never updated on the client device

The calendar is never updated on the client device, even if the agent schedule has changed.

Check iCalendar service log files to see that the iCalendar client sends requests and that the requests are correctly handled by the iCalendar service. The logs should include lines such as:

> Received request for user NNN
> Request successfully processed for user

Check that the schedule data is inside within the viewable range (the “Number of Weeks Visible in Agent Schedules” setting on the Application Management > Global Settings page in Unified Workforce Optimization).

Index